Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany

Helene Hahn

About this work

This publication is based on the Master's thesis ”Digital identification systems and the right to privacy in the asylum context. An analysis of implementations in Germany”, submitted in 2020 as part of Leuphana University's International Professional Master's Programme ”Governance and Human Rights“.

About the author

Helene Hahn is a researcher, writer and strategist based in Berlin, working internationally. Her work explores the spaces where human rights, governance and technology systems collide. She can be reached at <https://helenehahn.de/>.

Acknowledgements

This research and analysis would not have been possible in the same extent without the contribution of the interviewed experts. Special thanks to Bellinda Bartolucci (PRO ASYL), Lea Beckmann (GFF) and Anna Biselli for providing valuable input for this paper. Additional thanks to the Office of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) for the written statements on the subject.

Licence

Abstract

Establishing the identity of asylum seekers in the absence of credible documents represents a significant challenge for governments. To support decision-making processes in identity determination and verification procedures, Germany's Federal Office for Migration and Refugees introduced three digital identification systems under the "Integrated Identity Management - plausibility, data quality and security aspects (IDM-S)" programme. Because these algorithmic systems are deployed in highly political settings affecting vulnerable populations on the move, this research investigates how the Federal Office legitimises the policy and use of IDM-S that indicate a new direction of governance driven by so-called "innovative technologies". In this context, legitimacy - considered a core virtue of just, democratic institutions - is understood as a justificatory concept seen in conjunction with (good) governance and the right to privacy as guaranteed under Article 17 of the International Covenant on Civil and Political Rights. The data justice framework is applied to structure the evaluation of state practices. In addition, the qualitative content analysis is used to find patterns in publicly available documents. Expert interviews were carried out to include experiences of affected individuals and to verify identified information provided by the government. The analysis revealed that efforts to legitimise IDM-S included four patterns: referring to the rule of law and national security concerns, non-disclosing delegitimising information and limiting accountability, emphasising performance efficiency and the systems' high level of innovation, implying objective operations by means of a mathematical-technical approach. The results underscore profound discrepancies between justifications and state practices, outlining severe privacy violations as well as the lack of compliance to qualitative values in governance that pertain to participation, transparency, accountability, impartiality and scientific soundness of state operations.

Table of contents

List of illustrations

List of tables

List of abbreviations

AI	Artificial Intelligence
AmD	Analysis of mobile data devices (Auslesen von mobilen Datenträgern)
AnkER	Arrival, Decision and Municipal Distribution or Return (Ankunft, Entscheidung und kommunale Verteilung bzw. Rückführung)
AZR	Central Register of Foreigners (Ausländerzentralregister)
BAMF	Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge)
BfDI	Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)
BMF	Commissioner for Refugee Management (Beauftragter für Flüchtlingsmanagement)
BMI	Federal Ministry of the Interior, Building and Community (Bundesministerium des Innern, für Bau und Heimat)
CDU	Christian Democratic Union (Christlich Demokratische Union)
CSU	Christian Social Union (Christlich-Soziale Union)
DIAS	Automatic dialect recognition (Dialektbestimmungs-Assistent)
EURODAC	European Dactylographic comparison system
GDPR	General Data Protection Regulation
GGO	Joint Rules of Procedure of the Federal Ministries (Gemeinsame Geschäftsordnung der Bundesministerien)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology

IDM	Integrated Identity Management (Integriertes Identitätsmanagement)
IDM-S	Integrated Identity Management - plausibility, data quality and security aspects (Integriertes Identitätsmanagement - Plausibilisierung, Datenqualität und Sicherheitsaspekte)
INPOL	Police Information System (Informationssystem der Polizei)
MARiS	Central work-flow and documentation management system in asylum and Dublin procedures (Migrations-Asyl-Reintegrationssystem)
OECD	Organisation for Economic Co-operation and Development
PG DAS	Project group on the digitalisation of asylum procedures (Projektgruppe Digitalisierung des Asylverfahrens)
PTU	Physical-technical examination of identity documents (physikalisch-technische Untersuchung)
SPD	Social Democratic Party (Sozialdemokratische Partei Deutschlands)
S-T-A	Speech and text analysis by language experts (Sprach- und Textanalyse)
TraLitA	Name transliteration and analysis (Transliterationsassistent)
UNHRC	United Nations Human Rights Committee

1 Introduction

1.1 Topic and research question

The Federal Office for Migration and Refugees (BAMF) is the main government body responsible for the implementation and management of asylum procedures in Germany. Decisions on asylum claims are substantiated in identity determination and personal hearing procedures where the nationality of a person is verified and the individual history of persecution is established. However, the verification of information can prove to be problematic in cases where applicants lack identity documents. To cope with these challenges, the so-called "Integrated Identity Management - plausibility, data quality and security aspects (IDM-S)" programme paved the way for the use of new digital identification systems at the Federal Office. The following new components were implemented: the name transliteration and analysis developed to achieve standardisation in the transliteration of Arabic names, the automatic dialect recognition intended to recognise the applicants' spoken language and dialect, and the analysis of mobile data devices intended to determine asylum seekers' identity and origin (BAMF, 2017a). These digital systems assist in decisions pertaining to asylum claims through the analysis of personal information provided by asylum applicants. Developed in 2017 and still in use today, they indicate a new direction of governance in the context of asylum.

Because these algorithmic systems are set up in highly political and sensitive settings affecting vulnerable populations on the move, it becomes increasingly important to question the legitimacy of this governance mode that is often characterised by the desire for greater efficiency through the use of Information and Communications Technologies (ICTs). As more and more governments resort to digital means in the management of migration and asylum, this paper seeks to contribute to understanding these new data-intensive governance directions and their implications by investigating one specific, recent example. The policy and implementation of the Federal

Office's digital identification systems represent the subject of this thesis, explored in the greater context of democratic legitimacy, governance and the right to privacy. This paper addresses the following research question:

How does the Federal Office legitimise the policy and use of the digital identification system "IDM-S" as part of a new direction of governance in the context of asylum?

To not only identify but to make sense of the main patterns directed at legitimising decisions in regard to IDM-S de jure and de facto, this research investigates contradictions between the ministry's obligations, its aspirations and political reality. It focuses mainly on identity determination procedures where the three aforementioned IDM-S systems are utilised. It neither engages with Germany's entire asylum governance system nor with all legislative frameworks that underpin the asylum process. Only the most essential legal references are made, however, the main focus remains on the right to privacy as guaranteed under Article 17 of the International Covenant on Civil and Political Rights (ICCPR). This research does not adopt a child perspective and disregards the particular rights of (unaccompanied) minors.

The introduction outlines the socio-political and academic relevance of this research topic. Section two presents the key theoretical framework of political legitimacy that informs the analysis. As legitimacy relates to the exercise of power and legality, the notions of governance and the right to privacy are discussed. These discussions also include critical reflections of common fallacies related to the implementation of ICTs in public administrations. Section three describes the interpretative research design, the analysis methods, including the data justice framework as well as the qualitative content analysis, and the available data sources. The subsequent analysis proceeds in three parts. The first presents the studied case and situates it in its political environment. The second and third sections critically assess the legal background as well as the implementation and effects of IDM-S as part of the Federal Office's governance. In section five, the empirical findings and emerging legitimisation patterns are summarised and discussed based on the presented theoretical concepts. The final section engages with the study's core implications and suggests directions for further research.

Ultimately, this thesis encourages searching for better alternatives to the currently applied tech-heavy programme - alternatives that are firmly grounded in democratic governance principles and that adequately account for asylum seekers' right to privacy as well as their vulnerable status.

1.2 Social, political and academic relevance

The way how European states respond to the humanitarian costs of civil wars and conflicts forcing people to flee their homes shows the Union's struggle to live up to its proclaimed self-image (Guterres, 2014; Pai, 2020). Europe's restraint in response to the suffering of millions is not least expressed by the controversial debate about the proposal of the president of the European Commission Ursula von der Leyen. It echoed far-right language in relation to migration as the portfolio suggested "Protecting our European way of life" (von der Leyen, 2019) as the title for the new migration commissioner. Such harmful rhetoric not only stoke fear and xenophobia against vulnerable populations. They are also used as justifications for increasingly hardline responses of states in migration management and the implementation of ever stricter asylum procedures at European borders that are accompanied by digital identification systems which rely on automatic decision-making technologies (Sánchez-Monedero and Dencik, 2019). Germany is no exception. The Federal Government supports stricter rules in the Union, as the EU-Turkey deal indicates, and adopts a harsher response in its own jurisdiction, as evidenced not least through the introduction of the so-called “AnkER-Zentren” - admission centres for asylum seekers largely criticised due to their health and safety risks as well as their isolation effects on individuals (Eralp, 2016; PRO ASYL, 2018; Mouzourakis, Pollet and Ott, 2019).

These rejecting modes of governance are now aided by digital means. The experimentation with emerging technologies, contested digital identification methods and other algorithmic systems, particularly in the area of migration and asylum, lead to increasing governmental power over vulnerable individuals, threatening personal entitlements, human rights and civil liberties (Molnar, 2018a; Molnar, 2018b). The effects of technological systems on the lives of refugees and asylum seekers are extensive as studies in the EU show: On the one hand, they indicate unfair social impact through bias of practitioners entrenching unjust policies and shifting control of governance toward unaccountable private actors who develop digital platforms (Latonero, Hiatt, Napolitano, Clericetti and Penagos, 2019; Schoemaker, Currion and Pon, 2018; Reidy, 2017). On the other hand, when they have to engage with digital systems, refugees and asylum seekers loose agency and control over their personal and sensitive information (Kaurin, 2019; Kift, 2016). In this context, it is imperative to question and critically engage with these new digital developments in governance arrangements that manage migration and asylum.

For governments, a critical approach is important as they have the primary obligation and responsibility to respect, protect and fulfil human rights. A decision to implement digital identification systems in one country can set a new standard for other countries to follow as “technology travels” (Molnar and Gill, 2018: 62). Thus, governments may be responsible for human rights violations not only in their own jurisdiction but also for those that stem from the export of such systems to other states. Additionally, the disproportionate focus of decision-makers on technological trends in the pursuit to finding solutions to complex governance problems may lead to losing sights of policy alternatives beyond the digital realm that may be better suited in addressing existing challenges in the field of migration and asylum. Hence, a critical and thoughtful approach to developing and deploying digital systems is an essential condition for just, democratic state practices and, therefore, relevant to decision-makers and policy experts.

The debate on how to best manage migration and asylum claims will likely dominate the social, political and academic discourse in the international and domestic arena for years to come due to the increasing displacement of individuals in "a world at war" (Guterres, 2015). As digital systems will continue to play a role, researching and comparing cases will be crucial for policy reforms. To date, only marginal information is available about the Federal Office's development and implementation of IDM-S. This case of IDM-S at the BAMF became known publicly primarily through journalistic work (Biselli, 2017a; Schuler and Schwarze, 2017) and legal criticism (German Bundestag, 2017a; Gazeas, as cited in Podolski, 2017; Tabbara, 2019; Biselli and Beckmann, 2020). Apart from another identified study which focused on the legitimacy of the automatic dialect recognition (Keiner, 2020), there seems to be a lack of comprehensive, empirical evaluations of the said programme from a human rights-based perspective that takes into account procedural legitimacy aspects in governance. This research sets out to further address this gap and push for broader discussions among academic scholars and practitioners alike.

2 Theoretical approach

2.1 The concept of political legitimacy

To understand how democratic governance processes pertaining to policies are justified, they have to be considered in terms of political legitimacy, their qualitative and procedural features. Constitutions, nations, laws and processes are only few of the examined objects of political legitimacy in the field of social and political sciences (Gilley, 2006: 501). It is a multi-layered, normative concept that presupposes authority and power (Bekkers and Edwards, 2007: 37). Legitimacy refers to moral judgements about the exercise of power on the grounds of a legitimate authority (Ibid.: 40).

A legitimate authority is one that is recognised as valid by those who are being governed, for example, through democratic elections. If this applies, then decisions made by that authority are perceived as binding (Easton, as cited in Bekkers and Edwards, 2007: 37). Power can be broadly understood as the capacity of the state to enforce policies and regulate behaviour: It is "the ability to influence or control the actions of others" (Wrong, as cited in Beetham, 1991: 43). Power is not just relational (e.g. between individuals) but also depends on certain preconditions, such as material resources, personal capacities and the ability to act free from obstruction by others (Beetham, 1991: 43). While power is exercised at the expense of freedom, the restrictions thereof can be greater or less according to the seriousness of the deprivation inflicted upon people. In general, differences of power between individuals or groups are to a large extent results of social arrangements (Ibid.). In these settings, power is subject to rules that determine who has access to, for example, resources and authority positions and who is excluded from them. Because powerful actors have the ability to define the goals of the collective society and the means of realising their own interests under their control, the intentions of exercising power in a certain way need to be interrogated (Ibid.: 46-47). The exercise of power in governance arrangements refers to political decisions.

Decisions laid down in policies are legitimate, if they are recognised as lawful, just and rightful (Morris, 2008). These three conditions form the features of political legitimacy.

First, legitimacy relates to legality and the rule of law. Political decisions are legitimate, if they are in accordance with established rules, procedures and norms that address the issue in question (Beetham, 1991: 16). However, something that is legal is not per se just. Therefore, the second feature of legitimacy refers to the justifiability of the rules by reference to beliefs between those who govern and those who are governed (Ibid.: 17). Justifications in democratic societies can be based on the demonstration that power is derived from a valid source of authority, that authorities have the kind of qualities or abilities that are appropriate to the exercise of power, and that the exercise of power satisfies common interests, benefits and needs (Ibid.). Of course, no society has entirely uniform beliefs and sufficient justifications will be more open to disputes. In this regard, Beetham (Ibid.) states that "clear limits are set by logic and the beliefs of a given society to what justifications are plausible or credible within it". The shared belief system of people - how a society should be governed, and what rights, duties and liabilities are associated with it - can be seen not least in constitutions that form the codified belief system and guide recognised democratic procedures (Bekkers and Edwards, 2007: 38). Lastly, legitimacy needs to be confirmed through the expression of freely given consent (Beetham, 1991: 18). Actions that provide evidence for consent make contributions to legitimacy in two ways. First, they are binding to those who have taken part in them regardless of self-interests and other motives involved. They introduce a moral component and a commitment to the relationship. Second, expressive actions have a "publicly symbolic or declaratory force" (Ibid.). Authorities are enabled to use the confirmation of legitimacy and demonstrate it to third parties not part of the relationship. In general, consent should be linked to an individual, free choice between alternatives (Ibid.: 19). Non-cooperation, passive resistance, open disobedience and other actions of refusal of consent are measures that erode legitimacy - and the more people engage in such public refusal or withdrawal of consent, the greater the erosion of legitimacy will be (Ibid.).

Legitimacy improves the effectiveness of public administrations because with consent institutions are better able to achieve their purpose in governance (Ibid.: 33). However, it is not an "all-or-nothing affair" (Ibid.: 20) but what matters in modern state practices are judgements of degrees of legitimacy, the deviations between ideal and reality. The following table summarises the three features of legitimacy discussed so far.

	Features of legitimacy	*Non-legitimacy*
1	Conformity to rules (legal validity)	Illegitimacy (breaches of rules)
2	Justifiability of rules in terms of shared beliefs	Legitimacy deficit (discrepancy between rules and beliefs, absence of shared beliefs)
3	Expressed consent	Delegitimation (withdrawal of consent)

Table 1: The features of legitimacy
(Source: Following Beetham, 1991: 20)

Furthermore, binding decisions can be perceived as legitimate, if the proper processes have been followed in order to arrive at decisions (Bekkers and Edwards, 2007: 38). The so-called "procedural legitimacy" ("Legitimität durch Verfahren") (Luhmann, 1983: 28) takes into account the conditions and qualities of democratic procedures. Procedural legitimacy can be broken down into the stages of input, throughput and output legitimacy.

Scharpf (2003: chapter 1) outlines that legitimacy rests upon institutional arrangements that are thought to ensure responsive governing processes. Input legitimacy refers to the idea of "government by the people" (Ibid.). At its core lie opportunities for participation (Bekkers and Edwards, 2007: 43). Input legitimacy can be enhanced by guaranteeing that people have various opportunities to express their interests in regard to the issue at stake, including engagement in public debates of the policies proposed. It is important to ensure that the voices and preferences of those most affected are represented at least by intermediaries, interest groups and other experts in decision-making. Overall, the agenda-setting process for demands and concerns should be open and enable relevant institutions involved in decision-making to be responsive to the expressed issues (Ibid.: 44).

Throughput legitimacy can be defined as an umbrella concept for evaluating the quality of procedures (Schmidt and Wood, 2019). According to Schmidt (as cited in Ibid.: 729-730), throughput legitimacy consists of the various ways in which "the policy-making processes work both institutionally and constructively to ensure (…) the accountability of those engaged in making the decisions, the transparency of the information and the inclusiveness and openness to 'civil society'". It focuses on how collective decision-making is realised and, more specifically, how open the dialogues over policy decisions are. The greater the variety of interests incorporated in the procedure, the more they contribute to improving the collective learning process (Bekkers and Edwards, 2007: 45). Requirements that underpin throughput legitimacy, among others, place expectations about the qualities that policy-makers should have, such as "trust-worthiness, integrity, fairness, impartiality and credibility" (Schmidt and Wood, 2019: 730). Trust is at the centre of throughput legitimacy as it is an important component to the relationship between those making decisions and those affected by them (Levi, 2020). It pertains to the belief that decision-makers act without bias while meeting "expected ethical and moral standards as well as legal ones" (Levi, as cited in Schmidt and Wood, 2019: 730).

Lastly, output legitimacy focuses on the notion of "government for the people" (Scharpf, 2003: chapter 1). The underlying qualities refer to the overall performance of governance bodies: to effectiveness and (cost-) efficiency, as well as the responsiveness to the interests of people. In this sense, output legitimacy is concerned with the capacity of governing institutions to produce certain outputs and outcomes in order to remedy collective problems (Bekkers and Edwards, 2007: 45). The focus rests upon the intended and unintended effects of policy measures that have been realised, whereas in comparison throughput legitimacy focuses on the process itself. Rothstein (2008: 15) argues that political legitimacy is more dependent on the output side of the political system than on the input side as it has more to do with "the *exercise* of government power" than with just the access to it by participation in elections or the introduction of laws. In other words, if what the state does result in life-threatening actions, then this magnifies the erosion of legitimacy (Ibid.). Authoritative decisions require accountability for the results produced by those actors who made the decision. Accountability refers to an organised process between an actor and a forum about the actor's performance in decision-making (Meijer and Bovens, 2003: chapter 3). This account-giving consists of three elements. First, the actor feels obliged to inform the forum about the conduct by providing relevant information pertaining to the decision and its effects. Second, in a debating phase the forum questions the adequacy of the information provided or the legitimacy of the conduct. Third, the forum passes judgement on the conduct of the actor. It may approve or denounce a policy, or publicly condemn the behaviour. This represents some sort of sanctions that can be formal or informal, ranging from fines to negative publicity (Ibid.). Input, throughput and output legitimacy can be summarised as follows.

	Procedural legitimacy	*Qualities*
1	Input legitimacy	Participation and engagement (directly or through intermediaries), open and responsive agenda-setting process
2	Throughput legitimacy	Accountability, transparency, inclusiveness and openness towards civil society actors and minority groups, continuous dialogue and deliberation, trust, impartiality
3	Output legitimacy	Performance goals, effectiveness and (cost-) efficiency of results, transparency, accountability

Table 2: Qualities of procedural legitimacy
(Source: Following Bekkers and Edwards, 2007: 43-46; Scharpf, 2003: chapter 1; Schmidt and Wood, 2019: 729-733)

So far, the concept of political legitimacy has been outlined, including the core features: compliance with legal rules, justifications by reference to the belief system and expression of freely given consent. Adherence to democratic procedures in regard to input, throughput and output legitimacy further justifies decisions made by powerful actors. These qualities help to assess the measures taken in governance arrangements. The concept of governance is discussed next as legitimacy in a modern state cannot be understood without it.

2.2 The concept of governance

With the rise of global markets and the growing complexity of the modern world, the governments' ability to solve persistent challenges from a centralised position was questioned (Bekkers, Dijkstra, Edwards and Fenger, 2007: 3). Ineffective interventions were seen as the consequence of insufficient knowledge about the nature of complex problems as well as the mismatch between policy goals and measures used to address them (Ibid.). The shift from government to governance reflected the idea that actors from the public, private and semi-public sphere needed to be engaged. Through co-production and learning a shared understanding of societal issues can be achieved and translated into collective actions used to produce better results (Ibid.). Governance can be defined as "the process of decision-making and the process by which decisions are implemented" (Kioe Sheng, 2009). Van Kersbergen and Van Waarden (2004: 143) identify three characteristics. First, governance refers to pluralistic rather than unicentric systems. Second, networks play an important role in organising relations between autonomous but interdependent actors (Ibid.: 151). Third, the emphasis in governance rests upon processes of governing and not on the structures in government. As opposed to traditional processes of coercion, command and control, governance processes concern negotiation, consultation, cooperation and alliance formation (Ibid.: 152). Governance approaches prescribe an ideal as well as an empirical reality which holds true, especially, in regard to "good governance" and "new public management" (Ibid.). Both modes of governance influence modern state practices and, therefore, will be described in turn.

2.2.1 Good governance and new public management

In the 1990s, good governance has been predominantly proclaimed in the field of economic development by the World Bank, OECD and international (aid) organisations by comparing best practices in public management, business-government relations and social policy (Van Kersbergen and Van Waarden, 2004: 145; World Bank, 1992; Agere, 1999; Pillay, 2016: 24). Over time, the concept shifted away from the focus on economic efficiency towards a stronger value-based approach in public administrations (Teorell and Rothstein, 2009; Keping, 2017: 4). Moreover, it connects public administration processes to frameworks of human rights and, in turn, underlines the state's obligations and duties towards the population under its jurisdiction. Good governance can be seen as "the process whereby public institutions conduct public affairs, manage public resources and guarantee the realization of human rights in a manner essentially free of abuse and corruption, and with due regard for the rule of law" (OHCHR, 2020).

There is a broad variety of good governance principles (Kioe Sheng, 2009; Graham, Amos and Plumptre, 2003: 3; Keping, 2017: 5; OHCHR, 2020; UN, 2007: 4; Pillay, 2016: 24). Following the main commonalities of the literature, five characteristics stand out. First, the rule of law forms the foundation of good governance practices. It requires a sound legal system and legal frameworks that are enforced fairly and impartially (Teorell and Rothstein, 2009). Furthermore, it requires respect and full protection of human rights, with special attention paid to the rights of minorities and vulnerable groups (Keping, 2017: 5; Graham, Amos and Plumptre, 2003: 3; Kioe Sheng, 2009). Second, the principle of accountability entails that all actors involved in governance, including governments, must be accountable to the public and to those who will be affected by policy decisions. Accountability refers to the exercise of functions and obligations that are related to positions of power. In this sense, accountability entails that authorities should respond to the demands of the population in a timely and responsible manner. This principles cannot be enforced without the rule of law and transparency (Ibid.). Third, transparency is based on the free flow of information that is relevant to the public and relates to processes, rules, budgets, institutions, decisions and their implementation. Enough information should be communicated actively, be freely available and directly accessible in understandable forms and media (Ibid.). Fourth, the principle of participation is key in good governance. Participation can be ensured either directly or indirectly through legitimate intermediaries or institutions that represent their interest. It needs to be informed and organised (Graham, Amos and Plumptre, 2003: 3; Kioe Sheng, 2009). Lastly, the principles of effectiveness and efficiency both relate to performance. In line with good governance, processes and institutions make the best use of available resources in order to produce results that meet the needs of different groups of society. Administrative structures and procedures should be designed scientifically and operate rationally (Keping, 2017: 6; Graham, Amos and Plumptre, 2003: 3; Kioe Sheng, 2009). These principles outline a concept that allows to discuss the role of public administrative bodies and other actors involved in governance arrangements. The following table provides a summary for the aforementioned principles.

	Good governance principle	*Qualities*
1	Rule of law	Legal framework enforced fairly and impartially, protection of human rights (attention paid to minority/vulnerable groups)
2	Accountability	Powerful actors are accountable to the public forum and those most affected, responsiveness in timely and responsible manner
3	Transparency	Free flow of information, access and availability in understandable forms and media, active communication
4	Participation	Direct or indirect (through representatives), informed and organised
5	Effectiveness and efficiency (performance)	Making best use of resources available with regard to results, scientifically designed procedures, rational operation

Table 3: Good governance principles
(Source: Following Keping, 2017: 5-6; Graham, Amos, Plumptre, 2003: 3; Kioe Sheng, 2009)

The second mode of governance refers to "new public management". Developed in the 1980s, new public management initially entailed two meanings, namely corporate management and marketisation (Rhodes, 2000: 7). On the one hand, corporate management has led to the introduction of private sector management methods to the public sphere, including methods that stress the importance of hands-on professional management, standards and measures of performance, managing by results, value for money, and consumer orientation (Ibid.). On the other hand, marketisation has implied the introduction of incentive market structures into public service provision and conditions that facilitate them (Ibid.: 7-8).

This logic includes greater competition through outsourcing, disaggregating bureaucracies, and privatisation (Ibid.: 8; Van Kersbergen and Van Waarden, 2004: 148). According to Rhodes (2000: 8), marketisation became more dominant after 1988. Osborne (1993: 350) places great emphasis on productivity and efficiency in public administration. In his view, the "entrepreneurial government" (Ibid.: 352) encompasses the solution to the ineffectiveness of old top-down bureaucracies. All these reforms that fall under the term of new public management place the market logic at the centre of public decision-making and policy implementations (Van Kersbergen and Van Waarden, 2004: 148).

Despite its far reaching acceptance in all spheres of governance today (Pillay, 2016: 23), the concept has been heavily criticised: "[New public management's] stress on privatization, performance management, out-sourcing and the introduction of market-incentives within state organizations has led to a rather dysfunctional degree of fragmentation and differentiation in the public sector organization" (Fenger and Bekkers, 2007: 27). In similar critical tone, other scholars argue that the disproportionate emphasis on efficiency and market forces views people as mere economic units rather than democratic participants in governance (Hankey and Tuszynski, 2017; Pillay, 2016: 23). Therefore, while efficiency is important, it cannot be regarded as a standalone value but needs to be connected to other quality indicators.

2.2.2 Governance, digital identification systems and common fallacies

Nowadays, governance is determined by the implementation of ICTs that are used to support the key functions of governments both within the organisation and in its relations with the outside world (Meijer and Bovens, 2003: chapter 2). E-government initiatives defined as the public sector's use of ICTs call for wholesale reforms with the promises of reducing costs, enhancing efficiency and improving service delivery (Suleiman, Tsakuwa, Abdullahi and El-Tahir, 2017; Magno and Serafica, 2001; Juiz, Guerrero and Lera, 2013). However, academic studies indicate tensions between popular enthusiasm for such technologies and growing concerns with their societal implications (Clarke, 2017; Clarke, Lindquist and Roy, 2017: 457; Metcalfe and Dencik, 2019). In the field of asylum, ICTs and algorithmic systems as their foundation are increasingly used for decision-making and support. According to Goffey (2008: 16), algorithms are instructions fed to a computer or machine in order to solve a particular problem: "Without the algorithm (…), there would be no computing." Rather than seeing algorithms as isolated technical objects, this research approaches them as socio-technical systems that are embedded in culture and can be studied from different perspectives, including legal, technological, social and cultural (Wieringa, 2020: 2). Because algorithms are "multiple" (Mol, 2002: 4-5), composed of a variety of human interactions, they need to be considered in a more holistic, interdisciplinary way (Seaver, 2017: 5). Hence, the term "system" is used intentionally to shift the focus from mere technical components towards their entanglements in processes of governance, including the political context and interactions among the actors involved.

Digital identification systems are specific types of algorithmic systems that rely on identity information. In turn, identity can be divided in two categories: personal and legal identity. Personal identity refers to unique individual, fluid characteristics produced and reproduced through communicative activities and interactions with the environment (Whitley, Gal and Kjaergaard, 2014: 19; Thomas, 2009: 5; Rahman, 2019). Whereas legal identity is based on the official recognition by the state granting individuals access to entitlements and rights, for example, through birth registration and other forms of civil identification that recognises the individual as a subject of law and protection of the state (Whitley, Gal and Kjaergaard, 2014: 25; Molina, Carlos and Harbitz, 2010: 64). Identification implies "a process (...) to describe a proof, a system, or a transaction involving a subject and an evaluator, centered around verifying a claim that a person is one person and not any other" (Donner, 2018). Identification processes rely on various mechanisms ranging from paper-based documents, such as passports, to electronic systems, such as database matchings and biometrics. Biometrics refer to automated methods of identifying persons based on their unique physiological or biological characteristics (Farraj, 2011: 893; Ng, 2006: 428). The most common procedures involve facial recognition, iris recognition, hand geometry, voice recognition and fingerprinting imaging (Scott, Acton and Hughes, 2005: chapter 3.1).

Like all ICTs, digital identification systems have functional limitations. Green and Viljoen (2020) identify three common fallacies in regard to their practical application. First, algorithmic systems are often "argued for on the grounds that they are capable of making 'objective' and 'neutral' decisions" (Ibid.: 21). Such claims fail to consider that computational systems are not value-free but designed by human beings with specific intentions and interests in mind. Through their engagement and interaction, actors project their values and beliefs (un)intentionally onto the systems they are developing. In the context of societal problems deeply intertwined in history and politics, actors are responsible for choosing how they interact - which is never neutral (Ibid.: 22).

Second, algorithmic systems operate within boundaries in which only certain legible criteria and mathematically defined features are recognised (Ibid.). Hence, significant but complex social and political aspects of the world that don't fit into mathematical attributes are treated as static or left outside of the system's design. In practice this often means that the logic of efficiency as the primary "language of algorithms" (Ibid.) is imposed onto social domains at the expense of other values. Because of these trade-offs that inevitably occur as boundaries need to be made in every project, it is imperative to consider "when certain factors can be ignored and when they must be grappled with" (Ibid.: 23).

The third fallacy relates to universalism, "the sense that algorithms can be applied to all situations and problems" (Ibid.). This trend of "technological solutionism" (Morozov, 2013) or "technochauvinism" (Broussard, 2018) is critically explored by various scholars, presenting evidence that technical deployments may be more disruptive or harmful than the circumstances that they meant to improve (Baumer and Silberman, 2011: 2). Focussing on the (root causes of a) problem is generally more insightful than focussing on the solution. The process requires exploring alternative social approaches as they contribute to building communities, trust and civic interactions. Moreover, resources for maintenance and skill building that are needed to operate technology-heavy interventions are often underestimated when implementing new digital systems (Ibid.).

2.3 The right to privacy

The concept of legitimacy entails that state conduct follows the rule of law. Additionally, advancements in technologies cannot be separated from considerations of the right to privacy. Privacy is a fluid and contextual concept. What is considered to be private differs depending on the history, society, individual and situation (Lukács, 2016: 258). Consequently, it is difficult to define what it exactly describes (Solove, 2008: 2). In the 19th century, Warren and Brandeis (1890: 195) defined privacy as "the right to be let alone." With respect to our modern understanding, another definition suggests that privacy is "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'privacy sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals" (Lester of Herne Hill and Pannick, as cited in UN General Assembly, 2013: para. 22). Privacy is a fundamental human right and recognised in various international and regional human rights instruments[1], including the ICCPR. With its ratification in 1973, provisions of the ICCPR became legally binding for the German government (UN Treaty Body Database, 2020). Therein, privacy has been considered across three institutions: home, family, and correspondence (Bohlin, 2008: 35). Article 17 states:

[1] For example, see article 10 of the African Charter on the Rights and Welfare of the Child (African Union, 1990: 6); article 11 of the American Convention on Human Rights (UN, 1979: 148); and article 8 of the European Convention on Human Rights (ECHR, 1950: 11).

> “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks” (UN General Assembly, 1966: Article 17).

The UN Human Rights Committee (UNHRC) has given some guidance on the meaning of the right to privacy in its General Comment No. 16. The Committee (UNHRC, 1988: para. 2) states that protection should be granted for every person and enshrined in state legislation. Privacy is not an absolute right which means that exceptions are permissible but must be authorised by law and comply with the aims and provision under the Covenant (Ibid.: para. 3). Furthermore, the terms “family” and “home” are broadly defined. The former includes all those persons that are part of the family, while the latter refers to the place where a person resides or carries out his or her usual occupation (Ibid.: para. 5). “Correspondence” implies various means of communication and should be delivered without interception, surveillance or other intervening means. The integrity and confidentiality of correspondence should be guaranteed de jure and de facto (Ibid.: para. 8). As early as 1988, the Committee recognised the need for data protection as an important aspect of privacy[2]:

[2] Data protection has also been recognised as a standalone right (European Union, 2012).

> "The gathering and holding of personal information on computers, data banks and other devices (...) must be regulated by law. (...) [E]very individual should have the right to ascertain (...) what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files (...) have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination" (UNHRC, 1988: para. 10).

The Human Rights Council has been working to further clarify principles of the right to privacy in the digital age (UN General Assembly, 2018). The report of the High Commissioner for Human Rights underlines that, with the advent of ICTs and their increased processing power, informational privacy has become of particular importance. It extends to "information that exists or can be derived about a person and her or his life" (Ibid.: 5). Moreover, the report points out that the protection of privacy extends not only to information contained in communications but equally to metadata because it "may give insights into an individual's behaviour, social relationships, private preference and identity that go beyond even that conveyed by accessing the content of communication" (Ibid.: para 6). Equally important is the observation that the public and private spheres tend to overlap (Hissenbaum, 1997). Nevertheless, publicly available information shared, for example, on social media is still protected under the provisions of the right to privacy (UN General Assembly, 2018: para. 6). The report further states that "the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk" (Ibid.: para. 7). Thus, the risk is immanent even if data is not (yet) processed by a human or an algorithm.

In regard to personal data, the report contains six key principles and obligation that ensure the minimum level of protection (Ibid.: para. 29). First, the principle of lawfulness, fairness and transparency ensures that personal data is collected and processed by fair and lawful means, including through transparent policies. It should be based on “free, specific, informed and unambiguous consent” (Ibid.: para. 29). Second, the principle of purpose specification and limitation provides that data processing should be necessary and proportionate to a legitimate purpose specified further by the processing authority (Ibid.). Third, the amount, type and retention period of data need to be limited (Ibid.). Fourth, data must be accurate (Ibid.). The fifth principle provides for sufficient security measures considering the vulnerability of the information and the possibility of unauthorised disclosure (Ibid.). Lastly, parties who process personal data should be accountable for their compliance with existing legal frameworks (Ibid.).

Permissible interferences with the right have to comply with the principles of legality, necessity and proportionality: “A limitation can only be lawful and non-arbitrary, if it serves a legitimate purpose (…), [it] must be necessary for reaching that legitimate aim and in proportion to that aim and must be the least intrusive option available” (Ibid.: para. 10). Generally, states have the responsibility to respect, protect and fulfil the right to privacy. The obligation to respect requires states to ensure the right for *all* individuals within their territory and subject to their jurisdiction, without discrimination (Ibid.: para. 23). The duty to protect against adverse human rights impacts has extraterritorial effects (Ibid.: para. 25). In line with the obligation to fulfil, states must take positive actions to facilitate the enjoyment of the right to privacy, for example, by introducing data protection laws (Ibid.: para. 27).

The principles governing the right to privacy are applicable to individuals who are not nationals of the country in which they live (UN General

Assembly, 1985: Art 5(1); Council of Europe, 1981: Art 1). While the term "asylum seeker" has a social and legal meaning that matters, this study will refer to this broader definition to include various groups that may be affected by IDM-S. An asylum seeker is "an individual who is seeking international protection (...) [and] whose claim has not yet been finally decided on by the country in which the claim is submitted" (UNHCR, 2005: 441). For the examination of governance practices in which digital systems play a role, the provisions of the right to privacy will provide important guidance.

3 Research design

3.1 Interpretative methodology

This paper follows an interpretative research design that focuses on the understanding of meaning and meaning-making in the lifeworld of the actor(s) under study (Yanow, 2006: 23). Ontologically, an interpretative approach is based on the assumption that social reality is constructed or, in other words, shaped by human experiences and social context. It follows that, epistemologically, the subject is best studied within its social, political and historical context by taking into account subjective interpretations of various participants (Bhattacherjee, 2012: 103). Consequently, interpretative researchers engage in interpreting the reality through a sense-making process by asking "How?" rather than "Why?" (Haverland and Yanow, 2012: 8). This research seeks to understand how the Federal Office legitimises the policy and use of IDM-S as part of its new governance direction. As the researcher seeks to encounter new knowledge from the studied setting, it is important to link ideas or expectations to evidence found in the field (Ragin, 1992: 217). Theories prepare and inform the researcher but the research design needs to be flexible and responsive to the setting in order to account for possible tensions between expectations and lived experiences (Haverland and Yanow, 2012: 11-12). The logic of inquiry that informs the research is both iterative and recursive, moving between theory and practice (Ibid.: 12).

Furthermore, this research approach is rooted in the hermeneutic tradition of interpretation as it focuses on the Federal Office as a political actor and tries to understand how the digitally oriented direction of governance related to IDM-S is shaped by the subject's sense-making. Hermeneutics acknowledges that meaning made by members of a situation is not expressed directly but embedded in or projected onto a variety of artefacts (Yanow, 2006: 15). In turn, meaning can be understood through interpreting these artefacts vested with values, beliefs and intentions. The term "artefacts" needs to be understood in a broad sense to include text and written words (e.g. legislative text), text-like objects (e.g. built spaces), as well as acts and non-verbal communications (e.g. acting of subjects and their agents) that are treated as text analogues (Ibid.). The attention to language brings in "considerations of power and power relations, as well as privileged speech and silences in collective, public discourses" (Ibid.: 22). When examining governance practices, understanding who has a voice and who does not is particularly important. Also, the language used by state representatives plays a performative role, for instance, by proving arguments for a specific policy decision and by legitimising specific actions and measures. According to Yanow (Ibid.: 19), the strength of interpretive research lies in "its utility for studying situations in which the meanings of words and deeds are not or are not likely to be congruent." This means when word-deed tensions occur, researchers tend to trust the action as the more accurate reflection of a meaning (Ibid.). Considering the highly political setting studied in this research project in the field of asylum, it is important to make meaning of words in relation to actions because politics, in general, is understood as the struggle over idea(l)s and the struggle for power (Hawkesworth, 2006: 42). While policy documents may express a desired state of affairs, the subject's conduct may still differ greatly from the overall experience with enacted policies on the ground (Yanow, 2006: 19).

