The European Union's Biometric Border Control

A Critical Assessment of the Deployment of Biometric Technologies

JOHANNE RÜBNER HANSEN, 20162237

Department of Development and International Studies

MSc Global Refugee Studies, Aalborg University

10th Semester

31st May 2019

Supervisor:
Martin Lemberg-Pedersen

Number of Characters, with an accepted 10 per cent upper deviation:
184.979 (77 pages)

ABSTRACT

The European Union's Biometric Border Control

A Critical Assessment of the Deployment of Biometric Technologies

JOHANNE RÜBNER HANSEN, 20162237
MSc Global Refugee Studies, Aalborg University

Following the 2015-16 'refugee and migration crisis', as declared by the European Union, there has been an increasing interest in collecting, storing and analysing personal biometric data from irregular migrants and asylum seekers. The thesis at hand investigates three proposals to recast the regulations of respectively the Schengen Information System, Eurodac and the Visa Information System. Building on the theoretical lenses of governmentality, biopower, the relation between knowledge and power as well as studies on surveillance and social sorting, the thesis consists of an in-depth analysis of what the European Commission frames as problems in the proposals, whether there are elements that are left silenced, and what effects and potential risks these proposals will expose irregular migrants and asylum seekers to, if they are ratified. With this critical policy analysis and discussions of relevant implications, this thesis contributes to the academic field of science and technologies studies as well as border and migration studies.

It is found, that identification is a high priority for the European Commission for two principal reasons. First of all, because the political field of irregular migration and asylum seekers is intertwined with security issues, making it an issue that needs quick and drastic responses. Secondly, as several member states did not manage to register all those arriving at the European Union's external borders throughout the 'crisis' some remained unregistered and hence invisible to authorities and knowledge producers. This resulted in a situation with less control over who was staying and moving inside the European Union. A solution to the 'crisis', set forth by the European Commission, was to recast the purposes and functions of the digital and biometric borders, which the three large-scale information systems constitute. The promise was that applying biometric technologies would ensure a correct and exact identification of all irregular migrants and asylum seekers entering the European Union, as it was framed to be a neutral and objective technology, capturing unique personal features, such as fingerprints, palm prints, facial image and DNA. Relying and deploying biometric technologies and features would reinforce EUs managerial abilities to govern and direct future legislations on those registered. Additionally, it would create possibilities to socially sort, surveil and return those registered who are perceived to be anti-citizens/illegal/irregular. Despite the leading and powerful position the European Commission has and its convincing and powerful way of presenting solutions to its framed problems, it is also clarified throughout the thesis that there are a multitude of issues regarding the EUs reliance and deployment of biometric technologies, that are not mentioned in the proposals. These are important to shed light upon in order to understand the social and societal impacts the regulations have, and are therefore analysed and discussed. The first concerns the fact that changing the purposes and functions of the regulations is not without consequences for irregular migrants and asylum seekers. This can leave them in vulnerable situations as it becomes complex to comprehend what the personal data is used for, who can access it and for how long it can be stored. The second concerns technological limitations and errors that biometric technologies are prone to, and which contradict the promises made in the proposals, such as the fact that the technologies are only capable of giving matches based on probability, and that ensuring good data quality is difficult. The lack of acknowledgement of these can put people at risk of experiencing false matches and being met with mistrust. Another limitation found concerns that the technologies are *a priori* calibrated to a certain degree of whiteness, which occludes the registration of non-white people. These concerns are not some that the European Commission states that they are aware of, even though it creates possibilities to divide and discriminate between those who are depicted as dangerous/safe. Lastly, it is examined that template ages over time and that the larger the databases, the higher the risks of false matches are examined. These speak against the Commissions suggestions of making the systems interoperational, extending the data retention period and lowering the age of registration. In sum the thesis concludes that the European Commission silence all of these technological limitations, even though they have huge implications for those registered, as they will be more exposed to discriminating practices, such as profiling and social sorting, surveillance, tracking, false matches, higher return rates and occlusion of being registered at all.

Keywords: European Commission, databases, biometrics, irregular migration, governance, social sorting, surveillance

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ECRE – European Council on Refugees and Exile

EDPS – European Data Protection Supervisor

EP – European Parliament

EPRS – European Parliamentary Research Service

EU – European Union

eu-LISA - The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Eurodac – European Dactyloscopy

GDPR - General Data Protection Regulation

JRC – European Joint Research Centre

NGO – Non-governmental Organisation

UN – United Nations

UNHCR – United Nations High Commissioner for Refugees

SIS – Schengen Information System

TCN – Third-Country National

The Charter: The European Charter of Fundamental Rights

The Commission: The European Commission

The Parliament: The European Parliament

VIS – Visa Information System
WPR – What is the Problem Represented to Be?

LISTS OF TABLES AND FIGURES

List of Figures

List of Tables

1. INTRODUCTION

During the course of 2015, more than one million asylum seekers and migrants entered the European Union (EU), with more than 3,550 losing their lives on the journey (Spindler 2015). The vast majority of those arriving came from the conflicts in Syria, Afghanistan or Iraq (Ibid.) but also from other regions such as Africa or South Asia (IOM 2015). This number represented a fourfold rise of the total arrivals from the preceding year. The situation forced European governments to take action on immigration issues to handle the unexpectedly high influx of migrants and asylum seekers. Some member states inside the border-free Schengen zone, like Hungary, began to put up fences and reimpose frontier controls, while other countries, like Germany, allowed asylum seekers and migrants to arrive (BBC 2015). Figure 1 illustrates the Schengen Zone. Yet, especially far-right winged parties, appealing to fears and anti-immigrant sentiments, gained considerable support in many European countries (Steinmayr 2017), thus influencing the political agendas in the EU.

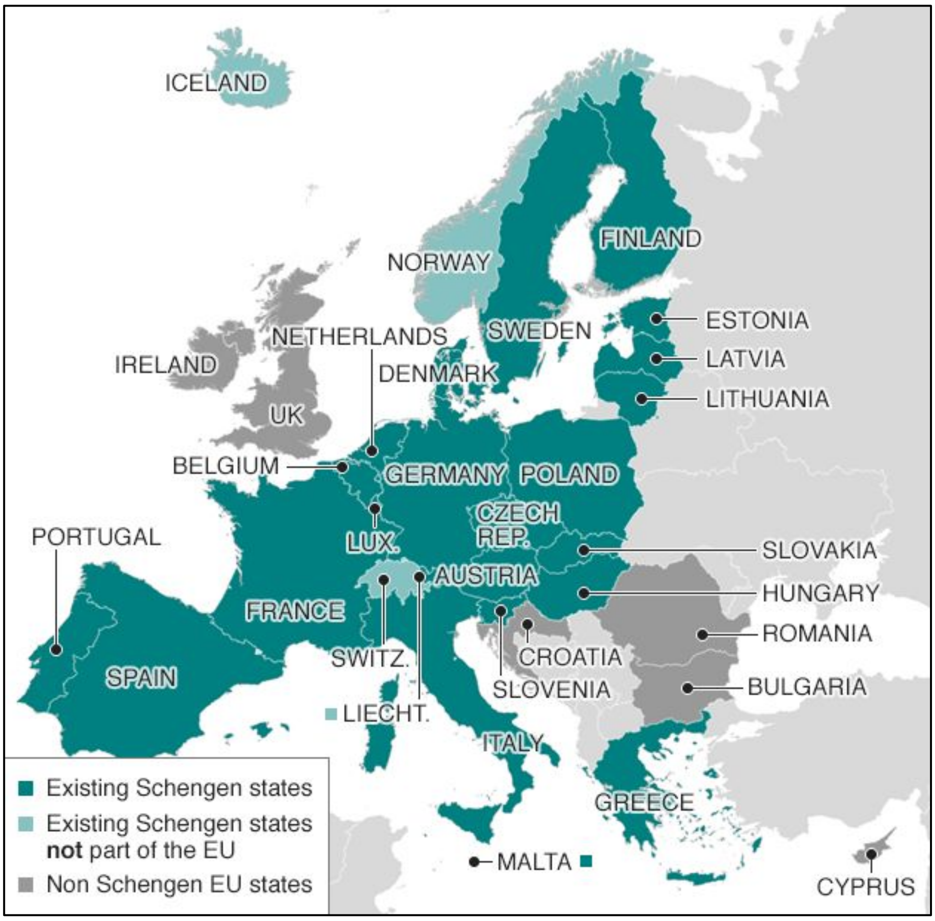


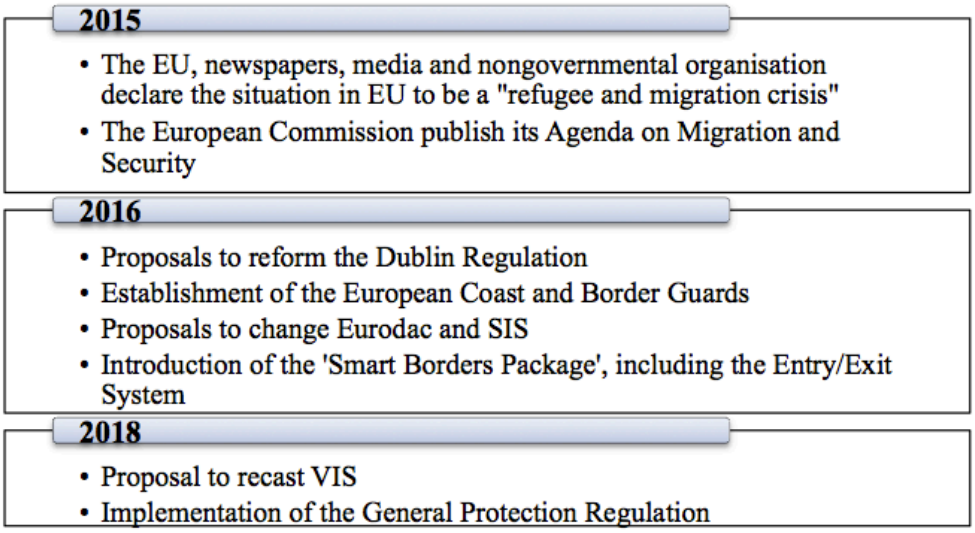
Figure 1: Map over the Schengen states in the EU (BBC 2015).

The European Commission (hereinafter: the Commission), influential newspapers and non-governmental organisations (NGOs) declared and framed the situation as a "migration and refugee crisis" which needed to be acted upon (EC 2017; Spindler 2015; IOM 2015; Oxfam

International 2019; BBC 2015; Bajekal 2015; Sly 2015). In a joint statement, the International Organisation for Migration (IOM) and the United Nations Refugee Agency (UNHCR) argued that a more common coordinated European response was needed, both in terms of allocating those entering the EU but also regarding improving the reception facilities, accommodation and process of registration. They emphasised a need to improve the process of identifying those who did and did not qualify for refugee protection as an essential issue (BBC 2015). Furthermore, did the EU react to these inflows by expanding the already established mobility control and border security, as it was perceived as necessary to control and hinder future migrants' movements (Ferreira 2018).

That registration into large-scale information systems and identification of irregular migrants entering the EU became an important element in the political landscape is the central theme for the thesis at hand. Irregular migrants cover over a term that includes a broad range of people and statuses. It can be said, that they in general have three different migration histories (Broeders 2007:85): First, they can have crossed the EU's external borders illegally, either with or without help. People entering the EU to seek asylum are included in this category. Secondly they can have been asylum seekers who stayed after the claim was rejected, or thirdly, they came on a legal visa and stayed after its validity expired. In the time of the 'refugee and migration crisis' biometric identity control got so much value, that it quickly became the most trustworthy method for member states to identify third-country nationals (TCNs). As such, did the EU take over the task of identifying all persons who entered EU territory and determined where they belong (Guild 2003:344).

In light of the increased focus on identification, the depicted 'crisis' led the EU to initiate a huge range of different types of actions (EC 2015a:6). First, the European Parliament (hereinafter: the Parliament) sped up the already on-going process of reforming the Dublin system, which determines which member state is responsible for processing asylum applications (EP 2017a). Second, the Parliament also began to implement new steps to manage what was now increasingly described as 'illegal' migration into and around the EU (Ibid.). This included tighter border controls at the external borders, such as changing the former Frontex into the European Border and Coast Guard (EP 2017a), and proposals to change already existing large-scale information systems, which collected and stored information on people entering the EU (Ibid.). As such, actions were launched both to physically strengthen the external borders of the EU, for example by deploying up to 10.000 border guards by 2027 (Ibid.), as well as initiatives to intensify the use of information systems containing biometric data, acting as digital and biometric borders. Figure 2 visualises the Commission's presented and implemented actions to strengthen the digital borders from 2015-2018.



2015

- The EU, newspapers, media and nongovernmental organisation declare the situation in EU to be a "refugee and migration crisis"
- The European Commission publish its Agenda on Migration and Security

2016

- Proposals to reform the Dublin Regulation
- Establishment of the European Coast and Border Guards
- Proposals to change Eurodac and SIS
- Introduction of the 'Smart Borders Package', including the Entry/Exit System

2018

- Proposal to recast VIS
- Implementation of the General Protection Regulation

Figure 2: The Commission's presented and implemented actions to strengthen the digital borders, from 2015-2018 (EP 2017a; Schmid-Drüner 2019; Bux 2018)

Important for the thesis is hand, are the Commissions suggestions to recast the large-scale information systems, in a response to the 'crisis'. In May 2016 the Commission launched a proposal to recast the regulation of the European Dactyloscopy (Eurodac) (EC 2016a), the information system that underpins the Dublin Regulation and stores fingerprint data on all asylum seekers in the EU (Ibid.). Later that year, the Commission also proposed to recast the Schengen Information System (SIS) (EC 2016b), that contains data on missing and wanted persons as well as objects, such as vehicles. Arguments put forward by the Commission included that the renewal of the system would make it easier to correctly identify those entering the EU and thus to manage "the challenges of migration and the fight against terrorism and organised crime" (EC 2016c:2). A later response to the 'crisis' was set forth in May 2018, as the Commission also declared a need to recast the Visa Information System (VIS), which stores data on short-stay visas (EC 2018a). These proposals to recast Eurodac, VIS and SIS as a reaction to the 'crisis' and as a means to strengthen the identification process will be critically scrutinised, as a main objective is to shed light upon some of the effects that the increased reliance on biometric technologies may cause for irregular migrants that are registered in the databases.

The EU 'migration and refugee crisis' and its reaction to hinder migratory movements into the EU through a boost of its border control through information systems has attracted substantial awareness within several academic disciplines throughout many years. Amongst many, this includes scholars working within the fields of refugee and migration studies (Papadopoulos et al. 2008; Mezzadra 2011; Lemberg-Pedersen 2018; Stenum 2012; Ajana 2013), science and technology studies (Jacobsen 2012, 2015; Tsianos & Kuster 2016), international politics and critical security studies (Epstein 2007; Huysmans 2006; Müller 2010; Bigo 2001, 2014), political geography (Amoore 2006), ethics of information and communication technologies (van der Ploeg 1999, 2005) racial and whiteness studies (Magnet 2011; Dyer 1997; Haraway 1991; Maguire 2012), surveillance studies (Ceyhan 2012; Lyon 2002, 2003, 2006; Broeders 2007; Hildebrandt 2007, 2009) and (critical) border studies (Vaughan-Williams 2012; Parker & Vaughan-Williams 2012; Rumford 2012). Whilst the political context of EU's reaction to the 'crisis' by expanding its biometric and digital borders has been subject to scrutiny from various disciplinary fields, the research done has not yet reached its limit. Accordingly, the thesis at hand contributes with a critical policy analysis and discussions of relevant implications. This is a combination that has not achieved much attention previously. It does so by asking the following research question and sub questions:

In the context of the EU border control, why does biometric registration of asylum seekers and irregular migrants into the information systems SIS, Eurodac and VIS hold such importance for the Commission?

- *Which issues does the Commission leave unproblematic in the proposals to change the regulations of SIS, Eurodac and VIS?*
- *What are the implications and effects of EU reliance on biometric technologies?*

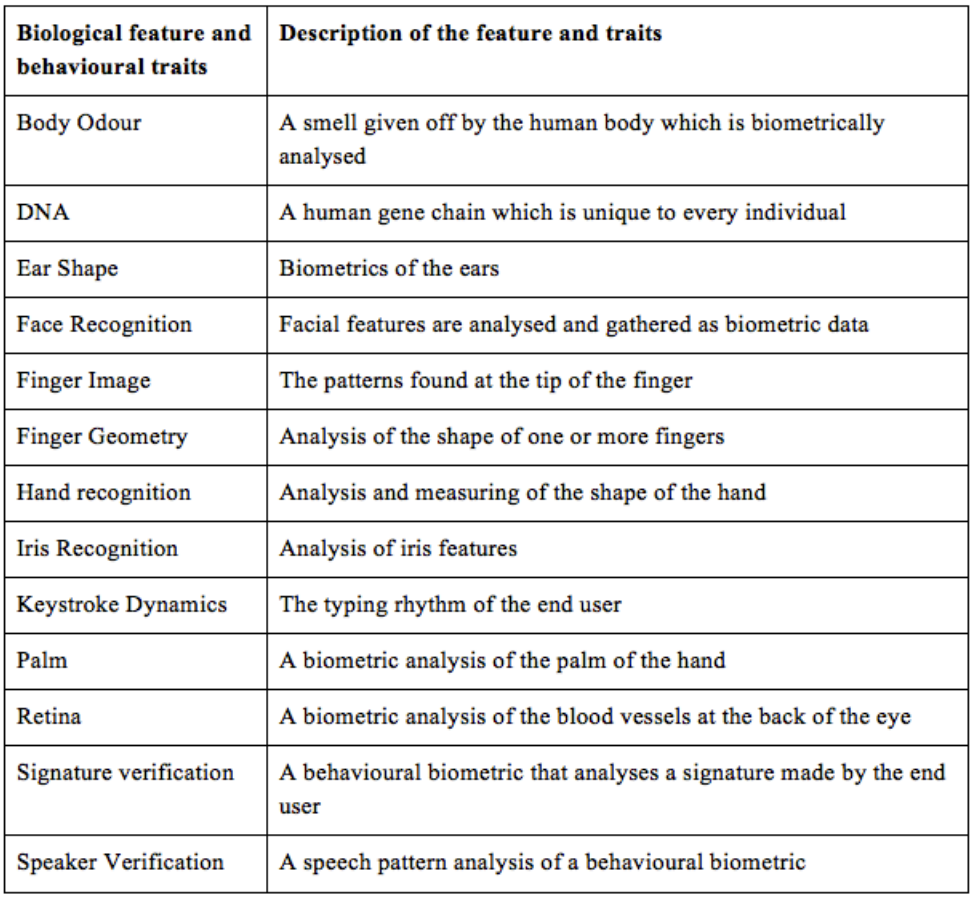
These questions connect refugee and migration studies with science and technology studies. Moreover, the thesis situates them in the theoretical framework of Michel Foucault's notion of biopower and the relation between knowledge and power, combined with theories on surveillance and social sorting. These theories and concepts allow a critical assessment of which discourses are prevalent within the Commissions proposals to change the regulations of respectively SIS, Eurodac and VIS. Furthermore, they enable an in-depth investigation of which issues and elements the proposals do not consider, despite the potential harm to those registered in the databases.

In order to facilitate this kind of investigation, a theoretical framework is needed. This will be presented in chapter 2. This chapter describes how the theoretical development of studying borders has changed throughout recent years, as well as expanding on Foucault's concepts of governmentality and biopower as these can facilitate an analysis of what intentions the Commission has when advocating for increased deployment of biometric technologies for identification purposes in the management of borders-, security and migration. In extension to this, the chapter consists of an examination of the relation between *Power/Knowledge*, a concept also developed by Foucault. This is relevant to bring forward since the thesis aims at illuminating the dominant discourses in the proposals. Last, this chapter touches upon theories of surveillance and social sorting as it is crucial have a continuous discussion of how the deployment of biometric technologies may pose new risks for those registered in the databases. Before continuing to read the critical examination of the proposals to change the regulations of SIS, Eurodac and VIS, it is important to become acquainted with the chosen methodological approach that this thesis is structured around. This is clarified in chapter 3. Chapter 4 contains an in-depth analysis of how the Commission frames certain issues to be of utmost importance for internal security, as well as the suggested solutions to these issues. This enables a broader examination of the underlying agendas and hence which direction the EU is heading, and for which reasons. Chapter 5 and 6 bring forward and discuss complex paradoxes and issues, which are not given attention in the proposals to change the regulations, even though an increasing number of actors have voiced serious concerns about the fallibility of biometric technologies.

2. GOVERNING THROUGH BIOMETRIC BORDER CONTROL

Borders have always been ubiquitous in political life, and the ways they are studied have changed tremendously throughout the last centuries (Vaughan-Williams 2012:1; Wilson & Hastings 1998; Balibar 1998; Epstein 2007; Rumford 2012). Borders have often been viewed as being the physical point from where territory, sovereignty and population can be protected from foreigners and external threats. Thus, it is often believed that borders are needed in order to securitise and protect the internal territory, population and sovereignty (Storey 2017:118; Elden 2005:2083). Yet, in recent years academics have contested this conception, and argued that borders are neither static, natural or neutral but rather historical contingent, politically changed and a dynamic phenomenon, which involve people and their everyday lives (Vaughan-Williams 2012:1). This has led to a reinterpretation of the traditional way of studying borders for several scholars (Vaughan-Williams 2012; Parker & Vaughan-Williams 2012; Rumford 2012).

