Race, Borders, and Digital Technology:

Submission to the Office of the United Nations High Commissioner for Human Rights on the Reinforcing, Reproductive and Compounding Effects of the Deployment of Digital Technologies in the context of Border Enforcement and Administration

Berlin, 15 May 2020 – The Gesellschaft für Freiheitsrechte e.V. (Society for Civil Rights, GFF) is a 2015 founded Berlin-based human rights organisation and coordinates litigation to defend basic and human rights. With it's lawsuits, amongst others, the GFF advocates for the strengthening of informational self-determination and data protection, especially in connection with digitization, and fights against the discrimination of disadvantaged groups. In order to take joint legal action against human rights violations, the GFF brings together suitable plaintiffs, civil society partner organizations and excellent lawyers. It's mission is to help protect and strengthen human and civil rights by legal means.

GFF welcomes the important initiative taken by the United Nations Special Rapporteur on contemporary forms of racism, xenophobia and related intolerance, E. Tendayi Achiume, to prepare a thematic report to the UN General Assembly examining how digital technologies deployed in the context of border enforcement and administration reproduce, reinforce, and compound racial discrimination. Following the invitation by the Special Rapporteur to prepare written input to aid the preparation of the report, GFF is pleased to submit the following information for consideration.

Scope of the submission

Due to geographical reasons and the fact that Germany is an EU member state and part of the Schengen Agreement, German border enforcement and administration does not focus on the actual physical borders of the country, but on the administration of asylum procedures of those refugees who have entered the country. Since 2017, various IT assistance systems were introduced, namely image biometrics including an automatic photo matching, voice biometrics aimed at the recognition of Arabic dialects, a software-based transliteration of Arabic names as well as a data carrier evaluation. We will focus the following submission on the Federal German Migration Office[1]'s routine evaluations of refugees' mobile phones. For more information, we are happy to include and refer our recently published and more detailed study on the subject, which we include in our submission.[2]

Phone data evaluation of refugees: Brief overview over the facts

Phone data evaluations are deep infringements of privacy right: Mobile phones carry highly personal information from different aspects of life, including payment information as much as personal

[1] Bundesamt für Migration und Flüchtlinge, BAMF.

[2] Biselli/Beckmann: Invading Refugees' Phones: Digital Forms of Migration Control, English Version published January 2020 (in the following: GFF study). With regards to the other IT assistance systems see p. 40 ff.

communication or photos. Refugees, on the other hand, are particularly vulnerable to the infringement of their privacy rights. Due to their separation from home, family, and friends, mobile phones often play a particularly central role in the lives of refugees.

Nonetheless, data carrier evaluations were introduced by the "Law on Better Enforcement of the Obligation to Leave the Country"[3] in Germany in 2017. The introduction of these invasive measures aimed at preventing abuse of asylum procedures through untruthful information given by refugees.[4] Ever since, the law obliges asylum seekers who are unable to produce a valid passport or replacement document to submit, hand over and surrender all data carriers that may be of relevance for establishing their identity or nationality on request (§§ 15, 15a Asylum Act). In practice, these data carrier readouts predominantly affect smartphones.

For this purpose, the Migration Office has acquired surveillance technology and is routinely reading out and analysing data from smartphones. Legally, the extracted data may only be used to corroborate information provided by the asylum seeker on their identity or their country of origin. Therefore, for example, German migration officers must not take into account location data taken from the phone to corroborate the asylum seekers statement about flight route.

The procedure could potentially affect a large number of refugees: 54.2 percent of all first-time applicants in 2018 and 49.1 percent in 2019 were unable to produce a valid passport, passport replacement or identification document.[5] Data carrier evaluations take place both in first application proceedings as well as in review proceedings: 2018 there was 161,931 first applications and 85.052 review proceedings, 2019 there was 142,509 first applications and 170,406 review proceedings.[6] Nonetheless, over that same time period, only a total of about 28,528 data carriers were attempted to be read out,[7] 21,505 of which were successful technically.[8] We do not know why phone data evaluations are not carried out more often, but since they are up to the migration officers' discretion, it seems that migration officers themselves have reservations to employ the method, either because they find them unnecessary, little helpful or overly invasive.