Lastly, since the context under study is constantly changing, the author of this paper acknowledges that one's own interpretation is "likely to be incomplete and even possibly erroneous" (Yanow, 2006: 16). While further investigations will be needed, this study seeks to make its approach and research design as transparent as possible.

3.2 Methods and approach

While digital systems play an important role in governance arrangements, there is a lack of sufficiently developed and tested research methods to understand many of their critical implications (Orlikowski and Iacono, 2001: 133). To account for the multiplicity of digital systems in governance that influence decision-making, the choice of this research is to apply an analytical tool-mix. The data justice framework is used to situate, structure and make sense of the studied setting. It is applied to analyse the Federal Office's implementation efforts relating to IDM-S. Additionally, the qualitative content analysis is used which, in the hermeneutic tradition, examines leads in empirical data.

The conceptual data justice framework is grounded in the relatively new field of critical data studies, emerging as a response to limited perspectives on the societal implications of data-driven technologies and the "datafication" of society (Dencik, Jansen and Metcalfe, 2018; Kitchin and Tracey, 2014; Dalton and Thatcher, 2014; Boyd and Crawford, 2012). This academic field seeks to broaden the debate to account for issues relating to democratic procedures, the entrenchment of inequalities and discrimination of certain groups, or the dehumanisation of decision-making around sensitive issues (Dencik, Hintz, Redden and Treré, 2019: 874). Confronting technological determinism, the overall approach is to position data embedded in systems in a way that engages more explicitly with questions of power, politics and interests, as well as with notions of legitimacy and governance (Ibid.). This reframing and the shift in focus away from technologies toward broader issues of data-intensive systems in governance and human rights is what makes the data justice approach so valuable for this research. While the framework is currently being refined and tested, nevertheless, it seems to be suited to provide an umbrella for sense-making and foregrounding the politics of data as well as the significance of context in which ICTs are implemented by governments. This approach was chosen because it can be applied in the local context as, for example, Heeks and Shekhar (2019) demonstrated in their analysis of the role of data systems in the field of urban development. A simplified version of the data justice model proposed by Heeks (2017) and the framework suggested by Dencik, Jansen and Metcalfe (2018) provide a set of guiding questions for the analysis:

	Dimensions	*Questions*
1	Structural	Who are the stakeholders and how is power distributed among them? Who is affected by the data-intensive system?
2	Procedural	How is data handled and transformed into results?
3	Instrumental	How is data being used in the system? What happens with the results?
4	Rights-based	Does the handling of data adhere to privacy rights?

Table 4: Dimensions of the data justice framework
(Source: Following Heeks, 2017: 11; Heeks and Shekhar, 2019: 995; Dencik, Jansen and Metcalfe, 2018)

The qualitative content analysis was chosen because it has been applied successfully in a variety of qualitative social studies and proved itself reliable in the field of interpretative research (Mayring, 2000; Diekmann, 2005: 510-511). The qualitative content analysis explores and describes complex settings following textual accounts of individuals' lifeworlds in a hermeneutic tradition (Erlingsson and Brysiewicz, 2017: 93). The analysis proceeds in several steps as proposed by Kuckartz (2007). First, available documents are read and re-read to get a sense of the whole. The text is roughly divided into sections for better orientation. Second, meaning units are identified in each text section and condensed into smaller parts. Third, these condensed units are then encoded. Codes are superordinate labels or terms used to identify ideas in the text (Ibid.: 60-61). To keep the analysis consistent, each code is characterised by coding rules that determine its content. They are formed deductively (e.g. based on the theory) and inductively (e.g. based on the text) to allow for sufficient flexibility, the review and adaptation of the coding system after re-reading (Ibid.: 60). Forth, these codes are grouped into categories that are derived both from the text itself (e.g. specific wording used by the actors) as well as the theoretical foundation (e.g. criteria of legitimacy, governance, right to privacy). If necessary, these categories are refined further after additional re-reading and the final revision of the results. Throughout the analysis, writing comments and memos proved to be a valuable technique, documenting impressions, ideas, interpretation possibilities and open questions (Strauss and Corbin, as cited in Kuckartz, 2007: 133). For coding and analysis the software MAXQDA is used. The coding system, including descriptions, main codes and rules, can be found in the appendix (Appendix A).

3.3 Data sources

The data sources on which the study relies include internal documents that outline practices at the Federal Office, such as instructions for identity determination procedures, handbooks on the three IDM-S systems and training manuals for employees. This material is made available through public requests at the freedom of information platform fragdenstaat.de. Additionally, press releases, the Federal Office's Digitalisation Agenda 2020 and published interviews with its leadership are taken into account. The majority of these sources is retrieved directly from the official ministry's website at bamf.de. Furthermore, policy-related documents play an important role in the assessment of justifications, intentions and official statements in regard to IDM-S. These sources consist of proposed legislations and draft laws, protocols of parliamentary debates and the public hearing procedure, written statements of civil society organisations and legal experts. Additionally, so-called "kleine Anfragen"[3] (small requests) of opposition parties were analysed as they provide valuable insights into the administration's practices and views. Answers to these requests are given by the Federal Government in close coordination with the requested authority (e.g. the Federal Office). All considered documents were published between January 2017 and July 2020, other material is excluded. Only sources that directly refer to the IDM-S systems as developed and applied at the Federal Office were considered. The material selected for analysis can be found in the appendix (Appendix B).

Between April and May 2020, expert interviews were carried out to verify the available information and to include (known) experiences of affected individuals through the involvement of intermediaries. The experts were selected based on their proven, long-standing experience in researching human rights and governance issues in relation to the Federal Office's asylum policies. The following experts were chosen: Bellinda Bartolucci, at the time head of the legal policy department at PRO ASYL who was involved in drafting the organisation's statement which addressed legal issues related to IDM-S; Lea Beckmann, lawyer and procedural coordinator at the Society for Civil Rights (GFF, Gesellschaft für Freiheitsrechte) which

[3] "Kleine Anfragen" (small requests) are information and control tools of parliamentarians that are used to request written answers on specific policy issues from the Federal Government (German Bundestag, 2020a).

issued legal actions against the Federal Office's method to analyse asylum seekers' mobile devices as part of IDM-S; and Anna Biselli, journalist and computer scientist who investigated the IDM-S systems over several years and was among the first to raise (privacy) concerns. The interview design was semi-structured and problem-centred, ensuring flexibility for both the researcher to react to narratives and for interviewees to add aspects important to them (Diekmann, 2005: 450). With the experts' consent, the conversations were recorded and transcribed in full for analysis. These three qualitative, oral interviews were conducted in the language of the interviewees' choice, each between 60 and 90 minutes (Appendix C). In addition, a written interview was carried out with the Office of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) that supervises the compliance of state institutions with existing privacy regulations. With the Office's consent, the correspondence is used in this research (Appendix D). The Federal Office for Migration and Refugees rejected the invitation to participate in this study.

4 Empirical analysis

4.1 The Federal Office's IDM-S system and its political context

This first part of the analysis examines the development of IDM-S at the Federal Office and situates it in the broader political context in the period between roughly 2014 and 2018. It clarifies how identity determination procedures of asylum seekers are carried out and how IDM-S is embedded in this process.

4.1.1 Development and political mandates

The analysis indicates that the development of IDM-S followed a gradual, strategic process on the Federal and Länder level. In 2015, the Heads of State and Government of the Länder decided the digitalisation of asylum procedures (IT Planning Council and BMI, 2018: 1). The IT Planning Council, which organises governmental collaborations in relation to questions concerning ICTs, was tasked with the coordination of technical implementations (IT Planning Council, 2016: 23-24). Under the leadership of the Federal Ministry of the Interior, Building and Community (BMI), a "project group on the digitalisation of asylum procedures" (PG DAS, "Projektgruppe Digitalisierung des Asylverfahrens") was established. Of various subgroups, the Federal Office was heading project number three, which focused on the documentation of the overall asylum process. It produced a detailed evaluation of data flows and IT systems in the Länder pertaining to asylum procedures, among other results (IT Planning Council and BMI, 2018: 5).

A direct outcome of these efforts was the introduction of the Integrated Identity Management programme (IDM, "Integriertes Identitäts-management") in May 2016 (IT Planning Council, 2016: 23-24). Upon registration, personal information of asylum seekers could now be stored in a core data system that expanded the Central Register of Foreigners (AZR, "Ausländerzentralregister") (IT Planning Council and BMI, 2018: 2). The system provided access to data for about 6.700 additional government authorities, resulting in a total of 14.000 institutions with access rights (BVA, 2016). IDM's legal basis, the Data Sharing Improvement Act ("Datenaustauschverbesserungsgesetz") from February 2016, was criticised for its broad data collection, insufficient data protection and the extension of access rights for security officials (PRO ASYL, 2016; Burzcyk, 2016; Classen, 2016; German Bundestag, 2020b: ID 18-71011). The extent of this data exchange among authorities was considered a novelty in Germany (Grote, 2018: 28).

Influenced by the work of PG DAS and other internal project groups, the Federal Office published its Digitalisation Agenda 2020 mid-2016. It outlined over 30 initiatives to improve existing processes and IT, including the central workflow and document management system MARiS ("Migrations-Asyl-Reintegrationssystem") (Ibid.). Within two years, the portfolio expanded significantly to over 115 initiatives, including the so-called "Integrated Identity Management - plausibility, data quality and security aspects" programme (IDM-S, "Integriertes Identitätsmanagement - Plausibilisierung, Datenqualität und Sicherheitsaspekte") (BAMF, 2019a: 11; BAMF, 2018a: 8-13). IDM-S draws on the infrastructure of IDM and consists of "intelligent systems to support decisions" (BAMF, 2018a: 12), among others, the automatic dialect recognition, the name transliteration and analysis, and the analysis of mobile data devices. The aim of IDM-S is to verify information provided by asylum applicants during registration procedures and to check for the plausibility of their statements during the personal hearing (Ibid.; BAMF, 2019a: 41).

Early 2017, the decision to develop IDM-S was made by the Commissioner for Refugee Management[4] (BFM, "Beauftragter für Flüchtlingsmanagement"), Frank-Jürgen Weise who was the former interim head of the Federal Office (German Bundestag, 2017b: 4; BAMF and BFM, 2017). The IT-department of the ministry, then under the leadership of Markus Richter, was responsible for coordination and management (BAMF, 2020a; BAMF, 2016b). IDM-S was developed in cooperation with a wide range of commercial actors who integrated additional products of other firms, including SVA and IBM for the name transliteration and analysis, Atos and Nuance for the automatic dialect recognition, as well as Atos, MSAB and T3K-Forensics for the analysis of mobile data devices (BMI, 2018b: 1; BMI, 2017b). No public tender procurement was carried out due to prioritisation requirements of existing contracts, as the government claimed (German Bundestag, 2017b: 4; German Bundestag, 2018a: 24).

While the exact development timelines for each system remain vague, it seems that the process was structured along three stages: a proof of concept phase, a pilot phase and a transitional phase where components were transferred into permanent structures (BAMF, 2018b). Testings took place in a reception facility based in Bamberg, Bavaria. Regarding the name transliteration and analysis, two software options were tested in the first half of 2017, the decision for the final product was made in July (German Bundestag, 2018a: 25). The order for the development of the automatic dialect recognition was placed on 12 April 2017. The pilot phase was extended in September (German Bundestag, 2017b: 3-4). Information

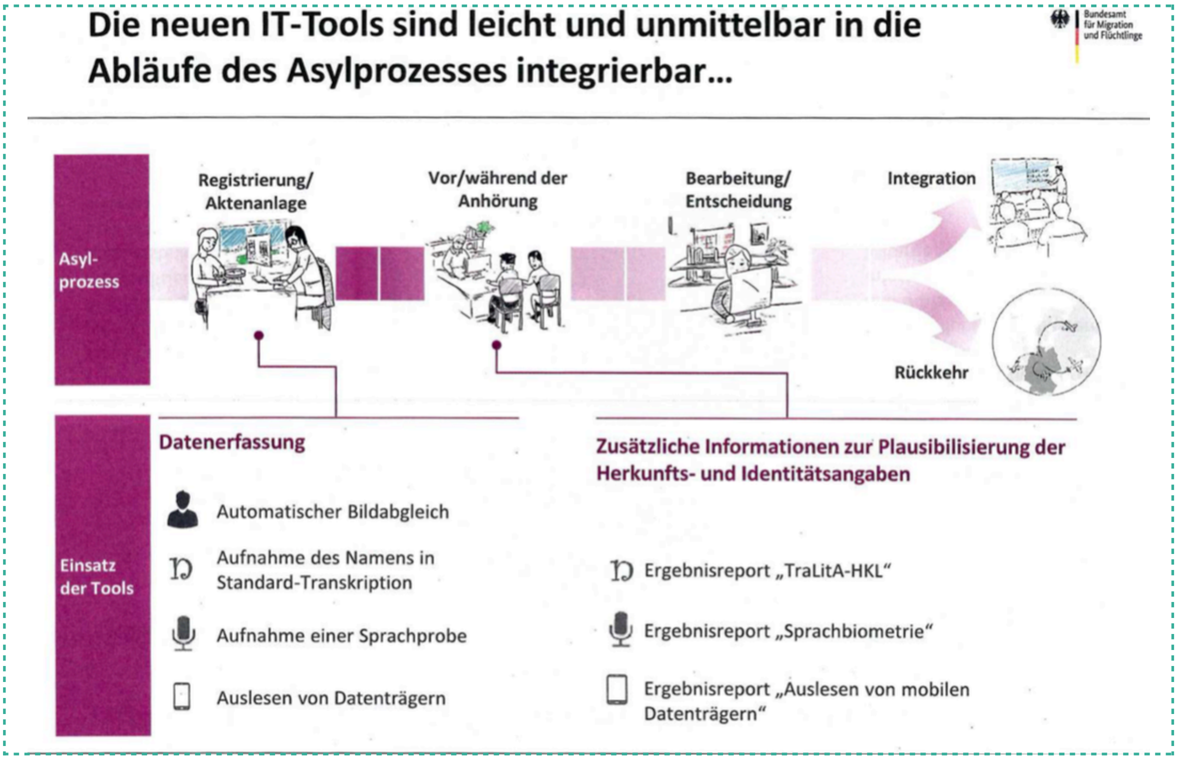
[4] In this newly established position, the Commissioner was tasked with the development of solutions for the implementation of asylum procedures, the facilitation of return, and the improvement of data quality across all competent authorities and governance levels. The mandate expired in 2017 (Grote, 2018: 29; BMI, 2017a; BMI, 2018a: 3).

about the testing and development phases of the system to analyse mobile data devices is not available. As live demonstrations of all three components took place on 25 July 2017, it can be assumed that these systems were developed mainly in the first half of 2017 (BAMF, 2017b; BAMF, 2017c; BAMF and BFM, 2017). According to the Federal Office, IDM-S was rolled out across all its branch offices and reception facilities in the beginning of 2018 (BAMF, 2019a: 41; BAMF, 2018a: 34).

4.1.2 Application in identity determination procedures

As the main authority responsible for matters relating to migration, the Federal Office is obligated to decide on asylum applications (BAMF, 2020b; BAMF, 2020c). Asylum is granted based on preconditions for international refugee and subsidiary protection, evidence for political persecution and whenever bans on deportation apply (BAMF, 2020d). Decisions are made on a case by case basis taking into account the individual's identity and history of persecution. In the area of asylum, identity is documented during registration and verified in the personal hearing procedure (Tangermann, 2017: 5). During the registration, personal information is collected (BAMF, 2020e; cf. BMJV, 2019a: AZR-law, section 1, para. 3). It is compared to existing data bases, such as the EU's fingerprint database EURODAC and INPOL of the Federal Criminal Police Office (BMI, 2018a: 7; BAMF, 2018c: chapter 1). If any security reservation or grounds for refusing entry exist, authorities responsible for decisions on residence matters are notified (BAMF, 2019b: 16-17). In the personal hearing, asylum seekers are questioned about the reasons for seeking protection and other details regarding life in the country of origin that can corroborate their claims. These interviews are led by a "decision-maker" (BAMF, 2020f) who verifies all information provided to make the final asylum decision. In general, asylum seekers are obliged to hand over any documents that can establish their identity and serve to illustrate their origin (BMJV, 2020: Asylum Act, section 15). Official documents are subject to a multi-stage physical and technical examination (PTU, "physikalisch-technische Untersuchung") in order to check for their authenticity. Travel documents (e.g. passports, identity cards) and papers indicating civil status (e.g. birth certifications, driver's licences) are accepted (BAMF, 2019c: Urkunden- und Dokumentenprüfung PTU).

Following internal guidelines for identity determinations, the name transliteration and analysis is used irrespective of the individual's possession of a passport (BAMF, 2018c: chapter 3.4). Whereas the automatic dialect recognition and the analysis of mobile devices are carried out if such documents cannot be provided or any doubts about the individual's origin exist. In the asylum procedure, IDM-S is used during the initial registration but can also be applied before or during the personal interview (Ibid.: chapter 3). For each system of IDM-S, a separate report is compiled that contains the results of the data analysis. These reports are used by decision-makers in preparation for the personal interviews (Ibid.). The three systems are applied as follows.



Die neuen IT-Tools sind leicht und unmittelbar in die Abläufe des Asylprozesses integrierbar...

Bundesamt für Migration und Flüchtlinge
Asyl-prozess
Registrierung/ Aktenanlage
Vor/während der Anhörung
Bearbeitung/ Entscheidung
Integration
Rückkehr
Einsatz der Tools

Datenerfassung

- Automatischer Bildabgleich
- Aufnahme des Namens in Standard-Transkription
- Aufnahme einer Sprachprobe
- Auslesen von Datenträgern

Zusätzliche Informationen zur Plausibilisierung der Herkunfts- und Identitätsangaben

- Ergebnisreport „TraLitA-HKL“
- Ergebnisreport „Sprachbiometrie“
- Ergebnisreport „Auslesen von mobilen Datenträgern“

Illustration 1: IDM-S embedded in the asylum process
(Source: BAMF, 2017a: Übersicht

The name transliteration and analysis (TraLitA, “Transliterationsassistent”) is used to transliterate Arabic names to Latin characters (BAMF, 2019a: 41; BAMF, 2018d). At a computer, Arabic-speaking applicants indicate their country of origin and their full name to prevent spelling mistakes, which can arise from regionally different phonetic forms or pronunciations and can dependent on the interpreter as well as the experience of the registration staff (BAMF and BFM, 2017: 2; BAMF, 2017a: Namenstranskription, Übersicht; BAMF, 2018d: 10; BAMF, 2019a: 14). Based on that name, references to the country of origin are made as part of the analysis (BAMF, 2019a: 41). These references are indicated in the final report as follows: “The name is used [rarely/very rarely] in the indicated country [Syria]. Instead, in [the countries/ the country] [Lybia, Algeria and Morocco] it is used frequently"[5] (BAMF, 2018c: chapter 3.4). According to the Federal Office, TraLitA improves data quality as it is based on standardised transliterations. This way multiple registrations of the same individual are avoided and the need for follow-up corrections is reduced (BAMF, 2018d: 5; BAMF, 2017a: Namenstranskription, Übersicht; BAMF and BFM, 2017: 3).

The automatic dialect recognition (DIAS, "Dialektbestimmungs-Assistent") determines the spoken dialect of an asylum applicant (BAMF, 2018e). This information is used to verify the region of origin (BAMF, 2017a: Sprachbiometrie, Übersicht). According to the Federal Office, the system is applied to applicants who claim to speak the following five Arabic (grand) dialects: Gulf, Iraqi, Maghrebi, Egyptian and Levantine (BAMF, 2018b; BAMF, 2019a: 14). To start the proceeding, an assigned staff member dials an internal phone number. On the phone, the asylum applicants describe one or more provided pictures in their native language (BAMF, 2017a: Sprachbiometrie, Ablauf; BAMF, 2018e: 6). These descriptions are recorded and terminated after approximately two minutes. Based on this biometric speech sample, probabilities for the spoken dialects are calculated automatically (BAMF, 2017a: Sprachbiometrie, Ablauf; BAMF, 2019a: 14). According to the Federal Office, the system provides for the speech-based verification of origin early on in the asylum procedure (BAMF, 2017a: Sprachbiometrie, Übersicht). The decision-making process is supported with an additional data point and put on a broader basis (Ibid.). It is argued that "potentials for misuse" ("Missbrauchspotenziale") (BAMF, 2018b) are limited and that the overall asylum process is accelerated. This way both

[5] Own translation. Original text: "Der Name kommt im angegebenen Land [Syrien] [selten/sehr selten] vor. In [den Ländern/dem Land][Libyen, Algerien und Marokko] kommt er hingegen häufiger vor" (BAMF, 2018c: chapter 3.4).

transparency and security in the asylum process are increased (BAMF and BFM, 2017: 3).

The analysis of mobile data devices (AmD, “Auslesen von mobilen Datenträgern”) is the third method applied as part of IDM-S (BAMF, 2018f; BAMF, 2018g). In its internal instructions, the Federal Office distinguishes between three stages: the read-out of mobile devices of asylum applicants, the automatic analysis of data contained on these devices, and the final evaluation and use of the results during the hearing procedure. Currently, smartphones, mobile phones and tablets are examined (BAMF, 2018c: chapter 3.1). On a computer, the assigned staff member records information about the devices, including the country name and purchase date. Then, asylum applicants unlock their devices and, if necessary, change existing settings. The read-out takes place in the presence of the individual concerned at a specialised computer to which the phones and tablets are connected. Extracted data are automatically analysed and the final results are compiled to a report. Unlike the other two IDM-S systems, this report is not immediately available to decision-makers. It is accessible to them after being given specific access permission by a fully-qualified lawyer eligible for judicial office (“Volljurist”). Only then the final report can be used in preparation for the personal interview (Ibid.: chapter 3.1.3). The Federal Office argues that identity determinations can be designed more purposefully during the hearing as claims of asylum applicants can be supported with an “additional technical lead” (“weitere[r] technische[r] Anhaltspunkt”) (BAMF and BFM, 2017: 6) - even if identity documents were lost.

In general, policy documents underline that the three systems only assist and never replace the human decision-making process. If discrepancies occur as part of the reports, asylum seekers can resolve potential conflicting information during the hearing (German Bundestag, 2018a: 26; BAMF and BFM, 2017). According to the Federal Office, IDM-S provides leads to the claims. It does not have evidential value, meaning that the systems' reports cannot be used in court (BAMF, 2018c: chapter 3.4; German Bundestag, 2017b: 7).

4.1.3 Political environment

In 2015, the number of individuals seeking protection from violent conflict, war and political persecution significantly increased in Germany, reaching a peak with almost half a million individuals applying for asylum - more than twice as many as in the previous year (BAMF, 2016a: 11). Public administrations were struggling to come up with viable responses to the complexity of migration, especially in regard to the timely registration and processing of all filed asylum claims (Grote, 2018: 32-36). The Federal Office faced an intense need of additional, qualified personnel to process all new arriving asylum seekers as well as those who resided in the country. Consequently, this led to an ever growing backlog of unregistered individuals and long waiting periods for the beginning of asylum procedures alone (German Bundestag, 2018b). By the end of 2015, more than 330.000 initial proceeding were pending at the Federal Office, while at the same time the average process duration extended to almost eight months (BAMF, 2016a: 55-56). The situation intensified in the following year with up to 579.000 pending asylum procedures as of September 2016 (Grote, 2018: 34).

To cope with these challenges at the Federal Office, additional reception facilities were established, thousands of new employees[6] were recruited and allocated from other administrations, the duration of staff training was reduced, and more budget[7] was secured to cover the growing expenses (Ibid.: 39-40). Internally, emphasis was given on accelerating asylum decisions and processes. On the one hand, various technical initiatives were introduced to support this development digitally as the expansion of the Digitialisation Agenda's portfolio indicates (BAMF, 2018a; BAMF, 2019a). On the other hand, new performance targets required decision-makers to make approximately two to three asylum decisions per day, leading to excessive demands on both existing staff members and new employees who were largely inexperienced due to insufficient trainings (Süddeutsche Zeitung, 2017). These consequences of mismanagement at the Federal Office were addressed publicly by the media and the ministry's own staff council, putting the leadership under pressure to act (Scheinost and Hüter, 2015; Aul, 2016; Jehle, 2016).

Political developments were also fuelled by pivotal events, including the attacks in Ansbach (2016), Berlin (2016) and Würzburg (2018) - committed by individuals who applied for asylum in part under different identities (Tagesschau, 2016; Augsburger Allgemeine, 2018). The case of Franco A., the far-right German soldier who successfully registered as an asylum seeker from Syria, subjected the Federal Office to harsh criticism (Schmidt

[6] For comparison: As of January 2014, 2.132 individuals were employed at the Federal Office (full-time equivalent) while in 2015 only 350 new position were created. As of December 2017, 6.653 employees were enlisted, including 1.704 decision-makers (Ibid.: 52).

[7] The budget stipulated expenses of 159 million in 2014 compared to overall cost calculations of 782 million in 2017 due to the increase in personnel and premises (Ibid.: 58).

and Erb, 2019). Since 2015, these situations opened a window of opportunity for restrictive asylum policies with severe human rights implications for asylum seekers who were put under general suspicion of engaging in criminal activities (BMI, 2018c: 2; Klages, 2017; German Bundestag, 2017c; Georgi, 2016: 192). About 30 new asylum laws were introduced over a period of several years with the votes of the Christian Democratic Union (CDU), the Christian Social Union (CSU) and the Social Democratic Party (SPD) (Bartolucci, 2020: Appendix C; Dernbach, 2019). Legislative initiatives expanded the contested concept of "safe countries of origin" ("sichere Herkunftsländer")[8], introduced the residence obligation, and categorised individuals in groups with better and lower prospects of permanent residence, resulting in the provision of services for one group and even harsher restrictions for others (Grote, 2018: 45-51). As a result, the Federal Office's decision-making powers were extended by legal means, enhancing its authority vis-à-vis asylum seekers with the intention to create "deterrent effects for further potential arrivals" (Bröker, as cited in Grote, 2018: 40). The Federal Office was increasingly promoted as a "safety authority" ("Sicherheitsbehörde") - one that utilises technologies to enhance security particularly in identity determinations (BAMF, 2019d; BAMF, 2020g; Kastner, 2017). Furthermore, commercial consultancy agencies, such as McKinsey, were hired to assess the "optimisation potentials" ("Optimierungspotenziale") for repatriations (McKinsey and BAMF, 2016; cf. Federal Government and McKinsey, 2016; cf. Lobenstein, 2017; cf. Schneider, 2016). In light of the upcoming parliamentary election in 2017, these developments were used to demonstrate political

[8] This means that by law, the concept establishes a "default presumption" to certain countries that there is no general risk of persecution and that the human rights situation for all groups of society is satisfactory (BAMF, 2018h). Countries like Albania, Ghana, Kosovo, North Macedonia, Senegal and Serbia are considered "safe countries of origin", among other countries.

decisiveness and control over the unfolding situation (Biselli, 2020: Appendix C).

Where public institutions failed to provide the most basic of necessities, citizens engaged in collective practices of solidarity which became coined in the public discourse as “welcome culture” (“Willkommenskultur”) not least because of its magnitude (Hamann and Karakayli, 2016: 74). In regard to governance issues, volunteering played a major role in the maintenance, compensation and provision of crucial services (Grote, 2018: 29-30). However, critical migration and border studies indicate limits of the “welcome culture” in the political arena (Hamann and Karakayli, 2016: 73). The term was used heavily from utilitarian standpoint, that is in connection with the recruitment of specialised workers - a historic focus and main driver in Germany’s migration policy reforms (Georgi, 2016: 190-193.; Hamann and Karakayli, 2016: 73-74; Castro Varela, 2014: 42). Although many engaged in volunteering, scholars observed that long-term committed parts of the movement eventually had no say in asylum policies (Fleischmann and Steinhilper, 2017: 19; Karakayli and Kleist, 2016: 4-5; Funk, 2016: 289). The overall public attitude towards migration and asylum remained stable and predominantly positive as scientific evaluations indicated (Ahrens, 2017: 13; SVR Integration Barometer, 2018; Gerhards, Hans and Schupp, 2016; Helbling et al., 2017).

4.2 Political legitimacy: Legal background of IDM-S

So far, the political environment and conditions under which the Federal Office developed and applied IDM-S in the area of asylum and identity determinations were taken into account. This second part of the analysis focuses on identifying the qualities of political (input) legitimacy and patterns of justifications in relation to the Federal Office's governance by examining first the legal foundation and legislative proceedings of IDM-S.

4.2.1 Legal provisions of the Asylum and Residence Act

The legal basis for both the automatic dialect recognition as well as the name transliteration and analysis system is covered by provisions of the Asylum Act. In general, the use of identification measures in asylum procedures is permitted to verify and determine the individual's identity and the country or region of origin. Oral statements can be used, if the affected individual was informed beforehand. In regard to documenting, establishing and verifying identity, section 16, subsection 1 of the Asylum Act states:

> "(1) Identification measures are to be taken to verify the identity of foreigners requesting asylum. (...) In order to determine the foreigner's country or region of origin, the foreigner's oral statements may be recorded on audio and data media other than at his formal hearing. Such recordings may only be made if the foreigner is informed beforehand" (BMJV, 2016: Asylum Act, section 16, subsection 1).

Regarding the automatic dialect recognition, the government refers to this section accordingly to signify the legal footing of the system (German Bundestag, 2017b: 6). Also, the Act outlines that data on identity documents - including the name of the person concerned - can be read, processed and used:

> (1a) In order to check the authenticity of the foreigner's document or identity, the biometric and other data stored electronically within the passport, official passport substitute or other identity documents may be read (...)" (BMJV, 2016: Asylum Act, section 16, subsection 1a).
>
> "(5) The processing and use of data obtained pursuant to subsection 1 shall also be permitted for the purpose of establishing the foreigner's identity or identifying evidence for purposes of criminal prosecution and threat prevention." (Ibid.: Asylum Act, section 16, subsection 5)

While both digital systems are not explicitly mentioned, formally, the automatic dialect recognition as well as the name transliteration and analysis system fall under these legal provisions.[9] Official references of the government to the legal basis of TraLitA could not be identified. The analysis of mobile data devices was a new measure introduced by the Act to Improve the Enforcement of the Obligation to Leave the Country ("Gesetz zur besseren Durchsetzung der Ausreisepflicht"), which entered into force on 29 June 2017 (German Bundestag, 2020c: ID 18-80058). The law amended both the Asylum and Residence Act. Section 15a of the Asylum Act authorises the analysis of mobile data devices that is only

[9] To what extent these systems comply with EU's laws, such as the GDPR, can not be determined in this study. It is worth mentioning that the compliance of the automatic dialect recognition was questioned in the past (German Bundestag, 2017b: 6).

permitted insofar as it is necessary to determine the identity and nationality of the asylum seeker and the purpose of the measure cannot be achieved by other less-intrusive means. The Federal Office is the main responsible authority:

> "(1) The analysis of data carriers is only permitted insofar as it is necessary to determine the identity and nationality of the foreigner in accordance with Section 15 subsection 2 number 6 and the purpose of the measure cannot be achieved by lenient means. Section 48 subsection 3a sentences 2 to 7 and Section 48a of the Residence Act apply accordingly. (2) The Federal Office is responsible for the measures mentioned in section 1."[10]

The regulation to cooperate was extended by section 15 subsection 2 number 6: In cases where a valid passport or a passport replacement cannot be provided, asylum seekers are obliged to assist in the acquisition of identity papers and, upon request, to present and hand over all devices in their possession that may be important for the determination of identity and nationality to relevant asylum authorities (Federal Government, 2017b: 11; BMJV, 2020: Asylum Act, section 15, subsection 2, number 6).

The regulation of the analysis of mobile data devices further points to provisions of the Residence Act, namely sections 48 and 48a that apply. Accordingly, section 48 of the Residence Act underlines limitations: "Where

[10] Own translation. Original text: (1) Die Auswertung von Datenträgern ist nur zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Absatz 2 Nummer 6 erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann. § 48 Absatz 3a Satz 2 bis 7 und § 48a des Aufenthaltsgesetzes gelten entsprechend. (2) Für die in Absatz 1 genannten Maßnahmen ist das Bundesamt zuständig" (BMJV, 2020: Asylum Act, section 15a; cf. Federal Government, 2017b: 11).

there is reason to believe that analysing data carriers would provide only insights into the core area of private life, the measure shall not be permissible" (BMJV, 2017a: Residence Act, section 48, subsection 3a). Asylum seekers are obliged to provide access data for the analysis of devices (e.g. unlocking their devices). The analysis can only be carried out by employees qualified to hold judicial office (Ibid.). If insights into the core area of private life are acquired in the course of the analysis, they cannot be utilised, and records thereof are to be deleted immediately (Ibid.). A written record is to be made of that acquisition and deletion. Where personal data acquired in the course of the said measure is no longer necessary for the purpose of identity determination, the data is to be deleted (Ibid.). If individuals do not provide access to their devices, section 48a of the Residence Act regulates that telecommunication service providers are required to transmit the necessary information to state authorities upon request (BMJV, 2017b: Residence Act, section 48a, subsection 1).

4.2.2 Aims, interests and justifications

Because the Act to Improve the Enforcement of the Obligation to Leave the Country expanded the legal powers of the Federal Office by introducing the analysis of mobile data devices, the legislation had to be politically justified and argued for. The legislative proceedings provided detailed insights into the aims, interests and justifications put forward by the proponents of the law, including representatives of the Federal Office, the BMI as the drafting authority and the ruling coalition CDU/CSU and SPD. Arguments and intentions can be studied in the draft legislations, plenary debates and the public hearing procedure.

As the title and explanatory memorandum suggest, the Act aims to improve the enforcement of the obligation to leave the country. The draft section refers directly to the migration of 2015 (Federal Government, 2017a: 8; Federal Government, 2017b: 13; Federal Government, 2017c: 1). The problem stated therein is that among those arrivals there are "numerous persons" ("zahlreiche Personen") (Federal Government, 2017c: 1) who are not entitled to asylum protection. As the number of returns increased in the past years, it is generally assumed that "the Federal Office is likely to continuously reject a high number of asylum applications in the next months concerning those persons who do not require protection."[11] The most direct representation of this aim was put forward during the public hearing procedure by Hans-Eckhard Sommer (CSU), then soon-to-be president of the Federal Office (BAMF, 2020h).

Arguing in favour of the law, he stated that the legislation and its interventions combined would contribute to "facilitating measures that terminate the residence of persons who state a false identity and of those without prospects of remaining"[12] in the country. The analysis of asylum seekers' devices is one intervention of many embedded in the law that also include the extension of detention pending deportation, the elimination of notifications prior to deportations, surveillance measures and further movement restrictions (Federal Government, 2017c: 1-2). While the analysis of devices is used to determine and verify the identity and

[11] Own translation. Origin text: "In den nächsten Monaten wird das Bundesamt für Migration und Flüchtlinge fortlaufend voraussichtlich eine hohe Zahl von Asylanträgen von Personen ablehnen, die keines Schutzes in Deutschland bedürfen" (Ibid.).

[12] Own translation. Original text: "dazu beitragen, (...) aufenthaltsbeendende Maßnahmen gegenüber Identitätstäuschern und Personen ohne Bleibeperspektive zu erleichtern" (Sommer, as cited in German Bundestag, 2017a: 21).

nationality of asylum seekers, it has to be interpreted in the context of the law.

The plenary debates by large refer to national security concerns, emphasising the past attacks (German Bundestag, 2017d; German Bundestag, 2017e). The analysis of mobile devices plays an important role in the line of reasoning as it was argued that identity frauds could have been avoided. For example, Burkhard Lischka (SPD) stated: "BAMF employees have failed in the simplest test steps. (…) A look at Franco A.'s cell phone, and the whole fraud would have been exposed."[13] Arguing for faster deportations based on national security grounds, Sommer (as cited in German Bundestag, 2017a: 21) underlined in his statement during the public hearing that among the arrivals, there are persons who sympathise with and actively support terrorist organisations. Throughout the legislative process, asylum seekers were portrayed as security threats, as individuals who do not cooperate with authorities and deliberately hide their identity. This general suspicion and the perceived need to improve identity determinations were often coupled with the idea of an assertive state and a strong rule of law. Thomas de Maizière (CDU/CSU), the Federal Minister of the Interior, stated: "In a constitutional state, we cannot accept that asylum seekers indicate seemingly without sanctions and at will different names and nationalities, do not provide useful information and hope that the

[13] Own translation. Original text: "Da haben Mitarbeiter des BAMF bei simpelsten Prüfschritten versagt. (…) Ein Blick auf das Handy von Franco A., und der ganze Schwindel wäre sofort aufgeflogen" (Lischka, as cited in German Bundestag, 2017e: 23728).

authorities (...) will get stuck when seeking to obtain papers."[14] Sommer (as cited in German Bundestag, 2017a: 22) goes so far as to accuse asylum seekers to actively cooperate with embassy staff in countries of origin to hide their identity. Proof for these claims was not put forward.