The biometric border is a form of border control that requires that one studies the borders of the states differently than the traditional perception of them being fixed on the outer edge of a state (Amoore 2006). After the events of 11 September 2001 in New York and Washington D.C., various biometric technologies have been implemented in border control systems, as they have been endorsed as a mean to ensure states' internal territory from what became defined as 'the new threat of global terrorism" (Jacobsen 2012:7). The rise of biometric technologies were based on a wish for greater security, as it was perceived to enable an accurate identification of every individual, while it at the same time enabled states to track a suspect person for longer periods. Biometrics literally means the 'measurement of life', and refers to the technology of measuring, analysing and processing the digital representations of biological data and behavioural traits (Ajana 2013:3). The most common biological features used for migration- and border management are fingerprints, palm prints and facial images. Yet, the whole list of biological features can be examined more closely in Table 1.



Biological feature and behavioural traits	Description of the feature and traits
Body Odour	A smell given off by the human body which is biometrically analysed
DNA	A human gene chain which is unique to every individual
Ear Shape	Biometrics of the ears
Face Recognition	Facial features are analysed and gathered as biometric data
Finger Image	The patterns found at the tip of the finger
Finger Geometry	Analysis of the shape of one or more fingers
Hand recognition	Analysis and measuring of the shape of the hand
Iris Recognition	Analysis of iris features
Keystroke Dynamics	The typing rhythm of the end user
Palm	A biometric analysis of the palm of the hand
Retina	A biometric analysis of the blood vessels at the back of the eye
Signature verification	A behavioural biometric that analyses a signature made by the end user
Speaker Verification	A speech pattern analysis of a behavioural biometric

Table 1: Biological features and behavioural traits (Mayhew 2019).

Biometric technologies are widely used for identification of persons for several reasons: First of all, because it has the ability to automate the process of linking bodies to identities. Subsequently, it is able to distribute biological and behavioural data across computer networks and databases. Thirdly, it can adapt the data to different uses and purposes, and finally, because it is believed to provide more accurate, reliable means of verifying identities (Ajana 2013:3).

The procedure of enrolment into databases consists of several stages (Ibid.), which is visualised in Figure 3, under the "enrolment" paragraph. This indicates an idealised non-problematic procedure of enrolment (and matching) of any type of person. Registration can take place at any location, as long as the technology is present. When illustrated by the case of an asylum seeker, the person is obliged to register into the EU information system called Eurodac. In order to enrol, the person has to be in front of the biometric machines (A). Hereafter the technology captures the biological features (B) and transforms them into digital representations through a sensor device. Then, the biometric features are processed through an algorithmic operation (C). Subsequently, the machine will find out whether the person's data is new to the system (D). If the person has not registered before, the machine adds the new template into the database (E). If not, it duplicates the template (F).

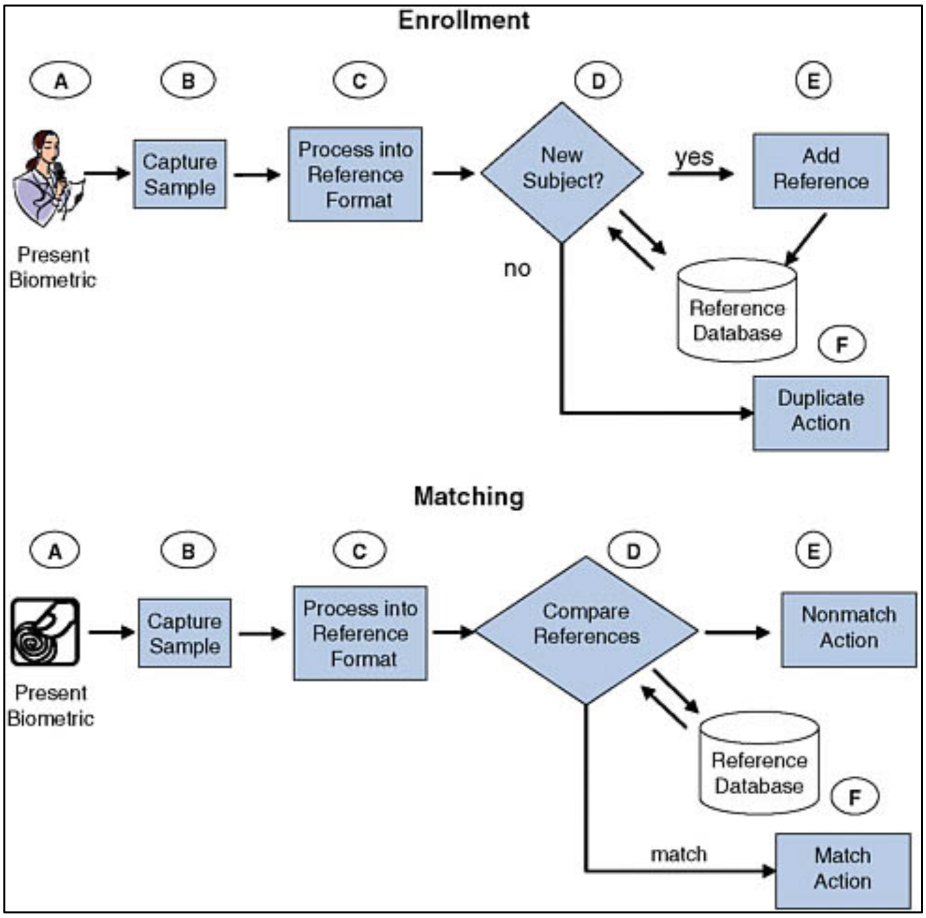


Figure 3: Idealised operations of a generic biometric system (Pato and Millett 2010:55).

If the asylum seeker has to register again in the future, s/he has to go through the matching process, also visualised in Figure 3. This process is similar to the enrolment phase, yet it differs as the last stage compares the 'live template' with the already stored template to establish whether the person is known to the system (D). If there is no match, then the person has not applied for asylum elsewhere (E), whereas if there is a match, then the person has most likely applied asylum in another member state (F).

Biometric technologies are widely used in border control, and since registration into large-scale databases can take place at several physical places biometric borders are more than physically marked border points (Amoore 2006). Thus, when studying biometric borders one needs to apply a new geographical imaginary of borders, as it is not any longer only physically fixed on the territorial limits of the state, but also is a portable border par excellence (Amoore 2006:338). This is because mobile bodies, such as travellers, migrants and asylum seekers, carry it around if registered. With this perspective in mind, it is relevant to bring Foucault's notion of biopower into play in section 2.1. By using biometric technologies combined with surveillance technologies, it becomes possible for states to monitor people. Simultaneously, it is also deployed as a means to identify and monitor large numbers of individuals that can be divided into different categorisations, defined on the basis of the individuals perceived level of future risk towards the state. This will be examined more closely in section 2.3. In that way, security and defence is no longer just a question of observing whether a neighbouring state is increasing its weaponry or carrying out research into more advanced defence technology.

Biometric borders are manifested as large-scale databases, containing biometric information about every registered individual. As such, it can be said that it entails a digitalisation of unique body parts into data systems. It consists of a multitude of bits and points that are linked together through networks of computerised databases (Bigo 2014:216). The databases exchange information about the traces left by the individuals, when they travel and information is constantly updated in order to be able to predict the future. That borders are digitalised they are becoming a 'timeline', which is constructed by the traces that individuals leave behind (voluntarily or involuntarily) when travelling (Ibid:217). These traces are collected, mined and analysed by border guards and police as well as through the exchange and verification of the means of identification between distant bureaucracies, consulates, intelligence services and private companies (Ibid.). This is also termed dataveillance (Clarke & Greenleaf 2017). As such, biometric features are key elements in translating the data between the world of physical bodies and the world of computerised digital bodies (Bigo 2014:218). In a study of the biometric border controls, it is found that the experts working in this field, view an individual as a 'body' that is needed to reveal the signs of identification in the database. This is confronted with the 'virtual body', which often tends to be perceived to be more truthful than the physical body (Ibid.). The biometric border is biopolitical precisely because it has its focus on the body of the populations a state has power over, and it is therefore relevant to elaborate upon Foucault's notion of governmentality and biopower in the next section.

2.1 Governmentality and biopower

In his lectures in 1978, Foucault spoke about the term governmentality (Foucault 1978; Epstein 2007:151). It captures a phenomenon that took shape very gradually from the sixteenth century and onwards, and it was supposed to counterpart contemporary theories about the state-as-sovereign and sovereignty. Throughout the eighteenth and nineteenth centuries Western Europe experienced a demographic explosion alongside industrialisation. This lead to what Foucault called "the population question", as the population was no longer only the attribute of the sovereign, but became a productive force within the market, which was key to developing states and their economics (Epstein 2007:151; Pugliese 2010:7). The population now emerged as an object of study, and through political science, statistics and political numbers, governments were able to construct issues of and in the population (Stenum 2012:281). The population was now an object invented for the use of knowledge and power (Ibid; Epstein 2007:151; Pugliese 2010:7-8). The concept of governmentality provided the vantage point to observe the modern states as essentially managerial (Epstein 2007:151), which according to Epstein (Ibid.) is a broad term describing different tactics and strategies of population management.

Biopower was a concrete method of state power, which emerged within this broader conceptual framework of governmentality (Ibid:152). This method used biological features from humans as a means for political strategy, and it enabled new techniques of governance (Vaughan-Williams 2012:79). Concerned with the body and its relation to power, Foucault argued that: “Bio-power brought life and its mechanisms into the realm of explicit calculations and made knowledge/power an agent of transformation of human life” (Foucault 1990:143). Hence, biopower was used to colonise the body, by overlaying it with calculatory grids and mathematically inscribing it with formulae that transformed it into an object of knowledge and power (Pugliese 2010:8).

Considering Foucault’s notion of biopower, it seems obvious to examine biometric technologies used in contemporary border control. Modern use of biometrics can be viewed as a technology of biopower, as it converts corporeal components into algorithms, which then become schematised templates in the systems (Ibid.). Since biometric technologies are able to scan a person’s entire body, its surfaces, its depths and its chemical emanations, it all together brings the effects of power within the whole body (Ibid.). These body parts thus become components within biopower, as it can be used for political ends, such as surveillance and identification (Ibid.). This will be scrutinised in depth in section 2.3. However, in order to grasp how surveillance can act as a way for states to socially sort between individuals, it is relevant to elaborate upon how states make people governable through knowledge production.

2.2 Making people governable through knowledge

Societies can be made readable by arranging and defining nature, space and people through state produced simplifications, which are aimed at creating administrative and spatial order and possibilities for control (Scott 1998:53). Applying biometrics in border control can thus be seen as an attempt for modern states to make the society more readably through identification and classification. Thus, irregular migrants and asylum seekers’ biometric data, which are stored in large-scale IT systems, can be used for producing knowledge about people who are moving. Since biometric technologies use this form of very unique and personal data, many state actors believe that they are capable of converting a person’s corporeal or behavioural attributes into evidentiary data, as it can verify the identify of a person (Pugliese 2010:3). Yet, several scholars have contested whether the technologies and the knowledge derived from it are really as neutral and objective as it is portrayed to be (Ibid; Jacobsen 2012; Magnet 2011). Hence, it is relevant to examine the concept of ‘truth’ as a category that gets its status as ‘truth’ through relations of power and knowledge. This is something Foucault (1980) has dealt with in his work *Power/Knowledge*. He argues that power is constituted through generally accepted forms of knowledge and scientific understandings of ‘truth’, which discursively determines and delimits the ‘truth’ of a particular subject (Pugliese 2010:3-4). In the words of Foucault:

> Truth is a thing of this world: it is produced only by virtue of multiple forms of constraint. And it induces regular effects of power. Each society has its *regime of truth, its 'general politics' of truth*: that is, the types of discourse which it accepts and makes function as true; the mechanisms and instances which enable one to distinguish true and false statements, the means by which each is sanctioned; the techniques and procedures accorded value in the acquisition of truth; the status of those who are charged with saying what counts as true (Foucault 1980:131, emphasis added).

The ”general politics” and “regimes of truths” that Foucault described, can be seen as the result of scientific discourse and institutions (Pugliese 2010:4). They are constantly reinforced and redefined in the educational system, in the media and in political and economic spheres. Foucault (1980:131) argued that ‘truth’ is characterised by five important traits. First, ‘truth’ is centred on scientific discourses and the institutions that produce it. In the context of this thesis it can be the Commission in it self, as it produce knowledge on the fields that it make proposals to (Boswell et al 2011:7). Another example can be the European Parliamentary Research Service (EPRS), which is a research unit connected to the Parliament. A second trait is that ‘truth’ is subject to constant economic and political incitement, as there is a huge demand for it. This means, that there is a huge demand for knowledge production on the field of e.g. how many migrants enter the EU, what are the statistics etc. The EU needs knowledge and hence the ‘truth’ in order to be able to govern. The third trait concerns ‘truth’ being widely diffused and used under different forms, such as in the educational and information apparatus of universities and research institutes. Research on migration studies has been a field in expansion in the past decade, with scholars producing a large amount of studies on all aspects of migration (Ibid.). Universities offer graduate programmes on international migration while research councils and foundations direct funding opportunities to projects within new research fields concerning migration (Ibid.). An information apparatus can be the Brussel-based Migration Policy Group, whose job is to transfer knowledge from research to policy makers vice versa (Ibid.). The fourth trait concerns ‘truth’ being produced and to some degree transmitted under control, in a few political and economic apparatuses, such as universities, armies and the media. Lastly, ‘truth’ is a central object in political debates, social confrontation and ideological struggles, influenced by e.g. the right-winged political parties gaining power throughout the EU. As such, a large part of migration policy concerns responding to popular pressures. These responses are often expected being based on expert knowledge, created by research groups and universities. Having this fundament makes it possible for the Commission to demonstrate that they are collecting the right kind of data and information and has sufficient knowledge on the field of irregular migration and asylum seekers in the EU, for example (Ibid.). Hence, one can argue that ‘truth’ is not autonomous and independent from its surroundings, including the knowledge producers, institutions or media. This makes it possible for policy makers to frame things in certain ways to their advantages (Ibid:2). These traits are crucial to be aware of, as they allow an assessment of how experts and professionals attempt to expand their power by applying e.g. securitarian practices and technologies to migration and border control (Ibid; Bigo 2001)

Another concern is that biometric technologies themselves can be underpinned by the discourse of science (Pugliese 2010:4), which is enabled to make its truth claims because it uses a scientific method. This method is based on empirical and observable evidence, which is gained through formalised experimentation. Other scientists can test these claims in order to verify them (Ibid.). Furthermore, can a discourse can get a ‘truth status’ because the institutional sites from which the scientists enunciate their discourse underpin it (Ibid.). These institutional sites, such as universities and laboratories, act as the sources of legitimacy and authorisation of the discourse (Ibid.). For these reasons, Foucault emphasise importance at asking: “Who is speaking? Who, among the totality of speaking individuals is accorded the right to use this sort of language? [....] What is the assurance, at least the presumption that what he [or she] says is true?" (Foucault 1985:5).

The point of asking these questions, is to highlight that the production of 'truth' is within relations of power and knowledge, which Foucault argues will always be socially situated (Pugliese 2010:4). When bearing this is mind, it becomes clear that biometric systems, which are technologies of 'truth', will always already be mediated through a cluster of relations of power and knowledge. That institutions legitimate the discourse of science, and that the production of 'truth' is always socially situated, has consequences for the understanding of biometric systems (Ibid.). That the socially mediated status of technology is effaced in many accounts of biometrics leads to claims that biometric systems are:

> Objective technologies that remove the biases and prejudices of human observers, and thus deliver impartial and unmediated knowledge of their respective objects of inquiry (Ibid:5).

It has been broadly discussed whether it is possible for something to be completely objective, within several schools of thoughts - such as feminist, race, ethnicity and whiteness studies (Ibid; Fanon 1986; Morrison 1992; Dyer 1997; Frankenberg 1993). Amongst many others they have tried to deconstruct the claim that science is an objective and impartial practice (Pugliese 2010:5). Along these lines, Pugliese displays biometric technologies as products of "situated knowledge's" (Ibid.), and thus challenges the common conception of them being objective. By using this term he draws on Donna Haraway (1991), who wanted to disclose the social and political dimensions inscribed within knowledge production, as a result of the locus that is embodied in the knowledge producer (Pugliese 2010:5). According to Haraway, this locus can be influenced by categories of gender, race, ethnicity, sexuality, class, (dis)ability and age (Ibid.). Furthermore, it can be argued that the main purpose of science always will be political government (Stenum 2012:282). Following this understanding, numbers and figures are "integral to the problematization that shapes what is to be governed, to the programmes that seek to give effect to government and to the unrelenting evaluation of the government that characterizes modern political culture" (Rose 1999:199). These reflections of the relation between knowledge and power are useful when studying how and for which reasons the EU gather more data on asylum seekers and irregular migrants, and how this information is used in the proposals to change the regulations of the large-scale IT systems.

2.3 Surveillance as social sorting

The growing global focus on external and internal threats, such as terror and cross-border crimes, have resulted in that states have an increased desire to have control over people's identities, especially those coming from outside the states, such as asylum seekers and irregular migrants (Jacobsen 2012:10). States interest in securing internal territory and populations has resulted in a wish to divide individuals into different groups of safe/dangerous, civil/uncivil or legitimate/illegal (Amoore 2006:338 Vaughan-Williams 2012:59). Since biometric and digital borders register everyone crossing, states obtain data which can be used to create knowledge about these different groups; are they legitimately inside the state, have they overstayed their visa or have they exited the territory? The data obtained are thus used to gain control over these peoples movement and also to secure the state from those who are believed to create risks internally. Didier Bigo's (2001:112) definition of the 'Möbius ribbon' is applicable for understanding states interest in internal and external security:

> Internal and external security are embedded in the figure of the 'enemy within,' of the outsider inside, which is increasingly labelled with the catchword 'immigrant,' who is, depending on the context and the political interests, a foreigner or a national citizen representing a minority. The outsiders are insiders (Ibid.).

Applying his lens of governmentality, which combines "technological sophistication, and the old disciplines of the body" (Ibid:100), enables an analysis of how immigration and security threats, such as terrorist attacks, are combined as a issue, which states needs to react on. He argues, that this happens because "scenes from everyday life are politicised, because day-to-day-living is securitized, and not because there is a threat to the survival of society and its identity" (Ibid.). An additional security concern for states is the desire to accurately identify the individuals who are regarded potential future threats before their potential materialise as reality (Jacobsen 2012:7).

Using biometric- and surveillance technologies in border controls, makes it possible to quickly target those who are perceived as a future threat and manage them; being both citizens, immigrants, employees, or consumers. Hence, surveillance and identification technologies have become the preferred way to manage risks and predict future dangers (Ceyhan 2012:42). With the emphasis put on these technologies, there has been a rise of people being labelled as suspicious, while at the same time surveillance techniques have become increasingly intrusive, opaque and secretive (Lyon 2003). However, surveillance is an old activity that has existed as long as humans have interacted with each other (Lyon 2006). Relying on Foucault's understanding of biopolitizised security, Ceyhan (2012:40) argues that surveillance can be understood as a way for liberal governmentality to seek maximum efficiency for the regulation of bodies - it is an activity that governments, institutions and the population itself undertake against each other. In order to regulate the population it has to be known in terms of its actual behaviour and possible future behaviour. Following Lyon (2002:13), surveillance has always been ambiguous, because it covers both care and control of a population and the role of visibility of the surveyed is taken as seriously as the process of observing, classifying and studying.

It is a general belief within states that access to improved speed of handling and richer sources of information about individuals and populations is the best way to monitor behaviour, to influence people and to anticipate and pre-empt risks (Ibid:14). A concrete way for states to identify a dangerous from a safe person is through surveillance. Hence the central aim of using searchable databases to process personal data, such as biometrics, is social sorting (Ibid:20). The drive for surveillance can be said to be the wish to classify the population into different groups and produce profiles and risk categories in order to plan, predict and prevent by classifying and assessing those profiles and risks (Ibid:13). The classifications produced through codes and algorithms are designed to influence and manage populations and persons, and thus directly or indirectly affecting the choices and chances of people. When classifying people and populations according to various criteria, the systems also determine who should be targeted for special treatment, suspicion, inclusion or exclusion (Ibid:20). Hence, it judges those whose data are in the system. The profile of these travellers are created by the physical and digital 'traces' they leave when travelling, and which are registered and monitored through data as bits of information - through dataveillance. This information makes it possible for databases and specialists working with the databases to construct categories of suspects, building profiles of people who have similar and certain patterns emerging from morphing the behaviour of thousand of individuals (Bigo 2014:218).

To summarise, chapters 4, 5 and 6 rely on theories on how to apprehend biometric borders as a way for states to govern and control migration movements, through practices of knowledge production, surveillance and social sorting. Applying these theories allows for an in-depth and critical investigation of the policy narratives in the Commission's recast of SIS, Eurodac and VIS, what is portrayed to be appropriate solutions to solve presented issues, as well as which impacts and effects these changes may have for asylum seekers and irregular migrants registered in the databases.

3. METHODOLOGY

This chapter explains the methodological reflections underpinning this thesis. I have found it relevant to apply theories on critical discourse and policy analyses, as they provides a vehicle for critically questioning how governing takes place and thus the activities that aim to shape, guide or affect the conduct of people (Bacchi & Goodwin 2016:5). The first section elaborates upon how to understand discourses as embedded in the social, material and technological practices, whereas the second section unfolds how to conduct a poststructuralist policy analysis. The third section unfolds the 'What's the Problem Represented to Be?' (WPR) approach in relation to how it will be adopted in respectively chapter 4, 5 and 6.