For the data evaluation, first a complete data set is read from the device and then analysed by special software. Subsequently, the digital result of the analysis is stored and can be used later, if deemed necessary.[9] The evaluation focuses on the following indicators: The country codes of contacts in the address book, outgoing and incoming messages and calls, as well as the country endings of domains accessed via internet browsers. Moreover, location data from photos and possibly also from apps are included. In addition, the login names and email addresses used by apps, such as the Facebook username or the name used in a dating app, are also displayed in plain text. Finally, a special program analyses and supposedly recognizes the language used in text messages.[10] Thus, with the exception of

---

[3] "Gesetz zur besseren Durchsetzung der Ausreisepflicht", BGBl. I 2017 S. 2780.
[4] BT-Drs. 19/8701, p. 1, 22, 26, 43; BT-Drs. 19/4456, p. 10.
[5] BT-Drs. 19/8701 p. 27 and BT-Drs. 19/18498. p. 31.
[6] BAMF 2020, Das Bundesamt in Zahlen 2019, S. 11, 48.
[7] Our own calculations, based on BT-Drs. 19/8701, p. 29, and BT-Drs. 19/18498, p. 33.
[8] BT-Drs. 19/8701, p. 28 and and BT-Drs. 19/18498 , p. 34.
[9] GFF study, p. 12ff.
[10] GFF study, p. 18 ff.

usernames and email addresses, the digital reports mostly show meta data, which are depicted in tort diagrams, maps and charts.

The data carrier evaluation has proven little help in preventing abuse of asylum procedures:[11] Around a quarter of the attempted readouts fail technically.[12] Most reports are unusable, in 2018 this was 64 percent, in 2019 58 percent.[13] Reports may be unusable, amongst other reasons, because the set of data review is too small or otherwise inconclusive. Of the usable reports, most confirmed the information given, and only very few contradicted it: In 2018, 34 percent confirmed and 2 percent contradicted the given information.[14] In 2019, 40 percent confirmed and 2 percent contradicted the information given by the asylum seeker.[15] Whereas 21,505 phones were successfully read-out between 2018 and 2019, only a total of about 118 cases over thus gave indication of a false testimony.[16]

Due to technical proneness to error but also the chosen indicators and the, the data evaluations are not suitable to verify the origin or identity of a person with any degree of certainty. Which country codes a person is in contact with, for example, may give an indication of the location of their social network. Particularly, since friends and family from home may also have fled to other countries, it cannot proof a person's nationality. Accordingly, the evaluation reports have no probative force in court proceedings and only serve as a basis for the competent migration officer to further research or ask questions in hearing in the asylum process. Nonetheless, we judge the risk for misuse to be great, particularly since migration officers are left alone in judging what importance to give the outcome or how to interpret it.[17] Additionally, since nothing is revealed on the algorithms and training data used, it is not possible to evaluate the technical reliability of the used software.[18] For obvious reasons, the degree to which migration officers rely on the reports is unknown.

GFF lawsuits pending: Legal basis violates fundamental rights

Together with affected refugees from Syria, Cameroon and Afghanistan, in May 2020 GFF launched three lawsuits before different administrational courts and is challenging the constitutionality of the legal basis in the Asylum Act.[19] In view of the extensive, often very intimate data stored on smartphones, the search and inspection of mobile phones represents a particularly serious and extensive encroachment on the privacy of those affected. Considering the inadequateness of the data analysed for the said purpose of corroborating identity and nationality, the severe infringements of privacy rights are highly disproportionate to the intended goals. To challenge the constitutionality of the legal basis, it is our intend to exhaust judicial review and file a constitutional complaint to the Constitutional Court.