During the public hearing, more narrow arguments in favour of the analysis of mobile devices were stated by Richter as the then direct representative of the Federal Office. He (as cited in German Bundestag, 2017a: 20-21) argued that the overall measure would improve administrative processes by increasing transparency and practicability, in addition to accelerating asylum procedures. The efficiency argument is put forward in more detail in his written statement on behalf of the Federal Office: Compared to other existing instruments for identity determinations that are complex and result in longer processing time, the analysis of mobile data devices would represent an additional "fast and straightforward" ("schnell und unkompliziert") instrument (Ibid.: 103). The extent of the measure is largely relativised in Richter's statements and responses. In regard to the legal foundation, he (Ibid.: 20) pointed out that the measure was already applied by other authorities and, consequently, would only be made usable for the Federal Office. It was emphasised repeatedly that access to data contained on devices would be carried out in a precise way, and that only necessary metadata would be read out - not the content (Ibid.: 29; Ibid.: 39). At the same time, the analysis of mobile devices would be applied only as a means of last resort to a specific, well-defined group - that is persons who do not have identity papers or any kind of information regarding their identity and

[14] Own translation. Original text: "In einem Rechtsstaat können wir es nicht hinnehmen, dass Asylbewerber scheinbar sanktionslos und nach Belieben verschiedene Namen und Staatsangehörigkeiten angeben, keine brauchbaren Auskünfte geben und darauf hoffen, dass die Behörden (...) bei der Beschaffung von Papieren nicht weiterkommen." (De Maizière, as cited in German Bundestag, 2017d: 22524).

nationality (Ibid.: 29; Ibid.: 39; Ibid.: 104). Contrary to Richter's statement, the explanatory section of the law outlines that approximately 50 to 60 percent of all asylum seekers cannot provide their passports and could, therefore, be considered as a potential target group (Federal Government, 2017b: 15). Furthermore, Richter (as cited in German Bundestag, 2017a: 20) assumed that asylum seekers have the sole responsibility to ensure the plausibility of their identity-related statements in order to prove who they are. However, circumstances that are not self-inflicted by the affected persons and outside their control, such as the way how governments design identity determination procedures, were excluded from official justifications. Representatives of the Federal Office did not refer to rights and freedoms of asylum seekers to whom the authority has particular responsibilities, showing bias in the argumentation. The most significant statement for the use of the analysis of mobile data devices stems from Richter's written statement on behalf of the ministry that included a "legal assessment" ("rechtliche Bewertung") (Ibid.: 103-104). It outlines the right of the legislator to react to situation where asylum is not only "requested in bulk" ("massenhaft beantragt") but is "unjustifiably desired" ("ungerecht-fertigt begehrt") in order to obtain residence rights (Ibid.). From the perspective of the Federal Office, this "attempt to misuse the right to asylum" ("Versuch einer missbräuchlichen Inanspruchnahme des Asylrecht-schutzes") (Ibid.: 104) has to be met at the level of identity determinations.

Throughout the legislative proceedings, the general lack of evidence for these claims, the use of vague numbers to imply the relevance of the law and the undifferentiated approach to the multifaceted issue at hand were largely criticised by civil society organisations (Becker, 2017: 2; PRO ASYL, 2017a: 5-9; PRO ASYL, 2017b). Similarly, in its assessment of the draft proposal, the Federal Council (2017: 12) pointed towards "substantial deficits of due process" ("erhebliches rechtsstaatliches Defizit") as the law did not provide for the evaluation of the impacts and assumed effectiveness of the measures proposed. The Council concluded that "(...) a regulation without the reflection of its steering potential calls into doubt the meaningfulness and appropriateness of legislative reactions."[15] Apart from the aims, interest and justifications, the non-compliance of the analysis of mobile data devices with constitutional provisions of the right to privacy was condemned.

4.2.3 Unlawful interference with the right to privacy

The right to privacy and its main essence, namely that *every* person should have an area of autonomous development, is protected by the general right of personality derived from Germany's Basic Law (Wehage, 2013: 11). Article 2, section 1 states: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law" (BMJV, 2019b: Art 2, section 1, GG). This Article is seen in conjunction with Article 1, section 1: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority" (Ibid.: Art 1, section 1, GG). The general right of personality was further development by judicial decisions. In 2008, the Federal Constitutional Court recognised a new fundamental right to the guarantee of the confidentiality and integrity of information technology systems (BVerfG, 2008: Judgement of 27 February 2008, 1 BvR 370/07):

[15] Own translation. Original text: "(…) eine Rechtssetzung ohne Reflexion über ihr Steuerungspotential [stellt] die Sinnhaftigkeit und Angemessenheit der gesetzgeberischen Reaktionen in Frage" (Ibid.).

> “The fundamental right to the guarantee of the integrity and confidentiality of information technology systems is to be applied (...) if the empowerment to encroach covers systems which alone or in their technical networking can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of the personality” (Ibid.: Judgement of 27 February 2008, 1 BvR 370/07, No. 203).

In regard to the person affected, the court stated:

> “What is first of all protected by the fundamental right to the guarantee of the confidentiality and integrity of information technology systems is the interest of the user in ensuring that the data which are created, processed and stored by the information technology system that is covered by its scope of protection remain confidential. An encroachment on this fundamental right is also to be presumed to have taken place if the integrity of the protected information technology system is affected by the system being accessed such that its performance, functions and storage contents can be used by third parties” (Ibid.: Judgement of 27 February 2008, 1 BvR 370/07, No. 204).

As the new legislation on mobile devices enables the access, analysis and storage of personal information of asylum seekers, it falls within the scope of the fundamental right as defined by the court. This was underlined during the legislative proceedings not least by the German Bar Association, the BfDI, and various civil society organisations (German Bar Association, 2017: 6; Voßhoff, 2017: 4; PRO ASYL, 2017a: 19). It was argued that the interference with the right to privacy takes place in such an extent and under conditions that are not permissible under the constitution. Criticism of the legal measure included the violation of the principles of proportionality and necessity, the lack of an adequate protection of the core area of private life and the absence of effective oversight mechanisms.

The principle of proportionality requires that the severity of the privacy interference is not disproportionate in relation to the justifying reasons and objectives put forward. This means that the legislator needs to consider both individual rights and common societal interests: In this case, the rights infringements of a person greatly outbalance common interests (Voßhoff, 2017: 7; German Bar Association, 2017: 9). The disproportionality of the analysis of mobile devices stems from its far-reaching scope in regard to asylum seekers' obligation to cooperate on the one hand and the Federal Office's authorisation to access, analyse and store personal data on the other. First, the legislation refers to all devices that asylum seekers possess, including laptops, mobile phones, USB sticks, and other devices (German Bar Association, 2017: 10; Voßhoff, 2017: 6). Second, it allows the Federal Office not only to look through personal information but, moreover, to analyse, copy and store data contained on these devices without legal limitations (German Bar Association, 2017: 10). Third, the circumstances of the most affected persons need to be taken into consideration to understand the degree to which the gathered information is particularly sensible and deeply personal (Voßhoff, 2017: 6). Asylum seekers' mobile phones represent the main communication channel with family members, friends and other close persons in their country of origin and the outside world. According to the German Bar Association (2017: 11), it is likely that these devices contain intimate information, notes and journey-like observations in the form of chat messages, videos and photos of their journey and personal life. If authorities read-out and analyse devices of asylum seekers, this measure directly encroaches on the protected core area of private life (Ibid.; Voßhoff, 2017: 7). In consequence, this means that much more personal data is accessed, analysed and stored by authorities than what is actually needed to achieve the aim of the measure, namely to determine the identity and nationality of a person without valid documents. The severity of the interference with the right to privacy is even greater since authorities can potentially access confidential communication, for example, with lawyers, doctors, and spiritual leaders - communication that is especially protected by law (German Bar Association, 2017: 13; Voßhoff, 2017: 6).

Furthermore, the extension of the obligation to cooperate violates the principle of necessity. While section 15a on the analysis of mobile devices refers to lenient measures, the obligation to cooperation in section 15, subsection 2 does not entail provision to ensure that less intrusive means are exhausted before the device is handed over for read-out (Voßhoff, 2017: 4-5; BMJV, 2020: Asylum Act, section 15, subsection 2, number 6; BMJV, 2020: Asylum Act, section 15a). According to the German Bar Association (2017: 8), this effectively means that persons without passports, upon request, must always provide their devices to authorities. Every employee has the right to make such a request, while at the same time the law does not impose requirements on staff members by outlining necessary conditions (Ibid.). This way, the obligation to cooperate amounts to a liability notwithstanding an actual misconduct or refusal to cooperate in the identity determination proceedings (Voßhoff, 2017: 5). The legislative provisions do not require substantiated doubts as to the identity statement of an asylum seeker which indicates that the measure can be applied arbitrary to every person without a passport, as was argued by the German Bar Association (2017: 15-16). In turn, this means that the necessity of the said measure is assumed and not based on reasonable, evidential grounds (Ibid.: 16).

The core area of private life is not sufficiently protected although it is referred to in section 15a, subsection 1 (Ibid.: 18; Voßhoff, 2017: 7). This section states that the use of the said method is restricted to cases where the access to devices leads *only* to insights about the core area of private life. However, considering the available personal data on devices and that every single e-mail can potentially contain intimate information, a clear distinction between more or less sensitive areas cannot be made in practice, especially, before the method is applied (German Bar Association, 2017: 19). Even if information of the core area of private life is accessed once, the interference does take place no matter if by a human being (e.g. confiscation of devices) or machine (e.g. analysis) (Voßhoff, 2017: 5).

Lastly, the legislation stipulates that access to analysed data of asylum seekers' devices is only permitted to fully-qualified lawyers who hold judicial office. However, these staff members do not represent independent entities, as they themselves are subject to the Federal Office's hierarchy and internal instructions (German Bar Association, 2017: 19; Voßhoff, 2017: 7). According to Beckmann (2020: Appendix C), this regulation seems to be inspired by judicial reservations that are applied to serious encroachments of fundamental rights, e.g. imprisonment cases. In addition to the legal qualification, such reservations introduce the external, judicial independence into control and oversight mechanisms (Ibid.). In regard to the analysis of mobile data devices, these safeguards are missing de jure, therefore, do not offer sufficient protection against state interference with the right to privacy (Ibid.).

4.2.4 Procedural quality issues

The introduction of the Act to Improve the Enforcement of the Obligation to Leave the Country was characterised further by quality issues in the legislative process. The proposal was pushed through means of accelerated proceedings without indicating reasons for its urgency (PRO ASYL, 2017a: 5): The cabinet decided upon the preparation of the Act on 9 February

2017 (Federal Government, 2017d). The first draft[16] was issued for comments on 16 February and was decided upon by the cabinet on 22 February (Federal Government, 2017e; BMI, 2017c; BMI, 2017d). The first proposal submitted to the Bundestag dates back to 23 February, the second was issued on 16 March, the final on 17 May, 2017. On 27 March, a public hearing procedure was carried out (German Bundestag, 2017f; German Bundestag, 2020d). The final plenary debates took place on 18 May, including the voting on the bill. The Act entered into force on 29 June 2017 (German Bundestag, 2020c).

According to the Joint Rules of Procedure of the Federal Ministries (GGO, "Gemeinsame Geschäftsordnung der Bundesministerien"), authorities are obliged to involve various actors "as early as possible" in the legislative process (BMI, 2011: section 47, para. 1, GGO). This includes relevant governmental departments and civil society organisations (Ibid.: section 47, paras. 1-3, GGO). In regard to the examination of draft laws, the deadline for engaging other state authorities is set to four weeks, in cases of extensive bills it is extended to eight (Ibid.: section 50, GGO). All submissions should be considered prior to cabinet decisions and include dissenting opinions as a result of the involvement (Ibid.: section 22, para. 1, no. 4; Ibid.: section 51, no. 4, GGO). All federal ministries involved in legislative proceeding shall be equally accountable for adopted bills (Ibid.: section 52, para. 1, GGO). Since the Federal Office was involved in the consultations, these provisions equally apply to that authority.

[16] The legislative process distinguishes between "Referentenenwurf" and "Gesetzesentwurf". The former are early draft laws that have not (yet) been adopted by the cabinet. The latter represent adopted legal proposals that enter the Bundestag procedure and become subject to parliamentary debates (BMF, 2020).

The analysis of procedural qualities demonstrates the lack of meaningful engagement. As the supervisory authority for data protection, the BfDI (2017: 101) repeatedly criticised the short deadlines for consultations that did not meet the requirements of GGO. Relating to the said Act, the office outlined that about one month was available to assess the draft law at first. As the legislation was revised, however, only a few days were available to issue up-to-date statements, leaving not enough time for sufficient evaluations of the law and its measures (BfDI, 2020: Appendix D.1, 1-4). Despite the critical remarks on the unlawful interferences with privacy outlined in the previous chapter, the concerns were not acted upon by the legislator as the BfDI (2019: 66) records in its annual report.

The engagement of civil society organisations and associations was formally respected to the extent that feedback on the draft legislation (Referentenentwurf) was requested. However, in their submitted statements on the draft law from 16 February, civil society organisations argued that due to the deadline of not even 24 hours a sufficient evaluation of the Act could not be provided (Keßler, 2017: 1; BumF, 2017: 1; Amnesty International, 2017: 1; Sedlmayr, 2017: 1; Loheide, 2017: 1). It was concluded that genuine engagement was not attempted by the government (Amnesty International, 2017: 1). As the cabinet decision was made only five days after the submission date, it is doubtful that even those submitted remarks were evaluated properly (Bartolucci, 2020: Appendix C). The engagement of civil society at this early point in the legislative process is crucial because once the draft passes through different committees and political discussions become increasingly deadlocked (e.g. during the parliament debate), it gets harder to make changes, as Bartolucci (Ibid.) points out. These short deadlines for engagement amount to a repeating issue in regard to asylum-related legislations (PRO ASYL, 2019: 1-2; BumF, 2017:1).

During the public hearing, six experts were presenting their views on the proposed legislation (German Bundestag, 2017a: 12). Interestingly, civil society organisations were invited on behalf of the opposition parties, whereas the governing coalition appointed Richter and Sommer as representatives. The fact that they both spoke on behalf of governmental authorities that were engaged in the drafting of the said Act raised criticism concerning the bias in the presented views. Ulla Jelpke (Die Linke) (as cited in German Bundestag, 2017a: 14) stressed that the aim of the hearing is to include expertise outside of governmental institutions to ensure impartiality. She (Ibid: 15; cf. German Bundestag, 2020e: para. 70) outlined that such conduct is not in line with the Rules of Procedure of the Bundestag and that exceptions need to be confirmed by the committee first, which was not the case in this instance.

Overall, a constructive dialogue and the adequate responsiveness to the raised issues were largely missing on the part of the government. Despite the various actors raising well-founded concerns in form of written and oral statements, provision of the law pertaining to the analysis of mobile data devices were not adopted. During the interviews only one example was referred to where the early draft law was changed: The analysis of devices initially outlined the additional purpose of determining travel routes of asylum seekers (BMI, 2017c: 22). These provisions were limited eventually, however, it was not explained whether the collection of data for that purpose was still intended and simply postponed into the future (Bartolucci, 2020: Appendix C; PRO ASYL, 2017a: 20).

4.3 Political legitimacy: Implementation and effects of IDM-S

The analysis of political intentions, the legal criticism as well as procedural issues in regard to the legislative background of IDM-S gave crucial insights into the qualities of legitimacy and governance on the input level. This third part of the analysis focuses on assessing the qualities of political (throughout and output) legitimacy and justification patterns by examining the implementation and (known) effects of IDM-S. By assessing the practices of the Federal Office, this section seeks to account for potential word-deed tensions to arrive at a more accurate reflection of meaning. Following the data justice framework, the structural, procedural, instrumental and rights-based dimensions are examined.

4.3.1 Structural issues: Affected groups and power relations

It is difficult to pinpoint who of the large group of asylum seekers is most affected by IDM-S because only marginal information is available on this subject. According to the Federal Office, only individuals without passports whose identity cannot be determined with reasonable assurance are affected (BAMF, 2018c). Federal statistics show that 54,2 percent of all asylum seekers were not able to present a valid document in 2018 (German Bundestag, 2019a: 27). This rate depends on the country of origin and varies accordingly. For example, most individuals from Syria provided a passport while 19,2 percent were not able to do so. In comparison, 86,8 percent of all asylum seekers from Nigeria did not have valid documents

(Ibid.; Biselli and Beckmann, 2020: 14). The reasons why individuals are not able to provide their passports are as complex as their journeys during which they are exposed to significant threats, from the moment they leave their homes, passing through camps and other temporal places, to the country of refuge (Privacy International, 2019: 1). Amidst these difficulties, documents might get stolen or lost, or confiscated by traffickers. Depending on the local administrative arrangements, some countries do not issue passports to all nationals or, in other circumstances, their documents are not recognised by German authorities (Tangermann, 2017: 33-34). For example, this is the case for all Somali documents issued after 1991 (BMI, 2016: 41; Biselli and Beckmann, 2020: 16). These statistics indicate that individuals from some countries are more likely to be affected by IDM-S than others. Every second asylum seeker who applies for protection in Germany is likely to be subjected to identity determination procedures where IDM-S is applied.

Asylum seekers are recognised as members of a vulnerable group *per se* in need of special protection (ECtHR, 2011: Case of M.S.S v. Belgium and Greece, para. 251; UNHCR, 2013: 9). They are in precarious positions as they have less access to robust human rights protection and fewer resources with which to defend their rights in the country of refuge. Language barriers and insufficient knowledge of local governing systems put them at a general disadvantage, resulting in further power imbalances, in particular, when facing government authorities. There are categories of asylum seekers who face distinct needs due to their physical, mental or social circumstances (ECRE, 2017: 7). These groups include and are not limited to victims of torture and human trafficking, traumatised persons, (pregnant) women, and persons persecuted on grounds of their gender and sexual orientation. Because vulnerable individuals are entitled to specific rights, it is important for states to adequately assess the status and situation of each individual to ensure that vulnerabilities are recognised in a timely and effective manner (Ibid.). While general vulnerability assessments as part of the asylum process are somewhat in place in Germany, they are criticised for being insufficient (ECRE, 2017; Von Bullion, 2019). None of the analysed IDM-S-related documents refer to or otherwise address the vulnerability of individuals. Precautions concerning these groups are not outlined which gives reason to believe that the vulnerable status is not taken into account when IDM-S is applied in practice.

The Federal Office has the most power over asylum seekers as it effectively decides over people's lives by issuing asylum decisions. These decisions are binding and can only be disputed in court. Over the last years, the ministry's power, resources and competencies were extended consistently by law. In the area of asylum, the Federal Office is the primary authority to engage with vulnerable individuals, as Bartolucci (2020: Appendix C) underlined. It constitutes an essential body for asylum seekers as it is the first entity on the government's side to carry out hearing procedures and engage with very personal, often traumatic experiences (Ibid.). Establishing trust is, therefore, a core element in the relationship between the ministry and asylum seekers to ensure that individuals describe their stories as they happened. Privacy-invasive digital system, such as IDM-S, can significantly disturb this relationship very early on in the process as they can reproduce inequalities and feelings of powerlessness (Ibid.).

Where state actors seek to develop and apply digital systems, it is often companies who offer technical resources far beyond governments' expertise (Rahman, 2017). Such public-private arrangements can build in long-term dependencies of administrations on actors with primarily commercial interests. Concerning IDM-S, various international firms were involved in the provision of digital infrastructure and technologies that built in technical and social dependencies. These dependencies exist in regard to IDM-S, for example, owing to ownership relations over software and components. While Richter (as cited in Frank, 2018: 24) argued that the "solution" relating to the automatic dialect recognition and all its linguistic models belong to the government, the ministry's budget contains regular payments for licensing fees, among others (German Bundestag, 2018a: 14). Other issues occur in the area of corporate accountability in regard to privacy breaches and human rights violations. MSAB, which provides products and services for the analysis of devices, faced harsh criticism in the media as it is known to be specialised in the forensic extraction of mobile data for primarily military, border control, police, and intelligence services - areas that are entirely opposed to requirements in the field of asylum (BMI, 2018b: 1; Biselli, 2020: Appendix C; MSAB, 2020; Greis, 2018; Meister, 2018). In worst cases, such partnerships can lead to state disengagements with vulnerable populations and the outsourcing of responsibilities to the private sector where potential human rights violations may remain undetected (Lethbridge, 2017).

4.3.2 Procedural issues: Participation, transparency, accountability

In the implementation phase, procedural aspects play an important role in regard to legitimacy. These aspects touch upon opportunities for participation and feedback-giving as well as the willingness to provide information and ensure responsive communication as part of a transparent and accountable state practice.

In the analysis opportunities for involvement outside the Federal Office could not be identified, suggesting that the implementation of IDM-S was closed off from public view. In response to a freedom of information request, the ministry explained that feedback - as described in the digital agenda in relation to IDM-S - refers to the exchange of departments involved in the development of the systems (BAMF, 2020i: 4). Rather vague references concerning only the automatic dialect recognition were made to "various institutions and scientific organisations" ("verschiedene Institutionen und wissenschaftliche Einrichtungen") (German Bundestag, 2017b: 5). Initially, it was stated that the Federal Office was working with the University of Pennsylvania, instead, a press inquiry to the said institution revealed solely the purchasing of a language package (Biselli, 2020: Appendix C; German Bundestag, 2018a: 14; Bewarder and Flade, 2018). Without further clarification, Richter (as cited in Frank, 2018: 22) stated in an interview that the ministry was "working primarily with experts for algorithms" ("primär mit Experten für Algorithmen zusammengearbeitet"), suggesting a rather technocratic approach.

The overall communication was hesitant, restrictive and did not allow for broader debates on the implementation and functioning of IDM-S. The responsiveness of the Federal Office was insufficient. Considerable delays occurred in relation to freedom of information requests. While state administrations are required to respond within four weeks by law, it took BAMF several months to provide information (Biselli, 2020: Appendix C). Other patterns demonstrated a general unwillingness to engage by ignoring subquestions and/or providing only brief answers to questions that would not contain new information (BAMF, 2018i; Biselli, 2020: Appendix C; Beckmann, 2020: Appendix C). Other freedom of information requests about IDM-S were rejected, for example, those concerning the planning, functioning, testing, risk and privacy assessments. The reasons put forwards related to potential threats to public security, identifications of software vulnerabilities, attempts at manipulation in asylum procedures, the impairment of federal fiscal interests in commercial transactions and the potential disclosure of trade secrets (BAMF, 2020i; BAMF, 2019e; BAMF, 2019f; BAMF, 2019g). The communication with journalists was shaped by similar reluctance. According to Biselli (2020: Appendix C), it was difficult to receive up-to-date material and statistics for the timely reporting of current developments around IDM-S, although at times information was already published elsewhere. Compared to other public administrations within Germany and the EU, where objective answers were generally provided in a reasonable timeframe, the Federal Office was much less willing to give access to information, creating barriers for journalistic work (Biselli, 2020: Appendix C). Attempts at in-person conversations with the Federal Office's employees about IDM-S during public conferences were likewise unsuccessful (Beckmann, 2020: Appendix C).

While the provision of critical information was kept at a bare minimum, other occasions were used to generate publicity and demonstrate a tech-savvy self-image as "leader in technology" ("Technologieführer") (BAMF, 2018b). The Federal Office received an e-government award (organised by the industry) in the category "Best Digitalisation Project 2018" ("Bestes Digitalisierungsprojekt 2018") for the automatic dialect recognition (BAMF, 2018j; BearingPoint and Cisco, 2020). The Federal Office repeatedly referred to this event as a success and public confirmation for its actions (German Bundestag, 2018a: 15; Richter, as cited in Frank, 2018: 22; BAMF, 2019a: 32). In an interview, several aspects relating to this new approach towards a so-called "digital, breathing public authority" ("digitale, atmende Behörde") (BAMF, 2019a: 5; BAMF, 2018a: 3) were emphasised as a general success, including being the first public administration worldwide to use such a technology, having developed the approach within only six months, and having used agile development methods (Richter, as cited in Frank, 2018).

While the Federal Office claims that it attaches importance to the transparency of results (Ibid.: 22), the analysis shows that decision-making processes that are supported by IDM-S remain to a major extent intransparent. During the interviews, this aspect was confirmed and repeatedly mentioned in relation to accountability issues. The lack of transparency represents the largest normative category concerning procedural aspects. For an independent assessment of how results are obtained, the source code and algorithmic functioning with the distribution and weighting of the underlying data samples - which are used for comparisons and the calculation of probabilities - need to be transparent. Despite clear recommendations, for example, by the Data Ethics Commission, IDM-S does not satisfy these requirements (German Bundestag, 2017b: 3; German Bundestag, 2018a: 15; Beckmann, 2020: Appendix C; Biselli, 2020: Appendix C; DEK, 2019: 25). Furthermore, it is unknown what biases the systems have, how they are considered and addressed in the decision-making process - from the moment the systems make suggestions to their interpretation and usage in the final asylum decisions (Biselli, 2020: Appendix C). As policy documents and statements of the Federal Office in regard to IDM-S consistently underline that final decisions are made by human beings instead of digital systems, it seems that no justification issues exist from the administration's perspective (Biseli, 2020: Appendix C). Nevertheless, the results of the systems have an influence on the overall decision-making process of employees, which in certain known cases can be traced back to asylum files, as Biselli (2020: Appendix C) explained. Yet, decision-makers are not required to document their decision-making and discretion process, creating space for risks of abuse (Beckmann, 2020: Appendix C). The lack of transparency regarding the interpretation of the systems' results is even greater in the case of the analysis of mobile devices: As the read-out data is immediately deleted once the automated report is generated, decision-makers de facto have to rely on unverifiable, summarised claims included in the reports (Beckmann, 2020: Appendix C; Biselli, 2020: Appendix C).

Insufficiencies relating to the quality of asylum decisions, however, remain a major issue for the Federal Office regardless of the use of digital identification systems (Bartolucci, 2020: Appendix C; Idler and Mantel, 2016; German Bundestag, 2020f). According to Bartolucci (2020: Appendix C), it were primarily the courts that made a sufficient assessment of the facts because the hearing procedures at the BAMF were carried out poorly. Indeed, statistical information indicates that administrative courts subsequently corrected 26,4 percent of negative asylum decisions issued by the Federal Office in 2019 (content-related decisions). The error rate concerning asylum seekers from Afghanistan, for example, was as high as 48,7 percent (Jelpke, 2020; German Bundestag, 2020f; cf. German Bundestag, 2017g).

4.3.3 Instrumental issues: Effectiveness and efficiency

In line with political legitimacy, performance assessments need to consider both the effectiveness and efficiency of IDM-S. This requires making the best use of available resources in relation to the set aims. All outcomes should result from scientifically designed procedures and rational operations.

A response to a small request indicates that between 2017 and 2019 a total of 17.356.342 euros was spent on IDM-S, among others, 2.062.159 euros on the biometric dialect recognition, 3.077.628 euros on the name transliteration and analysis, and 11.203.664 euros on the read-out and analysis of data devices (German Bundestag, 2018a: 14-25; cf. German Bundestag, 2018c: 32).[17] Product testings during the proof of concept phase amounted to 844.263 euros (German Bundestag, 2018a: 22-25). Additional costs for qualification measures of employees were as high as

[17] Based on economic assessments by the government as of July 2018, gross amounts (Ibid.).

168.628 euros in 2017 (Ibid.: 15). While the expenses for the analysis of mobile devices were initially estimated at 3.200.000 euros, the actual costs for this measure exceed these estimates by far (Federal Government, 2017c: 3). Compared to technical components, costs for additional qualification measure were rather low. As software and hardware need to be maintained regularly, it can be assumed that each year additional running costs, especially for support and licence renewals occur. A recent freedom of information request to disclose the cost-benefit analysis in regard to IDM-S was rejected by the government with reference, among others, to potential interferences with future procurement procedures (BAMF, 2020i: 4).

Of the three systems, the name transliteration and analysis serves two purposes: transliterating Arabic names and making references to the applicant's country of origin (BAMF, 2019a: 41). No performance evaluations were made available on the former while some details exist on the latter functionality. The database of TraLitA contains approximately one billion names from all over the world, however, the system is applied only to Arabic names (German Bundestag, 2018a: 24). Entries are broken down into several parts (so-called tokens) for which frequency statistics are compiled (Ibid.). Success scores for all Arabic states were tested based on 20.000 real names per country (Ibid.). For Syria and Iraq the system achieves a success rate between 85 and 90 percent, whereas for Maghreb states the rate reaches 35 percent. This result might be due to the historic mixtures of French and Italian languages, as the government claims (Ibid.). While internal instructions imply that TraLitA should be used as a standard procedure during registration for Arabic names, it seems that statistics for only 1.443 use cases were recorded as of April 2018 - more than six months after implementation (Ibid.: 26). For the majority of these cases (39 percent) references to the country of origin were not verifiable, followed by 34 percent that did not support the claims of applicants. In two percent no references could be made at all, and in 25 percent the results supported the claims of asylum applicants (Ibid.).

While the lack of transparency remains an issue, the quality improvement of transliterations represents a legitimate aim (Biselli, 2020: Appendix C). As the procedure follows standardised rules (character A is transformed into character B), it can contribute to eliminating spelling mistakes (Ibid.). However, making references to the country of origin based on an applicant's name is problematic. It seems the higher the diversity of names in a country is, the more complex the analysis gets and the more useless the result become (Ibid.). What's more important: It cannot be assumed that a person's name corresponds with state borders. Names are influenced by culture, personal preferences, religious beliefs, by changes in popularity etc.. There are no binding rules that forbid to name a child with, for example, a German nationality, "Anthony" or any name other than "Horst". Even if the data base contained more names, the problem of complex social dynamics at play still remain. During the interview, no (known) cases could be confirmed where the system's results had influenced asylum decisions (Ibid.).

The automatic dialect recognition makes reference to a region of origin based on a biometric speech sample of asylum applicants (BAMF, 2017a: Sprachbiometrie, Übersicht). To provide results, recorded speech is compared to existing data models of the system - which is comprised of 8.000 validated speech samples (German Bundestag, 2018a: 15). These samples are based on recordings of speakers from varying gender and age groups (German Bundestag, 2017b: 9). According to the government, more than 25 languages and dialects are stored, however, the system is applied only to Arabic dialects: Gulf, Iraqi, Maghrebi, Egyptian, and Levantine (BAMF, 2018c: chapter 3.2; German Bundestag, 2018a: 10; BAMF, 2018b). Between September 2017 and November 2018, it was applied 6.284 times (German Bundestag, 2018a: 5). Performance results, however, were only recorded in 2.333 cases (Ibid.: 12). The government (Ibid.) added that the difference was due to the time lag between the generation of the speech report prior to the hearing and the later manual entry of the results. Of these recorded cases, the outcomes were congruent with statements of asylum applicants on 1.906 occasions (82 percent), whereas in 427 cases (18 percent) they were not (Ibid.). The average success rate reaches about 85 percent across all dialects, for Arabic-Levantine it is over 90 percent (Ibid.:13). Common issues are short net speaking durations of applicants during the recording and the low number of underlying speech models (German Bundestag, 2018d: 8). Potential effects of linguistic disabilities, such as stuttering and lisping, are taken into account only during the hearing procedure (Ibid. 9). According to the government, the implementation of the system is considered a success not least because it promoted the digitalisation of public administrations (German Bundestag, 2018a: 15). The e-government award and requests by the Federal Office's partner organisations underline this statement of success, as the government argued (Ibid.).

While the success rate might appear high from a technical perspective, its significance is not reliable as only an average for the performance of all dialects is provided. Individual rates, especially the lowest, are not mentioned. From a human rights perspective, an average success rate of 85 percent still means that in 15 percent of the cases individuals concerned may face problems in asylum proceedings. Asylum decisions require special diligence due to the severity of consequences and possibly life threatening dangers that individuals face, if their asylum claims are wrongfully rejected. In this regard, the question is why an average error rate of 15 percent seems to be politically accepted and whether the same rate would satisfy expectations in other workflows and circumstances within public administrations. The interviews confirmed that results of the system can be inaccurate and influence asylum decisions in a negative way. In one case, the system's results suggested that individuals from Afghanistan were German native speakers - which was not the case (Biselli, 2020: Appendix

C). While this is a rather obvious mistake, other instances were more complex. Biselli (Ibid.) referred to a person whose asylum claim was rejected shortly after the automatic dialect recognition was applied. The system's results suggested that the person spoke Turkish with a 63 percent and Hebrew with a 22 percent likelihood (case details were changed to ensure anonymity). In fact, the individual was from Irak and spoke the Kurdish dialect Sorani that was not detected (Biselli, 2018; cf. Biselli 2017b). Results implying a high degree of conformity with one dialect do not necessarily correspond with the actual dialect spoken by an asylum applicant. Because the algorithmic functioning of the system is unknown, and so is the distribution of test samples across languages, it cannot be conclusively determined how accurate and reliable the final results are. In comparison, a scientific study which investigated different approaches for automatic dialect identification in Arabic broadcast speech concluded that for the five most widely used dialects - Egyptian, Gulf, Levantine, North African and Modern Standard Arabic - the accuracy was only about 59 percent (Ali, Dehak, Cardinal, Khurana, Yella, Glass, Bell and Renals, 2016). This is almost comparable with a coin toss, as Biselli (2020: Appendix C) adds. There are more issues that are not sufficiently considered by the Federal Office when utilising the results of the automatic dialect recognition. For example, dialects do not automatically correspond with state boarders. Even if a region of origin is assessed, this indication cannot be associated with nationality. Languages and especially dialects, are dynamic and subject to rapid changes. It is unlikely that technical systems are able to grasp the full phonetic diversity of one language let alone of five (Biselli, 2020: Appendix C). Moreover, individuals to whom the system is applied are asylum seekers and refugees - persons whose language and dialect are further shaped by their experiences during their journey. The way how a person speaks and possibly adopts a native dialect in accordance with the given situation, especially when facing authorities, may be influenced by experiences of discrimination. If individuals belong to minority groups who could be distinguished by their language and were therefore subject to abuse, it seems natural to alter speech as a means of self-protection. The Federal Office seems to acknowledge to some extent the existence of critical views among linguists about the accuracy of language analyses and dialect recognitions, nevertheless, it is stated: "There are (...) pronounced differences between the various trends in linguistic research. We took a different approach and worked primarily with algorithm experts. (...) Experts helped us to convert phonetics into codes."[18]

Finally, the analysis of data devices aims at verifying the claims of an asylum applicant based on the processing of personal data found on mobile devices (BAMF, 2017a: Auslesen von mobile Datenträgern, Übersicht). While recent statistics for the other two systems date back to December 2018, the latest information about the analysis of mobile devices includes its performance until the end of 2019. Between January and December 2019, 10.116 devices were read out from first applicants without passports or passport replacements aged 14 years and above (German Bundestag, 2020f: 33). In 4.582 (about 45 percent) cases, decision-makers requested the final report of the analysis, of which 3.436 (about 75 percent) were granted by fully qualified lawyers employed at the Federal Office (Ibid.: 34). Compared to the total number of read-outs, this means that about 34 percent were considered as part of the asylum decision. In about 40 percent (966 reports) of these considered cases identity claims of asylum applicants were confirmed, whereas in about two percent (52 reports) they were refuted. In the majority of all considered reports - about 58 percent (1.381 reports) - no usable results could be determined (Ibid.: 35).

[18] Own translation. Original text: "Es gibt (...) ausgeprägte Differenzen zwischen den verschiedenen Strömungen der Sprachforschung. Wir haben einen anderen Ansatz gewählt und primär mit Experten für Algorithmen zusammengearbeitet. (...) Experten haben uns dabei geholfen, Phonetik in Codes umzuwandeln" (Richter, as cited in Frank, 2018: 22).

The analysis showed that more devices were read out than were actually considered for the evaluation of an applicant's claim. At the same time, these statistics suggest that the analysis of data devices is not suitable to provide any substantial let alone reliable references to the nationality or identity of a person concerned. According to Beckmann (2020: Appendix C), the connection between data derived from mobile devices and statements of identity or nationality are particularly weak in regard to the affected group. Even if data suppose to provide only leads into the claims, the analysis is based on extremely poor indicators. For example, country and domain codes of websites (which are used for analysis) have no direct connection to the nationality of a person. During their journey, asylum seekers pass through various countries and are likely to seek information on the locations they are passing through. Difficulties during their journey might cause them to stay longer in countries not of their origin before they can continue travelling. In times of war and rapidly changing regional conflicts, it is likely that families are geographically dispersed and that, for example, area codes of their phone numbers differ from their country of origin (Ibid.). Moreover, results strongly depend on how a person is using the device, for what purpose, in what circumstances and for how long. That these aspects are poorly considered before the measure is applied was confirmed during the interviews. Beckmann (Ibid.) referred to a case where the mobile device of an individual who resided lawfully in Germany for six years was analysed during review procedures.[19] Considering the place of this person's residence (e.g. Germany) and the life cycle of a mobile phone which is about three to four years, it is unrealistic that contained data could provide any valuable insights in accordance with the overall purpose of the measure (Beckmann, 2020: Appendix C).

[19] These procedures are carried out by the Federal Office to assess whether the circumstances for asylum or refugee protection still exist. If the situation in the country of origin improves, then the protection status might be revoked under certain conditions (BAMF, 2019h).

It is unclear whether and to what extent IDM-S was subject to scientific, independent evaluations, despite the fact that the three systems were applied to thousands of asylum cases (Biselli, 2020: Appendix C). Regarding the automatic dialect recognition, an evaluation was implied in 2017 (German Bundestag, 2017b: 9). However, several follow-up enquiries and a recent freedom of information request revealed no progress as of May 2020 (BAMF, 2020i: 4; German Bundestag, 2018a: 14). Statistics for IDM-S are by large fragmented as the performance was not tracked consistently and throughly (German Bundestag, 2018c: 31; German Bundestag, 2018a: 12; German Bundestag, 2019a: 28-29). Only marginal indicators are used that refer to basic documentations in asylum files about whether references to the country of origin made by the three systems support the statements of the individual concerned, whether there was no reference or whether the reference could not be verified (BAMF, 2018c: chapter 3.2 - 3.4; BAMF, 2017a). In terms of quality control and monitoring, no information is available. Furthermore, it is not assessed if results of the systems negatively influence asylum decisions (German Bundestag, 2018a: 13-26; German Bundestag, 2018d: 7; German Bundestag, 2019b: 14; German Bundestag, 2020f: 35). Thus, experiences and (un)intended effects of IDM-S on asylum seekers are entirely ignored. The analysis indicates that IDM-S performs poorly in relation to its aim of making useful indications to the nationality or origin of a person concerned. The most expensive measure, the analysis of mobile data devices, provides no useful results in the majority of cases, yet it is still applied. The Federal Office stated recently: "The read-out of mobile data devices is currently the most important instrument for identity verifications."[20]

[20] Own translation. Original text: "Das Auslesen mobiler Datenträger stellt momentan das wichtigste Instrument zur Identitätsüberprüfung dar" (BAMF, 2020j: 2).