3.1 Discourses embedded in political, social and technological practices

Poststructuralism began as a movement in literary criticism and philosophy in France in the late 1960's (Jones 2013). It argued that language was not a transparent medium that connected one directly with "truth" or "reality" (Ibid; Bacchi & Goodwin 2016). Rather, it should be seen as a structure or a code, whose parts derived their meaning from their contrast with one another, and not from any connection with an outside world (Ibid.).

Poststructuralism not is a singular theory, as it spans a variety of different and sometimes conflicting views, which means that the terms should not be understood as a cohesive programmatic view (Fawcett 2008). Yet it is possible to identify some parameters of a common approach. Attention is often directed towards heterogeneous practices, especially in knowledge practices, that produce hierarchical and inegalitarian forms of rule (Bacchi & Goodwin 2016:4). The approach emphasises a plurality of practices, meaning that reality is contingent and always open to challenge and change (Ibid.). Bacchi and Goodwin state that: ""things" are "done" or "made", constituted, or brought into being" (Ibid.). This indicates that knowledge and terms are "*contingent* historical creations, human creations, that need to be interrogated rather than enshrined as "truth"" (Ibid.). As such, the main point is that one must pay attention to the contingent power/knowledge relation behind terminologies. This means, that there are discursive struggles hidden behind every demarcated concept.

Within social sciences, including the poststructuralist movement, discourses tend to be presented as language that is constitutive of social relations and not just a mirror of real of factual worlds (Huysmans 2006:91). Often discursive approaches to security and migration implicitly focus on statements by leading politicians, treaties and visible diplomatic agreements (Ibid.). This means that they tend to study the highly aggregated discourse, which is expressed at the top of the political and bureaucratic hierarchy (Ibid). Focusing solely on political discourses increase the risk of masking the technical nature of the implementation process and its constitutive nature (Ibid:92). Huysmans (Ibid:91) argues that this leaves the assertion of the constitutive power of discourse at a meta-theoretical level, which he maintains is a weakness. The reason for this is that it does not help one to understand how to conceptualise the embedding of discourses in social practices. This thesis broadens its focus, so that it also include the application and institutionalisation of technologies of government

(Ibid:86). This does not only refer to material devices, such as biometric technologies, or immaterial devices but also to different forms of knowledge, skills, diagrams, charts and calculations which make it possible to uphold dominant discourses (Ibid.). As such, it aims at critically studying discourses that are both embedded in in the speech act, but also in technological and material things (Ibid; Lemberg-Pedersen 2018:241).

3.2 Policy analysis

The starting point for a poststructural policy analysis is based on the statement that we live in societies "saturated" with policy (Bacchi & Goodwin 2016:5). This means, that from when we wake up in the morning until we go to bed, we are surrounded and influenced by legislative rules and regulations. Bacchi and Goodwin expand this perspective even further:

> A poststructural perspective highlights how these rules and regulations bring into play professional and "expert" knowledges that have a significant role in how we are governed and in producing these kinds of "subject" we are encouraged to become (Ibid.).

In a poststructural understanding, government thus involves more than solely conventional legislative institutions and political parties, since also including numerous sites and agencies, and ways of knowing, which interrelate and shape social rules. Hence, Bacchi and Goodwin (Ibid.) draw on Foucault, who proposed that the term *government* should mean the "conduct of conduct" (Ibid.), referring to any form of activity that aims to shape, guide or affect the conduct of people. Government can also concern state-generated rules, which is especially relevant for this thesis, as it examines proposals to change regulations and policies. From a poststructuralist point of view, policy refers to how order is maintained through politics, understood as the before mentioned heterogeneous relations that shape lives and worlds (Ibid:6). Order can be maintained through the production of categories of objects (e.g. traffic, addiction); of subjects (e.g. citizens, asylum seekers); and places (e.g. the EU, the state). Shore and Wright (2003:4) emphasises that people throughout their whole lives are classified, shaped and ordered according to policies. Thinking about the categories as effects of policies rather than necessary and natural ways of grouping people, clarifies that it is important to consider how these categories are produced and how they translate into lived realities (Bacchi & Goodwin 2016:6).

3.3 What's the problem represented to be?

Debates on migration, security and border management often revolve around rival values and interests, while they also invoke certain knowledge claims about causes, dynamics and impacts (Boswell et al. 2011:1). Boswell et al. (Ibid.) define these claims as policy narratives, as they set out beliefs and appropriate interventions. The WPR approach offers a way of analysing these policy narratives, as it makes one think differently about what are commonly accepted as categories and governing practices (Bacchi & Goodwin 2016:13). As such, the method involves an analytical strategy, which questions the common view that government's intentions with policies are to address and solve problems that exist. Rather, the WPR approach argues that policies do not address problems that exits, but instead they produce problems as particular sorts of problems (Ibid:16). An underlying goal is to make the politics involved in the practice of government visible. This is done by critically examining policies as something that frame problems in certain ways and which propose solutions to these depicted problems.For this thesis I have found it relevant to draw on the WPR approach and let it inspirer the analysis without adhering completely to Bacchi's questions. I have chosen to include three out of seven questions (Bacchi & Goodwin 2016:20), to enable an investigation of the dominant discourses embedded within political, social, material and technological practices, as well as what implications and effects these might have for those registered in the databases and the EU:

- *What's the problem represented to be in a specific policy or policies?*
- *What is left unproblematic in this problem representation? Where are there silences?*
- *What effects (discursive, subjectification, lived) are produced by this representation of the "problem"?*

Applying these WPR questions enables a critical analysis and discussion of the three proposals that this thesis focus on, namely SIS (COM(2016) 880 final), Eurodac (COM(2016) 272 final) and VIS (COM(2018) 302 final) (EC 2016b; EC 2016a; EC 2018a). Chapter 4 aims at identifying the policy narratives in the proposals, and as such how the Commission frames certain problems and solutions. As such, this chapter evolve around question 1. Bringing the represented problems and the suggested solutions into play along with an elaboration of the development of the policies, enables a discussion of some of the underlying assumptions that legitimise these representations and the implications that follow for how lives are imagined and lived (Bacchi & Goodwin 2016:6). Building on this, chapter 5 and 6 evolves around question 4 and 5. The objective of question 4 is to destabilise an existing representation of a problem, by drawing attention to things that are silenced (Ibid:22). Question 5 invites one to consider the effects of the identified problem representation. This is not thought of as measurable outcomes, but rather as political implications. Accordingly, it enables an examination of how certain ways of framing problems can create difficulties (or forms of harm) for members of some social groups more than for members of other groups (Ibid:23). Chapter 5 focus on what happens when policies' purposes and functions change over time, as it is not a covered aspect in the proposals or regulations. Chapter 6 includes an examination of what limitations the biometric technologies might be prone to and what this consequently can lead to, when not being aware or not showing consideration to it.

All chapters includes empirical examples and critical research from European Union Agency for Fundamental Rights (FRA), the European Council on Refugees and Exiles (ECRE), NGOs and the European Data Protection Supervisor (EDPS). Including rights-based examples makes it possible to illuminate some of the consequences the increased use of biometric technologies might have for people subjected to these policies. Yet, it is also important to underline that FRA and EDPS are EU agencies, why they might be subjected to some degree of censor and influenced by political agendas, despite their immediate independence. However, their concerns are vital and interesting to include, as their critical concerns and perspectives on rights-based matters both contest and contradicts the Commissions suggested increased reliance on biometric technologies.

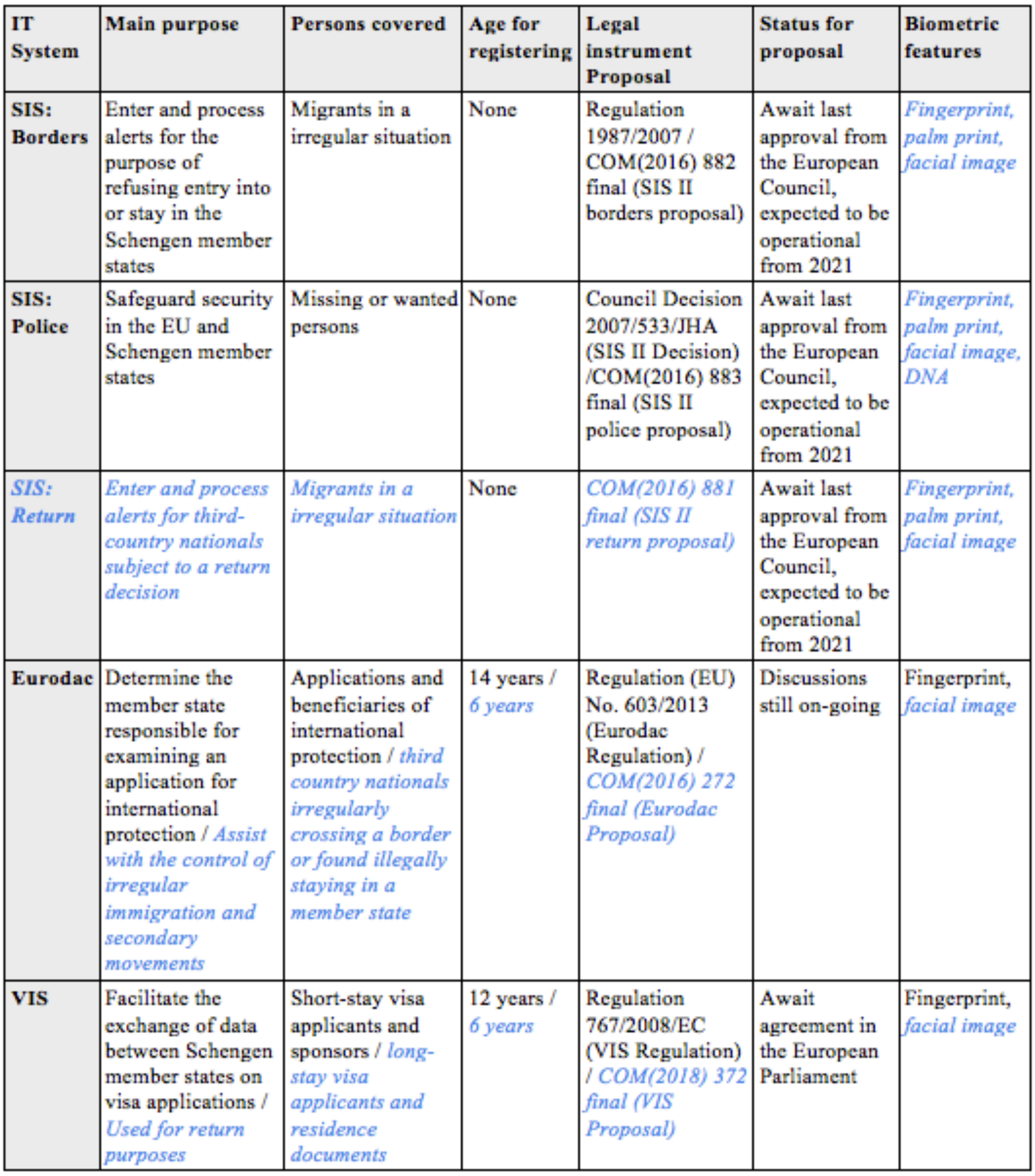
3.4 Limitations

Throughout the process of writing this thesis it has been necessary to exclude several interesting themes, due to limited time and scope. These will shortly be elaborated upon, as they illustrate important and related themes. The first concerns the geographical scope. The level of this thesis is regional as the focus is placed on the Commission's proposals to change EU regulations on large-scale information systems. The Commission is the EU institution that is responsible for proposing legislations, implementing the decisions made, and upholding EU treaties. Thus it concerns overall EU policies. Nonetheless, it is important to recognise that the Commission and the member states policies and political strategies influence and interact with each other. Anyhow, due to the narrow focus, there will not be an in-depth analysis of each of the member states' policies and practices of registration of irregular migrants and asylum seekers. This leads to the second theme intentionally left out in this thesis, concerning interactions between migrants and the EU. It the context of EUs biometric and digital border control it seems crucial to not only study the phenomenon from the perspective of the EU and the Commission. Rather, several scholars have emphasised importance at studying migrants' resistance and autonomy towards state structures. This means, that one should study the autonomy and performativity of migrants, as it is believed that the refusal and subversion of irregular migrants trigger social transformations first, and any transformation of the state follows this social change, as ways to stop, contain or channel the movements of migrants (Papadopoulos et al. 2008; Mezzadra 2011). Yet, since the objective within this thesis is to make a critical policy analysis of EUs recasts of large-scale information systems regulations, migrants' autonomy and performativity is a perspective not gaining much attention. The third consideration involves the types of registrations stored in information systems. Within SIS, VIS and Eurodac there are both registered alphanumeric details, such as name, sex, age and country of origin, as well as data about people's biometric features, being fingerprints, palm prints, facial images etc. Since the main interest has been placed on biometric technologies, it has been necessary to leave out the importance and implications of the stored alphanumeric data. Yet, for future research it would be relevant to include this, as if it is typed in wrong it can have implications for those registered in the databases, as it can lead to false matches (FRA 2018). The last theme intentionally left out, concerns the industry's involvement and influence on the political wish to increase the use of the technologies (Lemberg-Pedersen 2013, 2018). This is done despite its obvious relation to the focus on biometric technologies deployment in EU's information systems. Whilst this perspective is both relevant and intriguing, it is a theme that will not be included in the thesis, as the main objective is to make a critical policy analysis.

To summarise, the three chosen questions from the WPR approach guide and inspirer the following three chapters, as they – combined with the theoretical foundation – facilitate critical perspectives and stances when analysing and discussing discourses within the Commission's suggestions to recast the regulations of SIS, Eurodac and VIS, as well as in biometric technologies.

4. EU'S INFORMATION SYSTEMS

The Commission regularly publishes policy papers, including proposals to change regulations. These set a political agenda for the EU and bring forward solutions to what are framed as problems. The aim of this chapter is to scrutinise the three proposals to recast the regulations for Eurodac, SIS and VIS, made by the Commission. The theoretical outset is placed on perspectives of governmentality, biopower and the relation between knowledge/power. Empirically it relies on each of the proposals as well as reports and comments made by NGOs and the EDPS. Examining the proposals separately opens up for a study of how large-scale information systems are used as border-, migration-, and security management in the EU and why registration of asylum seekers and irregular migrants is important for the Commission. Each of these information systems has their own objectives, purposes, legal bases, user groups and institutional contexts, but they are complementary (EC 2016c:5), which is visualised in Table 2. The table reveals which regulations are currently ratified (in black) and the proposed changes in the regulations (in blue). Additionally it clarifies the purposes of the systems, who and at which age it is possible to register as well as what biometric features they contain. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is the EU institution, which is responsible for the operational management of the three information systems (eu-LISA 2019a).



IT System	**Main purpose**	**Persons covered**	**Age for registering**	**Legal instrument Proposal**	**Status for proposal**	**Biometric features**
SIS: Borders	Enter and process alerts for the purpose of refusing entry into or stay in the Schengen member states	Migrants in a irregular situation	None	Regulation 1987/2007 / COM(2016) 882 final (SIS II borders proposal)	Await last approval from the European Council, expected to be operational from 2021	*Fingerprint, palm print, facial image*
SIS: Police	Safeguard security in the EU and Schengen member states	Missing or wanted persons	None	Council Decision 2007/533/JHA (SIS II Decision) /COM(2016) 883 final (SIS II police proposal)	Await last approval from the European Council, expected to be operational from 2021	*Fingerprint, palm print, facial image, DNA*
SIS: Return	*Enter and process alerts for third-country nationals subject to a return decision*	*Migrants in a irregular situation*	None	*COM(2016) 881 final (SIS II return proposal)*	Await last approval from the European Council, expected to be operational from 2021	*Fingerprint, palm print, facial image*
Eurodac	Determine the member state responsible for examining an application for international protection / *Assist with the control of irregular immigration and secondary movements*	Applications and beneficiaries of international protection / *third country nationals irregularly crossing a border or found illegally staying in a member state*	14 years / *6 years*	Regulation (EU) No. 603/2013 (Eurodac Regulation) / *COM(2016) 272 final (Eurodac Proposal)*	Discussions still on-going	Fingerprint, *facial image*
VIS	Facilitate the exchange of data between Schengen member states on visa applications / *Used for return purposes*	Short-stay visa applicants and sponsors / *long-stay visa applicants and residence documents*	12 years / *6 years*	Regulation 767/2008/EC (VIS Regulation) / *COM(2018) 372 final (VIS Proposal)*	Await agreement in the European Parliament	Fingerprint, *facial image*

Table 2: Existing (black) and proposed (blue) large-scale information systems (FRA 2018:23; EC 2019a)

4.1 The Eurodac

The most relevant large-scale information system in the EU, when examining why registration of irregular migrants and asylum seekers is important for the Commission, is Eurodac. It was established in 2003 as a community-wide system that compared fingerprints of asylum seekers, using biometric technologies for identification (van der Ploeg 1999:298; Broeders 2007:82). Hence it underpinned the Dublin III Regulation its predecessors Dublin II and the Dublin Convention. The objective of the Dublin Convention was to limit the possibilities to claim asylum in more than one country and to determine which states were responsible for an asylum claim (Broeders 2007:82). Originally Eurodac stored fingerprint data and alphanumeric concerning the gender of the person (EC 2016a). Ever since it has been filled with fingerprints from three different categories of persons: 1) asylum seekers, which are necessary in order to detect 'asylum shoppers', in the light of the Dublin Convention, 2) people who have crossed the EU's external borders in an irregular manner and who cannot be turned back, 3) those who are found illegally staying on EU territory (Broeders 2007:83; Tsianos & Kuster 2016:235).

4.1.1 Recast of Eurodac, 2016

The high numbers of arrivals of irregular migrants and asylum seekers in 2015-16 resulted in that some member states did not manage or were not willing to capture fingerprints of all those arriving at the EU's external borders (EC 2019b; Lemberg-Pedersen 2018). This was especially happening in the member states that are physically close to the EU's external borders, such as Italy and Greece, as they often are the first countries of arrival (IOM 2015). When the asylum seekers and irregular migrants arrived in member states further distanced to the external borders, these states also remained reluctant or were unable to register everyone arriving. Instead they started to engage in a competition to deter prospective migrants from arriving (Lemberg-Pedersen 2018:244-245). Deterrence strategies included lowering living standards for asylum seekers and refugees and trying to close off migration routes from Southern to Northern Europe (Ibid.). The lack of registering everybody undermined the Dublin Regulation, as it became possible for irregular migrants to transit into other member states without risking being sent back to the first country of transit, as they were not registered there (EC 2019b; EC 2016a). In the proposal of recasting Eurodac, the Commission described that a consequence of this was that "thousands of migrants remain invisible in Europe" (EC 2016a:2).

The presence of 'invisible' migrants in the EU is not a new phenomenon and cannot solely be linked to what the Commission described as a 'migration and refugee crisis' (Ibid; Stenum 2017:7). However, it is a way to frame a situation where the internal security becomes embedded in the figure of an "enemy within" the EU, which in this context is labelled as the irregular migrant (Bigo 2001:112). Hence, irregular migrants and their invisibility becomes the enemy of politicians (Bigo 2002:6), which is considered a threat. Being invisible also makes it difficult to the EU and its member states to gain more knowledge about who is inside the territory and create knowledge upon the stored data.

The so-called 'crisis' resulted in that the Commission made a new proposal to reinforce Eurodac in 2016 (EC 2016a:2). It stated 17 possible solutions and interventions to what was framed to be a problem of irregular migrants and invisibility. Nine of these will now be discussed. The first provision in the proposal is to *extent the scope of Eurodac for return purposes*[1], of TCN's or stateless persons who are not applicants of asylum, or whose case has been rejected and thus remains illegally in the EU (Ibid:11). This means that Eurodac should not only contain fingerprint data on asylum seekers, but also data on "illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders" (Ibid:3). Hence, the Commission had a wish to register and identify undocumented migrants in general on EU territory, as they argued that there were too many who stayed 'invisible'. Furthermore, the choice of using the word 'illegally' emphasises the

[1] Article 1(1)(b)
[2] Article 2, 15 and 16
[3] Article 2
[4] Article 15 and 16
[5] Article 38
[6] Article 20(3)

representation of irregular migrants as being a threat towards the EU (Ferreira 2018; Boswell et. al 2011). In the proposal, it is stated that identification should be done through the use of biometric features and technologies, which was believed to fix the problem (Lemberg-Pedersen 2018:246). Another solution proposed was the possibility for member states to store and search for data belonging to TCNs or stateless persons, thus those people who are not applicants for asylum. This was believed to enable the identification of these two groups of people for return and readmission purposes. As such, the Eurodac were suggested to change into a database and instrument for wider immigration purposes, with an increased focus on return of both rejected asylum seekers and irregular migrants (Stenum 2017). With this practice, the EU acts as a managerial power that governs those seen as 'aliens' (Amoore 2006), with the political end of either detecting them through the mobile digital and biometric border, or by returning them to the first country of arrival or to their countries of origin. ECRE have criticised this provision, and argue that it is not a necessary action (as stated in the proposal) to take in order to meet the Commission's proclaimed aims of preventing irregular migration and facilitating return (ECRE 2016:7). According to them this practice would require a justification of an interference with the individual's rights under the European Charter of Fundamental Rights (the Charter), Article 7 and 8, which specifies that everyone has the right to private and family life, as well as the right to protection of data (Ibid:8; European Union 2012).