---

[11] GFF study, p. 28ff.
[12] In 2018 26 percent failed, BT-Drs. 19/8701, S. 29, 2019 it was 23 percent, BT-Drs. 19/18498, S. 34.
[13] BT-Drs. 19/8701, S. 29, BT-Drs. 19/18498, S. 34.
[14] BT-Drs. 19/8701, S. 29
[15] BT-Drs. 19/18498, S. 34.
[16] Our own calculations, based on BT-Drs. 19/8701, p. 29, and BT-Drs. 19/18498, p. 34 f.
[17] GFF study, p. 33ff.
[18] GFF study, p. 36 ff.
[19] For further information see https://freiheitsrechte.org/refugee-data/.

Discriminatory Dimension of the Phone Data Evaluation

We observe a pronounced discriminatory dimension of the phone data evaluation. Firstly, the measures were introduced without any evidence for abuse of asylum procedures and based on racist assumptions in the context of a political shift to the right. Secondly, they target a particularly vulnerable group. Thirdly, the measures demonstrate and produce mistrust between migration authorities and asylum seekers. Finally, the use of surveillance technology and the seriousness of the privacy rights infringement of the phone data evaluations are singular in Germany. In sum, we are thus observing the experimental use of surveillance technology on the most vulnerable group of society.

The introduction phone data evaluation was based on ungrounded and racist assumptions

The implementation of these systematic violations of refugees' private sphere must be analysed in the context of the domestic political situation. In 2015, almost half a million refugees had submitted their initial asylum application, more than twice as many as the previous year. By the end of that year, 337,331 initial proceedings were still pending, with an average process duration of almost eight months. The Migration Office came under great pressure from media reports that portrayed it as an overburdened agency. Simultaneously, racist positions and far-right demands drove the political debate from a predominantly empathetic and welcoming culture towards refugees in 2015 to a more and more hostile depiction. In 2017, only a short time before the upcoming parliamentary elections, racist terminology such as “waves of refugees” or the alleged risk of an “invasion” became popular themes of media coverage.[20] Refugees were increasingly framed as a national danger.

In this political context, the introduction of various IT assistance systems was presented as a possibility to speed up decisions and increase their quality. Additionally, they supposedly addressed the dangers presented by refugees. Particularly, the assumption was evoked, that amongst the refugees applying for asylum in Germany an unknown, but important number were lying about their origin or identity to be granted asylum on false grounds or to prevent otherwise law deportation. Already in 2017, the allegation was criticized by various organizations and parties. The allegation lacked any empirical basis and, with regards to the described outcome of the two years of phone data evaluation, now seems mostly disproven. Particularly, the numbers published for 2019 show no clear link between the proportion of asylum seekers “claiming” a certain nationality, but unable to show proof of it, and the recognition rate of the respective country.[21]

The introduction of the phone data evaluations must be seen as a reaction to this pressure and political climate. The law openly aimed to help disprove asylum claims more efficiently and accelerate the deportation of rejected asylum seekers. The measures are thus grounded in a general and ungrounded mistrust towards refugees.

Refugees constitute a particularly vulnerable group

Refugees are particularly vulnerable to the infringement of their privacy rights. No adequate procedural safeguards in the administrational procedure guarantee that decisions about phone data evaluation remain within the scope the law: The evaluation reports can be “unlocked” by an internal lawyer upon the request of the competent migration officer. The responsibilities of these lawyers are firmly integrated into the Migration Office’s chain of command, and therefore do not constitute an

---

[20] Biazza: Wenn der Mensch zur Naturkatastrophe wird, Süddeutsche Zeitung, 3 July 2018.
[21] BT-Drs. 19/18498, *p. 32f.*

independent control mechanism. Moreover, subsequent legal protection is difficult to access and not promising in the short-term: In view of the intransparent approach and the unknown evaluation procedures (algorithms) being used, neither the general public nor decision-makers or judges can properly assess the reliability of the results in individual cases.