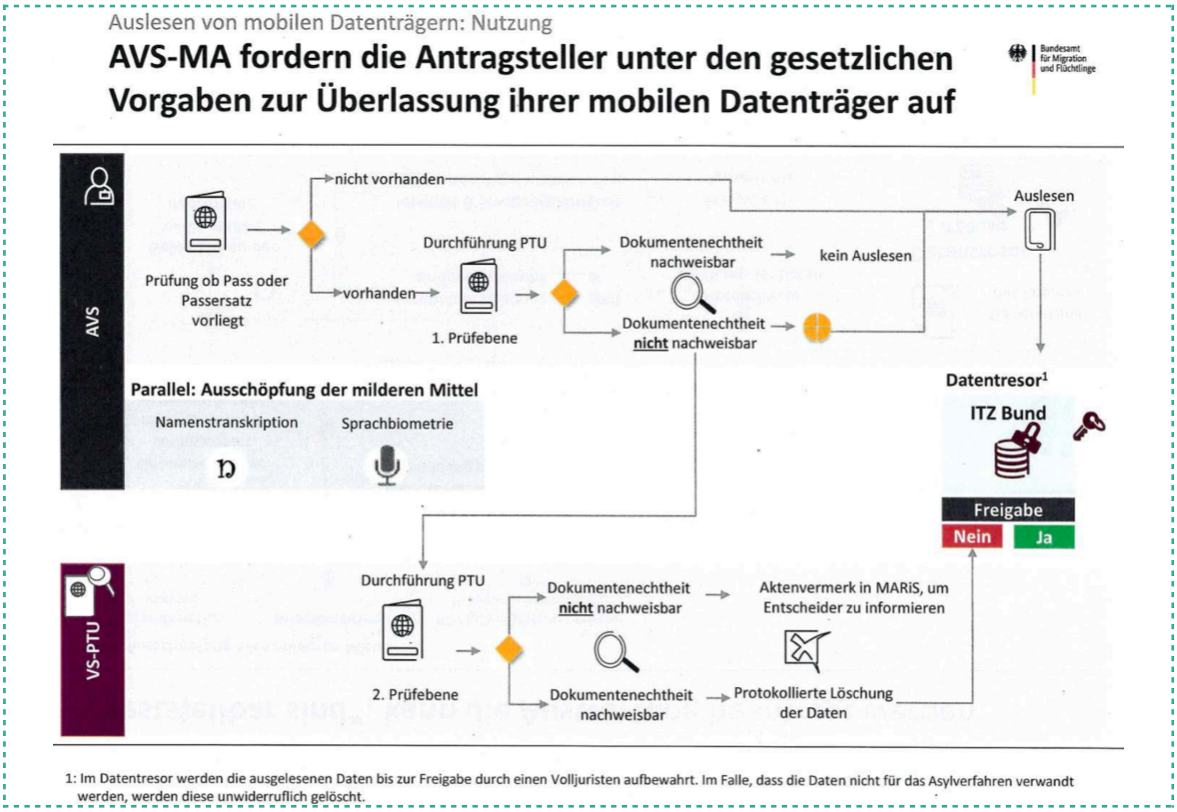
This measure's legal background was not assessed either. Bartolucci (2020: Appendix C) underlined that asylum legislations generally lack assessments of their effectiveness despite the government's high ambition to introduce ever more restrictive measures. Nationality references made by the name transliteration and analysis are vague, while the average success rates of the automatic dialect recognition are not reliable from a human rights perspective. In all cases, the IDM-S indications to identity and nationality are based on simplified assumptions about social reality as well as the informative value of the underlying and processed data. Thus, the overall performance does not satisfy the rationality and accuracy criteria that should be reflected in effectiveness and efficiency considerations of state practices.

4.3.4 Rights-based issues: Asylum seekers' right to privacy

The rule of law is a necessary basis of legitimate state practices. Hence, this section focuses on issues related to asylum seekers' right to privacy. The analysed documents contain first and foremost basic technical and operational guidelines applicable in identity determination procedures at the Federal Office whereas explicit and detailed elaborations on asylum seekers' right to privacy do not exist in regard to IDM-S.

4.3.4.1 Lawfulness, fairness, transparency and consent

The first principle of privacy and data protection requires that the collection and processing of data is carried out by fair and lawful means, including through transparent policies (UN General Assembly, 2018: para. 29). If data is collected and processed in breach of any statutory provision, then the action is considered unlawful. Both TraLitA and DIAS have a legal footing as the previous analysis outlined. Regarding the analysis of data devices, different interpretations as to the lawfulness of the underlying provisions are possible. The majority of statements put forward the view that its legal foundation is unconstitutional and should be rejected (Beckmann, 2020: Appendix C; German Bar Association, 2017; Voßhoff, 2017; PRO ASYL, 2017a). Other legal opinions might conclude that existing provisions need to be narrowed down to achieve conformity with constitutionally guaranteed rights ("in verfassungskonformer Auslegung"), as Beckmann (2020: Appendix C) points out. In both cases, the main issue pertains to the circumstance that the right to privacy is not sufficiently respected. Rather, the existing legislation is adopted very broadly in practice (Ibid.). This finding can be underpinned with several examples. While the Federal Office repeatedly underlines that the analysis of data devices is only carried out if individuals are unable to provide a passport or passport replacement, internal documents indicate non-compliance with this statements. Even though affected individuals are able to present a passport upon registration, they still may be subject to the said measure if the authenticity of their documents cannot be verified conclusively on the spot (BAMF, 2019c: PTU, 4; Beckmann, 2020: Appendix C; Biselli, 2020: Appendix C). At this first stage of the physical-technical examination, machine-readable documents from all countries of origin are scanned and examined visually. Papers are accepted from Syria, Iraq, Iran, Eritrea, Ukraine, Afghanistan and the Russian Federation (BAMF, 2019c: PTU, 4). Documents from other countries and those that are not machine-readable are send to a specialised examination office for the second-stage PTU (Ibid.: PTU, 5-6). If this is the case, then it is assumed that the individual's identity could not be established and, therefore, it is seen as valid to read out the devices (BAMF, 2018c: chapter 3.1.1). Same practices occur in situations where an available passport cannot be submitted immediately because other authorities are in possession of the individuals' documents (BAMF, 2018k: chapter 1). The following illustration depicts the PTU stages ("1./2. Prüfebene") and indicates that devices are read-out if documents are send to the second stage of PTU ("Dokumentenechtheit nicht nachweisbar, Auslesen"):



Auslesen von mobilen Datenträgern: Nutzung

AVS-MA fordern die Antragsteller unter den gesetzlichen Vorgaben zur Überlassung ihrer mobilen Datenträger auf

Bundesamt für Migration und Flüchtlinge

AVS

Prüfung ob Pass oder Passersatz vorliegt

nicht vorhanden

vorhanden

Durchführung PTU

1. Prüfebene

Dokumentenechtheit nachweisbar

kein Auslesen

Dokumentenechtheit nicht nachweisbar

Auslesen

Parallel: Ausschöpfung der milderen Mittel

Namenstranskription

Sprachbiometrie

Datentresor[1]

ITZ Bund

Freigabe

Nein

Ja

VS-PTU

Durchführung PTU

2. Prüfebene

Dokumentenechtheit nicht nachweisbar

Aktenvermerk in MARiS, um Entscheider zu informieren

Dokumentenechtheit nachweisbar

Protokollierte Löschung der Daten

1: Im Datentresor werden die ausgelesenen Daten bis zur Freigabe durch einen Volljuristen aufbewahrt. Im Falle, dass die Daten nicht für das Asylverfahren verwandt werden, werden diese unwiderruflich gelöscht.

Illustration 2: PTU stages and the read-out of mobile devices (Source: BAMF, 2017a: Auslesen von mobilen Datenträgern, Nutzung)

There are several implications to these findings that diverge from the requirements of the principles of fairness and transparency. Reasons and situations for which individuals are not themselves responsible are construed to their disadvantage even if passports are available. The measure is applied primarily to the advantage of the Federal Office: Devices are read out as early as possible in the process to ensure that personal information is available to authorities. The transparency of the policy can be contested because the communication of the Federal Office suggests a more narrow interpretation of the law which is not congruent with its practice. It can be disputed whether this application is covered by the wording of the law that permits the interference with privacy *only* in cases where a passport cannot be provided (BMJV, 2020: Asylum Act, section 15, subsection 2, number 6; Beckmann, 2020: Appendix C). This means that the interests of asylum seekers are not considered which results in the violation of the principle of fairness. According to Beckmann (2020: Appendix C), a privacy-intrusive measure such as the analysis of data devices is to date exclusively employed in law enforcement and only to cases with concrete suspicions of a crime in combination with a judicial reservation. This means that asylum seekers are the only groups - despite their vulnerable status - targeted by this surveillance-like measure in Germany which stresses the underlying discriminative nature of the practice, emanating directly from the state (Ibid.).

Furthermore, this first principle requires that data collection and processing is based on freely given, specific, informed and unambiguous consent (UN General Assembly, 2018: para. 29). For asylum seekers both the registration and identity determination procedures are mandatory, meaning that individuals have to provide personal information about themselves to be protected by the host state and to be able to access crucial services. Due to their vulnerable, precarious situation, it seems that they have no other choice than to abide by demands put forward. While it is understandable that governments need to request information to process applications, the way how such procedures are carried out is essential and concerning the practices of the Federal Office far from ideal.

Regarding the analysis of mobile data, upon request, individuals must submit their devices to employees of the Federal Office for the gathering and processing of personal data. This practice is not based on (freely given) consent but instead rests on a legal norm and duty introduced by the Act to Improve the Enforcement of the Obligation to Leave the Country (Beckmann, 2020: Appendix C). If individuals refuse to hand over their devices, instructions are given to address both the legal duty to cooperate and the possibility that the asylum application in question may be considered withdrawn as a consequence of non-compliance (BAMF, 2018c: chapter 3.1.1). Although guidelines at the Federal Office state that the ministry has no option to use coercion to obtain devices, in fact asylum seekers are forced or, in other words, persuaded to provide their data under such pressure and thread (Ibid.; BAMF, 2020k). In any way, the legal duty to hand over the mobile devices does not exempt the Federal Office from its transparency obligations. The ministry has to inform affected persons about the gathering and processing of data to achieve the openness required. In practice, the Federal Office requests an informed consent protocol signed by the individual concerned (Ibid). Such records, however, only indicate whether devices were handed over or not, in addition to a confirmation that instructions on the legal obligation to cooperate were given (BAMF, 2019i: D1705). Neither written nor verbal information is provided in detail as confirmed by the interviews, meaning the necessary criteria of informed, unambiguous consent is not satisfied. Biselli (2020: Appendix C), who spoke to several asylum seekers about their experiences, stated that in this situation individuals often did not understand what was happening and why as the procedure was not explained to them. Affected asylum seekers also worried about their relatives and friends whose information was accessible on their devices (Beckmann, 2020: Appendix C). It is this moment of fear - when persons hand over their phones expecting that all data can be accessed by authorities - which intensifies the fundamental rights and privacy violation. As Beckmann (Ibid.) explained further, such acts can ultimately alter a persons behaviour, trigger anxiety and lead to a loss of confidence - all decisive factors for asylum procedures that require individuals to recite their deeply personal histories of persecution. Bartolucci (2020: Appendix C) underlined this aspect that results in the severe erosion of trust in the relationship between authorities and asylum seekers very early on in the asylum proceedings which makes it especially difficult for affected individuals to speak freely and openly. The practices of the Federal Office were not yet evaluated by the supervising authority for data protection concerning their compliance with necessary information requirements, for example, as outlined in the GDPR, Art 12 and 13 because the latest review was undertaken before the GDPR entered into force in May 2018 (BfDI, 2020: Appendix D.2, 2; cf. European Union, 2016: L119, GDPR, 39-41).

Similar issues are encountered in regard to the other two analysed IDM-S systems. For the name transliteration, no information is provided to asylum applicants before the measure is applied, as the Federal Office's response to a freedom of information request indicates (BAMF, 2020l). Thus, it can be assumed that individuals are not aware that their names are being automatically analysed. Regarding the biometric dialect recognition, applicants receive a separate document where they indicate - with their signature - that they were informed about the reasons and procedure of this measure. However, this document does not contain detailed information on, for example, how their data is analysed and on what legal basis this measure is based on. Instead, it outlines that individuals were not able to prove their origin and, therefore, an automatic dialect analysis of two to three minutes can help to determine that information (BAMF, 2020m). Similar to the analysis of data devices, it seems that "consent" is implied or, rather, considered as an administrative necessity while no actual efforts are put into providing sufficient information and ensuring that individuals are informed about the procedure and systems affecting them directly (BAMF, 2020l). Initial instructions ("Erstbelehrung"), that individuals receive upon issuing their asylum application, provide some information on data collection and processing, however, they relate to the entire asylum procedure and contain general claims, such as that data are shared among various authorities (which are not specified), that data are processed in identity determinations, and that complaints can be made to the BfDI (BAMF, 2020k). However, the relationship between the Federal Office and the BfDI is not clarified. Throughout the document, the obligation to provide data is mentioned in combination with the threat that non-compliance may lead to the termination of asylum procedures (Ibid.: 7).

4.3.4.2 Purpose specification and limitation

For privacy interferences to be in accordance with ICCPR, this principle requires that data is gathered and processed for an explicit, specific and limited purpose (UN General Assembly, 2018: para. 29). Where there is imbalance of power, this rule ensures that individuals keep some control over their personal information that cannot be re-purposed in ways that they do not expect. Regarding the analysis of data devices, the law states that the measure is permitted to determine the identity and nationality of the person concerned (BMJV, 2020: Asylum Act, section 15a, subsection 1). The legal basis for both the name transliteration and analysis system as well as the automatic dialect recognition outlines the purpose of documenting, establishing and verifying identity (BMJV, 2020: Asylum Act, section 16; BAMF, 2018l). According to Beckmann (2020: Appendix C), the term "identity" has to be interpreted in the context of the law. It refers to the nationality of individuals and to information that can be found on their passports (Ibid.).

The possibility to collect and process vast amounts of data has undoubtedly awaken new political desires. In relation to privacy, signs of function creep - a process described as the gradual widening of the use of technical systems beyond their original purpose - can be evidenced (EDPS, 2012: 7). Regarding the analysis of mobile devices, past discussions about the recording of travel routes indicate these new possible directions. As geographical data is already collected, it would be easy to extend the original purpose (Richter, as cited in German Bundestag, 2017a: 103). The fact that the Federal Office broadly applies existing legal provisions causes concerns. Jutta Cordt (as cited in Seibert, 2017: 3), then president of the Federal Office, argued that an extension of the legal basis to cover content analysis of pictures would be desirable. In 2018, the government confirmed that an evaluation of the technical and legal opportunities for the extension of the analysis of data devices was under review (German Bundestag, 2018a: 22). Furthermore, the Federal Office is actively promoting IDM-S on the European level with the aim to deploy these systems elsewhere (German Bundestag, 2017b: 5; BAMF, 2018b). This observation applies to the name transliteration and analysis system as well as to the automatic dialect recognition (Richter, as cited in Frank, 2018: 24; BAMF, 2019a: 42). For example, Richter (as cited in Frank, 2018: 24) stated in an interview that DIAS could be beneficial throughout the entire refugee management, including EU's border control and other migration and refugee related contact points administered by governments.

4.3.4.3 Minimisation

Excessive data collections and processing pose significant risks from an individual's rights and an information security perspective (Privacy International, 2018: 41-42). Therefore, the third key principle is concerned with the limitation of the amount, type and retention period of data being collected from individuals (UN General Assembly, 2018: para. 29). In the case of the name transliteration and analysis as well as the automatic dialect recognition, the type and amount of data is limited to the applicant's name, a speech sample and personal indications of origin. Data is deleted ten years after the enforceable completion of the asylum procedure (BMJV, 2016: Asylum Act, section 16, subsection 6; BAMF, 2018l).

Regarding the analysis of data devices, the Federal Office (BAMF, 2018a: chapter 3.1) stated that on the basis of reconciliations with the BMI and the BfDI "predefined data points" ("vordefinierte Datenpunkte") are read out. Richter claimed: "It is about accessing - once, in a static, retrospective manner - a very limited field of data that does not depict the content of communication or the content of images, but rather the so-called metadata which provide information about identity and the country of origin."[21] Contrary to what the Federal Office appears to imply, this measure violates against the principle of minimisation. Considering the references spread across policy documents, the following is collected: metadata of pictures, contact information, messages, telephone lists (BAMF, 2018m); geographical information of pictures, apps, login-information to social networks (Richter, as cited in German Bundestag, 2017a: 103); information on spoken languages found, for example, in browser history, e-mails and chats (Ibid.); contact information on the SIM card used, calls, calendar, MMS, e-mails, files on the device and the memory card (BAMF, 2017a: Auslesen von mobilen Datenträgern, Schritt 9 - Daten auslesen). Because the data collection technically depends on the device and operating system, the type and amount of gathered information varies on a case by case basis (Ibid.). Nevertheless, the prevailing idea is that all information from these identified sources is made accessible to authorities. While the training manual indicates that deleted information cannot be used, the government refused to state publicly for reasons of confidentiality if encrypted data were accessed (German Bundestag, 2018a: 22). No exhaustive list of all types of accessed data is provided by the Federal Office.

Based on these collected data, a final report is automatically generated which contains the following information:

[21] Own translation. Original text: "Es geht darum, einmal statisch rückwirkend auf ein ganz begrenztes Datenfeld zuzugreifen, das nicht den Inhalt von Kommunikation oder den Inhalt von Bildern abbildet, sondern eben die sogenannten Metadaten, die Auskunft zu Identität und Herkunftsland darstellen" (Richter, as cited in German Bundestag, 2017a: 39).

	Categories		*Data processed in the final report*
1	General information		Time of extraction, data on asylum procedure, personal data of the asylum applicant, details on the fully qualified lawyer in charge, device information
2	Origin		
	2.1	Evaluations of calls	Diagrams depicting the distribution of incoming and outgoing calls along the identified top-five countries; tables containing the country, duration and number of calls with percentage ratings
	2.2	Evaluations of messages and chats	Diagrams depicting the distribution of incoming and outgoing messages along the identified top-five countries; tables containing the country and number of messages with percentage ratings; evaluations of languages used and their frequencies for both incoming and outgoing messages
	2.3	Dialect analysis of messages and chats	If Arabic languages are detected, then a dialect analysis is carried out additionally.
	2.4	Address book and contacts	Contact information saved in the address book is evaluated by quantity of contacts and by identified country with percentages
	2.5	Browser and location data	Evaluations of accessed websites displayed according to their respective country domains, location data derived from all apps are depicted separately by country in form of a table and a map
3	Identity		
	3.1	Information on the device	Names, account names, birthdays, and e-mail addresses derived from the device, including apps

Table 5: Analysis of mobile devices: Content of the cumulative report (Source: Following BAMF, 2017a: Auslesen von mobilen Datenträgern, Ergebnisbericht)

Data which is gathered during the read-out of devices is immediately deleted as soon as the report is compiled (BMJV, 2020: Asylum Act, section 15a, subsection 1, seen in conjunction with BMJV, 2017a: Residence Act, section 48, subsection 3a). If the fully qualified lawyer provides access to the report, then it is stored for ten years as part of the corresponding asylum file. If access is denied, the report is also deleted. In cases where the decision-maker decides that the report is not necessary for identity determination, then it is likewise deleted immediately (Beckmann, 2020: Appendix C; Biselli, 2020: Appendix C; BMJV, 2016: Asylum Act, section 16, subsection 6). The deletion and its reasons are recorded (BAMF, 2018c: chapter 3.1.4).

The Federal Office justifies this practice by repeating that only metadata is collected and that an evaluation of the content itself does not take place (Richter, as cited in German Bundestag, 2017a: 103; Ibid.: 20; BAMF, 2018c: chapter 3.1). Yet in result, content is being analysed, as Biselli (2020: Appendix C) concludes. Biselli and Beckmann, who examined asylum files as part of their work, confirmed that login-information to social networks - in these concrete cases to googlemail and facebook - were depicted under clear registration names. This means that authorities knew the e-mail address and facebook name of the applicant (Biselli, 2020: Appendix C; Beckmann, 2020: Appendix C). As the staff training manual of the Federal Office cites booking.com and dating apps as further examples, it cannot be ruled out that information found on these applications is also collected (BAMF, 2017a: Auslesen von mobilen Datenträgern, Ergebnisbericht, Umgang mit den Ergebnissen und Aussagekraft des Reports 4/4). At the same time, the ministry refuses to disclose a full list of apps that it evaluates (Biselli, 2020: Appendix C). Undeniably, gathering such information does not only intrude into the core area of private life but exposes the affected person to even more risks and harms. Information derived from dating apps, for example, may give insights into a person's sexuality - details that are particular sensitive considering that such data might also intersect with causes of persecution in the country of origin (Beckmann, 2020: Appendix C). Furthermore, data collections can directly influence the asylum decision by proving incentives to utilise this information. Biselli (2020: Appendix C) described one case where an employee used the applicant's facebook name to research the person on the said platform and to check whether the information found there could corroborate the applicant's claims: "[I]n the asylum file the evaluation of this facebook account could be traced where the person responsible at the BAMF said: 'Here, look, you liked the soccer club from country X but then said you are from [X], and this somehow does not quite fit in.'"[22] Effectively, this employee made a content analysis based on data derived from the read-out (Ibid.).

Whereas the Federal Office claims that the "storage of data generated by the BAMF for identity determinations of applicants is not a matter of data acquisition 'in stock' but rather a regulation with a clear and limited purpose of identity assurance. The storage of data (...) is, therefore, harmless in accordance with section 15a, subsection 1, sentence 2, Asylum Act seen in conjunction with section 48 subsection 3a of the Residence Act"[23], this assessment not only demonstrates the various types of data collected but, at the same time, suggests that in each of these categories a high amount

[22] Own translation. Original text: "[I]n der Asylakte war dann die Auswertung dieses Facebook-Accounts zu sehen, wo der Bearbeiter des BAMF gesagt hat: 'Hier, guck mal, du hast da den Fußballclub aus dem Land X geliked, aber hast dann gesagt, du kommst dann da her und das passt ja irgendwie nicht zusammen.'" (Ibid.).

[23] Own translation. Original text: "Bei der Speicherung der durch das BAMF generierten Daten zu Identitätssicherung von Antragstellern handelt es sich nicht um eine Datengewinnung 'auf Vorrat', sondern um eine Regelung mit klarer und eingegrenzter Zweckbestimmung der Identitätssicherung. Die Sicherung von Daten (...) ist daher unbedenklich nach § 15a Abs. 1 Satz 2 AsylG i.V.m. § 48 Abs. 3a AufenthG" (BAMF, 2018c: chapter 3.1).

of data is gathered and analysed. It is important to emphasise that through such advanced forensic data collection and analysis techniques, the Federal Office is gaining access to metadata and information that even the affected persons themselves cannot access by regular means (e.g. as a mobile phone user). Hence, individuals cannot anticipate what conclusions about their lives and identities can be drawn from the analysed amount of data. Especially without technical expertise, it is impossible to presume what kind of insights such technical interventions can pick up on. These factors not only add to the severity of the privacy intrusion but also put the persons in an even greater disadvantaged position when they are interrogated about the system's results and asked to verify or explain connections found in data. Overall, the analysis of mobile data devices contributes to creating what PRO ASYL coined as the "transparent refugee" ("gläserner Flüchtling") (Bartolucci, 2020: Appendix C). It remains unclear how these types and amount of personal data conclusively relate to the nationality of a person. It seems that this aspect is assumed by the Federal Office while no specific thoughts were given as to whether all data are necessary for the purpose.

4.3.4.4 Accuracy

The forth principle of privacy and data protection requires that collected personal information is accurate throughout the data lifecycle (UN General Assembly, 2018: para. 29). As shown in the previous analysis, the collected and processed data are not well-suited in relation to the desired aim because of flawed assumptions about complex social settings. Inaccuracy can further arise during the interpretation of data and results. In general, decision-makers are responsible for the usage and weighting of the system's reports. However, the assessment shows that guidance on how to interpret results of the three systems were insufficiently covered in the training manual and internal instructions. In 2017, IDM-S was introduced to regular and mandatory courses. For existing staff members a one-day seminar was included to the training portfolio (German Bundestag, 2017b: 7). This seminar was divided into several sections to cover all systems: 30 minutes each were spend on TraLitA and DIAS whereas 4,5 hours were allocated for the introduction to the analysis of data devices (BAMF, 2017a: Videoschulung). The course addressed both technical basics and practical applications of IDM-S (German Bundestag, 2018d: 5).

Regarding TraLitA, no in-depth indications on the calculation of results or their limitations are given (BAMF, 2018c: chapter 3.4). Interpretations for the automatic dialect recognition include only marginal information. Technical details, such as the Log Likelihood Ratio - a scientific measure to indicate how well a dialect is recognised - are not explained. The signal-to-noise ratio, which compares the level of background noise with that of the desired speech, is marked as "not relevant" ("nicht relevant") (BAMF, 2017a: Sprachbiometrie, Ablauf). While probability distributions across different dialects are presented, it is not explained how meaningful these values are and what they mean in practice (Ibid.). If decision-makers find themselves in stressful situations, have to consider various asylum cases in a short period of time, and do not know how to interpret these numbers, they might be tempted to believe the system's results (Biselli, 2020: Appendix C). Contrary to the implications that decisions are not based solely on these reports, a small request revealed that "the spoken dialect is often - in addition to the information provided by applicants - the only indication of their origin."[24]

[24] Own translation. Original text: "(...) der gesprochene Dialekt [stellt] neben den Angaben der Antragsteller häufig das einzige Indiz für deren Herkunft [dar]" (German Bundestag, 2018a: 15).

Regarding the analysis of mobile devices, the training manual lists four circumstances to be considered in order to assess the significance of the information contained in the final reports. These include: how data is stored on the device (smartphones contain more information than feature phones), how it was used and for how long, in addition to what type of data was read-out (BAMF, 2017a: Auslesen von mobilen Datenträgern, Ergebnisreport). Considering the use cases presented in the manual, it seems that simplified claims were made to break down complexity. For example, it is mentioned that the longer the device was in use, the more meaningful the report is. Another case suggests that the more data is gathered, the more valid the report will be (Ibid.). However, the significance of the data in relation to its general aim, namely to indicate a person's identity and origin, is not reflected upon. The highest validity of a report is given to cases where a high variety of applications was read out. It remains unclear which apps have higher or lower validity compared to others. In these cases, instructions are given to investigate different identities used in various timeframes (Ibid.). It is not clarified how these investigations are carried out and what boundaries exist.

At the time of writing, it could not be determined whether the quality of trainings has improved over the last two years (Biselli, 2020: Appendix C). Nevertheless, these few examples indicate that insufficient training measures can cause additional inaccuracies in the decision-making process. In this regard, the Federal Office states that if discrepancies between the individual's claims and the system's results occur, the persons affected get the opportunity in the personal hearing procedure to prove that their claims are true (BAMF, 2018k: chapter 1). In general, the issue with potential corrections is that decision-makers are not obliged to make references to results of the reports. In other words, they can but don't have to - this depends on the individual deliberation of the person in charge (Beckmann, 2020: Appendix C). In cases where discrepancies in reports are explicitly or implicitly addressed, it is not guaranteed that affected individuals fully understand the reason or source of doubt - especially because they are not properly informed about the IDM-S proceedings beforehand. As a general rule, asylum applicants are not allowed to see the generated reports - unless they are accompanied by their lawyers which is not the case for the majority of asylum seekers (Beckmann, 2020: Appendix C; BAMF, 2018k: chapter 2; BAMF, 2018c: chapter 3.1.5).

4.3.4.5 Security measures

The vulnerability of information that asylum seekers hand over for processing require the provision of sufficient security measures and safeguards (UN General Assembly, 2018: para. 29). Such safeguards might include physical (e.g. locked doors), organisational measures (e.g. access control, implementation of data protection), and technical precautions (e.g. encryption, anonymisation, pseudonymisation) to ensure adequate protection (Privacy International, 2018: 45).

The available documents provide marginal details on existing security measures. For the analysis of data devices instructions are given to lock doors of the relevant (server) rooms. The administrator's laptop has to be placed in a lockable cabinet (BAMF, 2017a: Auslesen von mobilen Datenträgern, Nutzung). For all three systems, the Federal Office seems to use pseudonymisation to replace individuals' names when data is collected (BAMF, 2017a: Namenstranskription, Nutzung; BAMF, 2017a: Sprachbiometrie, Nutzung; BAMF, 2017a: Auslesen von mobilen Datenträgern, Ablauf der Datenextraktion). Personal information of asylum applicants is stored in the main MARiS file system at the Federal Office (BMJV, 2016: Asylum Act, section 16, subsection. 1). The latest report of the BfDI (2019: 75) which evaluated MARiS from a data protection and privacy perspective indicated several flaws. However, recommendations were adopted promptly in that access management was improved, more sophisticated access restrictions were implemented and additional security measures were installed to ensure protection of especially sensitive data. At the end of 2018, these implementation were in their final stages (Ibid.).

While reports of the name transliteration and analysis system as well as the automatic dialect recognition are directly transferred to MARiS, those of the analysis of mobile devices are first stored in the so-called "data safe" ("Datentresor") (BAMF, 2017a: Auslesen von mobilen Datenträgern, Nutzung). According to internal instructions, these reports are protected from access by third parties. Further specifications are not provided (BAMF, 2018c: chapter 3.1). In general, access to this safe is managed by administrators (German Bundestag, 2018a: 23). Lawyers eligible for judicial office who approve the reports for decision-makers get access after providing proof of their qualifications (BAMF, 2018c: chapter 3.1.3). Upon receiving formal access requests from decision-makers, the said lawyers carry out a "necessity and proportionality" ("Erforderlichkeit und Verhältnismäßigkeit") assessment and record their resulting decisions (BAMF, 2019i: D1706; BAMF, 2018c: chapter 3.1.3). A negative decision leads to the denial of access. In case of a positive assessment, the report is transferred to MARiS and made available to the decision-maker in question (BAMF, 2018c: chapter 3.1.3). Reports temporary stored in the "data safe" are deleted in both cases - if access is denied and if reports are transferred to the main file system (Ibid.). By using the formalised request procedure and a ticketing system, the deletion of data is recorded. Deletion can be requested by lawyers and those decision-makers who conclude that they do not need the report in the first place (BAMF, 2018c: chapter 3.1.4). While the role of the fully-qualified lawyers is intended as a control and security measure to safeguard sensitive information of asylum seekers, practice shows that this already low degree of protection can be entirely bypassed, namely if decision makers are themselves lawyers (BAMF, 2018c:

chapter 3.1.3). Beckmann (2020: Appendix C) confirmed in the interview that she encountered a case where the person in charge for asylum decisions unlocked the protected report for him or herself. This effectively means that in such cases no additional safeguards apply.

4.3.4.6 Accountability

The final principle of privacy and data protection requires that those who collect and process personal data are accountable for their compliance with existing legal frameworks, principles and obligations (UN General Assembly, 2018: para. 29). Actors "must be able to explain, show, and prove that they respect people's privacy" (Privacy International, 2018: 46).

On the one hand, the previous findings demonstrated that the Federal Office's way to communicate, explain and prove compliance with privacy regulations concerning the use of IDM-S was neither open nor proactive. At the time of writing, in-depth information about the digital identification systems was not available, for example, on the ministry's website. IDM-S is mentioned primarily in relation to press statements (event-based) and the digitalisation agenda, emphasising in-house technical innovations (BAMF, 2017d; BAMF, 2019a; BAMF, 2020n). The lack of transparency directly affects accountability: The Federal Office seems to be unwilling to engage meaningfully with the public forum concerning its practices. On the other hand, it remains difficult for affected persons to hold authorities accountable. Counselling sessions organised by the Federal Office are not independent and referrals to lawyers specialised in asylum legislations are not provided (Bartolucci, 2020: Appendix C). The analysis showed that asylum seekers are unlikely to file complaints against authorities who violate their right to privacy. A request to the BfDI (2020: Appendix D.2, 1) demonstrates that not a single complaint was issued by asylum seekers since the analysis of mobile devices was implemented in 2017 (Beckmann, 2020: Appendix C). Due to fear of potential consequences in regard to asylum decisions, it can be assumed that individuals do not want to put themselves at additional risks by being vocal about their experiences or potential injustices that they encountered during asylum procedures. In uncertain circumstances related to asylum status, it seems reasonable that asylum seekers are primarily concerned with the outcome of their asylum application (Bartolucci, 2020: Appendix C). For the preparation of the law suit against the Federal Office's analysis of mobile data devices, it took a long time to find suitable cases and individuals willing to go through the lengthy process (Ibid.; Beckmann, 2020: Appendix C). Even in a successful scenario, Beckmann (2020: Appendix C) estimated that it might take more than six years to clarify this issue and hold the Federal Office accountable - which is why the government has a special responsibility for ensuring fundamental rights protection during the legislative process.

4.3.4.7 Alternative and less intrusive measures

Under the ICCPR, privacy-interfering measures must be the least intrusive options available to comply with the principles of proportionality (UN General Assembly, 2018: para. 10; UNHCR, 2010). Regarding IDM-S, no public information is available on whether an analysis of alternative measures was carried out prior to the development of the digital systems. It is also unclear whether existing mechanisms were evaluated to understand how they could be improved to better serve the purpose of determining and verifying identity and nationality of individuals seeking asylum. According to Bartolucci (2020: Appendix C), such alternatives could include the use of different questioning techniques to better assess the country of origin during the personal hearing. Instead of handing over their mobile phones, applicants could be asked to provide specific pieces of information stored on their device (Ibid.). As IDM-S is intended to collect information which is used in preparation for the hearing procedure, the hearing itself is not considered a less intrusive option of identity determinations (BAMF, 2018c: chapter 3.1).

While the legal foundation of the analysis of data devices provides that the measure should only be used if less intrusive options were exhausted, practice shows that these lenient means were not thought out. Internal instructions clearly outline that all three IDM-S systems are applied in parallel and independently (BAMF, 2018c: chapter 3.1). BAMF clarifies therein: "Eventually, only those documents that can prove the identity by means of a photograph and that can be examined for their authenticity by the Federal Office can be considered as lenient means."[25] As the previous analysis showed, documents need to pass the first stage of PTU - only then mobile devices are not read out (Beckmann, 2020: Appendix C; Biselli, 2020: Appendix C). This effectively means that - apart from the passport which is the standardised procedure - there are no less-intrusive measures that the Federal Office actually resorts to. Similar rules apply in regard to the automatic dialect recognition: According to internal instructions it is used unless a passports or passport replacement - which is considered a lenient option - can be checked and confirmed as valid without doubts (BAMF, 2018c: chapter 3.2; BAMF, 2017a: Sprachbiometrie, Ablauf; BAMF, 2018i).

Apart from this digital recognition to determine the spoken dialect of asylum applicants, the Federal Office can also commission language experts to carry out a scientific speech and text analysis (S-T-A, "Sprach- und Textanalyse") in cases of doubt (BAMF, 2018c: chapter 4). The process requires a speech recording of about 30 minutes (German Bundestag 2017d: 7). Compared to results of the automatic dialect recognition, these expert reports are legally binding and can be used as evidence in the court of law (German Bundestag 2017d: 7). When asked to justify this new digital approach to speech assessments, the government (Ibid.) argued that the automatic analysis represents an "independent, objective and scalable method" ("unabhängige, objektive und skalierbare Methode") to determine the origin of an affected person "by easy means" ("mit einfachen Mitteln"). The difference between two and 30 minutes speech recordings stems from the circumstance that during S-T-As several speakers are recorded (e.g. the

[25] Own translation. Original text: "Als mildere Mittel kommen letztendlich nur Dokumente in Betracht, die durch ein Lichtbild die Identität belegen können und vom Bundesamt auf ihre Echtheit überprüft werden können" (BAMF, 2018c: chapter 3.1).

asylum applicant, interpreter, decision-maker). Therefore, as claimed by authorities, speech recordings require special expert evaluations (Ibid.). In general, S-T-As are more established in identity determination proceedings than their digital counterparts. As this method relies on the availability of experts and causes substantial costs, internal instructions at the Federal Office indicate that its use should only be limited to a few exceptional cases (BAMF, 2018c: chapter 4; BAMF and BFM, 2017: 4). Contrary to what the Federal Office seems to imply, its internal communication suggest that DIAS was used to replace S-T-As. Applicants, whose language assessments were still due, were subjected to the automatic dialect recognition instead (BAMF, 2018n; cf. Appendix E; Biselli, 2020: Appendix C). In regard to the use of the automatic dialect recognition, the government indicated: "In many cases, the use of the tool prevented more complex and expensive language assessments to be commissioned."[26]

[26] Own translation. Original text: "Durch den Einsatz des Tools konnte in vielen Fällen verhindert werden, dass wesentlich aufwändigere und teurere Sprachgutachten in Auftrag gegeben werden mussten" (German Bundestag, 2018a: 15).

5 Results and discussion:

Patterns of (il)legitimacy

The assessment of available documents, internal instructions and expert interviews by means of the qualitative content analysis and the data justice framework provided valuable insights into the main research question: How does the Federal Office legitimise the policy and use of the digital identification system "IDM-S" as part of a new direction of governance in the context of asylum? To answer this question, this section summarises the main justifications for policy decisions in relation to state actions to account for word-deed tensions in the studied political setting. These findings are structured according to the main identified patterns of (il)legitimacy and interpreted by referring to the theoretical frameworks.