The second provision in the proposal, acting as a solution to the identified problem of invisibility, concerns the introduction of more *biometric identifiers*[2] (EC 2016a:12, 13). Within the currently ratified Eurodac Regulation it is only possible to compare fingerprint data (European Parliament and the Council 2013). However, this proposal add more biometric features, due to framed 'challenges' in the member states, as asylum seekers or irregular migrants subjected for registration had damaged fingertips or acted with non-compliance in the fingerprint process (Ibid; EC 2015a). Building on these former experiences it is suggested to be an obligation for member states to also capture facial images (EC 2016a). However, the EDPS has criticised this, and mentions that it is striking that the proposal does not contain any actual reference to cases of damaged fingerprints (EDPS 2016:8), and argues that this cannot serve as a justification to collect facial images (Ibid.). Additionally, ECRE express concerns, as focus is only put on technical solutions to situations where people act with 'non-compliance' instead of also including perspectives on trust in the identification process (ECRE 2016:9). Hence, there is an increased focus on technological fixes to certain issues (Lemberg-Pedersen 2018:246). ECRE argue, that the absence of trust between state authorities and individuals can make the registration process more cumbersome and difficult (ECRE 2016:9). Despite this critic, it is stated in the proposal that the facial images should be transmitted to the Central System, where the image would be compared with the fingerprint. This practice sustains and develops the digital and biometric border control. Additionally, it is declared that storing facial images within the Central System makes it possible to make future searches with facial recognition software. As such, the facial images may be used for surveillance purposes, when the software is installed and operational. ECRE (Ibid.) have also

[2] Article 2, 15 and 16

raised criticism on this change, as they emphasis how this would interfere with the fundamental rights to privacy and data protection. Another challenge is that introducing facial images could potentially lead to greater risks of self-harm for irregular migrations than damaging fingerprints in order to avoid identification (Ibid.). Yet, the Commission leaves perspectives concerning trust, privacy and data protection and risks of self-harm out of the equation in their quest to identify and register individuals who are perceived to pose a risk. By these means it is believed and framed as if the problem of invisible irregular migrants will be solved.

The third provision concerns the *obligation to take fingerprints and facial images* of the three categories of persons[3] (EC 2016a:12). These are applicants of international protection; TCNs or stateless persons crossing an external border irregularly; or found illegally staying in a member state (Ibid: 43, 47 & 50). This provision permits member states to introduce sanctions, if the migrant subjected for registration refuses to provide a facial image or hinder the fingerprinting procedure. The expansion of both purpose and types of data stored into Eurodac, as well as the introduction of the obligation to give fingerprints and facial images, do provide a legal basis in the EU law for the use of detention against those who refuse to give their data (ECRE 2016:13). This is a practice that ECRE (Ibid:13-14) oppose, as it would constitute an unlawful interference with the right of liberty under Article 6 of the Charter (European Union 2012). They furthermore argue, that verification or determination of nationality or identity for the purpose of examining an asylum application does not *per se* require that authorities need to have biometric data (Ibid.). This can also be determined on the basis on available documents. In cases where asylum seekers have not been registered before, biometric data does not necessarily serve any meaningful purpose for verification of determination, as it strictly forbidden to share this data with third countries, according to Article 37(1)-(2) in the proposal (EC 2016a:69-70). Consequently, one of the solutions to what is framed as a problem, is to sanction those who do not want to or for physical/psychological reasons cannot cooperate in the procedure of registering. If these people are not registered, it will not be possible for the EU to turn the otherwise invisible (not-registered) migrants into visible (registered) subjects in databases.

The fourth provision concerns *comparison and transmission of all categories of data*[4] (Ibid:13). This proposal makes it possible to search and compare both fingerprints and facial image data of all three categories of data subjects. Under the 2013 Eurodac Regulation, it was only possible to compare and search against fingerprint data from respectively TCNs or stateless persons who were applicants of international protection (European Parliament and the Council 2013). This change will allow member state authorities to check whether a TCN has claimed asylum or has been apprehended by authorities when entering the EUs external border in an irregular manner, but still remains in the EU illegally. With this widening of the scope of searches, it will be possible to follow patterns of secondary movements in the EU, and thus introduce more comprehensive tracing, monitoring and identification of irregular

[3] Article 2

[4] Article 15 and 16

migration movement in the EU. Consequently, the digital and biometric border is increasingly becoming as mobile as the people it is trying to detect.

The fifth provision concerns the *sharing of data with third countries*[5] (EC 2016a:15). Within the current Eurodac (2013) it is forbidden to share personal data with a third country, international organisation or private entities (European Parliament and the Council 2013). However, this provision derogates from the principle of not disclosing the fact that a person has made an asylum application, which makes it possible for member states to transfer data on asylum seekers or migrants to third countries, if it is deemed necessary for return purposes (ECRE 2016:16). The Commission advocates for that is should be possible to use data for identifying and re-documenting irregular migrants and asylum seekers staying in the EU irregularly, in situations of return and readmission. It is framed as if it in these situations is important to get a person's identity confirmed by authorities in the country of origin. This change increases the scope of Eurodac to have extensive return purposes, which makes it possible for the EU and its member states to physically remove the depicted problem from the EU. However, this provision has also provoked criticism. In the comment made by ECRE (Ibid.) they argue that this change would create risks for those which data are shared, as personal data of persons fleeing persecution or serious harm may be shared or unlawfully transmitted to countries of origin or other third countries where they may be at risk. This is a concern that the Dutch Meijers Committee share (Meijers Committee 2016:7), as they emphasise that some third countries consider it a crime to have emigrated. This can put asylum seekers or migrants at risk of being persecuted or detained under harsh conditions, if returned with the provision of their Eurodac information (Ibid.). Additionally, ECRE notes that the safeguards of the General Data Protection Regulation (GDPR) vis-á-vis such as transfer of data would not be possible in such situations, as the area of return is expressively excluded from the scope of that regulation (ECRE 2016:16).

The sixth provision deals with *access for law enforcement authorities and Europol*[6] (EC 2016a:15). With the 2013 Eurodac Regulation law enforcement authorities were given access to the data stored, for anti-terror and anti-serious crime purposes (Ibid; European Parliament and the Council 2013; Stenum 2017:7). With the 2016 recast the Commission suggested that law enforcement authorities should be able to make searches to compare all three categories of data stored in the Central System. Moreover, it is suggested that it should be possible to make searches that are based on a facial image. Hence, future facial recognition technologies can also be a part of the solution for quicker searches made by e.g. Europol. This suggestion clarifies that it is not only the EU and its member states' power that should be able to 'colonise' the body (Pugliese 2010:8), but also the law enforcement authorities and Europol. By doing so, it becomes easier for the EU to divide asylum seekers and irregular migrants into groups of being safe or dangerous, legitimised by claims of securitising the internal territory. Yet, there are issues concerning the data retention period for asylum seekers and migrants. Data of applicants for international protection is not accessible for law enforcement purposes after three years, where data for individuals who do not apply

[5] Article 38
[6] Article 20(3)

for or are granted protection will not be blocked (EC 2016a:15). The Commission's explanation of this difference is that the likelihood of renewal for residence of asylum seekers is claimed to be higher than for non-asylum seekers (Ibid.). The EDPS questions this explanation and argues that there are no indications or evidence that those not having asylum would be more subjected for law enforcement investigations than asylum seekers (EDPS 2016:11). Additionally, the mere likelihood of renewal of residence permit does not justify such a difference of treatment (Ibid.). For these reasons, the EDPS recommends that data should be inaccessible for both categories for law enforcement purposes after a three-year period (Ibid.). This means that data should only be searchable for law enforcement authorities for up to three years, thus limiting the period where asylum seekers and irregular migrants can be suspected as criminals. If the proposal is ratified as it is suggested now, then irregular migrants can be in a database of suspected criminals throughout the five years retention period.

The seventh solution to the represented problem, is *to lower the permissible age for taking fingerprints*[7] (EC 2016a:14). Many applicants of asylum and migrants arrive irregularly in the EU as very young children, who either travel with their families or on their own, as unaccompanied minors. The Commission makes it clear, that it is important for them to identify these children with biometric technologies, by capturing their fingerprints and facial images. The Commission suggests that the age for taking fingerprints should be lowered from 14 years to six years. This is based upon research made by the Commission's Joint Research Centre (JRC), which indicated that fingerprints taken from children at the age of six and above could be used in automated matching scenarios (JRC 2013). JRC is the Commission's science and knowledge centre, whose objective is to provide scientific advice and support to EU policy. The Commission relies on this kind of affiliated expert knowledge to underpin decisions, especially in areas of risk, a heading under which migration concerns is often placed (Boswell et al. 2011:2). However, it is important to be aware of that JRC research may be influenced by the political agendas. Anyhow, in the proposal it is framed as if that lowering the age to six will strengthen the protection of unaccompanied minors, as it would be possible to identify them and hereafter keep track of them, possibly being able to prevent them from ending up in exploitation. This has been criticised by 23 NGOs and United Nations (UN) institutions, which argues that it is a misguided claim (UNHCR et al. 2018). By contrast, they argue that if this provision is ratified, then it will put children in more vulnerable positions, as authorities will be obliged to obtain fingerprints from children, even if it has to be done with coercion. The 23 organisations declare that registration of children must always be done in a child-sensitive and child protective manner and in the best interest of the child, in accordance with Article 3 of the Convention of the Child (UNHCR et al. 2018; United Nations General Assembly 1989). However, even done with a child protective objective in mind, coercion of children in any manner in the context of migration related procedures would violate children's rights (UNHCR et al. 2018). EU member states are committed to respect and uphold the Convention of the Child. The organisations argue that a general reference to family reunification cannot in itself justify and provide a sufficient

[7] Article 10, 12, 14

basis for collecting biometric data from children (Ibid.). Instead, both ECRE and the 23 organisations argues that authorities to a much larger extent should facilitate efforts to locate family members or relatives in other countries, in case of family separation (ECRE 2016:8; UNHCR et al. 2018). Additionally, if ratified, it becomes possible for authorities to register much more people than beforehand, and thus extending the scope of data stored in Eurodac. This would mean that those 256,195 children under the age of 14 who applied for asylum in 2015 would have had to be fingerprinted (ECRE 2016:8; European Parliament and the Council 2013). With this practice, the number of invisible irregular migrants and asylum seekers would be considerably limited, which is a tactic strategy for the Commission when the main aim is to make these groups more legible and furthermore to make future control more determined.

The eighth provision concerns *data retention*[8] (EC 2016a:14). The data retention period for applicants of international protection, such as asylum seekers, is currently 10 years and it is proposed to stay the same in the proposal. The reason for this is declared to be that member states should be able to track applicants if moving further on to another member state after being granted protection. In these cases they should be transferred back to the member state that granted them protection. On the other hand, the new version will also contain data on ‘illegally’ staying migrants, who do not claim asylum. This data will be retained for five years, which is framed to be in order to monitor illegal immigration and secondary movements within member states sufficiently. The EDPS (2016:10) notice that the starting point for the retention period is suggested to be the date on which fingerprints were taken. If this is the case, it is important to note that fingerprints can be taken several times, by different operators, in different member states. The EDPS raises concerns over this, as it means that the period of storage of data can be renewed each time a person gets his/her fingerprints taken. This would lead to a possibly unlimited retention period. In this way, it becomes possible for member states in the EU to store information on these two groups of people for respectively 10 and five years, or even for an unlimited time range. This means, that irregular migrants can be tracked and even kept under surveillance by the use of future facial recognition software.

The ninth and in this respect the last provision in the proposal of recasting Eurodac, concerns *statistics*[9] (EC 2016a:15). Since the initial start of Eurodac statistics and research have been conducted on border and migration issues, based upon data from Eurodac. This is argued to be in an attempt to make Eurodac data more transparent. Yet, the proposal to recast Eurodac enables access for Justice and Home Affairs Agencies to obtain statistical data for analysis and research purposes (Ibid:15-16). Using biometric and alphanumeric data stored in Eurodac for future research and statistical purposes are the most explicit way to make former invisible irregular migrants and asylum seekers into being visible. Using biometric technologies are often claimed to be an objective and neutral way of obtaining knowledge about people, as biometric features are unique to the person in question. Nonetheless, it is important to be aware of the limitations that the technologies comprise, e.g. that they are

[8] Article 17
[9] Article 9

based on probability and non-uniqueness, as well as how the knowledge about the data stored is presented (see chapter 7). Relying on digitalised biometric data can create implications for the knowledge produced and hence for the bodies who are subjected to this technology (Jacobsen 2012:10). When e.g. the eu-LISA, the European Border and Coast Agency, JRC, the Commission or the EPRS make reports and statistics based upon this data, one should be aware of the political context that surrounds it and what technological limitations there are, but which are silenced.

Before examining what is left unproblematic in this specific proposal and what effects it might have, the following two sections examine the proposals to recast SIS and VIS, and what are framed as issues and solutions.

4.2 The Schengen Information System

SIS was the first large-scale information system in the EU and acted as the prime compensatory for the abolition of internal border controls in the Schengen Area (European Union 1990; Atanassov 2018). In 2013 a new regulation of SIS (SIS II) was ratified, and it is the version that is still operational, consisting of three different components (Broeders 2007:79). Firstly, it is a central system and database physically located in Strasbourg. Secondly, there are national systems implemented in each member state that communicate with the central system and database. Thirdly, SIS II has a communication infrastructure, which makes it possible for member states to enter, update, delete and search data via their national systems. The legal basis of SIS II is defined by three different sets of regulations[10]. In the context of EU border management, Regulation (EC) No 1987/2006 is relevant to highlight, as it deals with border control cooperation (European Parliament and the Council 2006). It enables border guards and member states´ migration- and visa issuing-authorities to enter and search within the database, for alerts on TCNs or objects, such as vehicles (EC 2019a). Additionally, can immigration authorities search in the database if they find it relevant to refuse TCNs entry into or stay in the Schengen area (Ibid.). SIS II checks are mandatory for processing both short-stay visas, for border checks of TCNs and on a non-systematic basis for EU citizens and other persons who have the right of free movement (Atanassov 2018). These checks take place on the basis on alphanumeric searches (e.g. name, sex, birth, nationality), but also on searches for fingerprints as it is framed to be a more correct way of verifying the identify of people that had already been identified on the basis of his/her name (EC 2016c:7). The use of biometrics is allowed for identifying a person’s identity, if the technology is available. As there is an increased focus on identifying people via their biometrics, this can be said to create incitement for the EU and its member states to deploy biometric technologies more extensively. Considering that SIS II is physically placed at different locations and that national immigration- and border control authorities can use it for getting and making alerts on TCNs who are not allowed to stay in the EU, it can be argued that SIS II functions as a digital border. When making searches and alerts in the systems, it connects otherwise disconnected geographical points (authorities in member

[10] 1) Regulation (EC) No 1987/2006, 2) Council Decision 2007/533/JHA, 3) Regulation (EC) No 1986/2006

states), through data- and information sharing of people, who are the target for this system. Additionally, SIS II is also a biometric border, because it contains fingerprints, used in the identification process when the technology is available. Hence this large-scale information system makes the EUs border just as mobile as the persons it is trying to register.

4.2.1 Recast of SIS, 2016

After the 'crisis' in 2015-16, did the Commission present three different sets of proposals, which aimed at revising the legal framework of SIS II (EC 2016b). The first proposal covered the use of the system for border management, whereas the second proposal was for police cooperation and juridical cooperation on criminal matters. The last proposal covered the use of the system for the return of illegally staying TCNs (Ibid.). In a press release of the proposals the Commissioner for Migration, Home Affairs and Citizenship said:

> We extend the scope of the Schengen Information System to close information gaps and improve information exchange on *terrorism, cross-border crime and irregular migration* – contributing to a *stronger control of our external borders* and an effective and sustainable EU Security Union. In the future, no critical information should ever be lost on potential terrorist suspects or irregular migrants crossing our external borders (Ibid.).

In this statement, three different themes are intertwined and framed as problems, namely *terrorism, cross-border crime and irregular migration*. Linking migration with security issues legitimate drastic practices that traditionally only has been reserved for responding to military threats (Boswell et al. 2011:163). One response was to extend the scope of SIS II and thus the digital and biometric border control. Additionally, the intertwining of migration and security issues creates a certain form of 'truth', which is socially situated and constantly exchanged between several actors who corroborates. In this context it is between EU institutions and knowledge producers such the EPRS and the media. Bigo defines those who produce this 'truth' as "managers of unease" (Bigo 2002:74) in the securitisation of migration. They do have the power to determine what is or what is not a threat (Ibid.).

The Commission and the Parliament relies on expert knowledge when making statements like this, why they deploy knowledge and statistics produced by e.g. the EPRS. Interestingly, the EPRS also framed the situation as one where "new migration and security challenges in recent years" (Atanassov 2018) created problems. In a briefing the EPRS contextualised the proposals of revising the legislative bases for SIS II on statistics produced by the former Frontex (Ibid.). According to former Frontex registrations, the number of non-EU citizens travelling into the EU increased from 49 million individuals (191 million border crossings) in 2014 to 50 million individuals (200 million border crossings) in 2015. Furthermore, as visualised in Figure 4, the number of detected illegal crossings at EU's external borders reached 1.82 million in 2015, despite efforts to stop these flows (Ibid.). In 2016 the number decreased to 0.51 million and around 0.20 million in 2017. These numbers of arrivals have been criticised for being based on double counting's. This is because it registered arrivals of those who first arrived to Greece, and after having been in non-EU Balkan countries re-entered into the EU, in e.g. Hungary (Nielsen 2015). Frontex admitted this, but continued the practice (Frontex 2015). As such, one should be aware of that these numbers might not show the reality, but rather an overestimation of arrivals. Yet, these numbers feed into specific ways of framing the situation, thus legitimising calling it a 'crisis' posing risks to the internal security, and thus called for action.

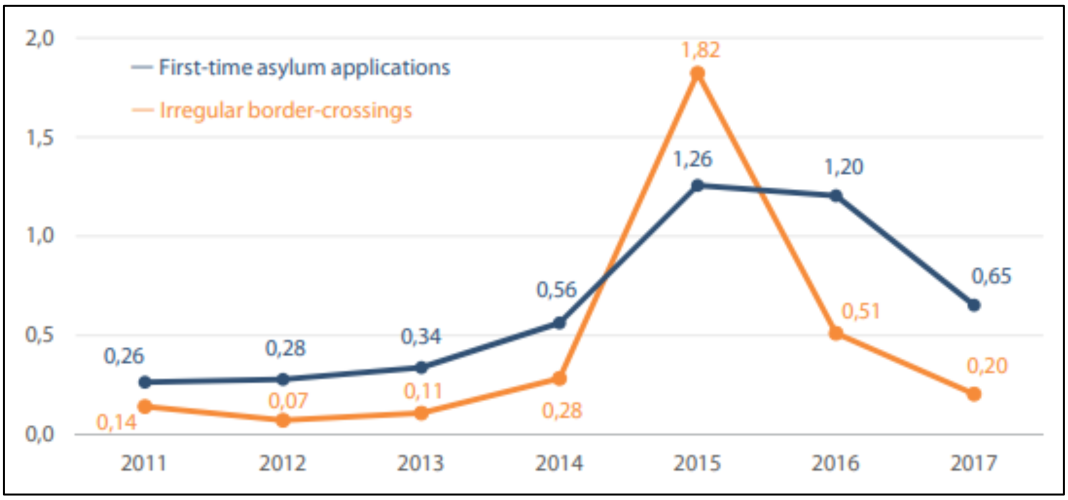


Figure 4: First-time asylum applications and irregular border crossings of EU external borders (in millions) (Atanassov et al. 2018).

Based on these numbers the EPRS continued arguing that the "unprecedented influx of migrants" put pressure on the EU border management system, leading to the reintroduction of internal border control in member states like Sweden and Denmark (Atanassov 2018). Estimates made for the Commission's evaluation of Smart Borders in 2014, moreover indicated that the number of non-EU travellers would continue to increase, and by 2025 will reach 76 million (302 million border crossings) (EC 2014). Based on these questionable inputs from Frontex and EPRS, the Commission can create a policy narrative that concerns that an increased exchange of information and alerts on non-EU nationals subject to a return decision will help tackle irregular migration (EP 2018; EC 2015a). Even though these numbers might not be correct, they feed into a general turn towards right-winged policies. Furthermore, they legitimise that the Commission proposes policies that aim at governing irregular migrants by extensively keeping them under surveillance through future SIS III. In the press release concerning the proposed changes to SIS II, a Dutch member of European People's Party said:

> Due to this lack of information exchange, a third country national with the obligation to return can easily avoid this obligation, by going to another member state (EP 2018).

Hence, one of the solutions to the framed problem of irregular migration was believed to be 'a boost' to the exchange of information and alerts on non-EU nationals, subjected to a return decision. This is a similar change, to what was seen in the recast of Eurodac. Thus, if ratified, the SIS III would also become an instrument with wider immigration purposes making the EU a managerial power, governing those who are framed to avoid the obligation of return (Stenum 2017; Amoore 2006). As such, the development of the SIS III will intensify the digital borders of the EU.

In extension to this, the Commission's recast included several other elements, two of which also directly targeted irregular migration to the EU. First of all, it was proposed that return decisions and entry bans in the future are obligatory parts of the information shared in the system. This includes the introduction of alerts on refusal of entry and stay of TCNs (EC 2019a). Currently, member states can enter alerts into SIS II if they have registered persons who are subject to an entry ban based on a failure to comply with national migration legislation. With the new proposal member states will be *obliged* to enter these alerts into SIS III, specifying the time and conditions for entering, after the TCN has left the territory of the member state (EC 2016b:16). Consequently, there would be produced more data, which SIS III shall store. This makes it possible for the EU and its member states to conduct future legislations directly at these people, making it more difficult for them to enter the EU and further monitor and surveil them and their movements in the EU. Yet, this change may also be in interference with the individual's rights under the Charters Article 7 and 8, specifying that everyone has the right to private and family life and a right to protection of data (ECRE 2016:7; European Union 2012).