When infringed upon their rights, refugees encounter specific difficulties with regards to legal remedies. Due to the lack of language skills and knowledge of German legal system, access to legal protection becomes challenging. In the concrete situation of the phone data evaluation, the almost complete lack of information about the concrete purpose and the exact scope of the data analysis, leaves refugees unable to assess the consequences of this evaluation. Additionally, refugees who have fled their home countries to another country very often find themselves facing more pressing problems than invoking their own data protection. They understandably fear negative consequences for their asylum procedure if they refuse to surrender their data and are under exceptional pressure to follow governmental requests. Expectedly, GFF had to undergo great efforts to find persons willing to file a lawsuit against the phone data evaluation.

The particular difficulties of the affected refugees to seek legal protection are aggravated by the fact that legal protection against an unconstitutional law proves particularly difficult: Only the Federal Constitutional Court can declare a law null and void. To enable the Court to decide upon the matter, the unsuccessful lawsuit has to be pursued through the course of the instance courts' decision and with statistically low success rates even to pass the Constitutional Courts admission for decision. Little surprising, the three GFF-lawsuits aside, no further cases are public which challenge the constitutionality of the law. Similarly, representatives of the Federal Data Protection Commissioner (Bundesdatenschutzbeauftragter) have pointed out that little to no data protection claims stem from the refugee community.

Demonstration and Creation of Mistrust

The phone data carriers is part of a larger system of invasive methods through which migration authorities, besides the concrete goal of the measures, establish a relationship of force and demonstrate mistrust and even hostility to the refugee community. The Migration Office's guide material for migration officers shows that refugees who are subjected to the measure are given little to no information as to what data is taken from their mobile phones and the outcome of the analysis is not shared with the asylum seekers. In conversations with the GFF, refugees have confirmed they were oblivious about the scope of the analysis and assumed migration officers would look at the content of messages and photos. Therefore, there is a long and lasting psychological effect on the persons affected, even in cases where the outcome of the data evaluations was favourable. The employment of these invasive measures leaves a trace on humans. One of the GFF's claimants explained to the GFF that after having been shown this blatant distrust, he found it hard himself to trust the Migration Office with the deeply personal accounts he had to give to argue his asylum case.

Similarly invasive technology is unprecedented in Germany

There is no other routine data evaluation in Germany concerning personal technical devices even remotely comparable to the described procedure in respect to refugees at German borders. There are only two other circumstances in which phone data is analysed: Either in criminal proceeding, if concrete evidence suggests a crime has been committed, or as part of police measures preventing

dangers, where concrete evidence suggest grave crimes or dangers. Even in this context, to the extent of our knowledge, no comparable software-based analysis takes place in these cases.

Lack of transparency and oversight

The Migration Office has shown itself to be highly opaque with regard to the employed technology and algorithms. Obtaining information on the Migration Office's data carrier evaluation remains an arduous process. The Office never actively informed the public or freely answered requests, but only reacted to parliamentary request or freedom of information requests, exceeding the deadlines and giving the least information possible. The Migration Office argues that exposing information about the technology employed would potentially impede its effectiveness. Therefore, it has consistently refused to disclose information about the training data set and algorithms on which the data evaluation and, in particular, the dialect recognition or speech recognition programs is based.

With regard to oversight, the Office of the Federal Data Protection Commissioner (Bundesdatenschutzbeauftragter) is the competent authority. The preceding Federal Data Protection Commissioner had expressed severe criticism in the legislative process introducing the phone data evaluation.[22] Still, we are not aware of any initiative taken to check the lawfulness of the practice since then. Particularly, the lawfulness of the technology employed has not been verified. As explained above, the lack of complaints to the Data Protection Commissioner from the refugee community is striking.

Conclusion

Under the political pressure of a shift to the right in German politics, the German Bundestag introduced extensive use of surveillance technology on it's refugee population, thus violating the privacy rights of thousands of refugees. Strikingly, despite little to no useful outcome, the Migration Office continues to infringe the rights of thousands.