5.1 Referring to the rule of law and public interests

The first identified pattern refers to the features of political legitimacy, most notably to legal references on the input level. According to the theoretical concept, decisions laid down in policies are legitimate, if they are recognised as lawful, just and rightful (Morris, 2008). Legitimate decisions are those that are based on the rule of law, justified by references to common interests and beliefs, and confirmed by the public through the expression of consent (Beetham, 1991: 20).

The introduction of the analysis of mobile data devices as part of the Act to Improve the Enforcement of the Obligation to Leave the Country was criticised the most in the media and among legal experts. Therefore, the Federal Office was more eager to justify the compliance of this new measure with the rule of law. Because the legislative procedures provide for well-defined steps that have to be followed to introduce new legislations, the analysis of mobile devices needed to be negotiated in the parliament - a process that made justifications and legal references particularly visible. For example, the written statement of the Federal Office included a "legal assessment" ("rechtliche Bewertung") (Richter, as cited in German Bundestag, 2017a: 103). It emphasised the right of the legislator to react to situation where asylum was not only "requested in bulk" ("massenhaft beantragt") but was "unjustifiably desired" ("ungerechtfertigt begehrt") in order to obtain residence rights (Ibid.). While this assessment did not go into (evidential) details and did not depict the legal obligations of the state towards asylum seekers, further arguments included the reference to permitted, legal interferences with the right to privacy. It was repeatedly argued that the new measure was lawful because it is applied only if other lenient means are exhausted ("als äußerstes Mittel") and only to individual cases of doubt ("Einzelfälle") (Ibid.: 20; Ibid.: 30; German Bundestag, 2020f: 35). For representatives of the Federal Office, it was important to emphasise that the read-out and analysis would only refer to "metadata" ("Metadaten") and not to the content (Richter, as cited in German Bundestag, 2017a: 39). These arguments imply that the domain of correspondence, protected under Art 17 ICCPR, as well as the integrity and confidentiality of its various means of communication are not affected by the interference on the content-level. Additionally, the Federal Office tried to legitimise the analysis of data devices by making references to national security laid out as a public interest. This measure was promoted as an instrument that would increase safety through the prevention of fraud early on in the asylum process - that is at the level of identity determinations (Ibid.: 104). Such references were not only made during the legislative process. Moreover, it was argued that all three measures of IDM-S combined would contribute to fraud prevention and, hence, to public safety (BAMF and BFM, 2017: 3; BAMF, 2020g; BAMF, 2019d; BAMF, 2017b; BAMF, 2020n).

Furthermore, it was argued that the governance approach relating to IDM-S was not only lawful per se but that procedures and norms were de facto followed correctly, indicating compliance with existing rules during the implementation. Regarding possible application errors concerning the automatic dialect recognition addressed in small requests, the government emphasised that it had no knowledge that established rules were not followed correctly (German Bundestag, 2018d: 6). Internal instructions on the analysis of mobile devices underlined that the "storage of data generated by the BAMF for identity determinations of applicants is not a matter of data acquisition 'in stock' but rather a regulation with a clear and limited purpose of identity assurance. The storage of data (...) is, therefore, harmless in accordance with section 15a, subs. 1, sentence 2, Asylum Act seen in conjunction with section 48 subs. 3a of the Residence Act."[27] These repeated references to the legal foundation and the wording can be perceived as a reaction to public criticism that certainly had de-legitimising effects. Relevant groups raised well-founded criticism, including the BfDI as the federal supervisory authority for data protection, legal scholars, civil society organisations and the media. The filed lawsuit against the practice of the Federal Office headed by the GFF can be interpreted as a form of disobedience, the withdrawal of consent and general refusal to accept the practice which was deemed unconstitutional and non-compliant with fundamental rights (Biselli and Beckmann, 2020; DW, 2020). These examples clearly indicate the importance of legality concerning state conduct that was communicated most dominantly in the legislative process but also in internal documents. However, it seems that once the new law passed, the Federal Office did not see further need to *publicly* and

[27] Own translation. Original text: "Bei der Speicherung der durch das BAMF generierten Daten zu Identitätssicherung von Antragstellern handelt es sich nicht um eine Datengewinnung 'auf Vorrat', sondern um eine Regelung mit klarer und eingegrenzter Zweckbestimmung der Identitätssicherung. Die Sicherung von Daten (...) ist daher unbedenklich nach § 15a Abs. 1 Satz 2 AsylG i.V.m. § 48 Abs. 3a AufenthG" (BAMF, 2018c: chapter 3.1).

proactively demonstrate the lawful application of the measures - after all, the identified references in regard to the implementation were made internally and only if specifically addressed in small requests. Indeed, the analysis showed severe discrepancies between words that seem to depict the desired state of affair (e.g. legal compliance) and deeds that indicate how the policy was enacted on the ground.

As the studied IDM-S systems are deployed to collect and process personal, unique physical and behavioural characteristics depicted in metadata, the underlying measures cause an interference with the right to privacy protected by Art 17 ICCPR. At this point, it makes no difference whether the interference is carried out by a human being or a machine because of similar results: The persons lose control over their information that puts their privacy at risk. Because metadata can give insights into individuals' behaviours, personal preferences and social relationships, using it is not as harmless as the Federal Office suggests. Although with varying degrees, compliance issues are present in regard to all six key principles that outline the minimum requirements of data and privacy protection. The use of all three IDM-S systems demonstrates issues relating to consent. To be protected by the host state and to access crucial services, individuals must provide their personal information upon request. Such actions are not

Because metadata can give insights into individuals' behaviours, personal preferences and social relationships, using it is not as harmless as the Federal Office suggests. Although with varying degrees, compliance issues are present in regard to all six key principles that outline the minimum requirements of data and privacy protection.

based on (freely given) consent but pertain to the legal norm to cooperate that was expanded to include the submission of mobile devices for read-out and analysis. At the same time, the Federal Office does not adhere to its transparency obligations as affected individuals are not adequately informed about the three IDM-S systems even at a basic level concerning the type of personal data collected, how it is processed and used in decisions. Informed consent requirements amount to empty administrative acts in regard to the analysis of data devices and the automatic dialect recognition, where additional detailed information is neither given in written nor in verbal form but is reduced to a signature that implies that explanations were given. In the case of the name transliteration and analysis no information is provided, leading to the well-founded concern that asylum applicants are not aware about the analysis of their names in relation to their origin. Furthermore, it remains unclear how the types of data collected and processed by all three systems conclusively, scientifically and rationally relate to the nationality and origin of a person. Given the lack of accuracy and effectiveness - meaning that gathered data provide rather vague and more flawed than reliable indications of origin - the overall usefulness of IDM-S' functions related to the determination and verification of nationality has to be fundamentally questioned.

Findings outline that the analysis of mobile data devices is the most privacy-intrusive system of the three IDM-S components. They reveal that this measure is applied too broadly in practice, including to individuals who are in possession of a passport but cannot immediately present it or whose documents cannot be authenticated by available means early on in the asylum process. In effect, reasons and situations for which asylum applicants are not themselves responsible are construed to their disadvantage. The measure greatly violates further against the principle of minimisation because not only various types of data are collected but also a high amount of information in each identified category is gathered. The prevailing idea seems to be that all data from the identified sources on mobile devices are made accessible to authorities. At the same time, information extracted from apps - such as user names - provide incentives to conduct unlawful, content-based analysis. The investigation of an asylum applicant's personal facebook account by a staff member of the Federal Office clearly demonstrates the existence of factual risks of misconduct once sensible, personal information - even in the form of metadata - is accessible. Additionally, the assessments of the fully-qualified lawyer, whose role is intended as a security measure to prevent breaches of privacy, does not amount to a reliable, independent, and impartial entity to ensure procedural safeguards. The analysis shows that this already low degree of protection can be easily bypassed if lawyers are themselves decision-makers. Overall, such intense privacy-interferences based on the analysis of data devices are carried out unlawfully as they are un-necessary in this extent, un-proportionate to their aim, and do not take into account other less-intrusive options to determine and verify the identity of individuals.

While Germany is generally considered a country with strong privacy-related awareness and protection, the state practices prove that much lower standards for respecting the core area of private life are applied concerning asylum seekers. Effectively, they are the only group subjected to such measures without demonstrating evidence for fraud and ensuring proper safeguards in the form of independent, judicial evaluations. It causes great concerns that the Federal Office for Migration and Refugees does not seem to act impartially but rather seeks to promote a political agenda. Intentions became apparent in particular by noticing aspects that were not mentioned, such as the state obligation to protect asylum seekers' rights. One could argue that the Federal Office only applies the laws that were put in place by the legislator. However, this seems to be a rather bureaucratic justification that seeks to morally relieve those in power from their responsibilities under international law and the constitution. The analysis shows that the Federal Office a) did take part in the legislative proceedings,

> While Germany is generally considered a country with strong privacy-related awareness and protection, the state practices prove that much lower standards for respecting the core area of private life are applied concerning asylum seekers.

b) did influence them by the choice of statements and arguments made, and generally c) has a certain margin of discretion in regard to the interpretation of laws. Considering these circumstances, the Federal Office is (likewise) responsible for any rights violations that result from its actions and operational priorities. At this point it is valuable to refer back to Rothstein (2008: 15) who argued that life-threatening actions magnify the erosion of legitimacy. While the introduction of laws and the formal adherence to legislative proceedings provide an important basis for legitimate state practices if they are in line with international laws and fundamental rights, what further matters is how governmental institutions *exercise* their powers. Compared to the input side, less emphasis was put on ensuring procedural qualities in regard to throughput and output legitimacy.

5.2 Non-disclosing delegitimising information and limiting accountability

The second identified pattern refers to the non-disclosure of information that could potentially delegitimise the use of IDM-S. Political decisions are perceived as legitimate, if certain qualities in governance processes are respected by powerful actors. In regard to throughput legitimacy, these qualities pertain, among others, to transparency and the free flow of information. Legitimacy is enhanced through dialogue and trust-building by providing enough information in a proactive and accessible manner (Schmidt, as cited in Schmidt and Wood, 2019: 729-730). In this regard, the performance of the Federal Office was insufficient. The lack of transparency remains a major issue that also affects accountability, as the findings of the analysis portray.

While the Federal Office repeatedly emphasised how it values and fosters transparency (Richter, as cited in German Bundestag, 2017a: 20-21; Richter, as cited in Frank, 2018: 22), the analysis shows that the implementation of the three IDM-S systems is seen exclusively as an internal affair. Transparency relates first and foremost to the internal flow of information between departments and chosen partners (e.g. EU member states, commercial entities). In contrast, the exchange with the public was strictly controlled: Communication was hesitant, restrictive and shaped by the general unwillingness to provide comprehensive answers to both public and press enquiries. Compared to other governmental institutions, the Federal Office was less willing to provide information for critical up-to-date reporting, creating barriers for journalistic work. Likewise, freedom of information requests on the functioning of IDM-S were not answered in full, either delayed or rejected (BAMF, 2018i; BAMF, 2020i; BAMF, 2019e; BAMF, 2019f; BAMF, 2019g). More in-depth explanations revealing some aspects of decision-making processes were by large provided as part of small requests to which the government has the obligation to reply. In these cases, questions were answered in a shortened form that complicated further enquiries into the subject matter (BMI, 2018b; German Bundestag, 2017b). Additionally, certain information was misleading and evasive as the Federal Office and the government tried to conceal commercial partners to avoid public scrutiny. Authorities also sought to create the impression that IDM-S was subject to scientific evaluations by referring to cooperations with the University of Pennsylvania which revealed solely a commercial transaction (German Bundestag, 2017b: 5; German Bundestag, 2018a: 14; BMI, 2018b). Contradictions of statements occurred in relation to the systems' impact on asylum decisions. While it was emphasised that IDM-S only supports decision-making, a small request demonstrated that results of the automatic dialect recognition are often the only indication of origin apart from asylum applicant's claims (German Bundestag, 2018a: 15). At the same time, proactive communication by the Federal Office as part of press releases and interviews, for example, was shaped by an overwhelmingly positive tonality regarding IDM-S governance (BAMF, 2017b; BAMF, 2017d; BAMF, 2017c; BAMF, 2018j). This strong contrast between critical public reporting and the Federal Office's positive way of communication indicate the ministry's aspired political gains: Communication is used primarily for own benefits (e.g. demonstrating the self-image of a vigorous authority) instead of engaging in the meaningful dialogue over policy decisions. Considering that the Federal Office was the focus of public criticism for poorly handling asylum applications, it seems that the deliberate approach was to rely on the secrecy of information in order to avoid the disclosure of inconsistencies in the Federal Office's practices, critical reporting and public debate, especially, before the parliamentary elections. The lack of transparency limits external validations of practices around IDM-S and the traceability of the systems' actual impacts and harms on affected individuals.

Justifications for the non-disclosure of information referred mostly to reasons of confidentiality and national security, among others (BAMF, 2020i; BAMF, 2019e; BAMF, 2019f; BAMF, 2019g). Yet, it seems that these justifications are applied too broadly. While the question whether the invoking of national security grounds is justified deserves separate investigation, the findings indicate that an overwhelming amount of information on the IDM-S policy and practice was not disclosed, ranging throughout various areas of public interests, such as statistics, algorithmic functioning, privacy risks, cost-benefits, evidence-based and independent evaluations. Even if national security grounds apply, states must respect the public's right to information, especially, if the disclosure of information concerns the violation of human rights and the exposure of wrongdoing or abuse of state power - as, for example, the Global Principles on National Security and the Right to Information outline (Open Society Foundations, 2013: 11-13). The over-invocation of national security concerns can seriously undermine the rule of law, press freedom, accountability, privacy and related human rights (Ibid.: 6).

> Findings indicate that an overwhelming amount of information on the IDM-S policy and practice was not disclosed, ranging throughout various areas of public interests, such as statistics, algorithmic functioning, privacy risks, cost-benefits, evidence-based and independent evaluations.

Eventually, the analysis demonstrates that only marginal, fragmented statistics and a limited amount of indicators were used to monitor and document the implementation of IDM-S (e.g. how often the systems were applied, if results matched the applicants' claims). Hence, these numbers do not provide meaningful, critical insights into the effects of the systems, in particular, on experiences and (un)intended impacts of asylum applicants who undergo the identity determination procedure. Notably, it is not assessed if the systems' results negatively influence asylum decisions (German Bundestag, 2018a: 13; German Bundestag, 2018d: 7; German Bundestag, 2019b: 14; German Bundestag, 2020f: 35). This perspective is ignored, despite publicly known cases that confirm such influence, leading to unjust asylum decisions. It seems that the Federal Office and the government turn a blind eye on the cases that do not fit the overall success narrative which is emphasised in relation to IDM-S. Authorities seem to assume that if information is not collected in the first place, it cannot be shared and, thus, it cannot be used to discredit the policy and practice. These examples show that decisions about how programs are measured, evaluated and assessed are inherently political - and in this case they are used to bypass accountability towards the public and asylum seekers who are required to reveal their entire "digital household" while the public administration does not adhere to the most basic transparency and accountability standards expected in democratic societies.

> Decisions about how programs are measured, evaluated and assessed are inherently political - and in this case they are used to bypass accountability towards the public and asylum seekers who are required to reveal their entire "digital household" while the public administration does not adhere to the most basic transparency and accountability standards expected in democratic societies.

5.3 Implying performance efficiency and IDM-S' high level of innovation

The third identified pattern indicates that the Federal Office was seeking to legitimise its approach by referring to the advantages of IDM-S primarily for internal processes and the administration's performance, most notably efficiency. Political decisions about policies and practices gain legitimacy, if they are able to produce outputs and outcomes that remedy collective problems. On the level of output legitimacy, the usefulness of IDM-S in regard to its aims was highlighted. As the Federal Office was seeking to establish itself as a tech-savvy administration - a self-proclaimed "leader in technology" ("Technologieführer") (BAMF, 2018b) - justifications referred to the systems' efficient results because of its high level of innovation.

Even if setting aside the inconsistent and fragmented performance statistics, the evaluation of the three IDM-S systems showcases unreliable and poor results in regard to their aim, which holds true for the name transliteration and analysis as well as the analysis of mobile data devices. Because references to the applicants' origin based on TraLitA were vague and in the majority of results not verifiable, the success narrative focused rather on its transliteration function (Richter, as cited in Frank, 2018: 24; German Bundestag, 2018a: 26). The analysis of mobile data devices - as the most cost-intensive measure in the IDM-S portfolio - is likewise flawed as the majority of all considered reports produced no usable results (German Bundestag, 2018a: 20; German Bundestag, 2020f: 34-35). Yet, the Federal Office holds on to these methods. No conclusions are drawn from the systems' de facto ineffectiveness. Instead, the analysis of data devices is seen as a "fast and straightforward" ("schnell und unkompliziert") (Richter, as cited in German Bundestag, 2017a: 103) instrument compared to other, more established methods like S-T-As that are considered as complex, cost-intensive and associated with long processing times. This line of reasoning points to the assumed usefulness of IDM-S in identity verifications by referring to financial savings, the systems' easy application, and the reduction of workload. The Federal Office claims: "The read-out of mobile data devices is currently the most important instrument for identity verifications."[28] On the one hand, facts and insufficiencies in regard to the systems' performance are ignored. On the other hand, criticism is brushed aside by underlining that the three digital systems *only* support the decision-making processes but do not make the final asylum decision which is done by decision-makers who have the upper hand (German Bundestag, 2018a: 26; BAMF and BFM, 2017; BAMF, 2018c). By implying that human beings control the results of "the machine" seemingly without influence, it is not seen as a legitimacy problem in itself that the systems are by large ineffective and de facto able to unjustly influence asylum decisions.

To promote the performance success of IDM-S as an innovative approach to governance problems, the Federal Office primarily referred to the automatic dialect recognition as an example - most likely because it

> By implying that human beings control the results of "the machine" seemingly without influence, it is not seen as a legitimacy problem in itself that the systems are by large ineffective and de facto able to unjustly influence asylum decisions.

[28] Own translation. Original text: "Das Auslesen mobiler Datenträger stellt momentan das wichtigste Instrument zur Identitätsüberprüfung dar" (BAMF, 2020j: 2).

produces the highest (average) success scores of all three IDM-S components from a technical perspective. Nevertheless, in regard to the severity of potential consequences that wrongful asylum decisions cause, it has to be questioned why an (average) error rate of 15 percent is politically accepted in this context. A notable factor that the analysis revealed pertains to settings that are considered a success in relation to the automatic dialect recognition, including being the first public administration worldwide to use such an innovative system, having developed the approach within only six months, having used agile development methods and having fostered digitalisation in public administrations (German Bundestag, 2017b: 2; German Bundestag, 2018a: 15; BAMF, 2018j; Richter, as cited in Frank, 2018: 24). While these results are promoted by the Federal Office by means of self-attributions, efforts are made to legitimise this approach by seeking out external acceptance. The winning of the e-government award in the category "Best Digitalisation Project 2018" ("Bestes Digitalisierungsprojekt 2018") (BAMF, 2018j) for the automatic dialect recognition is used as an example of public confirmation for the Federal Office's practices and so are requests from interested authorities of other countries which are, however, not further specified (German Bundestag, 2018a: 15; Richter, as cited in Frank, 2018: 22; BAMF, 2019a: 32). According to Beetham (1991: 18), actions that provide evidence for consent make contributions to legitimacy through their "publicly symbolic or declaratory force". Receiving the award enables authorities to demonstrate the confirmation of their actions to third parties (e.g. the public at large). What seems to be important to consider at this point is that actions of the Federal Office are legitimised as valid by commercial entities with economic interests who profit from the public sector's use of ICTs through not least the provision of technical infrastructure. Therefore, the extent of this legitimised action confirmed through the award needs to be questioned.

The strong emphasis on innovation, agility and efficiency is congruent with the framework of new public management, more specifically with notions of an "entrepreneurial government" (Osborne, 1993: 352) which adopts the rationale of the need for private sector management methods and market mindset in public administrations. In this studied governance case, business terms en vogue are adopted seemingly without critical deliberations and without sufficiently recognising the own role in the governance arrangement, including prioritising state obligations in regard to the protection of asylum seekers' (privacy) rights and the acknowledgement of their vulnerable status in institutionalised processes of decision-making. The findings suggest that with the focus on "innovation" and "agility" has come a tendency to take over the logic of business - that is emphasising product-development and accepting a risk-taking culture. The problem with this trial-and-error-driven approach for the sake of "innovation" is that asylum seekers are often those bearing the actual costs and consequences when failure occur - in worse cases they pay with their lives. Fostered by the sense of urgency that without doubt put intense pressure to act on the Federal Office since 2015, it seems that IDM-S was implemented as a development shortcut, solving big problems faster without being grounded in established theoretical and scientific evaluations. However, "efficiency" - no matter if time-, process-, or finance-related - cannot be regarded as a stand-alone value but has to be linked to the progressive realisation of

> With the focus on "innovation" and "agility" has come a tendency to take over the logic of business - that is emphasising product-development and accepting a risk-taking culture. The problem with this trial-and-error-driven approach for the sake of "innovation" is that asylum seekers are oftentimes those bearing the actual costs and consequences when failure occur.

democratic governance principles, such as transparency, participation and accountability - which was not the case both in regard to the legislative proceedings and even less so in implementation as demonstrated in the analysis. Additionally, intentions to simplify internal processes and to reduce work load do not justify encroachments of fundamental rights and the deployment of privacy-invasive systems as was pointed out by the BfDI (2017: 102). Glorifying digital systems as “the” solution fails to recognise that persistent, socio-political problems may not need innovative, technical solutions but rather require “committed long-term engagement that enables steady and less risky progress” (Seelos and Mair, 2012: 47). Likewise, it is ignored that high productivity is often based on careful evaluations of existing practices that enable improvements and learning over long(er) periods of time (Ibid.). Justifications of the Federal Office reveal the misleading assumption that innovation can *only* lead to successful outcomes: Accepting the failures and stepping away from the use of IDM-S seems not to be an option - because it is not congruent with adopted ideas and narratives of success. Instead, the systems are being developed further driven by political desires that come with new possibilities of data collection and processing, showing first sings of function creep. While the evaluation for the legal and technical extension of the analysis of data devices is under review, TraLitA and DIAS are promoted to European states for the purposes of refugee management and border control (German Bundestag, 2017b: 5; BAMF, 2018b; German Bundestag, 2018a: 22; Richter, as cited in Frank, 2018: 24). Such efforts indicate not only that asylum seekers’ privacy rights are ignored domestically by the use of IDM-S but that they are accepted elsewhere through the regional promotion.

5.4 Implying objective operations by means of a mathematical-technical approach

The final identified pattern is closely intertwined with references to performance efficiency as well as innovation and relates both to throughput and output legitimacy. According to good governance and legitimacy theory, administrative structures and procedures follow scientific standards and operate logically as well as rationally in order to constructively address collective problems (Keping, 2017: 6; Graham, Amos and Plumptre, 2003: 3; Kioe Sheng, 2009; Schmidt, as cited in Schmidt and Wood, 2019: 729-730). To increase political legitimacy, IDM-S was promoted to reproduce the impression of rational and scientifically robust operations - despite the lack of profound evidence and independent, scientific proof not only for the effectiveness of IDM-S but, especially, for the underlying assumptions and hypothesis that guided the development and implementation of the programme in the first place. Internally towards its staff and externally towards the public, justifications of the Federal Office suggested that the systems' results were precise and objective because of the advanced mathematical formulae and technical precision used to arrive at conclusions. Findings underline that the deployment of IDM-S was shaped by prevailing fallacies common in the public sector's use of ICTs, including the belief that digital systems provide objective results, that mathematical attributes and programming code can adequately depict the complexity of the real world and that digital systems can be applied universally as the primary solution to remedy governance problems related to asylum and migration.

From the perspective of state authorities, the automatic dialect recognition represents an "independent, objective and scalable method" ("unabhängige, objektive und skalierbare Methode") (German Bundestag 2017d: 7) to determine the origin of an affected person. This reference to a seemingly independent and objective approach blurs the fact that the government is the most powerful actor in the stakeholder ecosystem who deliberately chose to apply IDM-S based on beliefs and interests that serve political ends. While these intentions were not always immediately visible, all three systems follow the same questionable logic, namely to determine the identity and nationality of individuals without passports based on automated, rather vague allocations of collected data. The political agenda relating to IDM-S was seen most vividly in debates about the Act to Improve the Enforcement of the Obligation to Leave the Country which aimed at enhancing possibilities of repatriations. The identified barriers put on asylum seekers, such as extending the legal obligation to cooperate and being suspected of misleading authorities in identity determination procedures to receive residence status, corroborate these findings (Richter, as cited in German Bundestag, 2017a: 104).

Given sufficient data and information, it is assumed from a technocratic perspective that every problem can be controlled, modelled and estimated by means of data analysis and standardisation in order to reveal “potentials of misuse” (BAMF, 2018b). In this regard, the Federal Office repeatedly argued that the new systems provide “additional data points” (BAMF, 2017a: Sprachbiometrie, Übersicht) and “technical leads” (BAMF and BFM, 2017: 6) to support decision-makers in reaching more solid and better conclusions in asylum cases. However, the analysis showed that the highest financial investment was made into the technical development of IDM-S, its infrastructure, maintenance and support. On the contrary, training of decision-makers relating to the interpretation of the systems’ reports was insufficient and fragmented. The actual decision-making process in light of the systems’ results is left to the discretion of individual employees whose considerations cannot be traced. If decision-makers are ill-equipped to understand the processes of data collection and processing including the systems’ limitations and flaws - especially when frequency statistics and probabilities contained in the systems' reports imply reliability and accuracy - it seems reasonable to believe that they will less likely question the automatically generated results that appear objective and are communicated as such.

The strong belief in mathematical precision and the possibility to depict complex social settings in precise programming code leads to leaving important aspects of reality entirely outside of the systems' design (Green and Viljoen, 2020: 22). While the Federal Office acknowledges, for example, that linguists and researchers criticise the accuracy of language allocations in regard to the automatic dialect recognition, it is explained: "There are (...) pronounced differences between the various trends in linguistic research. We took a different approach and worked primarily with algorithm experts. (...) Experts helped us to convert phonetics into codes."[29] It is faded out that the more inaccurate data is gathered and analysed through likewise flawed digital systems, the more problems occur in the final asylum decisions. Combined with the Federal Office's focus on process efficiency, this inevitably results in accelerating error-making at scale nurtured by digital means. At the same time, this "language of algorithms" (Green and Viljoen, 2020: 22) is imposed onto social domains at the expense of other values, such as the focus on quality of asylum decisions, protecting fundamental rights and building a trusting relationship between authorities at the Federal Office and asylum seekers. The systems were developed based on simplified assumption about social realities, including that recorded speech samples of two minutes, the names of

[29] Own translation. Original text: "Es gibt (...) ausgeprägte Differenzen zwischen den verschiedenen Strömungen der Sprachforschung. Wir haben einen anderen Ansatz gewählt und primär mit Experten für Algorithmen zusammengearbeitet. (...) Experten haben uns dabei geholfen, Phonetik in Codes umzuwandeln" (Richter, as cited in Frank, 2018: 22).

applicants and data found on their mobile devices can be linked to (somewhat) valid nationality and identity assessments. Because of this flawed foundation, potential technical improvements of IDM-S' insufficiencies through feedback loops and programming code will not address the overall issue but likely intensify existing problems. Instead, it is necessary to explore alternative measures for supporting identity determinations and verifications, in particular, those that do not focus on contested digital systems but put human beings at the centre of procedures - especially when dealing with severe life-changing decisions and vulnerable groups of society.

> The systems were developed based on simplified assumption about social realities, including that recorded speech samples of two minutes, the names of applicants and data found on their mobile devices can be linked to (somewhat) valid nationality and identity assessments. Because of this flawed foundation, potential technical improvements of IDM-S' insufficiencies through feedback loops and programming code will not address the overall issue but likely intensify existing problems.

6 Conclusion

A strong technological state capacity and the use of new technologies are often perceived to account for better decision-making processes in the field of governance. Under the umbrella of the "Integrated Identity Management: plausibility, data quality and security aspects (IDM-S)" programme, the German Federal Office for Migration and Refugees developed a set of digital systems that aimed at supporting the determination and verification of those asylum applicants' identity claims who could not present their passports. This research set out to investigate how the Federal Office legitimised the policy and use of the digital identification system "IDM-S" as part of its expanding portfolio of digital initiatives that indicate a new direction of governance.

The study is grounded in legitimacy theory - considered a core virtue of just institutions and their exercise of public authority, hence, power over individuals. Legitimacy is understood as a justificatory concept seen in conjunction with (good) governance, the processes of making and implementing decisions by considering human rights frameworks - in this particular case the right to privacy as protected under Art 17 ICCPR. While the chosen theoretical concepts could have been used independently as they each are based on a rather broad foundation of norms recognised as valid within public administrations and as necessary for democratic state practices, this research drew on the overlapping effects of these theories. Through this combination it was possible to analyse the Federal Office's justifications and practices as well as their de jure and de facto qualities comprehensively in the political context. The qualitative content analysis proved to be a valuable method to find patterns and (in)consistencies in the studied documents. Although subject to adjustments and academic discussions, the data justice framework complemented this approach by providing a helpful structure that reflected the understanding that digital systems are embedded in existing (power) structures and should be studied along different dimensions instead of focussing on mere technical components.

The results of the analysis revealed four main patterns: The references to the rule of law and shared beliefs implied that both policy and practice followed legal standards perceived as necessary to protect society from security threats. Information that could potentially delegitimise state conduct was not disclosed whereas proactive communication was largely positive to demonstrate successful operations. The emphasis on efficiency and IDM-S' high level of innovation implied the usefulness of the digital systems stemming from their easy application, cost and time efficiency, as well as the ability to produce fast results. Innovation and agility underlined the self-proclaimed image of a modern, tech-savvy administration - an "entrepreneurial government" (Osborne, 1993: 352). The last pattern portrayed efforts to uphold the impression of rational and objective operations based on the mathematical-technical approach used to generate the systems' results. These patterns imply to the outside world that the Federal Office is capable to meet the needs and satisfy expectations of democratic societies and just state practices. However, it can be concluded that references alone do not affirm legitimacy per se, rather they indicate justifications, political intentions and tactics to maintain the image of a rightful state conduct. On the contrary, the findings outlined word-deed tensions, the insufficient adherence to fundamental privacy rights and state obligations of effectively protecting vulnerable populations as well as the lack of compliance to qualitative values in governance, including participation, transparency, accountability, impartiality and scientific soundness.

The turn to data-driven systems and automatisation offered a supposedly easy way out of the complexity in regard to the challenges the Federal Office faced since 2015: the flaws in identity determinations, insufficient staff trainings and the high number of unprocessed asylum claims. Underpinned by the perceived "crisis" that strengthened the rhetorics of national security, stricter border control and politics of repatriations, IDM-S embodied the current trend of political data accumulation and business-like "innovations" in public administrations in terms of its development, implementation and execution. Yet, so much of this "crisis" is not a crisis of numbers but a crisis of politics (Betts, 2015). The research has shown that the overall IDM-S governance approach is shaped by a technocratic worldview and deeply contested assumptions not only about asylum but about the potentials and limits of digital systems in regard to their problem-solving capacity in complex, social settings. In this researched case, the use of the systems strengthened existing inequalities, violated fundamental privacy rights, contributed to power imbalances and distrust in the relationship between the government and asylum seekers. To fully understand the implications of rights violations, future studies could focus on the experiences of asylum seekers subjected to IDM-S procedures. Based on the interviews, this research identified some individual cases that prove the Federal Office's de facto non-compliance with privacy rights. Because the three studied IDM-S systems were applied to thousands of cases, it gives reason to believe that many more individuals might have been unjustly affected by the systems' use. Furthermore, the amount of available material across the three systems was unevenly distributed. Less information was provided on TraLitA than on the other two systems. Thus, future research could focus on investigating these knowledge gaps. Lastly, researchers and practitioners alike should scrutinise digital "AI" (Artificial Intelligence) systems (BAMF, 2019a) developed by the Federal Office (and elsewhere in public administrations) with the aim to identify governance issues and to push for alternative reforms that are carried out with due diligence, account for nuances and complexity, and put human being at the centre of decision-making processes. With the view to positively affect future policies in the context of asylum from a strong human rights-based perspective, it is necessary to engage in more fundamental questions about the "raison d'être" of such systems and look past the often proposed techno-fixes. The illegitimate development and implementation of harmful digital systems in state institutions is not inevitable - decisions not to implement have to become a real option.

7 Appendices

A Coding system

This table provides an overview of the applied coding system, including the code categories, descriptions, main codes and examples. These codes are listed alphabetically and do not follow a hierarchical order.

Code category	*Code*	*Example*
Automatic dialect recognition (DIAS) Description: Information, claims, statements, assessments, facts, descriptions that refer directly to how DIAS is applied in practice.	Alternative measures	"kann im Einzelfall geprüft werden, ob eine S-T-A durchgeführt werden kann"
	Benefits	"Somit wird nicht nur die Transparenz gesteigert, sondern auch die Sicherheit im Asylprozess"
	Functionality descriptions	"Die Antragsteller beschreiben dazu ein oder mehrere detailreiche Bilder in freier, nicht unterbrochener Sprache"
	Future scenarios	"Der Austausch mit Vertretungen von Migrationsbehörden anderer Länder zeigt interessante Ansatzpunkte zur Zusammenarbeit auf, insbesondere im Bereich der Sprachbiometrie"
	Involved parties and stakeholders	"Sie wird vom marktführenden Unternehmen Nuance Inc. angeboten, mit dessen Muttergesellschaft Atos SE ein Rahmenvertrag besteht."
	Issues	"Die Sprachaufnahmen der Antragstellenden müssen deutlich und ausreichend lang sein, um aufschlussreiche Ergebnisse zu erzielen"

Code category	*Code*	*Example*
	Legal reference	"Grundlage für den Einsatz der Software ist § 16 Absatz 1 Satz 3 ff. des Asylgesetzes (AsylG)."
	Performance and statistics	"Angaben hierzu können nicht gemacht werden. Eine statistische Erfassung erfolgt nicht."
	Scientific, rational operations	"Die Evaluationsergebnisse werden voraussichtlich im zweiten Quartal 2018 vorliegen."
	Software and data used	"Die Sprach-/Dialekterkennung basiert auf einem Softwareprodukt, welches ein Sprachmodell mit über 25 Sprachen und Dialekten beinhaltet."
	Statements of success/ failure	"Die Bundesregierung bewertet den Nutzen der Sprachbiometrie als sehr positiv, da der gesprochene Dialekt neben den Angaben der Antragsteller häufig das einzige Indiz für deren Herkunft darstellt."
Common fallacies Description: Indications, signs and examples of common fallacies in regard to the use of IDM-S.	Legible criteria and trade-offs	"ausgeprägte Differenzen zwischen den Strömungen der Sprachforschung. Wir haben einen anderen Ansatz gewählt und primär mit Experten für Algorithmen zusammengearbeitet."
	Objectivity and neutrality	"stellt eine unabhängige, objektive und massentaugliche Methode dar"
	Universalism	"Eine zweiminütige Aufzeichnung ist daher ausreichend, um die Herkunft eingrenzen zu können"

Code category	*Code*	*Example*
Implementation process of IDM-S - justifications Description: Justifications that are used frequently and repeatedly to argue for the usefulness of IDM-S.	Accuracy and precision	"zusätzliche Datenpunkte"
	BAMF's self-descriptions	"Technologieführer"
	Easy application	"unkompliziert einzusetzendes Zusatzinstrument"
	External validation and confirmation	"der Gewinn eines E-Government-Preises und interessierte Anfragen von Partnerbehörden des BAMF aus aller Welt bestätigen den Erfolg"
	Innovation	"weltweit einzigartig"
	"Only support"	"lediglich eine unterstützende Zusatzinformation für den Entscheider"
	Performance efficiency	"schneller zu plausibilisieren"
	Technocratic perspectives	"primär mit Experten für Algorithmen zusammengearbeitet"
Implementation process of IDMS - qualities Description: Information that refers to the implementation qualities of IDM-S.	Access to information, communication of information	"Die entsprechenden Informationen zur Funktionsweise unterliegen der internen Verwendung"
	Affected groups	"Antragsteller, die keinen gültigen Pass, Passersatz oder ein anderes Identitätspapier (siehe hierzu vergleichend DA Asyl Abschnitt Urkundenprüfung) vorlegen können"
	Costs	"Im Jahr 2017 sind für Qualifizierungsmaßnahmen zur Einführung der IDM-S IT-Tools nicht haushaltswirksame Kosten von 168 628 Euro entstanden."

Code category	*Code*	*Example*
	Facts, dates and development stages	"Die Testphase erfolgte im AZ Bamberg"
	Information that is not assessed	"Die Bundesregierung hat keine Kenntnis über anhängige Gerichtsverfahren im Sinne der Fragestellung. Statistische Daten zu dem jeweiligen Verfahrensgegenstand im Sinne der Fragestellung werden nicht erfasst. "
	Participation	"lediglich eine für IT-Projekte typische agile Vorgehensweise beschrieben, in der sich die beteiligten Fachbereiche in einem dynamischen Prozess kontinuierliche Rückmeldung zu einzelnen Ideen geben"
	Reasons for non-disclosure	"Gefährdung der öffentlichen Sicherheit"
	Transparency	"Transparenz im Umgang mit dem Ergebnis unserer Entwicklung ist uns wichtig."
Legislative proceedings - justifications of AmD Description: Aims, explanations and justifications put forward by authorities (BAMF, BMI as drafting/ supervising body) to justify the introduction of the analysis of mobile devices (AmD).	AmD affected groups	"Es ist so, dass, wenn wir uns anschauen, welche Personen Adressaten sind, wir in der Tat zunächst einmal die Zielgruppe als absolute Maximumgröße von 60 Prozent der Asylbewerber sehen, die kein Identitätsausweispapier mitbringen"
	AmD aims	"es geht darum, in einer bestimmten Zielgruppe die Plausibilität des Asylantrages zu erleichtern."
	AmD application and scope	"Es geht also um die Metadaten, nicht um die Inhalte."