The second element in the proposal is the Commission's wish to increase the number of biometric features enrolled into the systems and technologies used in the EUs border control. This is framed to be the solution to the framed problem (Ibid: 4, 9). It is already possible to use TCN´s fingerprints or facial images, but only if the technology is available, and if the person has his/her name registered in the system. As mentioned the increased focus on identifying people by their biometric features gives incentives to implement biometric technologies more widely. Moreover, it is also suggested that palm prints should be introduced as a new biometric feature and that it should be mandatory to carry out fingerprint searches in situations where a person's identity cannot be ascertained in any other way (Ibid: 4, 12, 16, 19). If photographs, facial images or fingerprints are not suitable for identification, it should be possible to use DNA profiles in the identification process (Ibid.). As such, the SIS III develops into a complete digital and biometric border, which is biopolitical because it enables the EU to regulate and monitor TCNs through the increased use of and focus on their physical bodies and biological characteristics. This practices convert corporeal components of fingerprints, palm prints and even DNA into algorithms, which are schematised into templates in SIS III. Thus, it can be said that the EU brings its effects of power directly into the body, and the irregular migrants body parts become components used for political ends. In this specific regard, the political end or wish is to identify, monitor and regulate those registered. Yet, it is relevant to include some of the concerns ECRE raised as a response to the Eurodac recast (2016:9), as they relate to the same issue. If solely focusing on technological solutions to situations where people either are not physically able or disobey registering it might add to an already existing mistrust between state authorities and individuals. ECRE (Ibid.) is worried that this will make the process of registration more cumbersome and difficult to operate.

4.3 The Visa Information System

The third and last relevant information system is the VIS. It was established in 2002, under the heading of "measures to combat illegal immigration" (Council of the European Union

2002:7). The system became operational in 2011 and does also act as a technological solution in the EUs digital and biometric border control. The EU member states use this to facilitate short-stay visa procedures and helping visa, border, asylum and migration authorities to check the necessary information on TCNs who need a visa to travel to the EU (EC 2018a:1). Like Eurodac and SIS, does VIS consist of a central IT system and of a communication infrastructure that link the central system to national the systems. The system is built to perform biometric matching, primarily of fingerprints, for identification and verification purposes (EC 2019a). Frequent travellers to the Schengen Area are not obliged to give new finger scans every time they apply for visa, as their scans stay as templates in the system over a 5-year period (Ibid.). In that way, frequent travellers, who most often are those coming to the EU to work, are given advantages compared to those visiting the Schengen Area less regularly. This indicates that the systems is also used to create different categories of people, which makes it possible for the EU and its member states to directly target, monitor and regulate a specific group if needed.

When people enter the Schengen Area's external borders, the person's finger scan will be compared to those that are held in the VIS database. In cases of mismatches between fingerprint does the system automatically refuse entry into Schengen. However, the Commission state that this "will *merely* lead to further checks of the traveller's identity" (Ibid, emphasis added). Hence, if the biometric technologies are not able to capture the TCNs´ biometric features, they will be subjected to further checks, than if the person were a EU citizen. This practice tends towards being discriminating, as some groups will be more exposed for suspicion than other groups. According to Bigo (2014:218), this is not uncommon, as border guards have a tendency to trust the technologies more than the person in front of them. Because biometric technologies and features are seen as an objective and neutral way to identify people, the personal narratives of the persons are reduced and do in many context not count as valid. This is a concern that several scholars have raised concerns about (Jacobsen 2012; Pato & Millett 2010; Magnet 2011; Pugliese 2010; Ajana 2013; Nanavati et al. 2002). However, discriminating practices may not only happen in situations where border guards do trust technologies more than human narratives. These dividing practices are crucial to shed light upon and will therefore be examined and discussed further in chapter 5 and 6.

4.3.1 Recast of VIS, 2018

In 2018, the Commission proposed to revise the VIS Regulation, stating that visa policy should remain "a tool to facilitate tourism and business, while preventing security risks and the risk of irregular migration to the EU" (EC 2018a:1). Hence, it indicated that there is a political wish to distinguish between those who are wanted and those who are not. An example of this could be to give advantages to the businessman visiting the Schengen Area frequently versus barriers for an irregular migrant traveling to the Schengen Area for family visits or work. This depicted problem is thus framed to be *security risks* and *the risk of irregular migration to the EU.* Additionally, the Commission states that the environment in which the visa policies operate has changed "drastically" because of "migration and security challenges" (Ibid:1). A way to keep control of the situation is declared to be through VIS, as it framed to "protect the EU's external borders, manage migration and improve internal security for all citizens" (Ibid.). Thus it is claimed that a ratification of the VIS recast will improve the internal security for all citizens. With this, irregular migrants are opposed to EU citizens and are framed to pose threats to citizens in the EU. Once again, the themes of migration and security risks are combined, which legitimates the Commission bringing forward ways to proceed, in order to solve the problem. As in the previous recasts of regulations, the proposal of revising VIS also contains several provisions, of which four will shortly be discussed.

The first provision declares that VIS should *include long-stay visas* and not only short-stay visas. In the proposal it is stated that including information about these visa and residency documents and their holders in the large-scale IT system will make it possible to facilitate a better exchange of information amongst member states on TCNs. This would, in the words of the proposals: "help to improve the internal security of the Schengen area" (Ibid:8). As such, there is a wish to strengthen the digital border for security reasons. Furthermore, this provision makes it possible to increase the number of registered in the database. Currently, can the central system hold up to 52 million short-stay visa applications. If the recast is ratified it would be necessary to add data on some 22 million long-stay visas and residence permits issued by member states (Statewatch 2018). Consequently, this change would embed the power of the member states and the Commission into the actual bodies of around 74 million people who will be registered with their personal sensitive biometric data. Gaining information about so many people makes it possible for the EU to govern, social sort, regulate and direct future legislations at these people. According to Statewatch (Ibid.) there have been made no attempts by the Commission to demonstrate the necessity and proportionality of the suggestion of gathering sensitive data from a huge number of individuals, yet this is a requirement under the Charter (EDPS 2019).

A second provision concerns *interoperability* between large-scale information systems in EU. This will be realised through the future European Search Portal, visualised in Figure 5 (Ibid.). Under the current rules, consulates are only obliged to check travellers under a visa obligation in SIS when determining whether a visa applicant is subject to an entry ban. Yet, when the European Search Portal become operational (EP 2017b), it will be possible for border guards or other relevant authorities to carry out a single search and receive results from all the systems they are authorised to access, rather than making individual searches in each of the information systems. The European Search Portal are designed to have access to other information systems, such as the Interpol System, European Data, SIS, Entry/Exit System, European Travel Information and Authorisation System, VIS, Eurodac and The European Criminal Records Information System. In extension to this, the proposed visa processing will be able to reach specific risk indicators, based on statistics and information provided by member states on "threats, abnormal rates of refusal or overstay by certain categories of third country nationals, and public health risks" (Ibid:9). By implementing these means to solve the framed problem of irregular migration and other linked security threats, it becomes possible for relevant authorities not only to quickly access all large-scale information databases in EU, but also to gain information about risk indicators for the person of concern (Broeders 2007; Amoore 2006). This enables a practice of categorising people into pools of risk, where some might be seen as safe and other as dangerous, which future security policies can target and for whom the degree of surveillance will be intensified

(Amoore 2006:343). Linking TCNs with risks can furthermore influence the knowledge production on this field, as scenes from the everyday life becomes politicised and securitised (Bigo 2001:100).

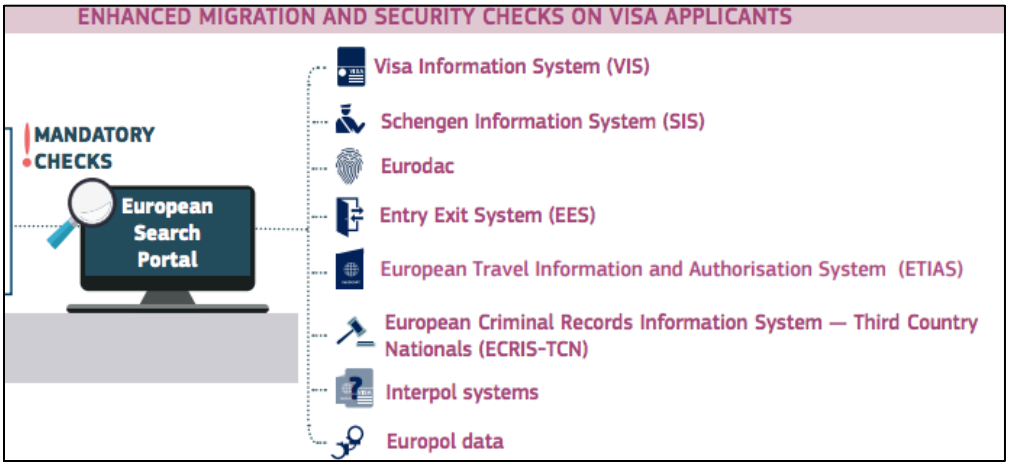

ENHANCED MIGRATION AND SECURITY CHECKS ON VISA APPLICANTS
MANDATORY CHECKS
European Search Portal
Visa Information System (VIS)
Schengen Information System (SIS)
Eurodac
Entry Exit System (EES)
European Travel Information and Authorisation System (ETIAS)
European Criminal Records Information System — Third Country Nationals (ECRIS-TCN)
Interpol systems
Europol data

Figure 5: European Search Portal (EC 2018b)

A third provision in the proposal of revising VIS, brought forward by the Commission in 2018, declared a wish to *lower the fingerprinting age for child applicants from 12 years to 6 years* (EC 2018a:9). This is similar to the change put forward in the Eurodac recast. Including this measure is claimed to enable authorities to "verify a child's identity in the visa application procedure, and will enable checks when crossing an external border" (Ibid.). Important to be aware of, is that when lowering the age of when it is possible to capture a child's biometric features will increase both the number of those registered for short-stay visas, as well as long-stay visas. This means, that the number of registered increase drastically, leaving fewer people with the possibilities to stay invisible, and thus not being countable and readable for the EU. This acts as a solution, for the Commission, in its quest of identifying greater amounts of irregular migrants, since it enables member states to have greater control over them and returning them in situations where they are not allowed to stay on EU territory. Yet, it is crucial to remember that the recast of Eurodac received extensive critic amongst 23 NGOs and UN institutions as well as ECRE, all being alarmed about the infringement with Article 3 in the Convention of the Child, stating that registration of children must always be done in a child-sensitive and protective manner (UNHCR et al. 2018; ECRE 2016:8; United Nations General Assembly 1989).

The fourth and, in this context, last provision, concerns *storing a copy of the bio-page of the applicant's travel document in the VIS to support return procedures* (Ibid:10). This proposal introduces a new category of data to be stored in VIS when submitting a visa application, namely a copy of the bio-page in the travel document. This is the page in the passport with a person's biographical data and picture. It is believed that this will make it possible to run better checks of these documents as well as "increase the efficiency of return procedures" (Ibid.). By implementing this provision, VIS will support EU's return policy, and thus also evolve into an instrument with wider immigration control mechanisms, like Eurodac (Stenum 2017). Furthermore, this provision includes the possibility for member states to share this data with third countries, for the purpose of proving the identity of a TCN for the purpose of return. As such, the EU and the member states can gain control over irregular migrants by returning them to their countries of origin, and thus physically remove the depicted problem out of the EU. This means that when people are registered into VIS, it becomes possible for the relevant authorities to directly monitor and regulate, in the name of internal security.

In sum it appears as if that the overall solution is to increase the number of registered in VIS and make the system interoperable with other systems. Hence it aims at strengthening the digital and biometric border, as it will be possible for relevant border and migration authorities to monitor and regulate irregular migrants, with the perspective of future return in mind.

4.4 Subconclusion

This chapter has scrutinised the Commission's proposals to change the regulations of Eurodac, SIS and VIS. It has been found that identification of irregular migrants is of utmost importance for the Commission, as migration concerns are continually intertwined with security issues. This is used to legitimise drastic actions, such as those set forth by the Commission, among which have been identified to be the introduction of more biometric features, lowering the age of registration, extending the retention period, using the data for return purposes and making the systems interoperable. When irregular migrants are identified, registered and thus visible, is it possible for the EU and authorities to direct future policies at these groups with the aim of governing them. As such, power becomes deeply embedded within irregular migrants bodies and the EUs borders will follow them everywhere. Furthermore, the categorisation of people makes it possible to distinguish between people and pool them into different risk categories. And making the systems interoperable makes it possible for border guards to make one search on a person in all systems at once. This makes it easier and quicker to identify, track and even surveil irregular migrants. Yet, it seems as if the overall agenda is to use the stored data extensively for return purposes. Several organisations and institutions – both NGOs as well as EU and UN institutions – have been alarmed about the future consequences for the irregular migrants who will be obliged to register in the three information systems. Yet, the Commission has a powerful position and legitimises their proposals through expert knowledge, such as the JRC and the EPRS. Hence, it would be expectable that the Commission also adjusted the proposals to meet criticism from respectively FRA and the EDPS. However, this chapter has found that it seems as if the Commission neglect their concerns, as they contravene the overall political agenda. It can be concluded that the Commission produces a certain type of truth, which solely problematises the presence of irregular, invisible migrants and asylum seekers in the EU. They do their best to solve the framed issues through an expansion and reliance on biometric technologies and do not focus much on the social and societal impacts the proposals may have.

5. PURPOSES AND FUNCTIONS ARE CREEPING

In the preceding chapter it has been found, that ever since the so-called 'migration and refugee crisis' in Europe in 2015-16, the EU has intensified the development of biometric technologies aiming at managing populations and the mobility of migrants entering the EU. This has resulted in proposals for changes in the regulations of Eurodac and VIS in 2016 and of VIS in May 2018, in attempts to solve the framed problem of invisible irregular migrants. Meanwhile, debates concerning data protection of personal data have taken place, resulting in the ratification of the GDPR (European Parliament and the Council 2016), that regulates the protection of personal data at EU level, and which entered into force in May 2018. In line with the GDPR, the Charter also contains articles concerning data protection. According to Article 8(1) of the Charter, everyone has the right to the protection of personal data (European Union 2012). Building on these political agendas, debates and developments, it is crucial to examine what happens when purposes and functions of regulations change and develop over time, also called purpose and function creeps (Wisman 2013; Broeders 2007:81; Tsianos & Kuster 2016:241; Stenum 2017:6). These terms specifically describe the development of databases containing personal information. A purpose creep is when data is used for different goals than originally collected for, whereas function creeps are the use of a technology to perform a function it was not originally intended for (Stenum 2017:6; Wisman 2013). This chapter sheds light upon some of the most relevant purpose and function creeps.

5.1 Purpose creeps

There are several interesting purpose creeps within the proposals of recasting the regulations of Eurodac, SIS and VIS. However, this section will only draw attention to four such creeps, as they exemplify the development of increased focus on targeting the framed problem of invisible migrants and asylum seekers.

5.1.1 A "fight against" irregular migration

The first interesting purpose creep is that all proposals suggest targeting what are increasingly is defined as "irregular" migrants (EC 2016a:2). In the proposals of recasting Eurodac the Commission states that:" EURODAC could contribute to the *fight against irregular migration*" (Ibid:3, emphasis added). Hence, it is depicted to be a regular "fight against" irregular migration, where irregular migrants are framed as a threat to member states, which has to be fought against by storing their fingerprints and allowing them to be compared with other data stored in the databases. This is also suggested in the VIS recast::

> VIS is indispensable when it comes to supporting external border controls and checks on irregular migrants found on the national territory (EC 2018a:4).

It is clearly stated that the VIS is perceived to be "indispensable" when it comes to supporting border controls and checks of irregular migrants found on the territory. When considering that the two regulations suggest to include irregular migrants, it can be argued that both Eurodac and VIS changes into technologies of governing undocumented "anti-citizens", by some scholars defined as irregular migrants, refugees, asylum seekers, potential criminals, or as non-citizens such as illegalised non-EU migrants (Stenum 2017:7; Walters 2015). Using biometric technologies to capture their biometric features makes irregular migrants' body parts components in what Foucault defined as biopower, used for political ends (Pugliese 2010:8). Within the proposals there are several political ends, namely to make this group of people visible, through the use of biometric technologies, by bringing the effects of power into the irregular migrant bodies. And when the irregular migrants become visible, it is possible for the EU to make them governable, through several legislations directly targeting that group. As such, the EU's border becomes just as flexible as the people they are trying to target. Another political end is that when this group is registered in either Eurodac or VIS, there is a political wish to use this data for return purposes. This changes the purpose of VIS, which originally was to register those who had applied for short-stay visas and facilitate the exchange of visa application information between Schengen member states. As with Eurodac, this is being legitimised through a focus on returning irregular migrants to countries of origin or transit. This leads to an examination of the next purpose creep.

5.1.2 Creeps and deportations

The second purpose creep concerns the intention of using the data for return or deportation purposes. In the VIS recast, it is stated that one of the objectives is to "assist in the process of identifying and returning any person who may not or no longer fulfil the conditions for entry to, stay or residence in the Member States" (EC 2018a:4). Thus, it refers to the status of irregular migrants or asylum seekers who have either overstayed their visa or have decided to stay in the EU after their asylum case has been rejected or has expired (Broeders 2007:85). Return of irregular migrants has also gained importance in the proposals of respectively SIS and Eurodac. In SIS recast, it is stated that the focus is on: "the purpose of enhancing [the data´s, ed.] use for the return of irregular migrants and for preventing their re-entry" (EC 2016b:11, 68). Thus, the data is no longer just used for making alerts on irregular migrants or missing persons, but also to return people made visible and prevent their return to the EU. In the proposal for the reform of Eurodac, it is declared that:

> The use of biometrics would contribute to improve the *effectiveness* of the EU return policy, notably in relation to irregular migrants who use *deceptive means to avoid their identification and to frustrate re-documentation* (EC 2016a:3, emphasis added).

Beforehand, Eurodac was only used as a way to return those who had applied for asylum in more than one country. However, with this proposal it becomes possible to use data concerning irregular migrants for return purposes, to country of origin or transit. Once again, it becomes a way for the EU to govern those not wanted, those described in the EU terminology as actively avoiding registration and re-documentation. In the EU's quest of maintaining internal security, in which irregular migrants are perceived as a risk, it is suggested that the purpose of the regulations should be changed, so that it becomes possible to remove them from the EU's territory (Stenum 2017:7).

5.1.3 Interoperable information systems

The third purpose creep concerns how all three proposals focus on interoperability. Currently it is only possible to make separate searches in each of the databases, but the proposals will change that. The Commission defines interoperability as the ability of information systems to exchange data and enable the sharing and access to information, and it considers interoperability as a means to enhance both border management and external security (EC 2015a; EC 2015b; EC 2016c). In the view of data protection, the issue of interoperability is an interesting purpose creep, as it will change how and by who the data in the databases can be accessed. As an example, the Eurodac proposal state that:

> [The proposal, ed.] establishes EURODAC in a way that allows for future interoperability with other information systems, *where necessary and proportionate* (EC 2016a:3, emphasis added).

And in line with that statement, the VIS proposal states that:

> The European Search Portal will make it *easier to detect security and irregular migration risks* in the visa procedure by enabling visa officers to perform quick and efficient background checks on visa applicants (EC 2018a:8, emphasis added).

Interoperability will enable all the EU member states to access data stored on one person in all the EU information systems, by a single search. This will cover short-term travellers, asylum applicants, irregular migrants and TCNs (FRA 2017:16). Yet, it is important to note that it is a right for people whose data are stored in these systems to be able to claim informational privacy, being: "the claim of individuals to determine when, how and to what extent information about the person is communicated to others" (Wisman 2013). In addition to this, Article 5(1) in the GDPR declare that TCNs are required to be informed about the relevant aspects of their personal data being processed in a transparent, intelligible and easily understandable manner (European Parliament and the Council 2016). Similarly, Article 8 in the Charter declare that everyone has the rights to protection of data. That all three proposals suggest that the systems should become interoperable and furthermore give access to official border guards, law enforcement authorities, police and Europol, may contravene both Article 5(1) in the GDPR and Article 8 in the Charter, as it becomes extremely difficult for irregular migrants to know exactly who, when and why their data is accessed and used. As such, it may oppose their right of informational privacy.

According to FRA (2018:9), it has been found that the authorities collecting and storing personal data on asylum- and visa applicants and irregular migrants, find it challenging to live up to Article 5(1) in the GDPR, as it is difficult to provide information in an understandable manner to those being registered. This means, that those registered are often not informed about all aspects of data processing and have difficulties in understanding the information they receive (Ibid.). When SIS, VIS and Eurodac becomes interoperable it may become even more difficult for authorities to explain what the data is used for, how long time it is stored for and who can access it, as interoperability of systems make the systems more complex to understand. The Meijers Committee (2018:5) raises an additional concern, relating to a potential breach of Article 7 and 8 in the Charter. They state that when authorities have knowledge of that a person's data are included in a particular database, it gives them a view over that person's actions and movements. According to them, this can be an interference with the right to data protection laid down in Article 8 and the right to privacy, in Article 7 (Ibid.).