The Migration Office's approach must be understood as part of a national and international trend, in which new controlling and monitoring technology is being tested and used on refugees. Refugees are subjected to second-class data protection. Their particular vulnerability and defenselessness is exploited to test new control and monitoring technology. The most notably outcome of the measures may very well be the creation of distrust and exclusion of a particularly vulnerable group of society.

Gesellschaft für Freiheitsrechte e.V.
Hessische Straße 10, D – 10115 Berlin.
Telephone +49 30 549 08 10 – 0.
Fax +49 30 549 08 10 – 99.
https://freiheitsrechte.org/.
info@freiheitsrechte.org.

[22] Bundesdatenschutzbeauftragte, Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23 March 2017, Ausschuss-Drucksache 18(4)831.

Invading Refugees' Phones:

Digital Forms of Migration Control

In Germany and Europe

Gesellschaft für Freiheitsrechte

Publisher

Gesellschaft für Freiheitsrechte e.V.
Hessische Straße 10, D – 10115 Berlin.
https://freiheitsrechte.org/.
Telephone +49 30 549 08 10 – 0. Fax +49 30 549 08 10 – 99. info@freiheitsrechte.org.
English version, February 2020.
This study's intent is to prepare lawsuits and was supported by the Digital Freedom Fund, https://digitalfreedomfund.org/.

Typesetting and Design: Julia Zé, www.juliaze.com.

Translation: Julia Föll, juliae.foell@googlemail.com.

The Gesellschaft für Freiheitsrechte e.V.

The Gesellschaft für Freiheitsrechte e.V. (GFF, Society for Civil Rights) coordinates and finances legal proceedings to defend basic and human rights. With its lawsuits, the GFF advocates the strengthening of informational self-determination and data protection, especially in connection with digitization and technical change. In addition, many of its proceedings relate to discrimination against disadvantaged groups. In order to take joint legal action against violations of rights, the GFF brings together suitable plaintiffs, civil society partner organizations and excellent lawyers. Current projects include, among others, lawsuits against the mass storage of flight passenger data and constitutional complaints against the excessive use of spyware by police authorities, most recently in the new Police Act in Hesse. Further cases include a female journalist's equal pay lawsuit.

The GFF is financed by donations. Support the GFF and become a sustaining member.

https://freiheitsrechte.org/join/.

Authors

Anna Biselli is a journalist and computer scientist. She writes for, among others, netzpolitik.org. Anna has been researching and writing about the digitization projects carried out by the Federal Office for Migration and Refugees (BAMF).

Lea Beckmann is a lawyer at GFF with a focus on German constitutional law and international human rights. She will coordinate the GFF's legal action against the data carrier evaluation of refugees' devices performed by the Federal Office for Migration and Refugees.

Contents

A. Introduction

For refugees, a smartphone is a prized companion before, during and after their flight. With the help of this digital guide, they can get up-to-date news about their home country, stay in touch with family and use it as a translation aid. Often, their device also preserves the few memories that those seeking protection can take with them on their journey: Photos from their abandoned home and of documents, messages from friends. For many, smartphones are an indispensable tool. In recent years, several countries have started to read out immigrants' and asylum seekers' smartphones in order to obtain information on them, such as whether they actually are from the country they indicated. But sought for information also might include the route a person had taken to enter the country, or the question of if there is propaganda material from terrorist groups on their device, do they pose a danger?

In this way, smartphones are being turned from an indispensable everyday tool into a means of opening the floodgates to a comprehensive state-led invasion of privacy.

The main facts in brief

Since 2017, the central German migration authority, the Bundesamt für Migration und Flüchtlinge or Federal Office for Migration and Refugees (BAMF), has routinely been reading out and analyzing data from electronic devices in order to determine their owner's origin and identity. BAMF will resort to this measure when an asylum seeker cannot present a valid passport or passport replacement documents – without concrete suspicion that the statements made by the registered person regarding their origin do not correspond with the truth.