Code category	*Code*	*Example*
	AmD benefits	"aus meiner Sicht so, dass die Praktikabilität erhöht wird. Es ist so, dass wir eine Beschleunigung der Asylverfahren feststellen"
	AmD legality	"Es gibt bereits eine Norm. Das ist jetzt nicht etwas komplett Neues, was der Gesetzgeber hier vorhat, sondern §48 Absatz 3a Aufenthaltsgesetz ist bereits im gleichen Wortlaut existent."
	AmD necessity	"Daten auszulesen, die die Identität und das Herkunftsland identifizieren oder die dabei unterstützen."
	AmD permissible interferences	"wird als ein letztes mögliches Instrument betrachtet und nur in Einzelfällen in einem engen gesetzlichen Rahmen angewendet, wie beispielsweise bei Personen ohne gültigen Ausweis"
Legislative proceedings - justifications of law Description: Aims, arguments, explanations and justifications put forward by authorities (BAMF, BMI as drafting/ supervising body) to justify the introduction of the new law.	Aim	"Der Gesetzentwurf verbessert die Möglichkeiten der Identitätsklärung und Rückführung ausreisepflichtiger Ausländer"
	Enforcing rule of law	"Ausreisepflicht –selbstverständlich unter Beachtung rechtstaatlicher Vorgaben"
	Enhancing repatriations	"aufenthaltsbeendende Maßnahmen gegenüber Identitätstäuschern und Personen ohne Bleibeperspektive zu erleichtern."
	Evidence presented	"wird mit teils oberflächlichen Argumenten hantiert oder mit Zahlen, die nicht ausreichend evaluiert wurden"

Code category	*Code*	*Example*
	Faster asylum decisions	"ausreisepflichtige Migranten schneller und konsequenter abzuschieben"
	Misleading authorities in identity determinations	"Schwer vermittelbar ist auch, warum der Gesetzgeber weiterhin mit der Duldung die Rechtstellung derjenigen ausreisepflichtigen Ausländer verbessert, die ihre Ausreisepflicht durch Identitätstäuschung und Mitwirkungsverweigerung –oft im kollusiven Zusammenwirken mit dem Botschaftspersonal des Heimatstaates –aktiv hintertreiben."
	"Misusing" asylum	"Wer unter dem Deckmantel des Asylrechts nach Deutschland kommt"
	National security and public safety	"unter den illegal Einreisenden auch Personen sind, die mit terroristischen Organisationen sympathisieren und diese sogar aktiv unterstützen. Ich erinnere an die furchtbaren Anschläge in Würzburg, Ansbach und Berlin."
Legislative proceedings - qualities Description: Statements and assessments that refer to the qualities of the legislative proceedings.	Adherence to established procedures and rules	"Gemeinsamen Geschäftsordnung der Bundesministerien heißt es, dass die Zivilgesellschaft bzw. Fachverbände und Organisationen rechtzeitig zu beteiligen sind, ihnen damit auch frühzeitig eine Gesetzesvorlage zuzuleiten ist (§ 47 Abs. 1 und Abs. 3 GGO). Und all das ist in den letzten Jahren nicht geschehen."
	Evaluation of legal measures	"obwohl wir im Asyl- und Aufenthaltsrecht die ganze Zeit mit neuen Gesetzen konfrontiert werden. Und überhaupt keine Zeit genommen wurde, um zu evaluieren"

Code category	*Code*	*Example*
	Participation	“Und das in ein einhalb Tagen ausreichend qualifiziert zu bewerten, ist wirklich eine enorme Herausforderung. Es kann eigentlich nicht im Interesse eines Bundesministeriums sein, dass man den Fachverbänden nur so wenig Zeit gibt.”
	Responsiveness, openness to input	“Reiseweg aus der Begründung gestrichen wurde - ohne Erklärung, ob das jetzt auch heißt, dass man das nicht erheben darf oder ob man das gerade nicht öffentlich thematisieren will.”
Name transliteration and analysis (TraLitA) Description: Information, claims, statements, assessments, facts, descriptions that refer directly to how TraLitA is applied in practice.	Alternative measures	“Die Namenstranskription wird unabhängig davon durchgeführt, ob ein gültiger Pass oder Passersatz vorliegt.”
	Benefits	“Schwächen in der Datenaktualität und -validität in der Aktenhaltung identifiziert und bereinigt werden”
	Functionality descriptions	“transkribiert Namen in lateinische Schreibweise und stellt außerdem eine abgeleitete Herkunftslandprognostik zur Verfügung”
	Future scenarios	“Wir würden es begrüßen, wenn beispielsweise unser Assistenzsystem zur Namenstransliteration auch von anderen genutzt würde. Dafür suchen wir Partner im In- und Ausland.”
	Involved parties and stakeholders	“Individuallösung der Firma SVA (SVA bindet Produkte und Leistungen der Firma IBM ein)”

Code category	*Code*	*Example*
	Issues	“Die Erfolgsquote eines Herkunftshinweises ist abhängig vom Herkunftsland”
	Performance and statistics	“Bei den Maghreb-Staaten wird dagegen nur eine Erfolgsquote von ca. 35 Prozent gemessen”
	Software and data used	“In das Modell des verwendeten Softwareprodukts sind ca. eine Milliarde Namen aus aller Welt eingeflossen”
	Statements of success/ failure	“könnte mit der historisch entstandenen Vermischung mit der französischen und italienischen Sprache zusammenhängen”
Read-out and analysis of mobile data devices (AmD) Description: Information, claims, statements, assessments, facts, descriptions that refer directly to how AmD is applied in practice.	Alternative measures	“Als mildere Mittel kommen letztendlich nur Dokumente in Betracht, die durch ein Lichtbild die Identität belegen können und vom Bundesamt auf ihre Echtheit überprüft werden können.”
	Benefits	“Bereitstellung zusätzlicher Daten mit Hinweisen zur Identität und Herkunft”
	Functionality descriptions	“Die mobilen Datenträger (Mobiltelefon/Smartphone/Tablet) müssen durch den Antragsteller entsperrt werden.”
	Future scenarios	“Derzeit findet eine Püfung zu den technischen und rechtlichen Möglichkeiten einer etwaigen Ausweitung der Handyauswertung statt. Die Prüfung ist zum gegenwärtigen Zeitpunkt noch nicht abgeschlossen.”

Code category	*Code*	*Example*
	Involved parties and stakeholders	"Individuallösungen der Firma Atos (Atos bindet Produkte und Leistungen der Firmen MSAB und T3F-Forensics ein)"
	Issues	"Es ist auch objektiv nicht ersichtlich, ob das Handy überhaupt ein Mittel ist, das zur Identitätsfeststellung oder Staatsangehörigkeitsfeststellung dienen kann."
	Legal reference	"Bei der Speicherung der durch das BAMF generierten Daten zur Identitätssicherung von Antragstellern handelt es sich nicht um eine Datengewinnung "auf Vorrat", sondern um eine Regelung mit klarer und eingegrenzter Zweckbindung der Identitätssicherung."
	Performance and statistics	"wurden insgesamt 9 710 Datenträger von Erstantragstellern ohne Pass/ Passersatz ab 14 Jahren ausgelesen."
	Software and data used	"basierend auf z.B. Geodaten von aufgenommenen Fotos, aus Apps oder aus Login-Informationen sozialer Netzwerke können Rückschlüsse über die Staatsangehörigkeit gezogen werden."
	Statements of success/ failure	"Das Auslesen mobiler Datenträger stellt momentan das wichtigste Instrument zur Identitätsüberprüfung dar"

Code category	*Code*	*Example*
Right to privacy Description: Information that addresses the state obligations, principles and dimensions of privacy as outlined under Art 17 ICCPR.	Accountability	“Es sind keine entsprechenden Beschwerden bekannt.”
	Accuracy (incl. staff training)	“Interpretationshilfen zur Analyse der Ergebnisberichte sind Bestandteil der Schulungsunterlagen.”
	Amount, type, retention period of data	“in welchen Ländern wurden Browser aufgerufen”
	Consent	“Nach vollständig abgeschlossener Aktenanlage einschl. Aushändigung der Belehrungen und Einholung aller erforderlichen Unterschriften, wird der Antragsteller auf die gesetzliche Verpflichtung zur Mitwirkung”
	Lawfulness, fairness, transparency	“Wenn der Antragsteller angibt, einen Pass/ Passersatzdokument erst zu einem späteren Zeitpunkt vorlegen zu können - beispielsweise, weil dieser bei einer anderen innerdeutschen Behörde abgegeben wurde - so kann der mobile Datenträger ausgelesen werden.”
	Purpose specification and limitation	“Feststellung der Identität und Herkunft”
	Security measures and safeguards	“Erst nach Freigabe eines Ergebnisreports durch einen Volljuristen kann der zuständige Entscheider diesen auswerten”

Table 6: Coding system
(Source: Own tabular summary)

B Lists of coded and analysed documents

These lists depict the coded and analysed documents. Full details on these materials are provided in the bibliography.

B.1 Federal Office for Migration and Refugees

BAMF. 2017a. Integriertes Identitätsmanagement - Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in die neuen IT-Tools. Schulung AVS-Mitarbeiter, Entscheider und Volljuristen. [Training material] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung_idms_bamf.pdf>.

BAMF. 2017b. Moderne Technik in Asylverfahren: Vorsitzender der Innenministerkonferenz informiert sich über neue technische Assistenzsysteme. [Press release] <https://www.bamf.de/SharedDocs/Meldungen/DE/2017/20170726-am-vorstellung-modellprojekt-bamberg.html?nn=282388>.

BAMF. 2017c. Tool-testing in Bamberg, July 2017. [Facebook post] <https://www.facebook.com/bamf.socialmedia/posts/wir-haben-gestern-in-bamberg-neue-assistenztools-vorgestellt-die-bei-der-identit/1298844053561819/>.

BAMF. 2017d. Auszeichnung für digitale Transformation und Pioniergeist. [Press release] <https://www.bamf.de/SharedDocs/Meldungen/DE/2017/20170703-digital-leader-award.html?nn=282388>.

BAMF. 2018a. Digitalisation Agenda 2020: Success stories and future digital projects at the Federal Office for Migration and Refugees (BAMF). Third updated edition. [Digitalisation agenda] <http://www.wir-sind-bund.de/SharedDocs/Anlagen/EN_nvam/Publikationen/Broschueren/broschuere-digitalisierungsagenda-2020.pdf?__blob=publicationFileY>.

BAMF. 2018b. Sprachbiometrisches Assistenzsystem: Unterstützung der Feststellung von Herkunft und Identität im Asylverfahren. [Presentation] <https://www.egovernment-wettbewerb.de/praesentationen/2018/Kat_Digitalisierung_BAMF_Sprachbiometrie.pdf>.

BAMF. 2018c. Dienstanweisung Asylverfahren: Identitätsfeststellung. [Internal instructions] <https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_identitaetsfeststellung.pdf>.

BAMF. 2018d. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch "Namenstranskription" (TraLitA). [User manual] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_namenstranskription.pdf>.

BAMF. 2018e. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch "Sprachbiometrie" (DIAS). [User manual] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_sprachbiometrie.pdf>.

BAMF. 2018f. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch "Auslesen mobiler Datenträger" (AmD). [User manual] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_amd.pdf>.

BAMF. 2018g. Integriertes Identitätsmanagement - Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in das IDM-S Tool Auslesen von mobilen Datenträgern (AmD). Schulung AVS-Mitarbeiter. [Training material] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung_avs_kurz.pdf>.

BAMF. 2018i. Biometrische Sprachsoftware zur Erkennung von Dialekten. [Internal instructions] <https://fragdenstaat.de/anfrage/biometrische-sprachsoftware-zur-erkennung-von-dialekten/>.

BAMF. 2018j. eGovernment Preisverleihung: 1. Platz. [Press release] <https://www.bamf.de/SharedDocs/Meldungen/DE/2018/20180621-am-egovernment.html?nn=282388>.

BAMF. 2018k. Dienstanweisung für das AVS. Auslesen von mobilen Datenträgern. Verfahrensweise bei persönlicher Erstantragstellung. [Internal instructions] <https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_ams.pdf>.

BAMF. 2018l. Verfahrensverzeichnis: Sprachbiometrisches Assistenzsystem. [Procedure index] <https://fragdenstaat.de/anfrage/verfahrensverzeichnis/92175/anhang/SprachbiometrischesAssistenzsystem.pdf>.

BAMF. 2018m. Verfahrensverzeichnis: Auslesen mobiler Datenträger. [Procedure index] <https://fragdenstaat.de/anfrage/verfahrensverzeichnis/92175/anhang/AuslesenmobilerDatentrger.pdf>.

BAMF. 2018n. Weisung zum Umgang mit anhängigen STA-Verfahren. Internal e-mail communication. [Internal instructions] <https://fragdenstaat.de/anfrage/dienstanweisung-vom-1-dezember/>.

BAMF. 2019a. Digitalisierungsagenda 2020: Bisherige Erfolge und Ausblick auf weitere digitale Projekte im Bundesamt für Migration und Flüchtlinge. Fourth updated edition. [Digitalisation agenda] <https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/broschuere-digitalisierungsagenda-2020.html>.

BAMF. 2019c. HKL-Anfragen zur Sachaufklärung. Leitfaden für AA-Anfragen und für Gutachten. Dienstanweisung Asylverfahren: Urkunden- und Dokumentenprüfung PTU. [Internal instructions] <https://fragdenstaat.de/anfrage/leitfaden-aadienstanweisung-ptu/415590/anhang/SPRN92119082708120.pdf>.

BAMF. 2019d. BAMF-Chef: Ein Asyl-Chaos wie 2015 wird sich nicht wiederholen! [Interview Sommer] <https://www.bamf.de/SharedDocs/Interviews/DE/InterviewsFachartikel/191105-interview-dr-sommer-bams.html?nn=282388>.

BAMF. 2019e. Bilder für sprachbiometrische Tests. [Notice] <https://fragdenstaat.de/anfrage/bilder-fur-sprachbiometrische-tests-1/>.

BAMF. 2019f. Testergebnisse biometrischer Sprachsoftware zur Erkennung von Dialekten. [Notice] <https://fragdenstaat.de/anfrage/testergebnisse-biometrischer-sprachsoftware-zur-erkennung-von-dialekten/353954/anhang/2019_697_IFG_NAME_geschwaerzt.pdf>.

BAMF. 2019g. Datenschutz-Folgenabschätzung: Anfrage nach dem Informationsfreiheits-gesetz (IFG). [Notice] <https://fragdenstaat.de/anfrage/datenschutz-folgeabschatzungen/353952/anhang/2019_689_IFG_Biselli_geschwaerzt.pdf>.

BAMF. 2019i. Überlassung und Auslesen eines Datenträgers (D1705), Auswertung eines Datenträgers (D1706), Antrag auf Auswertung eines Datenträgers (D1735). [Internal forms] <https://fragdenstaat.de/anfrage/dokumentenvordrucke/415595/anhang/SPRN92119082708280.pdf>.

BAMF. 2020g. Sicherheit im Kontext von Migration. [Website] <https://www.bamf.de/DE/Themen/Sicherheit/sicherheit-node.html>.

BAMF. 2020i. Digitalisierungsagenda 2020 & IDM-S POC, Kosten-Nutzen, Evaluation, Feedback. [Notice] <https://fragdenstaat.de/anfrage/digitalisierungsagenda-2020-idm-s-poc-kosten-nutzen-evaluation-feedback/482915/anhang/SPRN90620050609180_geschwaerzt.pdf>.

BAMF. 2020j. Ihr Antrag nach dem Informationsfreiheitsgesetz (IFG). Auslesen mobiler Datenträger: FAQ-Liste und Antworten. [Notice] <https://fragdenstaat.de/anfrage/auslesen-mobiler-datentrager-faq-liste-und-antworten/510153/anhang/SPRN91220072208050.pdf>.

BAMF. 2020k. Wichtige Mitteilung: Erstbelehrung. D0179. [Consent form] <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/503448/anhang/D0179.pdf>.

BAMF. 2020l. Belehrung von Antragstellenden: Sprachbiometrie (DIAS), Namenstranskription (TraLitA). [Consent form] <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/>.

BAMF. 2020m. Information zur Abgabe einer Sprechprobe für die Sprachbiometrie. D1728. [Consent form] <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/503448/anhang/D1728.pdf>.

BAMF. 2020n. Identitätsmanagement. [Website] <https://www.bamf.de/DE/Themen/Sicherheit/Identitaetsmanagement/identitaetsmanagement-node.html>.

BAMF; BFM. 2017. Integriertes Identitätsmanagement - Assistenzsysteme. [Press release] <https://docplayer.org/108534301-Presseinformation-integriertes-identitaetsmanagement-assistenzsysteme-1-integriertes-identitaetsmanagement-im-ueberblick.html>.

Frank, Dorothee. 2018. Digitale Unterstützer im Asylverfahren: Wie Sprachbiometrie Asylentscheidungen auf eine noch breitere Grundlage stellt. In: Cyber Security Report/ Sicherheitstechnischer Report. 2018. Mittler Report Verlag GmbH. [Interview Richter]

Seibert, Evi. 2017. SWR2 Interview der Woche vom 11.11.2017. [Interview Cordt] <https://www.swr.de/-/id=20383132/property=download/nid=659202/3lstzu/swr2-interview-der-woche-20171111.pdf>.

B.2 Legislative proceedings

Becker, Kerstin. 2017. Stellungnahme des Paritätischen Gesamtverbandes zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht vom 23.02.2017. (BR-Drucksache 179/17). [Submitted statement] <https://www.bundestag.de/resource/blob/500018/6088152efe793c12973a8309cf74d627/18-4-825-B-data.pdf>.

BMI. 2017c. Referentenentwurf des Bundesministeriums des Innern. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. [Draft law] <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-15-Referentenentwurf-Gesetz-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Federal Council. 2017. Stellungnahme des Bundesrates: Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Drucksache 179/17. [Submitted statement] <https://dipbt.bundestag.de/dip21/brd/2017/0179-17B.pdf>.

Federal Government. 2017a. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 179/17. [Draft law] <https://dipbt.bundestag.de/dip21/brd/2017/0179-17.pdf>.

Federal Government. 2017b. Gesetzentwurf der Bundesregierung: Entwurf eines Gesetztes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 18/11546. [Draft law] <https://dipbt.bundestag.de/dip21/btd/18/115/1811546.pdf>.

Federal Government. 2017c. Beschlussempfehlung und Bericht des Innenausschusses zu dem Gesetzentwurf der Bundesregierung. Drucksache 18/12415. [Draft law] <https://dipbt.bundestag.de/dip21/btd/18/124/1812415.pdf>.

German Bar Association 2017. Stellungnahme des Deutschen Anwaltverein durch den Ausschuss Gefahrenabwehrrecht zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht (BT-Drs. 18/11546). [Submitted statement] <https://anwaltverein.de/de/newsroom/sn-39-17-gesetz-zur-besseren-durchsetzung-der-ausreisepflicht-60305>.

German Bundestag. 2017a. Wortprotokoll der 111. Sitzung. Innenausschuss. Öffentliche Anhörung. Protokoll-Nr. 18/111. [Public hearing protocol] <https://www.bundestag.de/resource/blob/511642/d4c03aa26137310cf5568fa7e9f179fc/Protokoll-111-Sitzung-data.pdf>.

German Bundestag. 2017d. Stenografischer Bericht. 225. Sitzung. Plenarprotokoll 18/225. [Plenary protocol] <https://dipbt.bundestag.de/dip21/btp/18/18225.pdf>.

German Bundestag. 2017e. Stenografischer Bericht. 234. Sitzung. Plenarprotokoll 18/234. [Plenary protocol] <https://dipbt.bundestag.de/dip21/btp/18/18234.pdf>.

German Bundestag. 2020c. Gesetz zur besseren Durchsetzung der Ausreisepflicht. Dokumentations- und Informationssystem DIP. ID: 18-80058. [Legislative procedure] <https://dipbt.bundestag.de/extrakt/ba/WP18/800/80058.html>.

PRO ASYL. 2017a. Sachverständigen Stellungnahme für die öffentliche Anhörung am 27. März 2017 vor dem Innenausschuss des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 179/17. [Submitted statement] <https://www.proasyl.de/wp-content/uploads/2015/12/2017-03-23-Sachverst%C3%A4ndigen-Stellungnahme-PRO-ASYL-Gesetzentwurf-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Voßhoff, Andrea. 2017. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. German Bundestag. Innenausschuss. Ausschussdrucksache 18(4)831. [Submitted statement] <https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf>.

B.3 Federal Government and BMI

BMI. 2017b. Von Herrn MdB Roland Claus erbetene Sachinformation. [Response to opposition requests] <https://cdn.netzpolitik.org/wp-upload/2017/12/nuance.pdf>.

BMI. 2018b. Schriftliche Fragen des Abgeordneten Alexander Ullrich: Monat Juni 2018. Arbeits-Nr. 6/225. [Response to opposition requests] <https://andrej-hunko.de/start/download/dokumente/1186-software-fuer-sprachbiometrie-forensik-handyauswertung-beim-bamf-mdb-alexander-ulrich/file>.

German Bundestag. 2017b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Petra Sitte, Anke Domscheit-Beim Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/190. [Response to small request] <https://dipbt.bundestag.de/doc/btd/19/001/1900190.pdf>.

German Bundestag. 2017g. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Frank Tempel, Sevim Dağdelen, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 18/11262. [Response to small request] <https://www.ulla-jelpke.de/wp-content/uploads/2017/02/1811262-Asylstatistik-IV-2016-1.pdf>.

German Bundestag. 2018a. Antwort der Bundesregierung auf die kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/6647. [Response to small request] <https://dip21.bundestag.de/dip21/btd/19/066/1906647.pdf>.

German Bundestag. 2018b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/1631. [Response to small request] <https://dipbt.bundestag.de/dip21/btd/19/016/1901631.pdf>.

German Bundestag. 2018c. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das zweite Quartal des Jahres 2018. BT-Drucksache 19/4961. [Response to small request] <https://dipbt.bundestag.de/dip21/btd/19/049/1904961.pdf>.

German Bundestag. 2018d. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von Spracherkennungssoftware durch das Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/1663. [Response to small request] <https://dipbt.bundestag.de/dip21/btd/19/016/1901663.pdf>.

German Bundestag. 2019a. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2018. BT-Drucksache 19/8701. [Response to small request] <https://dip21.bundestag.de/dip21/btd/19/087/1908701.pdf>.

German Bundestag. 2019b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/13945. Available at: <https://dip21.bundestag.de/dip21/btd/19/139/1913945.pdf>.

German Bundestag. 2020f. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2019. BT-Drucksache 19/18498. [Response to small request] <https://dip21.bundestag.de/dip21/btd/19/184/1918498.pdf>.

C Oral expert interviews

As part of this thesis, three oral expert interviews were carried out with the following individuals, each between 60 - 90mins:

- Bellinda Bartolucci, at the time head of the legal policy department at PRO ASYL;
- Lea Beckmann, lawyer and procedural coordinator at the Society for Civil Rights (Gesellschaft für Freiheitsrechte);
- Anna Biselli, journalist and computer scientist.

With the experts' consent, their interview statements, names and references are used in this paper. The interview transcripts are excluded from this publication due to their extensive length.

D Written expert interview with the Office of the BfDI

In addition to the oral expert recordings, a written interview was conducted to include the perspectives of the Office of the BfDI, the Federal Commissioner for Data Protection and Freedom of Information. The following answers were provided by the responsible authority/ Press Office. With the Office's consent, the answers are included in this paper.

D.1 Response of 07 May 2020

In dem Tätigkeitsbericht 2015 bis 2016 kritisiert die BfDI die kurzen Fristen zur sachgerechten Prüfung (S. 101) der gesetzlichen Inhalte im Gesetzgebungsverfahren im Bereich Asyl.

1. Frage: Wie viel Zeit wurde dem BfDI vonseiten des Gesetzgebers eingeräumt, um schriftlich Stellung zu nehmen und zielführend zu prüfen? (Angabe bitte bezogen auf das Gesetz der besseren Durchsetzung der Ausreisepflicht aus dem Tätigkeitsbericht 2017/18, S. 66 und im Vergleich das Datenaustauschverbesserungsgesetz)

   BfDI Office: Für eine Stellungnahme zum Entwurf des Gesetzes zur besseren Durchsetzung der Ausreisepflicht hatte der BfDI etwa einen Monat Zeit. Später hat der BfDI eine überarbeitete Fassung erhalten und wurde gebeten, innerhalb von wenigen Tagen erneut eine Stellungnahme zu verfassen. Beim Entwurf des Datenaustauschverbesserungsgesetzes sollte der BfDI ebenfalls innerhalb einer kurzen Frist von wenigen Tage eine Stellungnahme verfassen. Zusätzlich hat uns das Bundesministerium des Innern kurzfristig zu einer Besprechung eingeladen, um seine Position zu erläutern.

2. Frage: Wie viel Zeit ist für eine angemessene Gesetzprüfung aus Sicht des BfDI adäquat und notwendig?

   BfDI Office: Die Gemeinsame Geschäftsordnung der Bundesministerien sieht für die Beteiligung anderer Ressorts in der Regel eine Frist von vier Wochen, bei umfangreichen oder rechtlich schwierigen Entwürfen sogar von acht Wochen, vor. Diese Fristen halten wir für angemessen und erforderlich.

Die BfDI kritisierte die "Datenträgerauswertung" - u.a. als verfassungswidrig, nicht erforderlich und unverhältnismäßig. Zusätzlich wurde angemerkt, dass die gewonnenen Informationen keine Rückschlüsse auf die tatsächliche Herkunft einer Person zulassen. (siehe u.a. S. 66, Tätigkeitsbericht BfDI 2017/18)

3. Frage: Die u.a. vom BfDI genannten Kritikpunkte wurden von dem Gesetzgeber vor in Kraft treten des Gesetzes (Entwurf) und bis zum Tätigkeitsbericht 2017/18 nicht umgesetzt. Gab es Verbesserungen seit 2018 vonseiten des BAMF? Welche?

   BfDI Office: Das Bundesamt für Migration und Flüchtlinge hat die im Gesetz vorgegebenen Aufgaben umzusetzen. Verbesserungen an gesetzlichen Regelungen kann der Gesetzgeber nur selbst vornehmen.

4. Frage: Wie bewertet der BfDI die Qualität des Dialogs mit dem Gesetzgeber bzw. des Gesetzgebungsverfahren zum Gesetz zur besseren D. der Ausreisepflicht?

   BfDI Office: Wir hatten zu wenig Zeit für die erforderliche umfassende Prüfung datenschutzrechtlicher Belange. Das haben wir gegenüber dem Bundesministerium des Innern auch deutlich zum Ausdruck gebracht.

5. Frage: Welche Schlüsse für die praktische Beratung für Gesetzgebungsprozessen zieht der BfDI aus diesem Gesetzgebungsverfahren? Sind bessere (Beratungs-)Abläufe geplant und wenn ja, welche?

   BfDI Office: Seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) besteht mit Art. 36 Abs. 4 eine Pflicht zur Konsultation der Aufsichtsbehörde bei der Ausarbeitung von Gesetzgebungsvorhaben. Leider enthält diese Regelung keine zeitlichen Vorgaben, so dass knappe Fristsetzungen weiterhin nicht ausgeschlossen sind. Der BfDI kann sich darüber hinaus jederzeit direkt an den Deutschen Bundestag wenden und auf datenschutzrechtliche Probleme in Gesetzentwürfen hinweisen. Dies sollte aber die Berücksichtigung der Positionen des BfDI bereits vor der parlamentarischen Beratung nicht ausschließen.

6. Frage: Die Datenträgerauswertung ist seit 2017 in Kraft und sollte in der Form - folgt man der Kritik - nicht geben. Welche Möglichkeit hat der BfDI, um "Druck" auf den Gesetzgeber auszuüben und um Teile des Gesetzes ggf. wieder außer Kraft zu setzen? Inwieweit wurde von den Möglichkeiten Gebrauch gemacht? Gab es derartige Fälle im

Amtsbereich des BfDI bzw. ist das theoretisch möglich (wenn Gesetze derartige datenschutzrechtliche Mängel aufweisen)?

BfDI Office: Der BfDI hat die gesetzliche Aufgabe, den Gesetzgeber in datenschutzrechtlichen Angelegenheiten zu beraten. Es gehört nicht zu seinen Aufgaben und ist auch nicht sein Ziel „Druck auf den Gesetzgeber“ auszuüben.

7. Frage: Welche Mechanismen stehen dem BfDI zu, um letztendlich die Umsetzung datenschutzrechtlicher Aspekte in diesem Fall beim BAMF zu bewirken? Welche zusätzlichen Befugnisse und Ermächtigungen sollte der BfDI rechtlich besitzen, um noch besser die Aufsicht und Kontrolle v.a. über andere Behörden auszuüben?

   BfDI Office: Dem BfDI stehen die in der DSGVO enthaltenen Befugnisse zur Verfügung. Zum Beispiel können wir verwarnen, bestimmte Änderungen anweisen oder in letzter Konsequenz auch die Datenverarbeitung verbieten.

8. Frage: Inwieweit stehen ausreichend finanzielle und personelle Ressourcen dem BfDI zur Verfügung, um einen derartigen Fall stärker und kontinuierlich über mehrere Jahre zu verfolgen, zu kritisieren und öffentlich bekannter zu machen?

BfDI Office: Seit der Selbständigkeit des BfDI am 1. Januar 2016 hat sich die Personalsituation der Dienststelle deutlich verbessert. Bis zum Jahr 2019 konnte ein Stellenzuwachs auf insgesamt 253,5 Planstellen verzeichnet werden. Neben der Einrichtung der notwendigen Behördenstrukturen waren diese Stellen unter anderem für die Erledigung der zusätzlich – insbesondere durch die DSGVO – übertragenen Aufgaben (z. B. Justitiariat, Bußgeldstelle, Zentrale Anlaufstelle, Datenschutzaufsicht über die Finanzbehörden, kommunale Steuerämter und Jobcenter) sowie als Reaktion auf geänderte Verfahrensweisen (z. B. förmliches Beschwerdeverfahren, Vertretung im europäischen Datenschutzausschuss) notwendig. Für das Jahr 2020 hat der Haushaltsgesetzgeber weitere 67 Planstellen zugesprochen. Diese fortschreitende positive Entwicklung begrüßt der BfDI sehr, da dies die Möglichkeiten zur Beratung der beaufsichtigten Stellen, des Bundestages und der Öffentlichkeit stärkt, eine bessere Kontrolle gewährleistet und Ressourcen für verstärkte internationale Kooperation und damit Harmonisierung beim Datenschutz schafft.

9. Frage: Kann der BfDI rechtliche Schritte gegen andere Behörden einlegen bei extremen Verstößen? Unter welchen Umständen? Wenn nein: Wäre dies wünschenswert?

BfDI Office: Die DSGVO gibt uns bereits viele Möglichkeiten unsere Rechtsauffassung durchzusetzen. Da es sich hierbei um Verwaltungsakte handelt, können die Behörden dagegen klagen. Am Ende entscheiden die Gerichte.

Der BfDI stellt im Tätigkeitsbericht 2017/18 fest: "Wegen der unterschiedlichen Auslegung der gesetzlichen Grundlagen zu den Voraussetzungen für die Nutzung der ausgelesenen Daten stehe ich derzeit mit dem BAMF in Kontakt." (S. 66)

10. Frage: Welche "unterschiedlichen Auslegungen der gesetzlichen Grundlagen" sind hier konkret gemeint?

    BfDI Office: Zunächst bestand ein Dissens wegen der Voraussetzungen für die Auswertung der ausgelesenen Daten. Das konnte mittlerweile geklärt werden.

11. Frage: Wie wurde die Kontrolle des BAMF durch den BfDI von 2017 bis 2020 ausgeübt? Als wie effektiv schätzt der BfDI die Maßnahmen bislang ein? Wie gut geht das BAMF auf die Kritik ein?

    BfDI Office: Der BfDI tauscht sich unter anderem mit dem behördlichen Datenschutzbeauftragten des BAMF aus. Außerdem kontrolliert er regelmäßig in der Zentrale und den Außenstellen des BAMF. Kritische Anmerkungen nimmt das BAMF normalerweise umgehend auf und stellt festgestellte Mängel ab.

12. Frage: Wie konkret laufen die Kontrollbesuche des BfDI beim BAMF ab? Wer ist beteiligt und welche Abläufe werden überprüft? Finden vertrauliche Gespräche mit Mitarbeitenden statt? Wie viel Zeit wird pro Besuch eingeplant? Wie werden Prioritäten gesetzt? In welcher Form berichtet das BAMF an den BfDI außerhalb der Kontrollbesuche?

    BfDI Office: Kontrollbesuche gliedern sich in der Regel und drei Phasen: Vorbereitung, Durchführung, Nachbereitung. Im Rahmen der Vorbereitung werden ggf. für die Durchführung des Besuchs erforderliche Unterlagen angefordert und ausgewertet. In Abstimmung mit dem

BAMF wird ein grober Zeitplan ausgearbeitet, der die zu kontrollierenden Stellen und Aufgaben umfasst. Die Kontrolle vor Ort beginnt und endet mit einem Gespräch mit der Behördenleitung, in welchem die beabsichtigten Prüfschritte bzw. die festgestellten Mängel aufgezeigt werden. Der Ablauf einer Kontrolle richtet sich im Wesentlichen nach den zu kontrollierenden Stellen und Aufgaben und kann von technischen Erläuterungen, über Gespräche bis hin zu Arbeitsplatzbesichtigungen reichen. Der zeitliche Rahmen einer Kontrolle richtet sich nach dem Bedarf. In der Vergangenheit wurden stets mehrere Tage, bis zu knapp einer Woche, für Kontroll- und Beratungsbesuche eingeplant. Im Anschluss an den Vor-Ort-Termin wird ein Kontrollbericht erstellt, der dem BAMF zur Stellungnahme zugeleitet wird. Hieran können sich ggf. weiterer Schriftwechsel oder im äußersten Fall auch die o.g. Maßnahmen nach Art. 58 Abs. 2 DSGVO anschließen. Wie bereits oben erläutert, steht der BfDI mit dem BAMF in regelmäßigem Austausch. Darüber hinaus meldet das BAMF z.B. Verstöße gegen datenschutzrechtliche Bestimmungen im Rahmen des Art. 33 DSGVO.

13. Frage: Inwieweit wird vom BAMF eine datenschutzrechtliche Evaluation und Begleitung der Datenträgerauswertung durchgeführt? Seit wann? Mit welchem Ergebnis? Wurde vonseiten des BfDI darauf oder zu ähnlichen Maßnahmen hingewiesen?

BfDI Office: Diese Fragen muss das BAMF beantworten.

14. Frage: Wie verbindlich sind die Hinweise des BfDI für Behörden - in dem Fall das BAMF? Was passiert, wenn das BAMF die bekannten Mängel im Bereich des Datenschutzes nicht einhält - welche Sanktionen

kann der BfDI aussprechen und wie läuft das Verfahren ab?

BfDI Office: Der BfDI kann verbindliche Entscheidungen im Rahmen seiner Abhilfebefugnisse treffen. Vor Erlass einer solchen Maßnahme werden die entsprechenden Stellen angehört. Zudem erhält die zuständige Rechts- oder Fachaufsichtsbehörde Gelegenheit zur Stellungnahme. Sofern die Mängel hiernach noch immer nicht abgestellt sind, wird die entsprechende Maßnahme erlassen.

15. Frage: Inwieweit steht der BfDI in Kontakt mit dem Datenschutzbeauftragten des BAMF? In welchen Punkten stimmt der Datenschutzbeauftragte des BAMF mit der Kritik des BfDI überein und wie wird jetzt ggf. gemeinsam vorgegangen?

BfDI Office: Der BfDI steht in regelmäßigem Kontakt mit dem behördlichen Datenschutzbeauftragten (bDSB) des BAMF. Die Bewertungen der datenschutzrechtlichen Fragestellungen durch den bDSB des BAMF und des BfDI stimmen in der Regel überein. Der bDSB verfügt nicht über vergleichbare bereits o.g. gesetzliche Befugnisse wie der BfDI. Dies schließt jedoch die übereinstimmende gemeinsame Arbeit für einen wirksamen Schutz personenbezogener Daten nicht aus.

D.2 Response of 20 May 2020

Betreff: AW: Ihre Interviewanfrage an den BfDI

Von: Pressestelle Postfach <PRESSESTELLE@bfdi.bund.de>

Datum: 20.05.2020, 08:36

An: Helene Hahn

Sehr geehrte Frau Hahn,

gerne reichen wir Ihnen folgende Antworten nach:

1) Es sind keine entsprechenden Beschwerden bekannt.

2) Eine entsprechende Kontrolle der Datenträgerauswertung beim BAMF wurde vor Inkrafttreten der DSGVO durchgeführt, so dass aktuell keine Erkenntnisse bezüglich der Umsetzung der Informationspflichten nach der DSGVO vorliegen.