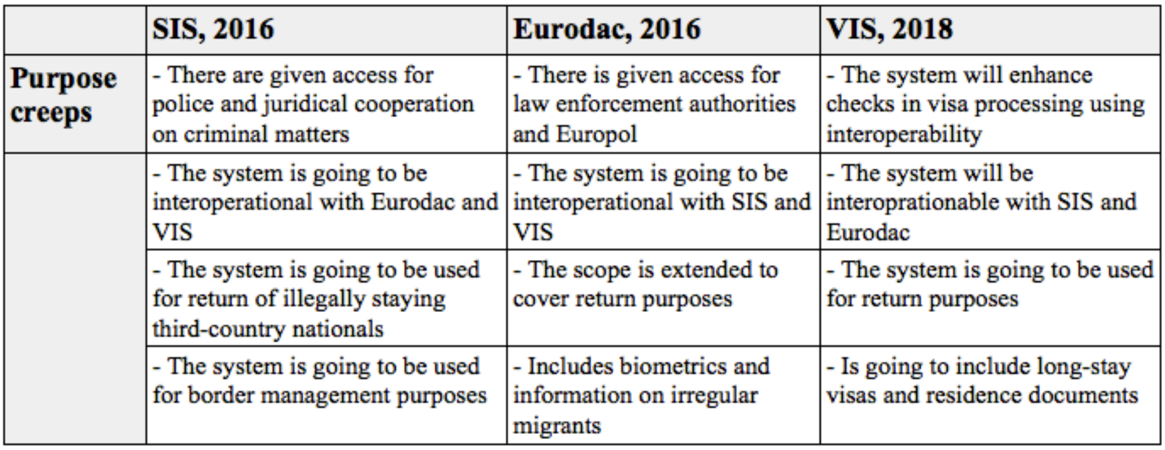
Interestingly to notice is, that the right of informational privacy, or data protection, is often balanced against other interests, like the rights of others, national security, public order and the economic wellbeing of a country (Wisman 2013). This is illustrated both in the former quote from the VIS recast, but also in the proposal of recasting SIS. Here it is declared that interoperability, and thus the possibly lack of complete data protection, is important for addressing security challenges:

> Investing in swift, effective and qualitative information exchange and information management and ensuring the interoperability of EU databases and information systems is an important aspect of *addressing current security challenges* (EC 2016b:3, emphasis added).

As written in all the proposals, it is framed as if there are several valid rationales behind making the systems interoperable, as it is increasingly argued to be for "security reasons" and "detecting security and irregular migration risks". Yet, this is not necessarily without consequences. The EDPS (2017:9) is concerned about that migration, internal security and the fight against terrorism is repeatedly referred to, almost interchangeably. According to them, it is important to be aware of this way of framing situations, as it may risk that the boundaries between migration management and the fight against terrorism is blurred (Ibid.). Consequently, it may contribute to creating assimilation between terrorists and foreigners (Ibid.), which can result in discriminatory practices, such as profiling into the future or social sorting (Hildebrandt 2007; Lyon 2002).

5.1.4 Law- and immigration authorities access to personal sensitive data

The last purpose creep concerns the impacts of when law- and immigration authorities can access and use the data for return purposes of irregular migrants. One silenced consequence of this might be that if irregular migrants know or fear that they might be apprehended or reported to the authorities, they will be discouraged from approaching providers of basic services, such as hospitals, NGOs that offer legal advice, or from sending their children to school (FRA 2018:41). Other issues not given any attention in the proposals is that if irregular migrants are victims of crime, research find that they might be more reluctant to approach the police, because they would fear to be returned to the first country of arrival or the country of origin (Ibid.). This can put them at risk of further victimisation and also allow perpetrators to remain unpunished (Ibid.). If the provisions concerning interoperability and law- and immigration authorities access to data are ratified, it can additionally result in situations where irregular migrants who are victims of crime will fear contacting the police, as they would be afraid of being deported. This can conflict with Article 10 in the EU's Victims' Rights Directive (European Parliament and the Council 2012), that declares victims right to be acknowledged as victims and have access to justices, no matter of their residence status.



	SIS, 2016	Eurodac, 2016	VIS, 2018
Purpose creeps	- There are given access for police and juridical cooperation on criminal matters	- There is given access for law enforcement authorities and Europol	- The system will enhance checks in visa processing using interoperability
	- The system is going to be interoperational with Eurodac and VIS	- The system is going to be interoperational with SIS and VIS	- The system will be interoprationable with SIS and Eurodac
	- The system is going to be used for return of illegally staying third-country nationals	- The scope is extended to cover return purposes	- The system is going to be used for return purposes
	- The system is going to be used for border management purposes	- Includes biometrics and information on irregular migrants	- Is going to include long-stay visas and residence documents

Table 3: A selection of the identified purpose creeps in the proposals to recast the SIS, VIS and Eurodac regulations.

These are just some relevant purpose creeps which are not problematised in the proposals for changing Eurodac, SIS and VIS. They can be compared with each other in Table 3. It is interesting to note, that even though the Commission does not illuminate these issues in the proposals, it seems of utmost importance for FRA and the EDPS to highlight these creeps that may contravene with legislations written down in the GDPR, the Charter and the EU's Victims Rights Directive. An interference with these laws will influence irregular migrants rights at several levels, both in terms of data protection and transparency, as well as increase their risk of being deported back to their country of origin or exclude them from their rights of being acknowledged as victims. That EU agencies, such as FRA and EDPS, contest the Commission's policies may undermine the political agenda and system, which aims at increasing the possibilities to govern and control irregular migrants through biometrics.

5.2 Function creeps

In the preceding part, four purpose creeps have been identified. However, it is not only the purposes that have crept, functions have too. This means, that the technologies, in this context the information systems, are used to perform a function that they were not originally intended for. There are three major function creeps within the proposals of recasting Eurodac, SIS and VIS, which will be examined.

5.2.1 Multimodalities

The first function creep concerns the introduction of more biometric features into Eurodac and SIS. In the Eurodac recast it is suggested that it should not only contain fingerprints, but also facial images. The reasons given for using this particular biometric feature have been the increased efficiency, and the facilitation of transnational communication between the EU member states (EC 2016a:5). Furthermore, it is argued that using this feature will make the Eurodac more compatible with future facial recognition software (Ibid.). In the proposal of recasting SIS it is also suggested that the system should contain facial images, palm prints and in some situations DNA. Palm prints will be used in the same way as fingerprints, but using multimodalities is claimed to make it possible to confirm the identity more accurately. No reason is given for the storage of TCNs DNA profiles, however the reason for introducing facial images is that it will be used for identification purposes at regular border controls at self-service kiosks and electronic gates (EC 2016b:25).

The use of facial images as a stored feature of a person is different from e.g. a fingerprint. It is easier to obtain a facial image, because the person only has to stand in front of the machine, without having to do anything (Stenum 2017:8). When taking a fingerprint, it needs much more user cooperation from the person who is subjected to registration. A facial image is additionally believed to be much more difficult to spoof – to falsify – why it should be easier to identify people in a correct manner.

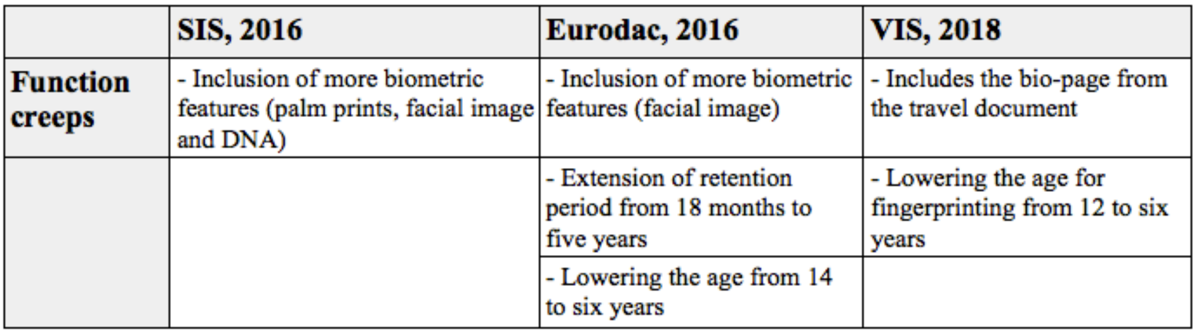
Facial images do facilitate a unique key to surveillance in both public and private places (Stenum 2017; Amoore 2006; Tsianos & Kuster 2016; Broeders 2007; Magnet 2011; Ceyhan 2012; Lyon 2002). This is also mentioned as a future possibility with the use of facial recognition software in the proposals. If installed in public places and the police is given access to software and data, it will be possible for them to track suspected irregular migrants in the streets of a city, waiting for the perfect moment to approach the person. As such, the data obtained in the biometric border control can be used for member states to gain knowledge about the different types of people entering the territory. This may be used to control these people's further movements and thus to secure the internal territory from people who are perceived to constitute a risk. This is an efficient method for the member states to regulate bodies for purposes of "internal security". Nonetheless, it is crucial to acknowledge and illuminate what situations it puts the suspected into. If being 'watched' by facial recognition software, it may happen that persons are put under suspicion and even arrested without reason. Furthermore, being 'watched' can be seen as an intrusive method used by authorities, as the persons under surveillance may not be aware of it. As such, surveillance by the use of facial recognition easily becomes an ambiguous question and strategy of care and control of respectively EU-citizens and irregular migrants or asylum seekers. This function creep is a limitation that is left completely silenced in the proposals, which can be because the political agenda and interest is to implement this software and technologies, despite the social and societal impacts, as it can be legitimised under the heading of securing the internal EU, in the "fight against irregular migration".

5.2.2 Lowering the age of registration

The second function creep is lowering the age of taking fingerprints and facial images. As already examined, this is suggested in the Eurodac and VIS proposals. In the Eurodac proposal it is suggested that the age of taking fingerprints and facial images should be lowered from 14 years to six years, as it is framed to be helpful for families in the case of separation (EC 2016a:14). Another argument is that it can be used to register children from third-countries who are found undocumented within the EU. In the VIS proposal the age of taking fingerprints is lowered from 12 years to six years. Facial images are taken from all persons of all ages. Similarly, the main argument is to identify undocumented children and to protect them from being exploited (EC 2018a:9). No matter what the reasons are for lowering the age, it is left unproblematic that when the number of people who are registered increase within the information systems, it becomes easier for member states and the EU in general to govern, monitor and surveil those registered. Consequently, this can lead to social sorting and discrimination between people. Another issue that is left unproblematic within this function creep is that when a child grows, the accuracy of a biometric match diminishes (FRA 2018:11). So, taking young children's fingerprints will affect the quality and reliability of future matches to the fingerprints taken. The risk of a wrong match increases when the fingerprints or the facial images are compared more than five years after they were taken (Ibid.).

5.2.3 Storing of data for longer periods

This leads to the third and last function creep, concerning the extension of the data retention period in Eurodac, from 18 months to 5 years for irregular migrants. For asylum seekers the retention period will stay the same, 10 years. Yet, even though the period does not change for asylum seekers, there is one important element in relation to that which is not problematised. This concerns children who are applicants for international protection. FRA research has found that children's biometric data should only be stored in databases for a maximum of 5 years, as their features would otherwise change too much, resulting in higher rates of false matches (FRA 2018:11). This would consequently result in cases such as a six-year-old child being registered in Eurodac, and whose data will be stored in the system for 10 years. However, after the first five years, it is likely that the child will be exposed to the risk of a false match if the fingerprint or facial image is compared (Ibid:14). This article requires measures to prevent future stigmatisation of children for acts they have committed in the past (Ibid.). These are just some function creeps that the proposals not problematise. They can be compared with each other in Table 4.



	SIS, 2016	**Eurodac, 2016**	**VIS, 2018**
Function creeps	- Inclusion of more biometric features (palm prints, facial image and DNA)	- Inclusion of more biometric features (facial image)	- Includes the bio-page from the travel document
		- Extension of retention period from 18 months to five years	- Lowering the age for fingerprinting from 12 to six years
		- Lowering the age from 14 to six years	

Table 4: A selection of the identified function creeps in the proposals to recast the SIS, VIS and Eurodac regulations.

5.3 Subconclusion

This chapter has examined what happens when the Commission puts forward proposals to change regulations: the issues concerning purpose and function creeps. These are issues that are not mentioned to be problematic in the proposals, which means that several important elements are left silenced. To summarise, it has been found that all three proposals suggest extensive use for return purposes for those who are framed as staying irregularly in the EU or whose asylum application or visa has expired. If ratified, these suggestions will change the purposes of the systems into being technologies of governing and monitoring irregular migrants. Additionally, it places the irregular migrants and asylum seekers, subjected to registration, in vulnerable situations as they might have a genuine fear for their lives if returned to the country of origin, which they might not be able to prove, other than by their telling their stories. Moreover, it is proposed that the purposes should be changed so they are compatible with future interoperable systems. It makes it difficult for those registered to know for whom the data is accessible and when and for which reasons the data is accessed. As such, it might become more difficult to live up to the Charter (Article 7 and 8) and GDPR (Article 5(1)).

It has also been found that the proposals contain function creeps that are not considered as problematic or conflictual issues. This include the reliance on multimodalities, as it implies an introduction of more biometric identifiers, such as facial images, palm prints and DNA. Additionally, it is suggested that these should be stored for a longer period than originally intended, and also capturing data of children down to the age of six. This increases the number of registered people in the databases, which makes it easier for the EU to monitor, regulate and surveil these people's movements and actions. These creeps are not without implications for the lives of those registered at many different levels. Firstly, it becomes more difficult to know where one's personal sensitive data is, who can access it, how long time it can and will be stored, as the retention period may be renewed every time you register. Secondly, they may be exposed to forced return, which they cannot oppose. Thirdly, they might be placed under increased surveillance through future facial recognition software. Yet, all of these issues are left unproblematic in the proposals, as they are not mentioned anywhere. As such it can be said, that irregular migrants and asylum seekers become the target in the EUs quest for monitoring, controlling and governing through technologies in 'crisis situations'.

6. RELYING ON ERROR-PRONE BIOMETRIC TECHNOLOGIES?

Biometric technologies are highly endorsed and deployed by states, as it is believed to be a vital security technology, when confronted with the wide range of threats and dangers (Jacobsen 2012; Hayes 2017:184). In the context of biometric border control in the EU, these threats and dangers are framed to be the combination of irregular migrants and asylum seekers who stay invisible and the security threats of terror and cross-border crime. The objective for this chapter is to discuss technological limitations that biometric technologies are prone to, but which are not mentioned in the proposals. These are crucial to address and scrutinise before political decisions are made, as it would otherwise enable an uncritically deployment of the technologies as a solution through which to attain a certain conception of security for states (Jacobsen 2012:10). Having identified these limitations makes it possible to discuss some of the implications and risks that are posed to asylum seekers and irregular migrants.

6.1 Unique identification?

Biometric technologies are often portrayed to be able to 'verify' a person aligned with the political agenda of identification (Jacobsen 2012:10). Hence, a primary motivation for using biometrics is to easily and repeatedly recognise an individual and to enable actions based on that specific recognition (Pato & Millett 2010:20). However, several scholars (Ibid; Jacobsen 2012; Magnet 2011; Pugliese 2010; Ajana 2013; Pugliese 2010; Nanavati et al. 2002) have raised concerns on this trust in the technologies, as they can be prone to technological errors and be influenced *a priori* by those who have developed and designed the technologies. It is crucial to be aware of that using biometrics for identification is a powerful tool, as it connects a person with earlier entered personal sensitive data, which then acts as basis for decisions which can affect their future: their right to asylum, their right to private and family life or if they are at risk of detention (FRA 2018:81). This section aims at shedding light at these issues, as when being left unproblematised, they can put the persons who are registered in the databases in vulnerable situations.

In the Eurodac recast it is declared that deploying biometrics makes it possible to "establish the *exact identity*" of the registered asylum seekers and irregular migrants (EC 2016a:19, emphasis added). This is framed to be possible by using multi-modalities such as fingerprints and facial image data. According to the Eurodac recast this practice will ensure a "*better and more accurate identification"* (Ibid:9, emphasis added). Similarly, VIS relies on biometric matching "for *identification and verification purposes*" (EC 2018a:1, emphasis added). The use of biometrics combined with interoperable information systems have enabled the police to "identify a person with the biometric data of that person taken during an identity check" (Ibid:9). The same goes with SIS, as this information system also "permit the processing of biometric data in order to assist in the *reliable identification* of the individuals concerned" (EC 2016b:9, emphasis added).

When the Commission applies such convincing language and makes strong statements like these, it can be understood as a fact that cannot be contested. This is because there is a tendency to trust in the abilities of technologies, as they are developed by scientific methods and underpinned by the discourse of science (Pugliese 2010:4), making it possible to make claims about what is framed to be the truth (Ibid.). Framing the possibilities of making this *exact* establishment of an identity reflects the powerful position that the Commission has. The Commission can shape and influence the political agenda, so it is widely believed that the deployment of biometric technologies in the EU is unproblematic. At such, one quickly finds that the deployment of these information systems relies heavily on notions of that biometrics will ensure "accuracy", "reliable identification", "verification" and the "establishment of the exact identity" of the persons who is registered in the databases. However, there are several issues that can hinder such notions and thus contest the 'truth status' of these statements. This concerns issues on probability, data quality and normative conceptualisations inscribed in the technology when it is produced (Ibid; Pato & Millett 2010).

6.1.1 Matches based on probability

As just examined the Commission actively advocates for a deployment of biometric technologies by applying a powerful and hence convincing language. However, one can question whether it is possible for the Commission to guarantee a hundred per cent correct match and identification of people. According to a study conducted by the U.S. National Research Council it is found that the accuracy of biometric recognition is merely probabilistic and not absolute (Pato & Millett 2010:1). This contradicts the otherwise predicted outcomes of deploying biometric technologies in SIS, VIS and Eurodac. This applies especially to systems that only contain one type of biometric feature, like the Eurodac originally did with fingerprint data. This is one of the key limitations of the technology, as an identification or match, which is not a hundred per cent correct in many cases will be unfit for use (Jacobsen 2012:10). This means, that using a single biometric feature may not always provide the performance needed from a given system (Pato & Millett 2010:35).

Interestingly, this limitation has been taken into consideration in the proposals as all of them suggest that they should contain a minimum of two different types of biometric features. Their solution to the limitation of probability is thus to introduce multi-modality (Ibid.). When registering more than one feature, it becomes more likely that when a biometric match is achieved in the systems, then it is a correct one (Mane and Jadhav 2009:90), as it is less likely that someone have both a fingerprint and facial image that matches yours (Jacobsen 2012:11). However, false matches do happen quiet frequently in EU information systems. This can be seen in statistics collected between 2012 and 2014 for the deployment of SIS II (FRA 2018:76). In this period Germany reported 100-200 instances of mistaken identities, while Austria, Estonia, Lithuania, Malta and the Netherlands recorded between zero to 50 instances. Since it is not unusual that false matches happens, it is of utmost importance to pay attention to, and not silence, that the technologies are not always capable of the "establishment of the exact identity" of a person, as a non-correct match can have major consequences for asylum seekers, as they can come to suffer from mental health issues (Ibid.). Furthermore, when the Commission does not pay attention to the fact that biometric features may not be unique, it can result in that people experiencing false matches are continuously met with distrust. This is because there often tend to be a greater trust in a match and the technologies than the narratives of the people in question (Bigo 2014:218). Because of that, it can be difficult for asylum seekers or irregular migrants to rebut a wrong assumption, in cases were decisions of return or relocation is based upon a false matches or even no match. In such cases, the match and technology becomes the stabiliser of a person's identity. Hence, the question of identity is shifted from the domain of the narrative of the person (the story of who someone is) to that of digital templates (digital samples of a person's biological data) (Ajana 2013:86).

6.1.2 Rejected due to bad data quality or embedded norms?

At first glance, it seems that the process of enrolling into biometric systems is a straightforward process. However, this is not always the case. The quality of data can affect the result of the enrolment or matching process (visualised in Figure 1). A person working for the national visa authority in Belgium have explained that: "[A false match] is very rare, but on a data set of 40 million fingerprints, 0.003 % is still a significant percentage" (FRA 2018:88). Since the large-scale information systems in the EU contain large amounts of data, then even a low per cent of mistakes will affect a significant number of people.

In 2018, the central system of Eurodac rejected around 20,929 fingerprint datasets, due to insufficient quality (eu-LISA 2019b:13). This can happen because of the low quality of the fingerprint image or because the fingerprints were taken in a wrong order. There are several things that can influence the quality of fingerprint leading to a potential future false match (FRA 2018:90), such as weather conditions, the characteristics of the person concerned, such as age, or that the personal data of another person has been attached to the fingerprints. The quality of facial images depends on factors such as the background and object occlusion, illumination and light reflection, ergonomics, the time elapsed since the acquisition of the image, age, gender and skin colour.

In the Eurodac recast it is stated that the collection of facial images is the precursor to introducing facial recognition software in the future, which may be used for surveillance purposes (EC 2016a:5). Interestingly, similar software is already on trial in the United Kingdom, where the British police use a system that utilises surveillance footage for facial recognition (Metropolitan Police 2019). This system has a 'watch list' that contains information about suspects who are wanted by the police or courts (Ibid.). Even though facial images are perceived to be an effective method to identify people, results from the South Wales Police indicate that the system have high rates of false matches (Fox 2018). In between May 2017 and March 2018 the system had made 2,685 matches, of which 2,451 were false alarms (Ibid.). This is just one example of high failure rate, which puts 2,451 people in vulnerable situations, as they were suspected and arrested without reason. Because of the varying degrees of data quality and the issue of probability, it is important to acknowledge that there are risks for higher numbers of mistakes in the matches and the discriminating actions this can lead to.