This problem affects a large number of refugees: Of all first-time applicants, 54.2 percent in 2018[1] and as many as 55.4 percent in the first quarter of 2019 were unable to produce a valid passport, passport replacement or identification document.[2] There are many reasons why a refugee might not be able to produce identity documents: Some lose their passport during their flight, while others have had their papers confiscated by traffickers. Some come from countries where having a passport is not common, or from regions where the authenticity of an identity document is almost impossible to be determined, which means that the BAMF will not recognize them.

Data carrier readouts mainly affect smartphones. If refugees are asked to surrender their mobile phones, they are legally obliged to comply. Legally, the extracted data may then only be

[1] Bundestags-Drucksache (Document of the German Federal Parliament): 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 8.

[2] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to question 5.

used to check provided information on names or countries of origin. The result of the evaluation has no evidentiary value in the asylum procedure, but merely an indicative effect.

In about a quarter of the cases, the data carrier readouts already fail on the technical level. From January 2018 to June 2019, a total of about 17,000 data carriers were successfully read out.[3] Since the beginning of data carrier evaluations, these have on average only been usable in less than half of the cases. And only in one to two percent of the cases did the evaluation result in a contradiction to the information provided. In all others, the test confirmed asylum seekers' submissions.

In contrast, this is offset by the cost, which between the introduction in 2017 until the end of 2019 has totaled at 11.2 million euros. In addition, each year further costs of an estimated two million euros are incurred for the system support.[4]

For data evaluation, a complete data set is first read from the device and then analyzed by special software. After this, the result of this analysis is stored and used later if necessary. The evaluation focuses on the country codes of contacts in the address book, outgoing and incoming messages and calls, as well as the country endings of domains accessed via internet browsers. Location data from photos and possibly also from apps are also included. In addition, the login names and email addresses used by apps, such as the Facebook user name or the name used in a dating app, are also displayed in plain text. Finally, a special program analyzes the language used in text messages.

However, experts do not consider these data evaluations to be suitable for verifying the origin or identity of a person, for various reasons. It is currently not possible to check the BAMF's reliability data, as the Office refuses to disclose its algorithms and technical details. As a result, it is difficult for all those involved in the asylum procedure to properly assess the significance of the results.

Key constitutional and data protection critiques

According to the GFF, the Federal Office's practice thus violates the fundamental right to integrity and confidentiality of IT systems and the right to informational self-determination. The migration policy objective of this legal regulation, namely the prevention of unauthorized asy-

[3] Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 9; Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to question 6 b; Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the second quarter of 2019, answer to question 6.

[4] Bundestags-Drucksache 19/1663: Use of voice recognition software at the Federal Office for Migration and Refugees, April 16 2018, answer to question 13; Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 15.

lum grants and the ability to deport rejected asylum seekers more quickly, does not justify such an intensive, causeless and comprehensive encroachment on basic rights. At the same time, the people concerned have no effective means of defending themselves against the measure. Due to the high proportion of unusable test reports and the low reliability of those results that are usable, it is doubtful whether mobile phone evaluation is at all suitable for obtaining reliable clues as to the identity and origin of those seeking protection.

The consequences of false results, on the other hand, can be fatal: If there are errors in the evaluation or interpretation of the results, this can lead to distrust towards the applicants and thus endanger their asylum applications.

In conclusion, data processing by the BAMF is also in conflict with various data protection principles, in particular the minimization of data and the appropriateness of the measures, but also the transparency and traceability of data processing.

Factual gap in legal protection for asylum seekers: a gateway?

It is hard to imagine any other social group being subjected to such intensive infringements without suspicion – without legal and, above all, constitutional compliance being checked by the courts. This is largely due to the fact that access to effective legal protection for asylum seekers is in fact severely restricted. They arrive in a new country whose language they are just learning and whose legal system is foreign to them. They may be traumatized, find themselves in a financially precarious situation and have to cope with many everyday difficulties. In addition, they are particularly dependent on Germany as their host country in the asylum procedure and beyond and are therefore less inclined to take legal action. Finally, a fundamental judicial clarification of the legality of their mobile phone's evaluation will take many years and thus come too late in their personal case.