Mit freundlichen Grüßen

****

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Pressesprecher

Graurheindorfer Straße 153, 53117 Bonn

Fon: (0228) 9977995100

Fax: (0228) 991077995101

E-Mail: pressestelle@bfdi.bund.de

Internet: http://www.bfdi.bund.de

-----Ursprüngliche Nachricht-----
Von: Helene Hahn
Gesendet: Samstag, 16. Mai 2020 16:08
An: Pressestelle Postfach <PRESSESTELLE@bfdi.bund.de>
Betreff: Re: Ihre Interviewanfrage an den BfDI

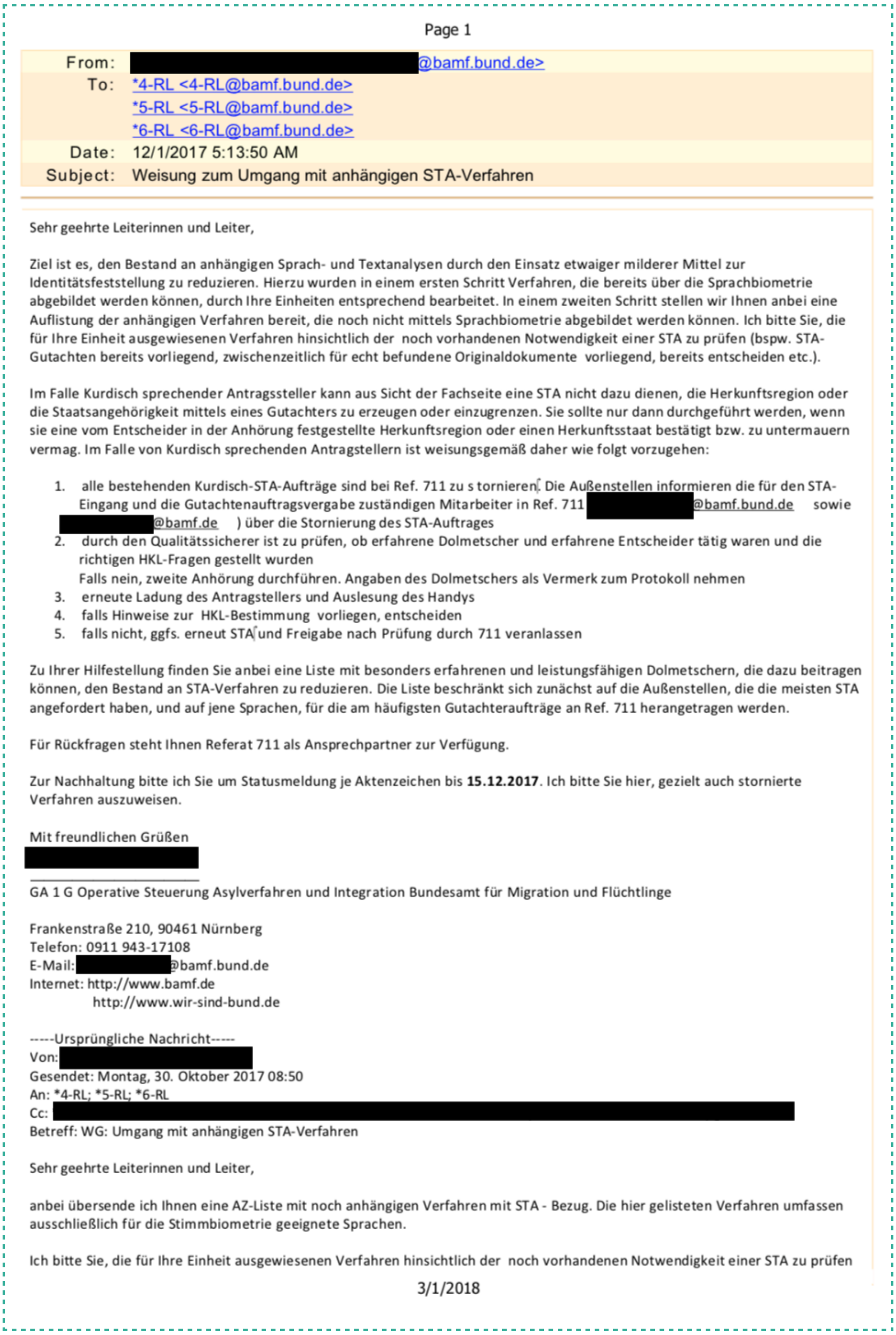
Sehr geehrte Frau (...),
ich bedanke mich für die Antworten. Könnten Sie auf zwei kurze Rückfragen noch eingehen?

1) Wie viele Beschwerden gegen die Datenträgerauswertungen beim BAMF sind von Asylbewerber*innen bzw. geflüchteten Menschen seit 2017 beim BfDI eingegangen (wenn eine Übersicht vorliegt: im Vergleich zu anderen Bevölkerungsgruppen)?

2) Inwieweit hat sich bei der Überprüfung des BAMF vonseiten des BfDI bisher ergeben, dass betroffene Personen im Rahmen der Datenträgerauswertungen nach DSGVO Artikel 12 & 13 über ihre Rechte und die Nutzung/Verarbeitung ihrer Daten informiert werden? Zu welchen Schlüssel ist der BfDI gekommen?

Ich bedanke mich vielmals für die Mühen.
Viele Grüße
Helene Hahn

E Federal Office's internal communication on S-T-As



Page 1

From: [redacted]@bamf.bund.de>
To: *4-RL <4-RL@bamf.bund.de>
*5-RL <5-RL@bamf.bund.de>
*6-RL <6-RL@bamf.bund.de>
Date: 12/1/2017 5:13:50 AM
Subject: Weisung zum Umgang mit anhängigen STA-Verfahren

Sehr geehrte Leiterinnen und Leiter,

Ziel ist es, den Bestand an anhängigen Sprach- und Textanalysen durch den Einsatz etwaiger milderer Mittel zur Identitätsfeststellung zu reduzieren. Hierzu wurden in einem ersten Schritt Verfahren, die bereits über die Sprachbiometrie abgebildet werden können, durch Ihre Einheiten entsprechend bearbeitet. In einem zweiten Schritt stellen wir Ihnen anbei eine Auflistung der anhängigen Verfahren bereit, die noch nicht mittels Sprachbiometrie abgebildet werden können. Ich bitte Sie, die für Ihre Einheit ausgewiesenen Verfahren hinsichtlich der noch vorhandenen Notwendigkeit einer STA zu prüfen (bspw. STA-Gutachten bereits vorliegend, zwischenzeitlich für echt befundene Originaldokumente vorliegend, bereits entscheiden etc.).

Im Falle Kurdisch sprechender Antragssteller kann aus Sicht der Fachseite eine STA nicht dazu dienen, die Herkunftsregion oder die Staatsangehörigkeit mittels eines Gutachters zu erzeugen oder einzugrenzen. Sie sollte nur dann durchgeführt werden, wenn sie eine vom Entscheider in der Anhörung festgestellte Herkunftsregion oder einen Herkunftsstaat bestätigt bzw. zu untermauern vermag. Im Falle von Kurdisch sprechenden Antragstellern ist weisungsgemäß daher wie folgt vorzugehen:

1. alle bestehenden Kurdisch-STA-Aufträge sind bei Ref. 711 zu s tornieren. Die Außenstellen informieren die für den STA-Eingang und die Gutachtenauftragsvergabe zuständigen Mitarbeiter in Ref. 711 [redacted]@bamf.bund.de sowie [redacted]@bamf.de) über die Stornierung des STA-Auftrages
2. durch den Qualitätssicherer ist zu prüfen, ob erfahrene Dolmetscher und erfahrene Entscheider tätig waren und die richtigen HKL-Fragen gestellt wurden
   Falls nein, zweite Anhörung durchführen. Angaben des Dolmetschers als Vermerk zum Protokoll nehmen
3. erneute Ladung des Antragstellers und Auslesung des Handys
4. falls Hinweise zur HKL-Bestimmung vorliegen, entscheiden
5. falls nicht, ggfs. erneut STA und Freigabe nach Prüfung durch 711 veranlassen

Zu Ihrer Hilfestellung finden Sie anbei eine Liste mit besonders erfahrenen und leistungsfähigen Dolmetschern, die dazu beitragen können, den Bestand an STA-Verfahren zu reduzieren. Die Liste beschränkt sich zunächst auf die Außenstellen, die die meisten STA angefordert haben, und auf jene Sprachen, für die am häufigsten Gutachteraufträge an Ref. 711 herangetragen werden.

Für Rückfragen steht Ihnen Referat 711 als Ansprechpartner zur Verfügung.

Zur Nachhaltung bitte ich Sie um Statusmeldung je Aktenzeichen bis **15.12.2017**. Ich bitte Sie hier, gezielt auch stornierte Verfahren auszuweisen.

Mit freundlichen Grüßen
[redacted]
____
GA 1 G Operative Steuerung Asylverfahren und Integration Bundesamt für Migration und Flüchtlinge

Frankenstraße 210, 90461 Nürnberg
Telefon: 0911 943-17108
E-Mail: [redacted]@bamf.bund.de
Internet: http://www.bamf.de
http://www.wir-sind-bund.de

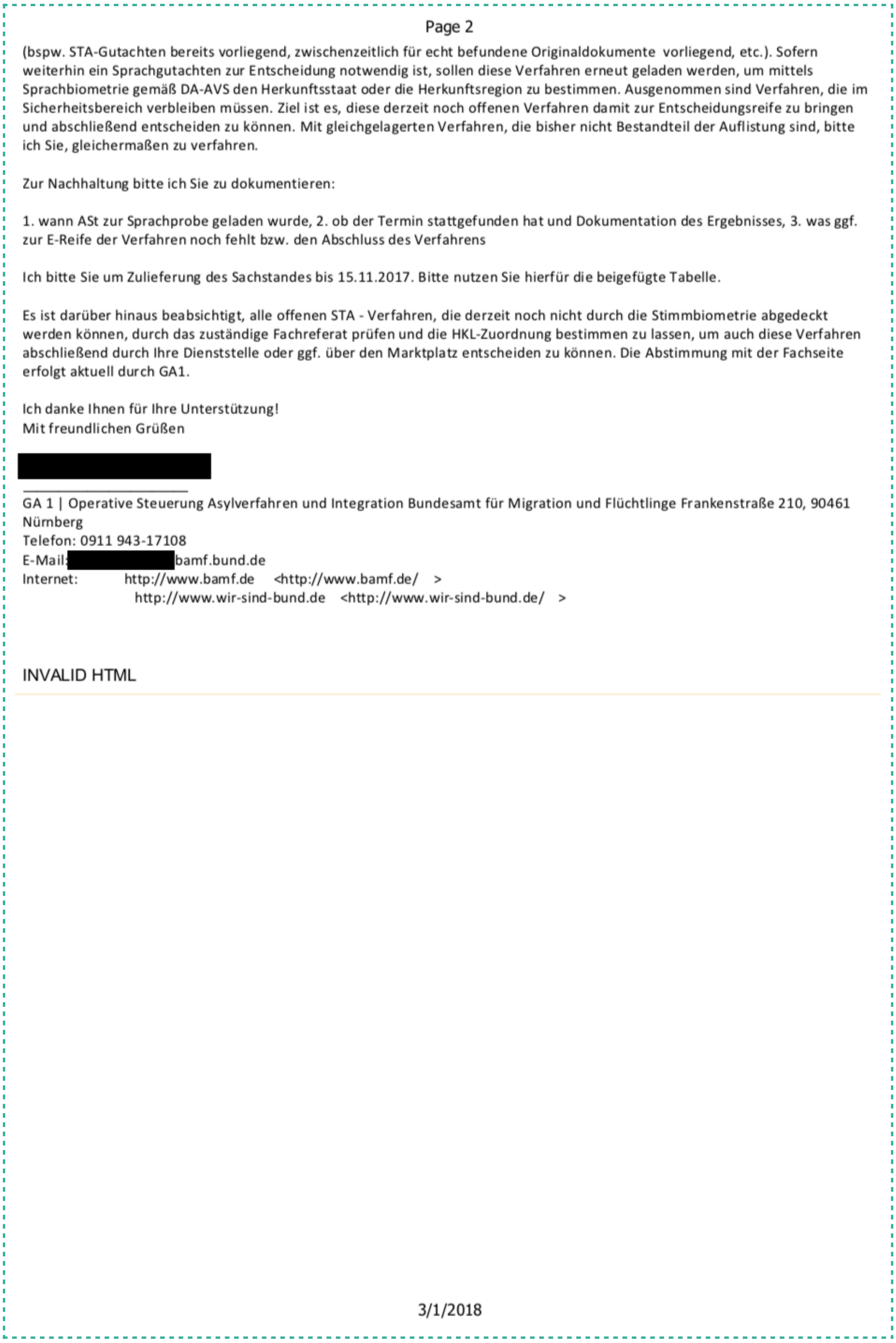
-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Montag, 30. Oktober 2017 08:50
An: *4-RL; *5-RL; *6-RL
Cc: [redacted]
Betreff: WG: Umgang mit anhängigen STA-Verfahren

Sehr geehrte Leiterinnen und Leiter,

anbei übersende ich Ihnen eine AZ-Liste mit noch anhängigen Verfahren mit STA - Bezug. Die hier gelisteten Verfahren umfassen ausschließlich für die Stimmbiometrie geeignete Sprachen.

Ich bitte Sie, die für Ihre Einheit ausgewiesenen Verfahren hinsichtlich der noch vorhandenen Notwendigkeit einer STA zu prüfen

3/1/2018



Page 2

(bspw. STA-Gutachten bereits vorliegend, zwischenzeitlich für echt befundene Originaldokumente vorliegend, etc.). Sofern weiterhin ein Sprachgutachten zur Entscheidung notwendig ist, sollen diese Verfahren erneut geladen werden, um mittels Sprachbiometrie gemäß DA-AVS den Herkunftsstaat oder die Herkunftsregion zu bestimmen. Ausgenommen sind Verfahren, die im Sicherheitsbereich verbleiben müssen. Ziel ist es, diese derzeit noch offenen Verfahren damit zur Entscheidungsreife zu bringen und abschließend entscheiden zu können. Mit gleichgelagerten Verfahren, die bisher nicht Bestandteil der Auflistung sind, bitte ich Sie, gleichermaßen zu verfahren.

Zur Nachhaltung bitte ich Sie zu dokumentieren:

1. wann ASt zur Sprachprobe geladen wurde, 2. ob der Termin stattgefunden hat und Dokumentation des Ergebnisses, 3. was ggf. zur E-Reife der Verfahren noch fehlt bzw. den Abschluss des Verfahrens

Ich bitte Sie um Zulieferung des Sachstandes bis 15.11.2017. Bitte nutzen Sie hierfür die beigefügte Tabelle.

Es ist darüber hinaus beabsichtigt, alle offenen STA - Verfahren, die derzeit noch nicht durch die Stimmbiometrie abgedeckt werden können, durch das zuständige Fachreferat prüfen und die HKL-Zuordnung bestimmen zu lassen, um auch diese Verfahren abschließend durch Ihre Dienststelle oder ggf. über den Marktplatz entscheiden zu können. Die Abstimmung mit der Fachseite erfolgt aktuell durch GA1.

Ich danke Ihnen für Ihre Unterstützung!
Mit freundlichen Grüßen

[redacted]

GA 1 | Operative Steuerung Asylverfahren und Integration Bundesamt für Migration und Flüchtlinge Frankenstraße 210, 90461 Nürnberg
Telefon: 0911 943-17108
E-Mail:[redacted]bamf.bund.de
Internet: http://www.bamf.de <http://www.bamf.de/ >
http://www.wir-sind-bund.de <http://www.wir-sind-bund.de/ >

INVALID HTML

3/1/2018

F Bibliography

African Union. 1990. African Charter on the Rights and Welfare of the Child. Available at: <https://au.int/en/treaties/african-charter-rights-and-welfare-child>.

Agere, Sam. 1999. Promoting good governance. Principles, practices and perspectives. OECD iLibrary. Available at: <https://doi.org/10.14217/9781848597129-en>.

Ahrens, Petra Angela. 2017. Skepsis und Zuversicht. Wie blickt Deutschland auf Flüchtlinge? Sozialwissenschaftliches Institut. Available at: <https://www.siekd.de/wp-content/uploads/2018/06/Skepsis_und_Zuversicht.pdf>.

Ali, Ahmed; Dehak, Najim; Cardinal, Patrick; Khurana, Sameer; Yella, Sree Harsha; Glass, James; Bell, Peter; Renals, Steve. 2016. Automatic dialect detection in Arabic broadcast speech. Available at: <http://dx.doi.org/10.21437/Interspeech.2016-1297>.

Amnesty International. 2017. Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht in der Fassung vom 16.02.2017. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-20-Stellungnahme-Amnesty-zum-Referentenentwurf-Gesetz-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Augsburger Allgemeine. 2018. ZDF: Ermittler bezweifeln afghanische Herkunft des Täters von Würzburg. Available at: <https://www.augsburger-allgemeine.de/bayern/ZDF-Ermittler-bezweifeln-afghanische-Herkunft-des-Taeters-von-Wuerzburg-id38547067.html>.

Aul, Rainer. 2016. Weise verteidigt Maulkorb für Personalrat. BR. Available at: <https://www.br.de/nachrichten/bayern/weise-verteidigt-maulkorb-fuer-personalrat,64uk8chj6gtk0c9k6wv30c9j68w3g>.

BAMF. 2016a. Das Bundesamt in Zahlen: Asyl, Migration und Integration. Available at: <https://www.bamf.de/SharedDocs/Anlagen/DE/Statistik/BundesamtinZahlen/bundesamt-in-zahlen-2015.pdf?__blob=publicationFile&v=16>.

BAMF. 2016b. Organisationsplan. Available at: <http://biaj.de/images/bamf-organigramm-stand-01-10-2016.pdf>.

BAMF. 2017a. Integriertes Identitätsmanagement - Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in die neuen IT-Tools. Schulung AVS-Mitarbeiter, Entscheider und Volljuristen. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung_idms_bamf.pdf>.

BAMF. 2017b. Moderne Technik in Asylverfahren: Vorsitzender der Innenministerkonferenz informiert sich über neue technische Assistenzsysteme. Available at: <https://www.bamf.de/SharedDocs/Meldungen/DE/2017/20170726-am-vorstellung-modellprojekt-bamberg.html?nn=282388>.

BAMF. 2017c. Tool-testing in Bamberg, July 2017 [Facebook]. Available at: <https://www.facebook.com/bamf.socialmedia/posts/wir-haben-gestern-in-bamberg-neue-assistenztools-vorgestellt-die-bei-der-identit/1298844053561819/>.

BAMF. 2017d. Auszeichnung für digitale Transformation und Pioniergeist. Available at:

<https://www.bamf.de/SharedDocs/Meldungen/DE/2017/20170703-digital-leader-award.html?nn=282388>.

BAMF. 2018a. Digitalisation Agenda 2020: Success stories and future digital projects at the Federal Office for Migration and Refugees (BAMF). Third updated edition. Available at: <http://www.wir-sind-bund.de/SharedDocs/Anlagen/EN_nvam/Publikationen/Broschueren/broschuere-digitalisierungsagenda-2020.pdf?__blob=publicationFileY>.

BAMF. 2018b. Sprachbiometrisches Assistenzsystem: Unterstützung der Feststellung von Herkunft und Identität im Asylverfahren. Available at: <https://www.egovernment-wettbewerb.de/praesentationen/2018/Kat_Digitalisierung_BAMF_Sprachbiometrie.pdf>.

BAMF. 2018c. Dienstanweisung Asylverfahren: Identitätsfeststellung. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_identitaetsfeststellung.pdf>.

BAMF. 2018d. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch “Namenstranskription” (TraLitA). Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_namenstranskription.pdf>.

BAMF. 2018e. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch “Sprachbiometrie” (DIAS). Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_sprachbiometrie.pdf>.

BAMF. 2018f. Integriertes Identitätsmanagement IDM-S. Benutzerhandbuch "Auslesen mobiler Datenträger" (AmD). Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/idms_amd.pdf>.

BAMF. 2018g. Integriertes Identitätsmanagement - Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in das IDM-S Tool Auslesen von mobilen Datenträgern (AmD). Schulung AVS-Mitarbeiter. [Training material] <https://fragdenstaat.de/anfrage/foliensatze-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung_avs_kurz.pdf>.

BAMF. 2018h. Safe countries of origin. Available at: <https://www.bamf.de/EN/Themen/AsylFluechtlingsschutz/Sonderverfahren/SichereHerkunftsstaaten/sichereherkunftsstaaten-node.html>.

BAMF. 2018i. Biometrische Sprachsoftware zur Erkennung von Dialekten. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/biometrische-sprachsoftware-zur-erkennung-von-dialekten/>.

BAMF. 2018j. eGovernment Preisverleihung: 1. Platz. Pressemitteilung. Available at: <https://www.bamf.de/SharedDocs/Meldungen/DE/2018/20180621-am-egovernment.html?nn=282388>.

BAMF. 2018k. Dienstanweisung für das AVS. Auslesen von mobilen Datenträgern. Verfahrensweise bei persönlicher Erstantragstellung. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_ams.pdf>.

BAMF. 2018l. Verfahrensverzeichnis: Sprachbiometrisches Assistenzsystem. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/verfahrensverzeichnis/92175/anhang/SprachbiometrischesAssistenzsystem.pdf>.

BAMF. 2018m. Verfahrensverzeichnis: Auslesen mobiler Datenträger. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/verfahrensverzeichnis/92175/anhang/AuslesenmobilerDatentrger.pdf>.

BAMF. 2018n. Weisung zum Umgang mit anhängigen STA-Verfahren. Internal e-mail communication. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/dienstanweisung-vom-1-dezember/>.

BAMF. 2019a. Digitalisierungsagenda 2020: Bisherige Erfolge und Ausblick auf weitere digitale Projekte im Bundesamt für Migration und Flüchtlinge. Fourth updated edition. Available at: <https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/broschuere-digitalisierungsagenda-2020.html>.

BAMF. 2019b. The stages of the German asylum procedure: An overview of the individual procedural steps and the legal basis. Available at: <https://www.bamf.de/SharedDocs/Anlagen/EN/AsylFluechtlingsschutz/Asylverfahren/das-deutsche-asylverfahren.pdf?__blob=publicationFile&v=12>.

BAMF. 2019c. HKL-Anfragen zur Sachaufklärung. Leitfaden für AA-Anfragen und für Gutachten. Dienstanweisung Asylverfahren: Urkunden- und Dokumentenprüfung PTU. Freedom of information request at fragdenstaat.de. Available at:

<https://fragdenstaat.de/anfrage/leitfaden-aadienstanweisung-ptu/415590/anhang/SPRN92119082708120.pdf>.

BAMF. 2019d. BAMF-Chef: Ein Asyl-Chaos wie 2015 wird sich nicht wiederholen! Available at: <https://www.bamf.de/SharedDocs/Interviews/DE/InterviewsFachartikel/191105-interview-dr-sommer-bams.html?nn=282388>.

BAMF. 2019e. Bilder für sprachbiometrische Tests. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/bilder-fur-sprachbiometrische-tests-1/>.

BAMF. 2019f. Testergebnisse biometrischer Sprachsoftware zur Erkennung von Dialekten. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/testergebnisse-biometrischer-sprachsoftware-zur-erkennung-von-dialekten/353954/anhang/2019_697_IFG_NAME_geschwaerzt.pdf>.

BAMF. 2019g. Datenschutz-Folgenabschätzung: Anfrage nach dem Informationsfreiheits-gesetz (IFG). Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/datenschutz-folgeabschatzungen/353952/anhang/2019_689_IFG_Biselli_geschwaerzt.pdf>.

BAMF. 2019h. Wiederrufs- und Rücknahmeverfahren. Available at: <https://www.bamf.de/DE/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/Ausgang/WiderrufRuecknahme/widerrufruecknahme-node.html>.

BAMF. 2019i. Überlassung und Auslesen eines Datenträgers (D1705), Auswertung eines Datenträgers (D1706), Antrag auf Auswertung eines Datenträgers (D1735). Freedom of information request at fragdenstaat.de. Available at:

<https://fragdenstaat.de/anfrage/dokumentenvordrucke/415595/anhang/SPRN92119082708280.pdf>.

BAMF. 2020a. Vice-President Dr. Markus Richter. Available at: <https://www.bamf.de/EN/Behoerde/Aufbau/Vizepraesident/vizepraesident-node.html>.

BAMF. 2020b. Our remit. Available at: <https://www.bamf.de/EN/Behoerde/Aufgaben/aufgaben-node.html>. Effective 23.04.2020.

BAMF. 2020c. The stages of the German asylum procedure (brochure). Available at: <https://www.bamf.de/SharedDocs/Anlagen/EN/AsylFluechtlingsschutz/Asylverfahren/das-deutsche-asylverfahren.html?nn=456422>.

BAMF. 2020d. The implementation of the asylum procedure. Available at: <https://www.bamf.de/EN/Behoerde/Aufgaben/Asylverfahren/asylverfahren-node.html>.

BAMF. 2020e. Ankunft und Registrierung. Available at: <https://www.bamf.de/DE/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/AnkunftRegistrierung/ankunftregistrierung-node.html>.

BAMF. 2020f. The personal interview. Available at: <https://www.bamf.de/EN/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/Anhoerung/anhoerung-node.html>.

BAMF. 2020g. Sicherheit im Kontext von Migration. Available at: <https://www.bamf.de/DE/Themen/Sicherheit/sicherheit-node.html>.

BAMF. 2020h. The President Dr. Hans-Eckhard Sommer. Available at: <https://www.bamf.de/EN/Behoerde/Aufbau/Praesident/praesident-node.html>.

BAMF. 2020i. Digitalisierungsagenda 2020 & IDM-S POC, Kosten-Nutzen, Evaluation, Feedback. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/digitalisierungsagenda-2020-idm-s-poc-kosten-nutzen-evaluation-feedback/482915/anhang/SPRN90620050609180_geschwaerzt.pdf>.

BAMF. 2020j. Ihr Antrag nach dem Informationsfreiheitsgesetz (IFG). Auslesen mobiler Datenträger: FAQ-Liste und Antworten. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/auslesen-mobiler-datentrager-faq-liste-und-antworten/510153/anhang/SPRN91220072208050.pdf>.

BAMF. 2020k. Wichtige Mitteilung: Erstbelehrung. D0179. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/503448/anhang/D0179.pdf>.

BAMF. 2020l. Belehrung von Antragstellenden: Sprachbiometrie (DIAS), Namenstranskription (TraLitA). Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/>.

BAMF. 2020m. Information zur Abgabe einer Sprechprobe für die Sprachbiometrie. D1728. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/503448/anhang/D1728.pdf>.

BAMF. 2020n. Identitätsmanagement. Available at: <https://www.bamf.de/DE/Themen/Sicherheit/Identitaetsmanagement/identitaetsmanagement-node.html>.

BAMF; BFM. 2017. Integriertes Identitätsmanagement - Assistenzsysteme. Available at: <https://docplayer.org/108534301-Presseinformation-integriertes-identitaetsmanagement-assistenzsysteme-1-integriertes-identitaetsmanagement-im-ueberblick.html>.

Baumer, Eric P. S.; Silberman, Six M. 2011. When the implication is not to design (technology). Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. Available at: <https://doi.org/10.1145/1978942.1979275>.

BearingPoint; Cisco. 2020. eGovernment-Wettbewerb. Available at: <https://www.egovernment-wettbewerb.de/>.

Becker, Kerstin. 2017. Stellungnahme des Paritätischen Gesamtverbandes zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht vom 23.02.2017 (BR-Drucksache 179/17). Available at: <https://www.bundestag.de/resource/blob/500018/6088152efe793c12973a8309cf74d627/18-4-825-B-data.pdf>.

Beetham, David. 1991. The legitimation of power. Basingstoke: Palgrave Macmillan.

Bekkers, Viktor; Edwards, Arthur. 2007. Legitimacy and democracy: A conceptual framework for assessing governance practices. In: Bekkers, Viktor; Dijkstra, Geske; Edwards, Arthur; Fenger, Menno (Eds.). 2007. Governance and the democratic deficit. Assessing the democratic legitimacy of governance practices. Aldershot: Ashgate.

Bekkers, Viktor; Dijkstra, Geske; Edwards, Arthur; Fenger, Menno (Eds.). 2007. Governance and the democratic deficit. Assessing the democratic legitimacy of governance practices. Aldershot: Ashgate.

Betts, Alexander. 2015. Human migration will be a defining issue of this century. How best to cope? The Guardian. Available at: <https://www.theguardian.com/commentisfree/2015/sep/20/migrants-refugees-asylum-seekers-21st-century-trend>.

Bewarder, Manuel; Flade, Florian. 2018. Viele Behörden können Identität von Asylbewerbern nicht prüfen. Available at: <https://www.welt.de/politik/deutschland/article176623392/Fluechtlingskrise-Viele-Behoerden-koennen-keine-Fingerabdruecke-ueberpruefen.html>.

BfDI. 2017. Tätigkeitsbericht zum Datenschutz 2015 - 2016. 26. Tätigkeitsbericht. Available at: <https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.html?nn=5217212>.

BfDI. 2019. Tätigkeitsbericht zum Datenschutz 2017 - 2018. 27. Tätigkeitsbericht. Available at: <https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/27TB_17_18.html?nn=5217212>.

Bhattacherjee, Anol. 2012. Social science research: Principles, methods, and practices. University of South Florida. Textbooks Collection. Book 3. Available at: <https://scholarcommons.usf.edu/oa_textbooks/3>.

Biselli, Anna. 2017a. Digitalisierte Migrationskontrolle: Wenn Technik über Asyl entscheidet. Netzpolitik.org. Available at: <https://netzpolitik.org/2017/digitalisierte-migrationskontrolle-wenn-technik-ueber-asyl-entscheidet/>.

Biselli, Anna. 2017b. Syrien oder Ägypten? Software zur Dialektanalyse ist fehleranfällig und intransparent. Netzpolitik.org. Available at: <https://netzpolitik.org/2017/syrien-oder-aegypten-software-zur-dialektanalyse-ist-fehleranfaellig-und-intransparent/>.

Biselli, Anna. 2018. Eine Software des BAMF bringt Menschen in Gefahr. Available at: <https://www.vice.com/de/article/a3q8wj/fluechtlinge-bamf-sprachanalyse-software-entscheidet-asyl>.

Biselli, Anna; Beckmann, Lea. 2020. Invading refugees' phones: Digital forms of migration control in Germany and Europe. Gesellschaft für Freiheitsrechte e.V.. Available at: <https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf>.

BMF. 2020. Gesetze und Gesetzesvorhaben. Available at: <https://www.bundesfinanzministerium.de/Web/DE/Service/Gesetze_Gesetzesvorhaben/Gesetze_Gesetzgebungsvorhaben.html>.

BMI. 2011. Joint Rules of Procedure of the Federal Ministries (GGO). Available at: <https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/moderne-verwaltung/ggo_en.pdf?__blob=publicationFile&v=1>.

BMI. 2016. Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes. Vom 6. April. 2016. BAnz AT 25.04.2016 B1. Available at: <https://rp-darmstadt.hessen.de/sites/rp-darmstadt.hessen.de/files/content-downloads/16-04-06_Allgemeinverf%C3%BCgung%20BMI%20%C3%BCber%20die%20Anerkennung%20eines%20ausl%C3%A4ndischen%20Passes%20oder%20Passersatzes.pdf>.

BMI. 2017a. Wechsel an der Spitze des Bundesamtes für Migration und

Flüchtlinge. Verabschiedung von Dr. Frank-Jürgen Weise und Ernennung von Jutta Cordt zur neuen Präsidentin des BAMF. Available at: <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/01/amtswechsel-bamf.html>.

BMI. 2017b. Von Herrn MdB Roland Claus erbetene Sachinformation. Available at: <https://cdn.netzpolitik.org/wp-upload/2017/12/nuance.pdf>.

BMI. 2017c. Referentenentwurf des Bundesministeriums des Innern. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-15-Referentenentwurf-Gesetz-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

BMI. 2017d. Änderungen zur Erleichterung von Abschiebungen auf den Weg gebracht. Available at: <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/02/kabinettsbeschluss-ausreisepflicht.html>.

BMI. 2018a. Digitalisierungsvorhaben des Bundesministeriums des Innern sowie des Bundes im Gesamtkontext Asyl. Available at: <https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/25_Sitzung/19_I_DAS.pdf?__blob=publicationFile&v=2>.

BMI. 2018b. Schriftliche Fragen des Abgeordneten Alexander Ullrich: Monat Juni 2018. Arbeits-Nr. 6/225. Available at: <https://andrej-hunko.de/start/download/dokumente/1186-software-fuer-sprachbiometrie-forensik-handyauswertung-beim-bamf-mdb-alexander-ulrich/file>.

BMI. 2018c. Masterplan Migration: Maßnahmen zur Ordnung, Steuerung und Begrenzung der Zuwanderung. Available at:

<https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/migration/masterplan-migration.pdf;jsessionid=5E020B5EAB7C82F1212A991138115293.1_cid364?__blob=publicationFile&v=7>.

BMJV. 2016. Asylum Act. Available at: <https://www.gesetze-im-internet.de/englisch_asylvfg/englisch_asylvfg.html#p0177>.

BMJV. 2017a. Residence Act. Section 48: Obligations relating to identification papers. Section 48a: Collection of access data. Available at: <https://www.gesetze-im-internet.de/englisch_aufenthg/englisch_aufenthg.html#p1007>.

BMJV. 2017b. Residence Act. Section 48a: Collection of access data. Available at: <https://www.gesetze-im-internet.de/englisch_aufenthg/englisch_aufenthg.html#p1018>.

BMJV. 2019a. Gesetz über das Ausländerzentralregister (AZR-Gesetz). Available at: <https://www.gesetze-im-internet.de/azrg/BJNR226500994.html#BJNR226500994BJNG000200000>.

BMJV. 2019b. Basic Law for the Federal Republic of Germany. Available at: <https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0023>.

BMJV. 2020. Asylgesetz. Available at: <https://www.gesetze-im-internet.de/asylvfg_1992/>.

Bohlin, Anna. 2008. Protection at the cost of privacy? A study of the biometric registration of refugees. Available at: <http://lup.lub.lu.se/student-papers/record/1556387>.

Boyd, Danah; Crawford, Kate. 2012. Critical questions for big data. Information, Communication & Society. Volume 15(5): pp. 662-679. Available at: <https://doi.org/10.1080/1369118X.2012.678878>.

Broussard, Meredith. 2018. Artificial Unintelligence: How computers misunderstand the world. MIT Press.

BumF. 2017. Stellungnahme des Bundesfachverband unbegleitete minderjährige Flüchtlinge (BumF) zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-17-Stellungnahme-BumF-Entwurf-eines-Gesetzes-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Burzcyk, Dirk. 2016. Geflüchtete als Datenmasse: Riesiger Datenpool für viele Behörden. Netzpolitik.org. Available at: <https://netzpolitik.org/2016/gefluechtete-als-datenmasse-riesiger-datenpool-fuer-viele-behoerden/>.

BVA. 2016. Digitalisierung von Asylverfahren: Bundesverwaltungsamt nimmt ersten wichtigen Meilenstein. Available at: <https://www.bva.bund.de/SharedDocs/Kurzmeldungen/DE/Aufgaben/S/AZR/2016-03-31-DAVG_Erster%20Meilenstein.html?nn=44066>.

BVerfG. 2008. Judgment of the First Senate of 27 February 2008. 1 BvR 370/07. Paras. 1-333. Available at: <http://www.bverfg.de/e/rs20080227_1bvr037007en.html>.

Castro Varela, Maria do Mar. 2014. Interview: Prof. Dr. Maria do Mar Castro Varela zur aktuellen Debatte um Willkommenskultur. In: Szuktisch, Yvonne and Merx, Andreas (Eds.). Inklusiv, offen und gerecht? Deutschlands langer Weg zu einer Willkommenskultur.

Dossier zum Thema: pp. 42-45. Munich: IQ- Fachstelle Diversity Management. Available at: <https://www.netzwerk-iq.de/fileadmin/Redaktion/Downloads/IQ_Publikationen/Thema_Vielfalt_gestalten/2014_Broschuere_Willkommenskultur.pdf>.

Clarke, Amanda. 2017. Digital government units: origins, orthodoxy and critical considerations for public management theory and practice. Available at: <https://dx.doi.org/10.2139/ssrn.3001188>.

Clarke, Amanda; Lindquist, Evert A.; Roy, Jeffrey. 2017. Understanding governance in the digital era: An agenda for public administration research in Canada. Canadian Public Administration. Volume 60 (4): pp. 457-475. Available at: <https://doi.org/10.1111/capa.12246>.

Classen, Georg. 2016. Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken (Datenaustauschverbesserungsgesetz). Flüchtlingsrat Berlin e.V.. Available at: <https://www.proasyl.de/wp-content/uploads/2016/01/FlueRatBln_Stellungnahme_DatenaustauschG_2016.pdf>.

Council of Europe. 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series - No. 108. Available at: <https://rm.coe.int/1680078b37>.

Dalton, Craig; Thatcher, Jim. 2014. What does a critical data studies look like, and why do we care? Space and Society. Available at: <https://www.societyandspace.org/articles/what-does-a-critical-data-studies-look-like-and-why-do-we-care>.

DEK. 2019. Gutachten der Datenethikkommission der Bundesregierung. Kurzfassung. Available at:

<https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_Kurzfassung.pdf?__blob=publicationFile&v=2>.

Dencik, Lina; Hintz, Arne; Redden, Joanna; Treré, Emiliano. 2019. Exploring data justice: Conceptions, applications and directions. Information, Communication & Society. Volume 22(7): pp. 873-881. Available at: <https://doi.org/10.1080/1369118X.2019.1606268>.

Dencik, Lina; Jansen, Fieke; Metcalfe, Philippa. 2018. A conceptual framework for approaching social justice in an age of datafication. Available at: <https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/>.

Dernbach, Andrea. 2019. Bis zu 30 Asylgesetze in fünf Jahren. Die unnötige Hektik der GroKo in der Flüchtlingspolitik. Der Tagesspiegel. Available at: <https://www.tagesspiegel.de/politik/bis-zu-30-asylgesetze-in-fuenf-jahren-die-unnoetige-hektik-der-groko-in-der-fluechtlingspolitik/24353146.html>.

Diekmann, Andreas. 2005. Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

Donner, Jonathan. 2018. The difference between digital identity, identification, and ID. Available at: <https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563>.

DW. 2020. Germany: Refugees sue the government for invasion of privacy. Available at: <https://www.dw.com/en/germany-refugees-sue-the-government-for-invasion-of-privacy/a-53345609>.

ECRE. 2017. The concept of vulnerability in European asylum procedures. Asylum Information Database (AIDA). Available at: <http://www.asylumineurope.org/sites/default/files/shadow-reports/aida_vulnerability_in_asylum_procedures.pdf>.