However, these are not the only issues that can influence the enrolment process and thus generate a false match for a person. When studying biometric technologies and systems, whiteness does also seem to be an unspoken norm which is embedded within the very infrastructures (its technologies, institutions, apparatuses) of the societies in question, which affect how the technology function in the end (Pugliese 2010:74; Dyer 1997; Magnet 2011;

Nanavati et al. 2002). Research on the field has shown, that failure to enrol into biometric systems is not something that happens for everyone. Rather, it appears that only certain ethnic or demographic groups experience this (Nanavati et al. 2002). Thus, when it comes to finger-scan technologies, three types of users - elderly, construction workers, and those of Pacific Rim/Asian descent - are more prone to fail to enrol than the control groups. They experience this, due to faint, highly worn or non-existent fingerprints (Ibid:37). Moreover, may dark-skinned users also experience failure to enrol when they present their irises for the technology, because the technology has limitations to locate distinctive features in very dark irises (Ibid.). The testing's of facial-scan solutions indicated that the biometric technology would not be adept at enrolling very dark-skinned users. The reason for this is that the quality of the image provided to facial-scan systems is optimised for lighter-skinned users (Ibid.):

> Facial-scan systems' sensitivity to lighting and gain *can actually result in reduced ability to acquire faces from individuals of certain races and ethnicities*. Select Hispanic, black and Asian individuals can be more difficult to enrol and verify in some facial-scan systems because *acquisition devices are not always optimised to acquire darker faces*. At times, an individual may stand in front of a facial-scan system and *simply not be found*. While the issue of failure-to-enrol is *present in all biometric systems*, many are surprised that facial-scan systems occasionally encounter faces they cannot enrol (Ibid:66, emphasis added)

Interesting to note, is that Nanavati et al. claim that issues of failure-to-enrol is present in all biometric systems, which might be because they are calibrated to a certain type of whiteness. For Pugliese (2010:60), this leads to what he defines as a 'double moment of occlusion'. First there is the systemic, empirical occlusion of non-white faces, which happened before the biometric system was calibrated to the white gauge. Second, it is an ideological occlusion, meaning that there is a very white calibration of the biometric systems, which precludes the acquisition of the features of non-white subjects. These forms of occlusions can be sign of technological and discursive points of irreflectivity, which is why it is crucial to rectify the systems, so everyone can enrol (Ibid.). First of all, there is a need to articulate the technological/race nexus of these systems, so that these occlusions do not appear as "surprises". Secondly, the technology should be changed, so that non-white bodies can function as reflective subjects that emit sufficient light to register precisely as template subjects in the biometric systems. Pugliese (Ibid:7) emphasise that *a priori* conceptualisations of race, gender, class, age and (dis)ability are embedded in the infrastructure of the biometric technologies:

> They constitute the *a priori* conditions of the technology's operations; their *a priori* status guarantees their invisibility. As such, these infrastructural normativities produce biopolitical effects for those subjects who fall outside their normative parameters (Ibid.).

Hence it is relevant to examine the structuring power of whiteness in the context of biometrics (Ibid:6). Because these conceptualisations of the above-mentioned categories are argued to be *a priori* present in the technologies, they constitute the infrastructural fabric of the everyday function of them and the practices associated with them. This enables the advocates for biometrics, such as the Commission, to celebrate and declare the technology as impartial, objective and non-discriminatory, while at the same time excluding certain groups to enrol, which increase the mistrust towards them (Ibid:7).

In sum, it can be argued, that the use of biometric multi-modalities in itself is neither an unproblematic nor reliable way to accurately identify asylum seekers or irregular migrants, as claimed by the Commission. As closely examined, a biometric match is solely based on probability and will consequently in some instances be a false match. This can have consequences for the person who is falsely matched with another person, due to poor data quality. Furthermore, scholars have emphasised that the technologies are infrastructural calibrated to whiteness, meaning that whiteness is configured as the universal gauge that determines the technical settings and parameters for the visual imagining and capture of a subject. This can result in occlusion and discrimination of non-white persons in the enrolment process. If experiencing failure to enrol or false matches, asylum seekers or irregular migrants can either be returned to what is perceived to be their first country of registration, even though they have never been there, or be sent back to the country of origin. Furthermore, they can continuously be met with distrust in the legal system, as it is difficult for them to prove why a false match happened. This happens, as there is a tendency for people to trust more in the response made by biometric technologies than personal narratives. As a result, some persons subjected to false matches might consequently suffer from mental health issues, if it is a harsh registration process.

6.2 Outdated biometric data

Another limitation not given attention the proposals concerns that biometric data cannot be used indefinitely, as the templates age over time (Jacobsen 2012:12). This means that biometric technologies may not be able to recognise and match a live biometric (e.g. a live fingerprint) of a person, who had registered in the system at an earlier stage (Ibid.). This happens because biometric features change over time (Ibid; Tistarelli & Nixon 2009; Bowyer 2011; FRA 2018:92, 116). According to Jacobsen (2012:11) this is problematic, because government's promise of security through biometric technologies relies on the assumption that once an individual is enrolled and stored in the system, then it can be recognised forever. To minimise this limitation, iris recognition technology has gained prominence, because this type of biometric information is less likely to change over time (Ibid:13). However, irises are not perfect either, as there might be challenges in the registration process, if the individual is blind, have cataracts (Khaw 2002:9), or has very black irises as such discussed in the previous section.

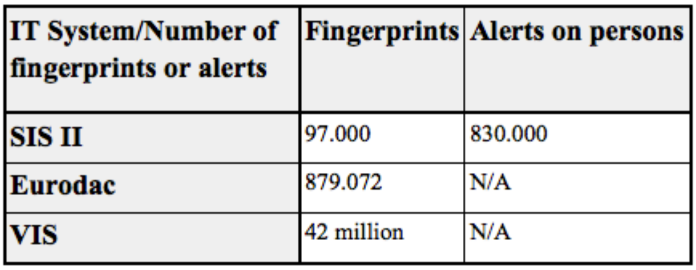
This problem is crucial to examine, especially in relation to the process of capturing children's biometric fingerprints. In both the VIS and Eurodac recasts it is proposed that the age of taking fingerprints should be lowered from respectively 12 and 14 years to six years. In the VIS recast, this decision is based on three different studies conducted on the matter, all confirming that fingerprint recognition for children can produce recognition rates similar to those of adults (EC 2018a:10). To legitimise this statement they rely on knowledge produced by the JRC, an affiliated EU research institute. The JRC concluded that: "fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy under certain conditions" (Ibid.). What the recast leaves out is to specify what "a satisfactory level of accuracy under certain conditions" actually means. It seems as if there are continuous risks of false matches, which are accepted even though it concerns children. Present technologies for fingerprinting and facial recognition does only guarantee a reliable match when the child was at least six years when the biometrics were taken, and the match happened within a time frame of five years (FRA 2018:109). Given that asylum seekers' fingerprints and facial images may stay in the Eurodac system for 10 years, there might consequently be higher future margins of error for children (Ibid.). The EU's strive to make this group of young children more visible, might consequently lead to them being exposed to false matches when they become older.

6.3 Restricted reliability of the technological performance

As already identified it is not without consequences when the Commission suggest making SIS, VIS and Eurodac interoperable, and hence creating a purpose creep. This section aims at bringing forward some of the declared statements in the proposals, which indicate what is believed to be the outcome of making them interoperable, and what could be framed as unproblematic in terms of the technological limitations of scalability. In the proposal of changing VIS it is declared that when making systems interoperable, it makes the identification process easier:

> Interoperability between the EU information systems allows systems to supplement each other to facilitate the correct identification of persons, contribute to fighting identity fraud (EC 2018a:22).

The recast of VIS thus relies on an assumption of that when the system is interoperable with other systems, then the identification process is more smooth and correct. However, VIS is an information system that makes 'one-to-many' matches. This is typically used when having a database containing huge numbers of biometric fingerprint templates and you have to identify one unknown person (Jacobsen 2012:13). When irregular migrants fingerprints are enrolled into biometric systems, then it is compared with all entries in the database. Hereafter the system will tell whether any of the already existing entries does match with the person you are trying to identify (Ibid.). When systems make 'one-to-many matches', Jacobsen (Ibid:14) and Magnet (2011:33) argue, that it is important to be aware of the reliability of the performance of such a system. The reason is that the performance can be limited depending on the size of the database that the search happens within. For this reason is it relevant to examine how many entries or alerts there are in all the information systems, as they are all proposed to be interoperable in the future (see Table 5).



IT System/Number of fingerprints or alerts	Fingerprints	Alerts on persons
SIS II	97.000	830.000
Eurodac	879.072	N/A
VIS	42 million	N/A

Table 5: IT systems and number of fingerprints or alerts on people. (FRA 2018; eu-LISA 2018, eu-LISA 2019b; Monroy 2018)

In September 2017, SIS II stored around 97.000 fingerprints, and there was made 830,000 alerts on persons. Compared to that did Eurodac store 879,972 sets of fingerprints and VIS 42 million fingerprints. According to Lawrence Nadel it is crucial to acknowledge that: "Biometric system scale and performance are inversely related. For example, a system's false non-match rate (FNMR) is linearly proportional to the size of the enrolled database" (Nadel 2007:2). Furthermore, Whitley and Hosein have highlighted that: "technological challenges here are significant and increase dramatically with the size of the population" (2010:212). This means, that one should be aware of that the larger the number of stored entries are in a database, the more likely is it that the match is not correct. In the words of Douwe Korff, international law professor at London Metropolitan University:

> Attempts to identify very rare incidents or targets from a very large data set are mathematically certain to result in either an *unacceptably high number of "false positives"* (identifying innocent people as suspects) or an *unacceptably low number of "false negatives"* (not identifying real criminals or terrorists)" (Hayes 2008, emphasis added).

These issues are not mentioned in the recasts, even though it can result in that irregular migrants or asylum seekers are incorrectly identified as suspects. This might stigmatise them and leave them in situations where it is difficult to rebut decisions already made, based on the perception of the technologies as being neutral and objective. An additional issue left unproblematic concerning scalability, is that the greater the number of false matches are the greater is the need for human intervention. In these cases, border guards or other authorities have to determine whether a match is true or false, and make corrections accordingly (Jacobsen 2012:14). According to results from a study conducted by Bigo (2014:218), those analysts working with the digital biometric borders believe that their work consist of:

> Detecting, filtering and preventing undesirables from entering, without interfering with those deemed desirable or bona fide. They regulate the control of mobility according to these profiles and independently of an examination of the body of the person (Ibid.).

When human interventions are needed to inspect whether a false match really is false, their subjective attitudes concerning who are deemed desirable and who are not, can consequently influence their decisions. The analysts working with the data see their job as preventative as they compare the match of a given person with data registered in the past (Ibid:217). By this they have the power to pool people into different categories of risk. They maintain, in the study, that visa regulations, pre-checks and entry-exit systems regulated by these large-scale databases that keep track of what is defined as "wrongdoers" and bona-fide travellers are to solve the problems of open borders for commercial purposes and the speed of travel for large number of people (Ibid.). This indicates that they see their task to socially sort between people, based upon data stored in the large-scale information systems. This means that they identify and make distinctions between those persons who are believed to pose a threat and those who are trusted citizens. The Council of Europe Commissioner for Human Rights argued that:

> While technologies that enable profiling and data mining may appear attractive security solutions, they are just as likely to lead to actions against large numbers of innocent people, on a scale that is unacceptable in a democratic society (Hammarberg 2008)

When considering all these issues it can be argued that biometric technologies are not capable of facilitating a hundred per cent "correct identification of persons" when the databases are as large as they are, and when taking into consideration that they are suggested to grow even bigger, as they should also store data on irregular migrants. Consequently, the proposals cannot fully live up to the promise of automated recognition of individuals. This may result in situations where human interventions are needed, which potentially lead to increased processes of social sorting and discrimination between people, based on data stored about them in the systems. The analysts working with digital biometric borders legitimise these actions, as it is broadly believed that they through profiling can anticipate and prevent future dangers for states' internal security (Bigo 2014:218). However, the profiles they make can be based on normative and discriminatory assumptions about race, class and gender. This can institutionalise discrimination against ethnic minorities and other portrayed 'suspect communities' (Hayes 2009:49). Conclusively, the Commissions' constant intertwining of security and migration issues affects both how the actual digital- and biometric border work take place as well as how those registered are affected by these practices. These societal and social impacts are not given any attention in the recasts, which might be because they stand in stark contrast to the overall political agenda, focusing on identification, risks, security and invisible migrants and asylum seekers.

6.4 Subconclusion

This chapter has engaged in an in-depth analysis and discussion of whether biometric technologies are as objective and neutral as they are framed to be. Furthermore, it has questioned whether the technologies are capable of ensuring a completely correct identification of irregular migrants and asylum seekers. These are issues that are important to address before political decisions are made, as if not, it makes it possible for member states to uncritically deploy the technologies as a solution through which to attain a certain conception of security for states.

Overall, it has been found that the technologies are prone to several kinds of errors. These errors will most likely contradict the political agenda set forth in the proposals, which might be the reason for why they are remain silenced. Yet, it seems it crucial to acknowledge in the political agendas and proposals, that biometric technologies are only capable of producing matches that are based on probability, because it means that member states will not be able to guarantee that a match is completely correct. In addition to this, it has been found, that capturing of data in good and correct quality is difficult and in some instances even impossible. It is found, that the technologies reacts on weather conditions, which have effects on the data quality and thus on future matches. Furthermore, it has been discussed whether the technologies *a priori* are calibrated to a certain degree of whiteness, affecting who is capable of enrolling into the systems in the first instance. Furthermore, it has been found that templates age over time. This can result in future false matches, especially for children, as they will be obliged to register down to the age of six years. When templates age and fingerprint patterns changes over time, it increases the risk of false matches and thus of potential stigmatisation. In essence, it can be concluded that all these technological limitations have huge effects for those registered, especially non-white people and children, as they will be more exposed to discriminating practices, such as profiling and social sorting, surveillance, mistrust, tracking, false matches, higher return rates and occlusion of being registered at all.

7. CONCLUSION

The so-called 'migration and refugee crisis' in 2015-16 meant increased awareness on how to solve the conflict-ridden situation. The pivotal point for the thesis at hand has been to critically examine and discuss the Commissions proposals to change the regulations of the large-scale information systems Eurodac, SIS and VIS. As such, the focus has been placed on EU's enhancement of its digital and biometric border control, which these systems constitute. It has been clarified that the Commission has a powerful position, as it can influence political agendas and ways of framing political issues in the EU. This makes it possible for the Commission to produce specific kinds of truth, which it upholds by applying convincing and powerful language. It can be difficult for the public and politicians to question and contest the proposed solutions, if they are not informed about potential consequences, limitations and social impacts. The Commission relies on knowledge and expertise produced by appointed and affiliated institutions to make proposals and solutions, such as the EPRS, the JRS, FRA and the EDPS. Relying on non-independent expert knowledge enhances the Commission's authority, power and reliability, even if they silence relevant and important facts or do not direct attention on their actual societal impacts. Yet, it is has continuously been exposed that the Commission seem to neglect recommendations and concerns raised by FRA and EDPS. This is done despite these expert inputs are crucial to include for the Commission, in order to ensure that their proposals are within the framework of relevant laws, such as the Charter, the GDPR, the Victims Rights Directive and the Convention of the Child. Undermining rights-based concerns can have adverse effects on the irregular migrants and asylum seekers who are obliged to register into the large-scale databases.

Within the thesis at hand it has been found that the Commission depicted the political landscape in the proposals of SIS, Eurodac and VIS as a 'migrant and refugee crisis' that needed prompt reaction. This is evident, as migration concerns are repeatedly intertwined with concerns of internal and societal security risks, such as terror and cross-border crime, which legitimises drastic actions. A main and common issue identified in all the proposals is framed to be the increasing numbers of irregular migrants and asylum seekers who entered the EU in irregular manners and who stayed invisible, as they were not registered into the databases. This situation was framed to be creating possibilities for subsequent movements into the EU, for irregular migrants. It has been found that the Commission declared it as important to intensify and expand the digital and biometric borders in order to identify all those entering 'irregularly' or 'illegally', as they were framed to pose risks for the internal security. It can be concluded, that when and if the proposals are ratified, the EU member states will be in a position where they can identify these people, enabling practices of monitoring, governing, returning irregular migrants and asylum seekers, in order to ensure that those who are depicted as terrorists or criminal cannot enter the EU, or that those entering in legal ways do not overstay their visa. It can thus be concluded, that an implicit goal for the Commission is to socially sort between those identified and divide them into groups of dangerous/illegal/anti-citizens and safe/legal/citizens and creating opportunities to keep them under surveillance by facial recognition software. This is with an constant view on deportation possibilities.

Within the thesis several solutions to enable a practice of identification have been examined. As these solutions are suggestions to change the purposes and functions of the original regulations, they have been classified as purpose and function creeps. Six such remarkable changes have been found. The first concerns the Commission's recommendation that the EU increasingly should rely and deploy biometric technologies, as it is depicted to be the most accurate, exact and reliable method for identification. This gives the impression that the Commission advocates for a technological fix, rather than focusing on developing methods to increase the trust in irregular migrants and asylum seekers' narratives. Secondly, it was proposed that the information systems should store a broader collection of biometric features so that they store fingerprints, palm prints, facial images and DNA, thus relying extensively on multimodalities. Thirdly, when the features were obtained, these should be used for production of statistics, increasing the platform for knowledge production and thus power, which the Commission relies on for gaining legitimacy. A fourth solution to the identified issues was to lower the age of fingerprinting to six years and extending the retention period from 18 months to 5 years for irregular migrants. As a result, this would enhance the numbers of registered and thus information stored in the systems, once again making it easier for the EU to govern, control or even return those registered. Fifth, it was also proposed that the information systems should become interoperable, meaning that it should be possible for relevant law authorities as well as Europol to gain access and search for persons' personally sensitive data in the databases. Sixth, the information systems should also be used for return purposes, which indicates that a solution was to physically remove the irregular migrants and asylum seekers out of the EU. In sum, it can be concluded that the proposed changes to the purposes and function make the information systems creep into being instruments for wider immigration purposes, aiming at deportations and sanctions, while also acting as digital and biometric borders. If and when the proposals are ratified the irregular migrants and asylum seekers will be obliged to enrol more features into the systems, while at the same time it will be possible for member states and law enforcement authorities to store and search through this personally sensitive information. As a result, it will be possible to access data for a much larger group and for a longer period. This indicates that the EU's power will become deeply embedded within the persons who are registered. It will be difficult for them to go under the radar, avoid being kept under surveillance, tracked or victims of social sorting, as future legislations can be directly targeted at these people.

Additionally, this thesis also gives strong indications that there are several effects and implications regarding the deployment of biometric technologies that the Commission does not address and thus leaves unproblematic. When not written in the proposals, it is information they conceal both the public and politician. Consequently, political decisions can be made on an uninformed basis. However, this thesis has included several experts' concerns about crucial technological limitations and social and societal impacts. This includes experts that are affiliated with the EU, such as FRA, EDPS and EPRS, but also independent ones, such as ECRE, Save the Children, UNICEF, UNHCR and academics working in the field. These concerns include facts about that the technologies are only capable of giving matches based on probability, and that it is therefore not possible to guarantee a hundred per cent correct identification, as promised in the proposals. Furthermore, it is difficult to ensure a good data quality, which also put people at risk of experiencing false matches. It has been found that relying on multimodalities will not completely solve this issue, as the technologies also face difficulties in making correct matches with e.g. facial images or iris scans. Rather, the inclusion of facial images can be used for future surveillance, which have huge impacts on the lives of those registered. It has also been found, that the technologies are calibrated to a certain degree of whiteness, which occludes the registration of people of colour. That it is more difficult for some to register creates clear divides and discriminating practices between those who the Commission depict as for example illegal immigrants vs. business people. Last, it has been found that template ages over time and that the larger the databases are, the higher the risks of false matches. This speaks against the Commissions suggestions of making the systems interoperable, extending the data retention period and lowering the age of registration. It can be concluded that all these technological limitations have huge effects for those registered, as they will be more exposed to discriminating practices, such as profiling and social sorting, surveillance, tracking, false matches, higher return rates, facing difficulties in getting help if victims of a crime and occlusion of being registered at all. In addition, it has also been found that it especially has effects and implications for those who are non-white and children. If non-white people are occluded from the enrolment- or matching process or experience false matches, they will be met with a high degree of mistrust by authorities that trust more in technologies than in human narratives. Furthermore, they tend to be profiled as posing a risk. Children registered at the age of six will be more likely to experience false matches in the future, raising the risk of being stigmatised. It can thus be concluded that the Commission's suggestions to solve the framed problems by means of biometric technologies will have vast implications and effects for irregular migrants and asylum seekers, especially those who are non-white people and children. These concerns are not addressed in the proposals, which might be because they contradict the political agenda of the Commission. As such, the Commission does not ensure that the policies will not have negative social and societal impacts if implemented.

8. BIBLIOGRAPHY

Ajana, B. (2013). *Governing Through Biometrics: The Biopolitics of Identity*. United Kingdom: Palgrave Macmillan

Amoore, L. (2006). "Biometric Borders: Governing mobilities in the war on terror," *Political Geography*, 25, pp. 336-351

Atanassov, N. (2018). "Revision of the Schengen Information System for border checks" at *The European Parliamentary Research Service.* Online 18th October. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599341/EPRS_BRI(2017)599341_EN.pdf [Accessed 28th April 2019]

Atanassov, N., Dumbrava, C., Mentzelopoulou, M., Radjenovic, A. (2018). "EU asylum, borders and external cooperation on migration - Recent developments" at *The European Parliamentary Research Service.* [Online] May. Available at: http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/621878/EPRS_IDA(2018)621878_EN.pdf [Accessed 28th April 2019]

Bacchi, C. & Goodwin, S. (2016). *Poststructural Policy Analysis - A Guide to Practice*. New York: Palgrave MacMillan

Bajekal, N. (2015). "The Big 5 Questions About Europe's Migrant Crisis," at Time. [Online] September. Available at: http://time.com/4026380/europe-migrant-crisis-questions-refugees/ [Accessed 10th May 2019]

Balibar, E. (1998). "The Borders of Europe", trans. J. Swenson, in P. Cheah and B. Robbins (eds), *Cosmopolitics: Thinking and Feeling Beyond the Nation* (London and Minneapolis: University of Minnesota Press, 1998), pp. 216– 33

BBC (2015). "Migrant Crisis: One Million Enter Europe in 2015," at BBC. [Online] December. Available at: https://www.bbc.com/news/world-europe-35158769 [Accessed 10th May 2019]

Bigo, D. (2001). "The Möbius Ribbon of internal and external security(ies)," in Albert, M, Jacobsen, D. and Lapid, Y.'s (ed.) *Identities, borders, orders: Rethinking international relations theory*, Minneapolis: University of Minnesota Press

Bigo, D. (2002). "Security and Immigration: Toward a Critique of the Governmentality of Unease" *Alternatives*, vol 27, pp. 63–92

Bigo, D. (2014). "The (in)securitization practices of the three universes of EU border control: Military/Navy - border guards/police - database analysts," *Security Dialogue*, vol 45(3), pp. 209-225

Boswell, C., Geddes, A. & Scholten, P. (2011). "The Role of Narratives in Migration Policy-Making: A Research Framework," *British Journal of Politics and International Relations*, vol 13, pp. 1-11

Bowyer, K. W. (2011). "The results of the NICE.II Iris biometrics competition," *Pattern Recognition Letters*, vol 33(8), pp. 965–969

Broeders, D. (2007). “The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants,” *International Sociology*, 22(1), pp.71–92

Bux, U. (2018). “Management of the External Borders,” at the European Parliaments Factsheets on the European Union. [Online] October. Available at: http://www.europarl.europa.eu/factsheets/en/sheet/153/management-of-the-external-borders (Accessed 10th May 2019]

Clarke, R. & Greenleaf, G. (2017). “Dataveillance Regulation: A Research Framework” at SSRN. [Online] 13rd March. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3073492 [Accessed 28th April 2019]

Ceyhan, A. (2012). “Surveillance as biopower,” in Ball, K., Haggerty, K. & Lyon, D.’s (ed) *Routledge Handbook of Surveillance Studies*, Florence: Routledge

Council of the European Union (2002). *Presidency Conclusions, Seville European Council, 21-22 June*, Brussels

Dyer, R. (1997). *White*, London: Routledge

Elden, S. (2005). “Territorial Integrity and the War on Terror,” *Environment and Planning A: Economy and Space,* vol. 37(12), pp. 2083-2104

Epstein, C. (2007). “Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders,” *International Political Sociology*, vol. 1, pp. 149-164

European Commission (EC) (2014). “Technical Study of Smart Borders - final report”. Brussels: European Commission

European Commission (EC) (2015a). *COM/2015/0240 final*, Brussels

European Commission (EC) (2015b). *COM/2015/0185 final*, Strasbourg

European Commission (EC) (2016a). *COM/2016/0272 final - 2016/0132 (COD)*, Brussels

European Commission (EC) (2016b). *COM/2016/0882 final - 2016/0408 (COD)*, Brussels

European Commission (EC) (2016c). *COM/2016/0205 final*, Brussels

European Commission (EC) (2016d). “Security Union: Commission proposes to reinforce the Schengen Information System to better fight terrorism and cross-border crime” at The European Commission Press Release. [Online] 21st December. Available at*:* http://europa.eu/rapid/press-release_IP-16-4402_en.htm [Accessed 28th April 2019]

European Commission (EC) (2017). “The EU and the migration crisis” at the European Commission. [Online] July. Available at: http://publications.europa.eu/webpub/com/factsheets/migration-crisis/en/ [Accessed 10th May 2019]

European Commission (EC) (2018a). *COM/2018/302 final,* Brussels

European Commission (EC) (2018b). “A stronger, more efficient and secure EU visa policy - an upgraded Visa Information System” at The European Commission, Migration and Home Affairs. [Online] 27th March. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180516_visa-information-system_en.pdf [Accessed 28th April 2019]

European Commission (EC) (2019a). “Schengen Information System” at The European Commission, Migration and Home Affairs. [Online] 27th March. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en [Accessed 28th April 2019]

European Commission (EC) (2019b). “Identifications of Applicants (EURODAC),” at The European Commission, Migration and Home Affairs. [Online] 27th March. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en [Accessed 28th April 2019]

European Commission’s Joint Research Centre (JRC) (2013). *Fingerprint Recognition for Children - final report*. Luxembourg: Publications Office of the European Union

European Commission’s Joint Research Centre (JRC) (2017). “2017 - Annual Activity Report,” at the European Commission. [Online]. Available at: https://ec.europa.eu/info/sites/info/files/file_import/jrc_aar_2017_final.pdf [Accessed 14th May 2019]

European Council on Refugees and Exile (ECRE) (2016). *ECRE Comments on the Commission Proposal to recast the Eurodac Regulation - COM(2016) 272*. Brussels.

European Data Protection Supervisor (EDPS) (2016). *Opinion 07/2016: EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*. Brussels

European Data Protection Supervisor (EDPS) (2017). “Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice,” at the EDPS. [Online] 17th November. Available at: https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf [Accessed 27th May 2019]

European Data Protection Supervisor (EDPS) (2019). “Necessity and Proportionality,” at the EDPS. [Online]. Available at: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en [Accessed 27th May 2019]

European Parliament (EP) (2017a). “The EU Response to the migrant crisis,” at the European Parliament. [Online] June. Available at: http://www.europarl.europa.eu/news/en/headlines/society/20170629STO78629/the-eu-response-to-the-migrant-crisis [Accessed 10th May 2019]

European Parliament (EP) (2017b). “Interoperability between EU Information Systems for Border and Security,” at Legislative Train Schedule. [Online] 20th December. Available at: http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-interoperability-between-eu-information-systems-for-borders-and-security [Accessed 24th May 2019]

European Parliament (EP) (2018). “Security: improving the Schengen Information System” at The European Parliament. [Online] 17th October. Available at: http://www.europarl.europa.eu/news/en/headlines/security/20181011STO15882/security-improving-the-schengen-information-system [Accessed 28th April 2019]

European Parliament and the Council (2006). *OJ L 381, 28.12.2006, p. 4–23,* Brussels

European Parliament and the Council (2012*). OJ L 315, 14.11.2012, p. 57–73*, Strasbourg

European Parliament and the Council (2013). *OJ L 180, 29.6.2013, p. 1–30,* Brussels

European Parliament and the Council (2016). *OJ L 119, 4.5.2016, p. 1–88,* Brussels

European Union (1990). "*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 ("Schengen Implementation Agreement"),*" at Refworld. [Online] 19 June 1990. Available at: https://www.refworld.org/docid/3ae6b38a20.html [Accessed 16 May 2019]

European Union (2012). *Charter of Fundamental Rights of the European Union*

European Union Agency for Fundamental Rights (FRA) (2017). "Fundamental Rights and the interoperability of EU information systems: borders and security". Luxemburg: Publications Office of the European Union

European Union Agency for Fundamental Rights (FRA) (2018). "Under watchful eyes: biometrics, EU IT systems and fundamental rights." Luxemburg: Publications Office of the European Union

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (2018). "Technical reports on the functioning of VIS," at eu-LISA. [Online] May. Available at: https://www.eulisa.europa.eu/Publications/Reports/2018%20VIS%20reports%20-%20Factsheet.pdf [Accessed 25th May 2019]

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (2019a). "Large-Scale IT Systems," at eu-LISA. [Online]. Available at: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems [Accessed 22nd May 2019]

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) (2019b). "Eurodac - 2018 Statistics," at eu-LISA. [Online] February. Available at*:* https://www.eulisa.europa.eu/Publications/Reports/Eurodac%20-%202018%20statistics%20-%20report.pdf [Accessed 28th April 2019]

Fanon, F. (1986 [1952]). *Black Skin, White Masks*. Translated by Markmann, C.L. London: Pluto Press

Fawcett, B. (2008). "Poststructuralism," in Lisa Givens (ed.) *The sage encyclopedia of qualitative research methods*, Thousand Oaks, CA: SAGE Publications, Inc.

Ferreira, S. (2018). "From Narratives to Perceptions in the Securitisation of the Migratory Crisis in Europe," at E-International Relations. [Online] 3rd September. Available at: https://www.e-ir.info/2018/09/03/from-narratives-to-perceptions-in-the-securitisation-of-the-migratory-crisis-in-europe/ [Accessed 14th May 2019]

Foucault, M. (1978). *La Gouvernementalité,* in Dits et Ecrits II. Paris: Gallimard

Foucault, M. (1980). *Power/Knowledge*, edited by Gordon, C., trans. Gordon, C., Marshall, L., Mepham, J., and Soper, K. Padstow: Harvester Press

Foucault, M. (1985). *The Archaeology of Knowledge*. London: Tavistock Publications

Foucault, M. (1990). *The History of Sexuality,* vol. 1. London: Penguin

Fox, C. (2018). "Face recognition police tools 'staggeringly inaccurate'" at BBC. [Online] 15th May. Available at: https://www.bbc.com/news/technology-44089161 [Accessed 28th April 2019]

Frankenberg, R. (1993). *White women, race matters, the social construction of whiteness*, London: Routledge

Frontex (2015) "Publications - FRAN Q1 2015," at Frontex. [Online] 9th July. Available at: https://frontex.europa.eu/publications/fran-q1-2015-Flg6BH [Accessed 25th May 2019]

Guild, E. (2003) "International Terrorism and EU Immigration, Asylum and Borders Policy: The Unexpected Victims of 11 September 2001," *European Foreign Affairs Review*, vol 8, pp. 331–46

Hammarberg, T. (2008) "Protecting the right to privacy in the fight against terrorism" at the *Council of Europe - Commissioner for Human Rights.* [Online] December. Available at: https://rm.coe.int/ref/CommDH/IssuePaper(2008) [Accessed 8th May 2019]

Haraway, D. (1991). *Simians, Cyborgs and Women*. New York: Routledge

Hayes, B. (2008). "Surveillance Society," at redpepper. [Online] 16th January. Available at: https://www.redpepper.org.uk/Surveillance-Society/ [Accessed 22nd May 2019]

Hayes, B. (2009) "NeoConOpticon - the EU Security-Industrial Complex," at Statewatch, in cooperation with Transnational Institute. [Online]. Available at: https://www.statewatch.org/analyses/neoconopticon-report.pdf [Accessed 22nd May 2019]

Hayes, B. (2017). "Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data"," *International Review of the Red Cross*, vol 99(1), pp. 179–209.

Hildebrandt, M. (2007). "Profiling into the future: An assessment of profiling technologies in the context of Ambient Intelligence" at FIDIS Journal, Issue 1. [Online]. Available at: http://journal.fidis.net/fileadmin/journal/issues/1-2007/Profiling_into_the_future.pdf [Accessed 28th April 2019]

Hildebrandt, M. (2009). "Who is Profiling Who? Invisible Visibility," in Reinventing Data Protection? (eds.) Gutwirth, Poullet, De Hert, De Terwaugne, Nouwt, and Dordrecht (2009). Springer

Huysmans, J. (2006). *The Politics of Insecurity, Fear, Migration and Asylum in the EU*, Florence: Taylor and Francis

International Organisation for Migration (IOM) (2015). "Irregular Migrant, Refugee Arrivals in Europe Top One Million in 2015," at IOM. [Online] December. Available at: https://www.iom.int/news/irregular-migrant-refugee-arrivals-europe-top-one-million-2015-iom [Accessed 10th May 2019]

Jacobsen, K. L. (2012). *Biometrics as Security Technology. Expansion amidst Fallibility,* Copenhagen: Danish Institute for International Studies

Jacobsen, K. L. (2015). *The politics of humanitarian technology, good intentions, unintended consequences and insecurity*, London New York: Routledge.

Jones, J.P.P. (2013). "Poststructuralism," In *The Wiley-Blackwell Companion to Cultural Geography*. John Wiley and Sons, pp. 23–28

Khaw, P. (2002). "Iris Recognition Technology for Improved Authentication", *SANS Security Essentials (GSEC) Practical Assignment*, Version 1.3

Lemberg-Pedersen, M. (2013). "Private Security Companies and the EU Borderscapes" in Nyberg Sørensen and Gammeltoft-Hansen (eds) The Migration Industry, pp.152-172

Lemberg-Pedersen, M. (2018). "Security, industry and migration in European border control" in Agnieszka Weinar's et al. (ed.) *The Routledge handbook of the politics of migration in Europe*, London: Routledge

Lyon, D. (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London: Routledge

Lyon, D. (2003). *Surveillance after September 2001*. London: Polity

Lyon, D. (2006). *Theorizing Surveillance: The Panopticon and Beyond.* Cullompton: Willan Publishing

Magnet, S. (2011). *When Biometrics Fail - Gender, Race and the Technology of Identity*. Durham and London: Duke University Press

Maguire, M. (2012). "Biopower, racialization and new security technology," *Social Identities*, 18(5), pp.593–607

Mane, V. & Jadhav, D.V. (2009). "Review of Multimodal Biometrics: Applications, Challenges and Research Areas", *International Journal of Biometrics and Bioinformatics*, vol. 3(5), pp. 66–95

Mayhew, S. (2019). "Glossary of Biometric Terms and Technique Classifications" at Biometric Update. [Online] 13rd March. Available at: https://www.biometricupdate.com/201205/biometric-terms-and-technique-classifications [Accessed 28th April 2019]

Meijers Committee (2016). "CM1610 - Note on the proposed reforms of the Dublin Regulation (COM (2016) 197), the Eurodac recast proposal (COM (2016) 272 final), and the proposal for an EU Asylum Agency (COM(2016)271 final)," at Commissie Meijers. [Online] June. Available at: https://www.commissie-meijers.nl/en/comments?year%5Bvalue%5D%5Byear%5D=2016&page=1 [Accessed 15th May 2019]

Meijers Committee (2018). "CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM (2017) 794," at Commissie Meijers. [Online] 19th February. Available at: https://www.commissie-meijers.nl/sites/all/files/cm1802_comments_on_com_2017_794.pdf [Accessed 27th May 2019]

Metropolitan Police (2019). "Live Facial Recognition trial" at Metropolitan Police. [Online] 24th April. Available at*:* https://www.met.police.uk/live-facial-recognition-trial/ [Accessed 16th May 2019]

Mezzadra, S. (2011). "The gaze of Autonomy - Capitalism, migration and social struggles," in Squire, V. (ed.) *The Contested Politics of Mobility: Borderzones and Irregularity.* Abingdon: Routledge.

Monroy, M. (2018). "New EU system for fingerprint identification activated," at digit. [Online] April. Available at: https://digit.site36.net/2018/04/25/new-eu-system-for-fingerprint-identification-activated/ [Accessed 19th May 2019]

Morrison, T. (1992). *Playing in the dark, whiteness and the literary imagination*, Cambridge, Mass. London: Harvard University Press

Müller, B. (2010). *Security, risk and the biometric state, governing borders and bodies*, London: Routledge.

Nadel, L. D. (2007). "*Approaches to Face Image Capture at US-VISIT Ports of Entry,*" NIST Biometric Quality Workshop

Nanavati, S., Thieme, M., Nanavati., R. (2002). *Biometrics: Identity Verification in a Networked World*. New York: John Wiley and Sons

Nielsen, N. (2015). "Frontex double counts migrants entering the EU," at euobserver. [Online] 13th October. Available at: https://euobserver.com/migration/130661 [Accessed 25th May 2019]

Oxfam International (2019). "Refugee and migration crisis," at Oxfam International. [Online]. Available at: https://www.oxfam.org/en/emergencies/refugee-and-migrant-crisis [Accessed 10th May 2019]

Pato, J. & Millett, L. (2010). *Biometric Recognition: Challenges and Opportunities*, Whither Biometrics Committee; National Research Council, Washington D.C: The National Academies Press

Parker, N. & Vaughan-Williams, N. (2012). *Critical Border Studies: Broadening and Deepening the 'Lines in the Sand' Agenda*, Oxon: Routledge

Papadopoulos, D; Stephenson, N & Tsianos, V. (2008). *Escape Routes - Control and Subversion in the Twenty-first Century*. London: Pluto Press

Pugliese, J. (2010). *Biometrics - Bodies, Technologies, Biopolitics*, New York: Routledge

Rose, N. (1999). *Powers of freedom. Reframing political thought.* Cambridge University Press, Cambridge

Rumford, C. (2012). "Towards a Multiperspectival Study of Borders," *Geopolitics*, 17(4), pp.887–902

Schmid-Drüner, M. (2019). “Immigration Policy,” at The European Parliaments Fact Sheets on the European Union. [Online] October. Available at*:* http://www.europarl.europa.eu/factsheets/en/sheet/152/immigration-policy [Accessed 10th May 2019]

Scott, J. (1998). *Seeing like a state. How certain schemes to improve the human condition have failed*. New Haven and London: Yale University Press

Shore, C., & Wright, S. (2003). *Policy: A new field of Anthropology.* In C. Shore, & S. Wright (Eds.), Anthropology of policy: Perspectives on governance and power. New York: Routledge

Statewatch (2018). “Visa Information System: Commission proposals sneak in mandatory biometrics for long-stay visas,” at Statewatch. [Online] 20th August. Available at: https://www.statewatch.org/news/2018/aug/vis-fingerprints-long-stay-visas.htm [Accessed 27th May 2019]

Steinmayr, A. (2017) “Did the Refugee Crisis Contribute to the Recent Rise of Far-Right Parties in Europe?,” at IFO Institute. [Online] 4th December. Available at: https://www.ifo.de/DocDL/dice-report-2017-4-steinmayr-december.pdf [Accessed 28th May 2019]

Stenum, H. (2012). “Making Migrants Governable - Counting and defining the ‘illegal migrant’.” *Nordic Journal of Migration Research*, vol. 2(4) pp. 280-288

Stenum, H. (2017). “The Body-Border - Governing Irregular Migration through Biometric Technology.” *Spheres Journal*, 4, pp.1-16

Storey, D. (2017). “States, territory and sovereignty.” *Geography*, vol 102(3), pp. 116-121

Tistarelli, M. & Nixon, M. S. (2009). “*Advances in Biometrics,*” Lecture Notes in Computer Science 5558

Tsianos, V. S. & Kuster, B. (2016). “Eurodac in Times of Bigness: The Power of Big Data within the Emerging European IT Agency.” *Journal of Borderlands Studies*, 31(2), pp. 235-249

Sly, L. (2015) “8 Reasons Europe’s refugee crisis is happening now,” at Washington Post. [Online] September. Available at*:* https://www.washingtonpost.com/news/worldviews/wp/2015/09/18/8-reasons-why-europes-refugee-crisis-is-happening-now/?utm_term=.5b755b2b294d [Accessed 10th May 2019]

Spindler, W. (2015). “2015: The year of Europes Refugee Crisis,” at United Nations High Commissioner for Refugees. [Online] December. Available at: https://www.unhcr.org/news/stories/2015/12/56ec1ebde/2015-year-europes-refugee-crisis.html [Accessed 10th May 2019]

United Nations General Assembly (1989). “Convention on the Rights of the Child,” available af refworld. [Online] 20 November. Available at*:* https://www.refworld.org/docid/3ae6b38f0.html [Accessed 14 May 2019]

United Nations High Commissioner for Refugees (UNHCR) et. al (2018). “JOINT STATEMENT: Coercion of children to obtain fingerprints and facial images is never acceptable,” at International Organisation for Migration. [Online] 2nd March. Available at:

https://eea.iom.int/news/joint-statement-coercion-children-obtain-fingerprints-and-facial-images-never-acceptable [Accessed 14th May 2019]

Van der Ploeg, I. (1999). “The illegal body: ‘Eurodac’ and the politics of biometric identification”, *Ethics and Information Technology*, vol 1(4), pp. 295– 302

Van der Ploeg, I. (2005). “Biometric identification technologies: ethical implications of the informatization of the body”, *Biometric Technology and Ethics* – BITE Policy Paper no. 1

Vaughan-Williams, N. (2012). *Border Politics - The Limits of Sovereign Power,* Edinburgh University Press: Edinburgh

Walters, W. (2015). “Reflections on migration and governmentality”, *Movements. Journal für Kritische Migrations- und Grenzregimeforschung*, vol 1(1), pp. 1–25

Wilson, T. H., and Hastings, D. (1998). *Border Identities: Nation and State at International Frontiers*, Cambridge: Cambridge University Press

Wisman, T. (2013). “Purpose and function creep by design: Transforming the face of surveillance through the internet of things.” *European Journal of Law and Technology*, 4(2)

Whitley, E. A. & Hosein, G. (2010). “Global identity policies and technology: do we understand the question?”, *Global Policy*, vol. 1(2), pp. 209–215