ECtHR. 2011. Case of M.S.S. v. Belgium and Greece. Application No. 30696/09. Judgment of January 21, 2011. Available at: <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-103050%22]}>.

ECHR. 1950. European Convention on Human Rights. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

EDPS. 2012. Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [.....] (Recast version). Available at: <https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf>.

Eralp, Nilgün A. 2016. Challenges of the German-led refugee deal between Turkey and the EU. CESinfo Forum. Volume 2. Available at: <https://www.ifo.de/DocDL/forum-2016-2-eralp-turkey-germany-june.pdf>.

Erlingsson, Christen; Brysiewicz, Petra. 2017. A hands-on guide to doing content analysis. African Journal of Emergency Medicine. Volume 7(3): pp. 93-99. Available at: <https://doi.org/10.1016/j.afjem.2017.08.001>.

European Union. 2012. Charter of the Fundamental Rights of the European Union. 2012/C/326/02. Available at: <https://www.refworld.org/docid/3ae6b3b70.html>.

European Union. 2016. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. L119. Volume 59. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2016:119:TOC>.

Farraj, Achraf. 2011. Refugees and the biometric future: The impact of biometrics on refugees and asylum seekers. Columbia Human Rights Law Review. Volume 42(3): pp. 891-942. Available at: <https://iow.eui.eu/wp-content/uploads/sites/18/2013/04/07-Rijpma-Background4-Refugees-and-Biometrics.pdf>.

Federal Council. 2017. Stellungnahme des Bundesrates: Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Drucksache 179/17. Available at: <https://dipbt.bundestag.de/dip21/brd/2017/0179-17B.pdf>.

Federal Government. 2017a. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 179/17. Available at: <https://dipbt.bundestag.de/dip21/brd/2017/0179-17.pdf>.

Federal Government. 2017b. Gesetzentwurf der Bundesregierung: Entwurf eines Gesetztes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 18/11546. Available at: <https://dipbt.bundestag.de/dip21/btd/18/115/1811546.pdf>.

Federal Government. 2017c. Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung. Drucksache 18/12415. Available at: <https://dipbt.bundestag.de/dip21/btd/18/124/1812415.pdf>.

Federal Government. 2017d. Ausreisepflicht besser durchsetzen. Available at: <https://www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/ausreisepflicht-besser-durchsetzen-187350>.

Federal Government. 2017e. Themen im Bundeskabinett - Ergebnisse. 137. Sitzung am 22. Februar 2017. Available at: <https://www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/kabinettssitzungen/themen-im-bundeskabinett-ergebnisse-490322>.

Federal Government; McKinsey. 2016. Contract agreement. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/aktueller-rahmenvertrag-mit-mckinsey/100149/anhang/1.VertraggegengezeichnetAN.pdf>.

Fenger, Menno; Bekkers, Viktor. 2007. The governance concept in public administration. In: Bekkers, Viktor; Dijkstra, Geske; Edwards, Arthur; Fenger, Menno (Eds.). 2007. Governance and the democratic deficit. Assessing the democratic legitimacy of governance practices. Aldershot: Ashgate.

Fleischmann, Larissa; Steinhilper, Elias. 2017. The myth of apolitical volunteering for refugees: German welcome culture and a new disposition of helping. In: Social Inclusion. Volume 5(3): pp. 17-27. 2017. Available at: <http://dx.doi.org/10.17645/si.v5i3.945>.

Frank, Dorothee. 2018. Digitale Unterstützer im Asylverfahren: Wie Sprachbiometrie Asylentscheidungen auf eine noch breitere Grundlage stellt. In: Cyber Security Report/ Sicherheitstechnischer Report. 2018. Mittler Report Verlag GmbH.

Funk, Nanette. 2016. A spectre in Germany: refugees, a 'welcome culture' and an 'integration politics'. In: Journal of Global Ethics. Volume 12(3):

pp. 289-299. Available at: <https://doi.org/10.1080/17449626.2016.1252785>.

Georgi, Fabian. 2016. Widersprüche im langen Sommer der Migration. Ansätze einer materialistischen Grenzregimeanalyse. In: Prokla. Zeitschrift für kritische Sozialwissenschaft. Volume 46(183): pp. 183-203. Available at: <https://doi.org/10.32387/prokla.v46i183.108>.

Gerhards, Jurgen; Hans, Silke; Schupp, Jürgen. 2016. The barometer of public opinion on refugees in Germany. DIW Economic Bulletin. No. 21. 2016. Available at: <https://www.diw.de/documents/publikationen/73/diw_01.c.534664.de/diw_econ_bull_2016-21-1.pdf>.

German Bar Association. 2017. Stellungnahme des Deutschen Anwaltverein durch den Ausschuss Gefahrenabwehrrecht zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht (BT-Drs. 18/11546). Available at: <https://anwaltverein.de/de/newsroom/sn-39-17-gesetz-zur-besseren-durchsetzung-der-ausreisepflicht-60305>.

German Bundestag. 2017a. Wortprotokoll der 111. Sitzung. Innenausschuss. Öffentliche Anhörung. Protokoll-Nr. 18/111. Available at: <https://www.bundestag.de/resource/blob/511642/d4c03aa26137310cf5568fa7e9f179fc/Protokoll-111-Sitzung-data.pdf>.

German Bundestag. 2017b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Petra Sitte, Anke Domscheit-Beim Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/190. Available at: <https://dipbt.bundestag.de/doc/btd/19/001/1900190.pdf>.

German Bundestag. 2017c. De Maizière: Entschlossen gegen radikalislamische Gefährder vorgehen. Available at: <https://www.bundestag.de/dokumente/textarchiv/2017/kw03-aktuelle-stunde-gefaehrder-488828>.

German Bundestag. 2017d. Stenografischer Bericht. 225. Sitzung. Plenarprotokoll 18/225. Available at: <https://dipbt.bundestag.de/dip21/btp/18/18225.pdf>.

German Bundestag. 2017e. Stenografischer Bericht. 234. Sitzung. Plenarprotokoll 18/234. Available at: <https://dipbt.bundestag.de/dip21/btp/18/18234.pdf>.

German Bundestag. 2017f. Pläne zur Ausreisepflicht unter Sachverständigen umstritten. Available at: <https://www.bundestag.de/dokumente/textarchiv/2017/kw13-pa-innen-ausreise-499064>.

German Bundestag. 2017g. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Frank Tempel, Sevim Dağdelen, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 18/11262. Available at: <https://www.ulla-jelpke.de/wp-content/uploads/2017/02/1811262-Asylstatistik-IV-2016-1.pdf>.

German Bundestag. 2018a. Antwort der Bundesregierung auf die kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/6647. Available at: <https://dip21.bundestag.de/dip21/btd/19/066/1906647.pdf>.

German Bundestag. 2018b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-

Drucksache 19/1631. Available at: <https://dipbt.bundestag.de/dip21/btd/19/016/1901631.pdf>.

German Bundestag. 2018c. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 19/3886. Ergänzende Informationen zur Asylstatistik für das zweite Quartal des Jahres 2018. BT-Drucksache 19/4961. Available at: <https://dipbt.bundestag.de/dip21/btd/19/049/1904961.pdf>.

German Bundestag. 2018d. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von Spracherkennungssoftware durch das Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/1663. Available at: <https://dipbt.bundestag.de/dip21/btd/19/016/1901663.pdf>.

German Bundestag. 2019a. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2018. BT-Drucksache 19/8701. Available at: <https://dip21.bundestag.de/dip21/btd/19/087/1908701.pdf>.

German Bundestag. 2019b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/13945. Available at: <https://dip21.bundestag.de/dip21/btd/19/139/1913945.pdf>.

German Bundestag. 2020a. Die Anfrage - ein wichtiges Recht der

Parlamentarier. Available at: <https://www.bundestag.de/webarchiv/textarchiv/2011/37215383_kw52_instrumente_bundestag-207296>.

German Bundestag. 2020b. Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken (Datenaustauschverbesserungsgesetz). Dokumentations- und Informationssystem DIP. ID: 18-71011. Available at: <https://dipbt.bundestag.de/extrakt/ba/WP18/710/71011.html>.

German Bundestag. 2020c. Gesetz zur besseren Durchsetzung der Ausreisepflicht. Dokumentations- und Informationssystem DIP. ID: 18-80058. Available at: <https://dipbt.bundestag.de/extrakt/ba/WP18/800/80058.html>.

German Bundestag. 2020d. Ausschüsse der 18. Wahlperiode. Öffentliche Anhörung am Montag, dem 27. März 2017, 16.00 Uhr zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht - BT - Drucksache 18/11546. Archiv. Available at: <https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse18/a04/anhoerungen/111-sitzung-inhalt-499212>.

German Bundestag. 2020e. Geschäftsordnung des Deutschen Bundestages und Geschäftsordnung des Vermittlungsausschusses. Available at: <https://www.btg-bestellservice.de/pdf/10080000.pdf>.

German Bundestag. 2020f. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2019. BT-Drucksache 19/18498. Available at: <https://dip21.bundestag.de/dip21/btd/19/184/1918498.pdf>.

Gilley, Bruce. 2006. The meaning and measures of state legitimacy: Results for 72 countries. In: European Journal of Political Research. Volume 25: pp. 499-525. Available at: <https://doi.org/10.1111/j.1475-6765.2006.00307.x>.

Goffey, Andrew. 2008. Algorithm. In: Fuller, Matthew (Ed.). Software studies: a lexicon. London: MIT Press.

Graham, John; Amos, Bruse; Plumptre, Tim. 2003. Principles for good governance in the 21st century. Policy brief no. 15. Institute on Governance. Available at: <https://iog.ca/docs/2003_August_policybrief15.pdf>.

Green, Ben; Viljoen, Salomé. 2020. Algorithmic realism: Expanding the boundaries of algorithmic thought. In: Conference on Fairness, Accountability, and Transparency (FAT '20). New York: ACM. Available at: <https://doi.org/10.1145/3351095.3372840>.

Greis, Friedhelm. 2018. Deutsche Behörden nutzen sieben Anbieter zum Handy-Auslesen. Available at: <https://www.golem.de/news/digitale-forensik-deutsche-behoerden-nutzen-sieben-anbieter-zum-handy-auslesen-1808-136030.html>.

Grote, Janne. 2018. Die veränderte Fluchtmigration in den Jahren 2014 bis 2016: Reaktionen und Maßnahmen in Deutschland. Fokusstudie der deutschen nationalen Kontaktstelle für das Europäische Migrationsnetzwerk (EMN). BAMF. 2018. Available at: <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11b_germany_changing_influx_final_de_0.pdf>.

Guterres, António. 2014. Europe must give Syrian refugees a home. The Guardian. Available at:

<https://www.theguardian.com/commentisfree/2014/jul/22/europe-syrian-asylum-seekers-refugees-illegal-trafficking>.

Guterres, António. 2015. Displacement of people "getting out of control in world at war." UN News. Available at: <https://news.un.org/en/audio/2015/06/601592>.

Hamann, Ulrike; Karakayli, Serhat. 2016. Practicing Willkommenskultur: Migration and solidarity in Germany. In: Intersections. East European Journal of Society and Politics. Volume 2(4): pp. 70-86. Available at: <https://doi.org/10.17356/ieejsp.v2i4.296>.

Hankey, Stephanie; Tuszynski, Marek. 2017. Efficiency and madness. Using data and technology to solve social, environmental and political problems. Heinrich Böll Foundation. Available at: <https://www.boell.de/en/2017/11/28/efficiency-and-madness-using-data-and-technologyto-solve-social-environmental-and-political-problems>.

Haverland, Markus; Yanow, Dvora. 2012. A hitchhiker's guide to the public administration research universe: Surviving conversations on methodologies and methods. Public Administration Review. Volume 72. Available at: <https://ssrn.com/abstract=1860105>.

Hawkesworth, Mary. 2006. Contending conceptions of science and politics. Methodology and the constitution of the political. In: Yanow, Dvora; Schwartz-Shea, Peregrine (Eds.). 2006. Interpretation and method: Empirical research and the interpretive turn. Armonk, New York: M. E. Sharpe.

Heeks, Richard. 2017. A structural model and manifesto for data justice for international development. Development Informatics Working Paper No. 69. Available at: <http://dx.doi.org/10.2139/ssrn.3431729>.

Heeks, Richard; Shekhar, Satyarupa. 2019. Datafication, development and marginalised urban communities: An applied data justice framework. Information, Communication & Society. Volume 22(7): pp. 992-1011. Available at: <https://doi.org/10.1080/1369118X.2019.1599039>.

Helbling, Marc; Schoen, Alexandra; Zindler, Armgard; Kossatz, Daniela; Frieß, Hans-Jürgen; Stavenhagen, Liane; Kiefer, Katja; Negrea, Nicoleta; Gray, Emily; Grimm, Robert; Hawkins, Stephen; Dixon, Tim; Wolff, Vincent; Juan-Torres, Míriam. 2017. Attitudes towards national identity, immigration, and refugees in Germany. Available at: <https://static1.squarespace.com/static/5a70a7c3010027736a22740f/t/5aec6160562fa73b77551801/1525440870626/More+in+Common+Germany+Report+Executive+Summary.pdf>.

Hissenbaum, Helen. 1997. Toward an approach to privacy in public: Challenges of information technology. Ethics & Behavior. Volume 7(3): pp. 207-219. Available at: <https://nissenbaum.tech.cornell.edu/papers/toward_an_approach.pdf>.

Idler, Julia; Mantel, Johanna. 2016. Memorandum für faire und sorgfältige Asylverfahren in Deutschland. Standards zur Gewährleistung der asylrechtlichen Verfahrensgarantien. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/Memorandum-f%C3%BCr-faire-und-sorgf%C3%A4ltige-Asylverfahren-in-Deutschland-2016.pdf>.

IT Planning Council. 2016. Aktionsplan des IT-Planungsrats für das Jahr 2016. Beschluss des IT-Planungsrats vom 1. Oktober 2015. Ergänzt durch die Beschlüsse des IT-Planungsrats vom 16. März 2016 und 16. Juni 2016. Available at: <https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/18_Sitzung/41_Aktionsplan.pdf?__blob=publicationFile&v=9>.

IT Planning Council; BMI. 2018. Koordinierungsprojekt Digitalisierung des Asylverfahrens. Zusammenfassung der Projektergebnisse. Available at: <https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/27_Sitzung/TOP13_Anlage2_DigAsyl.pdf?__blob=publicationFile&v=2>.

Jehle, Stefan. 2016. Lange Schlangen in Karlsruhe. Flüchtlinge müssen dreimal anstehen. Stuttgarter Zeitung. Available at: <https://www.stuttgarter-zeitung.de/inhalt.lange-schlangen-in-karlsruhe-fluechtlinge-muessen-dreimal-anstehen.efbc003a-243d-44d5-92ac-78e2b6baa5f8.html>.

Jelpke, Ulla. 2020. Gerichte korrigierten 2019 mehr als jeden vierten Asyl-Bescheid. Pressemitteilung von Ulla Jelpke, 17. April 2020. Available at: <https://www.linksfraktion.de/presse/pressemitteilungen/detail/gerichte-korrigierten-2019-mehr-als-jeden-vierten-asyl-bescheid/>.

Juiz, Carlos; Guerrero, Carlos; Lera, Isaac. 2014. Implementing good governance principles for the public sector in information technology governance frameworks. Open Journal of Accounting. Volume 3(1): pp. 9-27. Available at: <http://dx.doi.org/10.4236/ojacct.2014.31003>.

Karakayli, Serhat; Kleist, Olaf. 2016. EFA-Studie 2: Strukturen und Motive der ehrenamtlichen Flüchtlingsarbeit (EFA) in Deutschland. Berliner Institut für empirische Integrations- und Migrationsforschung. Available at: <https://fluechtlingsrat-brandenburg.de/wp-content/uploads/2016/08/Studie_EFA2_BIM_11082016_VOE.pdf>.

Kastner, Bernd. 2017. Software für die Sicherheit. Süddeutsche Zeitung. Available at: <https://www.sueddeutsche.de/politik/asylbewerber-software-fuer-die-sicherheit-1.3602853>.

Kaurin, Dragana. 2019. Data protection and digital agency for refugees. Centre for International Governance Innovation. World Refugee Council Research Paper No. 12. Available at: <https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees>.

Keiner, Alexandra E. 2020. Algorithmen im Asylprozess. Legitimität von Algorithmen in politischen Verwaltungsorganisationen am Beispiel der Dialekterkennungssoftware des BAMF. In: FIfF-Kommunikation 1/20: pp. 71-75. Available at: <https://www.fiff.de/publikationen/fiff-kommunikation/fk-2020/fk-2020-1/fk-1-20-p71.pdf>.

Keping, Yu. 2017. Governance and good governance: A new framework for political analysis. Fudan Journal of the Humanities and Social Sciences. Volume 11(1): pp. 1-8. Available at: <https://doi.org/10.1007/s40647-017-0197-4>.

Keßler, Stefan. 2017. Stellungnahme des Jesuiten-Flüchtlingsdienstes Deutschland zum Referentenentwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-16-Stellungnahme-Jesuiten-Fl%C3%BCchtlingsdienst-Gesetzentwurf-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Kift, Paula. 2016. In search of safe harbors - privacy and surveillance of refugees at the borders of Europe. Conference of the Association of Internet Researchers. Available at: <https://journals.uic.edu/ojs/index.php/spir/article/view/8669/6897>.

Kioe Sheng, Yap. 2009. What is good governance? United Nations. Economic and Social Commission for Asia and the Pacific (ESCAP). Available at: <https://www.unescap.org/resources/what-good-governance>.

Kitchin, Rob; Tracey, Lauriault. 2014. Towards critical data studies: Charting and unpacking data asemblages and their work. The Programmable City Working Paper 2; pre-print version of chapter to be published in Eckert, J., Shears, A. and Thatcher, J. (Eds.) Geoweb and Big Data. University of Nebraska Press. Forthcoming. Available at: <https://ssrn.com/abstract=2474112>.

Klages, Robert. 2017. Oberleutnant unter Terrorverdacht festgenommen. Available at: <https://www.tagesspiegel.de/politik/bundeswehr-oberleutnant-unter-terrorverdacht-festgenommen/19725936.html>.

Kuckartz, Udo. 2007. Einführung in die computergestützte Analyse qualitativer Daten. Wiesbaden: VS Verlag für Sozialwissenschaften.

Latonero, Mark; Hiatt, Keith; Napolitano, Antonella; Clericetti, Giulia; Penagos, Melanie. 2019. Digital identity in the migration and refugee context: Italy case study. Data & Society. CILD. Available at: <https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf>.

Lethbridge. 2017. Privatisation of migration and refugee services and other forms of state disengagement. European Public Service Union. Available at: <https://www.world-psi.org/sites/default/files/documents/research/final_psi_epsu_psiru_privatisation_of_migration_and_refugee_services.pdf>.

Levi, Margaret. 2020. A state of trust. Forthcoming as chapter 4 in: Braithwaite, Valeria and Levi, Margaret (Eds.). Trust and Governance. New York: Russell Sage Foundation. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.452.7186&rep=rep1&type=pdf>.

Lobenstein, Caterina. 2017. Behörde auf Speed: Unternehmensberater haben das Bundesamt für Migration und Flüchtlinge auf Effizienz getrimmt. Zulasten der Flüchtlinge – und der Gerichte, bei denen sich die Klagen stapeln. Available at: <https://www.zeit.de/2017/14/bamf-unternehmensberater-geschwindigkeiten-folgen-fluechtlinge/komplettansicht>.

Loheide, Maria. 2017. Stellungnahme der Diakonie Deutschland - Evangelischer Bundesverband zum Referentenentwurf des Bundesministeriums des Innern: Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-02-17-Stellungnahme-Diakonie-Gesetz-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

Luhmann, Niklas. 1983. Legitimation durch Verfahren. Frankfurt am Main: Suhrkamp Verlag. Available at: <https://epdf.pub/legitimation-durch-verfahren-german.html>.

Lukács, Adrienn. 2016. What is privacy? The history and definition of privacy. Available at: <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>.

Magno, Francisco; Serafica, Ramonette B. 2001. Information technology for good governance. Yuchengco Centre for East Asia. De La Salle University. Available at: <https://www.academia.edu/36097691/Information_Technology_for_Good_Governance>.

Mayring, Philipp. 2000. Qualitative content analysis. Forum: Qualitative Social Research. Volume 1(2): 20. Available at: <http://dx.doi.org/10.17169/fqs-1.2.1089>.

McKinsey; BAMF (2016): Rückkehr: Prozesse und Optimierungspotenziale. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/dokumente/76/>.

Meijer, Albert J.; Bovens, Mark. 2003. Public accountability in the information age. In: E-government. Workshop in conjunction with JURIX 2003. Palmirani, M.; van Engers, T.; Wimmer, M.A. (Eds.). International Federation for Information Processing. Laxenburg (Austria). 2003: pp. 16-28. Available at: <https://www.researchgate.net/publication/46689467_Public_accountability_in_the_information_age>.

Meister, Andre. 2018. Mit diesen sieben Programmen liest die Polizei Smartphone-Daten aus. Available at: <https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/>.

Metcalfe, Philippa; Dencik, Lina. 2019. The politics of big borders: Data (in)justice and the governance of refugees. First Monday. Volume 24(4). Available at: <http://dx.doi.org/10.5210/fm.v24i4.9934>.

Mol, Annemarie. 2002. The body multiple: Ontology in medical practice. Durham, London: Duke University Press. Available at: <https://edisciplinas.usp.br/pluginfile.php/4621896/mod_resource/content/2/MOL%2C%20Annemarie.%20The%20body%20multiple.pdf>.

Molina, Benítez; Carlos, Juan; Harbitz, Mia E. 2010. Civil registration and identification glossary. Inter-American Development Bank. Available at: <https://publications.iadb.org/publications/english/document/Civil-Registration-and-Identification-Glossary.pdf>.

Molnar, Petra. 2018a. Using AI in immigration decisions could jeopardise human rights. Centre for International Governance Innovation.

Available at: <https://www.cigionline.org/articles/using-ai-immigration-decisions-could-jeopardize-human-rights>.

Molnar, Petra. 2018b. The contested technologies that manage migration. Centre for International Governance Innovation. Available at: <https://www.cigionline.org/articles/contested-technologies-manage-migration>.

Molnar, Petra; Gill, Lex. 2018. Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system. University of Toronto, Faculty of Law. Citizen Lab. Available at: <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>.

Morozov, Evgeny. 2013. To save everything, click here. London: Penguin Book.

Morris, Christopher. 2008. State legitimacy and social order. In: Kühnelt, Jörg (Ed.). 2008. Political legitimacy without morality? Springer Science+Business Media B.V. Available at: <https://www.philosophy.umd.edu/sites/philosophy.umd.edu/files/Morris/2008%20morris%20state%20legitimacy%20and%20social%20order.pdf>.

Mouzourakis, Minos; Pollet, Kris; Ott, Jean-David. 2019. The AnkER centres. Implications for asylum procedures, reception and return. European Council on Refugees and Exiles. Asylum Information Database. Available at: <https://www.asylumineurope.org/sites/default/files/anker_centres_report.pdf>.

MSAB. 2020. Ecosystem. Available: <https://www.msab.com/de/ecosystem/>.

Ng, Rudy. 2006. Catching up to our biometric future: Fourth amendment privacy rights and biometric identification technology. Hastings

Communications and Entertainment Law Journal. Volume 28(3). Available at: <https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1629&context=hastings_comm_ent_law_journal>.

OHCHR. 2020. Good governance and human rights. Available at: <https://www.ohchr.org/EN/Issues/Development/GoodGovernance/Pages/GoodGovernanceIndex.aspx>.

Orlikowski, Wanda J.; Iacono, Suzanne C. 2001. Research commentary: Desperately seeking the "IT" in IT research - A call to theorizing the IT artifact. Information Systems Research. Volume 12(2): pp. 121-134. Available at: <https://doi.org/10.1287/isre.12.2.121.9700>.

Open Society Foundations. 2013. Global Principles on National Security and the Right to Information ("The Tshwane Principles"). Available at: <https://www.right2info.org/resources/publications/national-security-page/global-principles-on-national-security-and-the-right-to-information-english-booklet>.

Osborne, David. 1993. Reinventing government. In: Public Productivity and Management Review. Volume 16(4): pp. 349-356. Available at: <https://doi.org/10.2307/3381012>.

Pai, Hsiao-Hung. 2020. The refugee "crisis" showed Europe's worst side to the world. The Guardian. Available at: <https://www.theguardian.com/commentisfree/2020/jan/01/refugee-crisis-europe-mediterranean-racism-incarceration>.

Pillay, Pregala. 2016. The relationship between public administration and good governance. The case of South Africa. Anti-Corruption Center for Education and Research (ACCERUS). Stellenbosch University. Available at:

<https://pdfs.semanticscholar.org/b095/718a9d41b1fca7fc3f03aa9ef7c84a8c77fd.pdf>.

Podolski, Tanja. 2017. Sicherheitsrechtler zum Gesetzentwurf über Auslesen von Handys bei Asylsuchenden: "Kann nicht schaden, die Daten zu haben". Legal Tribune Online. Available at: <https://www.lto.de/recht/hintergruende/h/fluechtlinge-smartphones-auslesen-einreise-datenschutz-asylgesetz-bamf/>.

Privacy International. 2018. A guide for policy engagement on data protection. The key to data protection. Available at: <https://privacyinternational.org/report/2255/data-protection-guide-complete>.

Privacy International. 2019. Privacy International's contribution to Global Virtual Summit on digital identity. Available at: <https://privacyinternational.org/sites/default/files/2019-05/Global%20Virtual%20Summit%20submission-%20Privacy%20International.pdf>.

PRO ASYL. 2016. Neues Gesetz: Warum der Ankunftsnachweis keine Probleme löst. Available at: <https://www.proasyl.de/news/neues-gesetz-warum-der-ankunftsnachweis-keine-probleme-loest/>.

PRO ASYL. 2017a. Sachverständigen Stellungnahme für die öffentliche Anhörung am 27. März 2017 vor dem Innenausschuss des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 179/17. Available at: <https://www.proasyl.de/wp-content/uploads/2015/12/2017-03-23-Sachverst%C3%A4ndigen-Stellungnahme-PRO-ASYL-Gesetzentwurf-zur-besseren-Durchsetzung-der-Ausreisepflicht.pdf>.

PRO ASYL. 2017b. Zu wenig Abschiebungen? Wie mit unzulänglichen Zahlen Stimmung gemacht wird. Available at: <https://www.proasyl.de/news/zu-wenig-abschiebungen-wie-mit-unzulaenglichen-zahlen-stimmung-gemacht-wird/>.

PRO ASYL. 2018. Warum Ankerzentren eine schlechte Idee sind. Available at: <https://www.proasyl.de/hintergrund/warum-ankerzentren-eine-schlechte-idee-sind/>.

PRO ASYL. 2019. Stellungnahme zum Entwurf eines Dritten Gesetzes zur Änderung des Asylbewerberleistungsgesetzes. Available at: <https://www.proasyl.de/wp-content/uploads/PRO-ASYL_Stellungnahme-zum-Entwurf-zur-Dritten-%C3%84nderung-des-AsylbLG_29032019.pdf>.

Ragin, Charles C. 1992. "Casing" and the process of social inquiry. In: Ragin, Charles C.; Becker, Howards S. (Eds.). 1992. What is a case? Exploring the foundations of social inquiry. Cambridge: Cambridge University Press.

Rahman, Zara. 2017. Digital identification systems: Responsible data challenges and opportunities. Available at: <https://www.theengineroom.org/digital-identification-systems/>.

Rahman, Zara. 2019. Can data know who we really are? Available at: <https://deepdives.in/can-data-ever-know-who-we-really-are-a0dbfb5a87a0>.

Reidy, Eric. 2017. How a fingerprint can change an asylum seeker's life. The New Humanitarian. Available at: <https://www.thenewhumanitarian.org/special-report/2017/11/21/how-fingerprint-can-change-asylum-seeker-s-life>.

Rhodes, Roderick A. W. 2000. Governance and public administration. Available at: <https://www.researchgate.net/publication/246335680_Governance_and_Public_Administration>.

Rothstein, Bo. 2008. Creating political legitimacy: Electoral democracy versus quality of government. QoG Working Paper Series 2008(2). Available at: <https://dx.doi.org/10.2139/ssrn.1338615>.

Sánchez-Monedero, Javier; Dencik, Lina. 2019. The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. Cornell University. Available at: <https://arxiv.org/abs/1911.09156>.

Scharpf, Fritz W. 2003. Problem-solving effectiveness and democratic accountability in the EU. Max Planck Institute for the Study of Societies. MPIfG working paper 03/1. Available at: <http://www.mpifg.de/pu/workpap/wp03-1/wp03-1.html>.

Scheinost, Rudolf; Hüter, Gernot. 2015. Offener Brief an den Leiter des BAMF. Gesamt Personalrat; Örtliche Personalrat. BAMF. Available at: <https://www.tagesschau.de/inland/brandbrief-bamf-105~_origin-f6ce9f91-72e7-44f4-8685-ac9f20fbdf5e.pdf>.

Schmidt, Christina; Erb, Sebastian. 2019. Rechtes Netzwerk in Sicherheitsbehörden. Ein Kumpel wie jeder andere. Available at: <https://taz.de/Rechtes-Netzwerk-in-Sicherheitsbehoerden/!5625705/>.

Schmidt, Vivien; Wood, Matthew. 2019. Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance. Public administration. Wiley. Available at: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/padm.12615>.

Schneider, Melanie. 2016. Integriertes Flüchtlingsmanagement: Aufbau und Organisation der Ankunftszentren. BAMF. Available at: <https://docplayer.org/49498891-Vertraulich-aufbau-und-organisation-der-ankunftszentren-06-september-melanie-schneider-leiterin-ankunftszentrum-moenchengladbach.html>.

Schoemaker, Emrys; Currion, Paul; Pon, Bryan. 2018. Identity at the margins: Identification systems for refugees. Caribou Digital. Available at: <https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf>.

Schuler, Katharina; Schwarze, Till. 2017. Mit dem Grundgesetz nicht vereinbar. Available at: <https://www.zeit.de/politik/deutschland/2017-02/asylpolitik-fluechtlinge-bamf-handys-identitaet-faq>.

Scott, Murray; Acton, Thomas; Hughes, Martin. 2005. An assessment of biometric identities as a standard for e-government services. International Journal of Services and Standards. Volume 1(3). Available at: <http://dx.doi.org/10.1504/IJSS.2005.005800>.

Seaver, Nick. 2017. Algorithms as culture: Some tactics for the ethnography of algorithmic systems. Big Data & Society. Available at: <https://doi.org/10.1177%2F2053951717738104>.

Sedlmayr, Sebastian. 2017. Stellungnahme UNICEF zum Referentenentwurf des BMI "Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Available at: <https://www.unicef.de/blob/135620/6afb80d2eba7c2c06aa81706738fe1f5/stellungnahme-unicef-zum-re-ausreisepflicht-22-02-2017-data.pdf>.

Seelos, Christian; Mair, Johanna. 2012. Innovation is not the holy grail.

Stanford Social Innovation Review. Available at: <https://ssir.org/pdf/Fall_2012_Innovation_Is_Not_the_Holy_Grail.pdf>.

Seibert, Evi. 2017. SWR2 Interview der Woche vom 11.11.2017. Available at: <https://www.swr.de/-/id=20383132/property=download/nid=659202/3lstzu/swr2-interview-der-woche-20171111.pdf>.

Solove, Daniel J. 2008. Understanding privacy. The George Washington University Law School. Public Law and Legal Theory Working Paper No. 420. Legal Studies Research Paper No. 420. Chapter 1. Cambridge, London: Harvard University Press. Available at: <https://ssrn.com/abstract=1127888>.

Suleiman, Muhammad M.; Tsakuwa, Abubakar U.; Abdullahi, Amin M.; El-Tahir, Yusuf M. 2017. A review of improving good governance through ICT revitalization. Available at: <https://www.academia.edu/36815024/A_Review_of_Improving_Good_Governance_through_ICT_Revitalization>.

Süddeutsche Zeitung. 2017. Das BAMF verfehlt bei Asylentscheidungen die Zielvorgaben. Available at: <https://www.sueddeutsche.de/politik/fluechtlinge-das-bamf-verfehlt-bei-asylentscheidungen-die-zielvorgaben-1.3599329>.

SVR Integration Barometer. 2018. Stable integration climate in Germany: Summary of the 2018 Integration Barometer. The Expert Council of German Foundations on Integration and Migration. Available at: <https://www.svr-migration.de/wp-content/uploads/2018/09/SVR_Integration_Barometer_2018_Summary.pdf>.

Tabbara, Tarik. 2019. Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten. In: Humanistische Union. vorgänge. No. 227 (3/2019): pp. 123-133. Available at:

<http://www.humanistische-union.de/nc/publikationen/vorgaenge/online_artikel/online_artikel_detail/back/vorgaenge-227/article/ineffektiv-aber-nicht-ohne-wirkung/>.

Tagesschau. 2016. Mutmaßlicher Terror in Berlin: Fassungslosigkeit, Trauer und Entsetzen. Available at: <https://www.tagesschau.de/inland/breitscheidplatz-ueberblick-103.html>.

Tangermann, Julian. 2017. Documenting and establishing identity in the migration process: Challenges and practices in the German context. Focussed study by the German National Contact Point for the European Migration Network (EMN). Working Paper 76. Available at: <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf>.

Teorell, Jan; Rothstein, Bo. 2009. What is quality of government? A theory of impartial government institutions. Governance. Volume 21(2): pp. 165-190. 2008. Available at: <https://ssrn.com/abstract=1328817>.

Thomas, Robyn. 2009. Critical management studies on identity: Mapping the terrain. In: Alvesson, Mats; Bridgman, T; Willmott, H. (Eds.). Chapter 8. The Oxford Handbook of Critical Management Studies. Oxford: Oxford University Press. Available at: <https://www.researchgate.net/publication/43502757_Identity_Matters_Reflections_on_the_Construction_of_Identity_Scholarship_in_Organization_Studies>.

UN. 1979. American Convention on Human Rights. UN Treaty Series. Available at: <https://treaties.un.org/doc/Publication/UNTS/Volume%201144/volume-1144-I-17955-English.pdf>.

UN. 2007. Public governance indicators: A literature review. Department of

Economic and Social Affairs. Available at: <https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/2007%20Public%20Governance%20Indicators_a%20Literature%20Review.pdf>.

UN General Assembly. 1966. International Covenant on Civil and Political Rights. United Nations. Treaty series. Volume 999: pp. 171-346. Available at: <https://www.refworld.org/docid/3ae6b3aa0.html>.

UN General Assembly. 1985. Declaration on the Human Rights of Individuals Who Are Not Nationals of the Country in Which They Live: resolution / adopted by the General Assembly, 13 December 1985, A/RES/40/144. Available at: <https://www.refworld.org/docid/3b00f00864.html>.

UN General Assembly. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/23/40. Available at: <https://undocs.org/A/HRC/23/40>.

UN General Assembly. 2018. The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights. A/HRC/39/29. Available at: <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/29>.

UN Treaty Body Database. 2020. Ratification status for Germany. Available at: <https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=66&Lang=EN>.

UNHRC. 1988. CCPR General Comment No. 16: Article 17. The right to respect of privacy, family, home and correspondence, and protection of honour and reputation. Available at: <https://www.refworld.org/docid/453883f922.html>.

UNHCR. 2005. Global report 2005: Glossary. Available at: <https://www.unhcr.org/449267670.pdf>.

UNHCR. 2010. Improving asylum procedures: Comparative analysis and recommendations for law and practice. Available at: <https://www.unhcr.org/4c7b71039.pdf>.

UNHCR. 2013. Response to vulnerability in asylum. Available at: <https://www.refworld.org/pdfid/56c444004.pdf>.

Van Kersbergen, Kees; Van Waarden, Frans. 2004. Governance as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy. In: European Journal of Political Research. Volume 43: pp. 143-171. Available at: <https://dspace.library.uu.nl/handle/1874/20272>.

Von Bullion, Constanze. 2019. Traumatisierte Flüchtlinge: Asylbehörde weist Kritik zurück. Süddeutsche Zeitung. Available at: <https://www.sueddeutsche.de/politik/traumatisierte-fluechtlinge-asylbehoerde-weist-kritik-zurueck-1.4561608>.

Von der Leyen, Ursula. 2019. A Union that strives for more. My agenda for Europe. Political guidelines for the next European Commission 2019 - 2024. Available at: <https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en_0.pdf>.

Voßhoff, Andrea. 2017. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. German Bundestag. Innenausschuss. Ausschuss-drucksache 18(4)831. Available at: <https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf>.

Warren, Samuel D.; Brandeis, Louis D. 1890. The right to privacy. Harvard Lw Review. Volume 4(5): pp. 193-220. Available at: <https://doi.org/10.2307/1321160>.

Wehage, Jan-Christoph. 2013. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht. Universitätsverlag Göttingen. Available at: <https://www.univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-86395-123-8/Wehage_Diss.pdf>.

Whitley, Edgar A.; Gal, Uri; Kjaergaard, Annemette. 2014. Who do you think you are? A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems. Volume 23: pp. 17-35. Available at: <https://doi.org/10.1057/ejis.2013.34>.

Wieringa, Maranke. 2020. What to account for when accounting for algorithms: A systemic literature review on algorithmic accountability. In: Conference on Fairness, Accountability, and Transparency (FAT '20). New York: ACM. Available at: <https://doi.org/10.1145/3351095.3372833>.

World Bank. 1992. Governance and development. Available at: <http://documents.worldbank.org/curated/en/604951468739447676/pdf/multi-page.pdf>.

Yanow, Dvora. 2006. Thinking interpretively: Philosophical presuppositions and the human sciences In: Yanow, Dvora; Schwartz-Shea, Peregrine (Eds.). 2006. Interpretation and method: Empirical research and the interpretive turn. Armonk, New York: M. E. Sharpe.

Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany

Helene Hahn