This factual gap in legal protection for a particularly vulnerable segment of society means that the BAMF can currently test new forms of state surveillance on them. Experience with other invasive state measures in Germany, but also especially with mobile phone data readings in other countries, shows that the scope of such measures threatens to be expanded after their introduction. In Great Britain, for example, the mobile phones of victims of sexual violence are subjected to readouts by default, in order to use the data as evidence in criminal proceedings.[5]

[5] Big Brother Watch UK (2019): Digital Strip Watch. The Police's Data Investigation of Victims.

Background and aim of this study

The Gesellschaft für Freiheitsrechte e. V. (GFF) wants to contribute towards both closing this factual gap in legal protection and preventing similar developments. Together with affected persons and committed cooperating lawyers it is therefore preparing legal actions against the BAMF's data carrier readouts of asylum seekers' devices. Little is known about state access to sensitive data. For this reason, the GFF, together with journalist and computer scientist Anna Biselli, has investigated the BAMF's approach in a comprehensive research project, the results of which are being published in this report.

The long-term goal of the strategic litigations is to have the constitutionality of the legal basis reviewed by the Federal Constitutional Court, which is the only court that can "quash" a legal basis, i.e. declare it null and void. For this, a person whose mobile phone data readout was covered by the legal basis must sue before an administrative court. If this court itself does not submit the proceedings to the Federal Constitutional Court, an appeal to the Federal Constitutional Court is only possible after the legal process has been exhausted. In other cases, it may already be expedient in the short term to clarify the limits of the scope of application of the currently applicable statutory provision and to press for a narrow interpretation. The GFF also hopes, in the course of appeal proceedings, to obtain further information on the algorithms and technical details that are being used.

Funding

The GFF is a non-profit organization and is financed in approximately equal parts by contributions from its sustaining members, individual donations and institutional support from various foundations. This study was made possible by a grant from the Digital Freedom Fund (DFF).

Support the GFF in this work and become a sustaining member.

https://freiheitsrechte.org/join/.

Methods and Sources

For this study, the GFF comprehensively researched and evaluated available sources. These include documents from the legislative process and statements by legal scholars, refugee organizations and associations. In addition, the study is based on further information that was made public by parliamentary inquiries in the Bundestag, the German Federal Parliament, and Länderparlamente, state parliaments. The findings from various background discussions with refugees, lawyers and legal scholars, procedural advice centers and human rights organizations in Germany and other European countries were included as well. These discussions, as well as the consulted evaluation reports and asylum files, painted a complete picture of the use of data carrier evaluation in practice. BAMF staff declined invitations to be interviewed. Following previous research by Anna Biselli and numerous freedom of information requests, however, official BAMF documents were made available as well and incorporated into the report. These documents include official internal regulations regarding document verification, establishment of identity and for reading mobile data carriers, as well as a user manual for reading mobile data carriers and extensive training documents for BAMF employees.

B. Data carrier evaluation in Germany

Compatibility with basic and human rights

When the state wants to read out and evaluate data carriers belonging to refugees, it is restricted in this by the basic rights in particular: The general right of personality guaranteed in the Grundgesetz, or German Basic Law (Article 2 para. 1 in conjunction with Article 1 para. 1 GG) obliges the state to protect the basic conditions of free personality development and self-determination. Hence, it follows that the state must protect the right of the individual to determine for themselves the data concerning their person (the so-called "right to informational self-determination").[6] Because a large number of personal data sets from various areas of life are collected in IT systems, the state need to ensure these systems' confidentiality and integrity in particular (so-called "right to the protection of confidentiality and the integrity of information technology systems").[7]

The evaluation of cell phones, in which a wide array of sensitive data from different areas of life is bundled, undoubtedly represents a serious encroachment on fundamental rights. The fact that these measures are carried out across the board and without foundation, i.e. any without concrete suspicions, weighs even more heavily.

The objectives of preventing the unwarranted granting of asylum applications and being able to deport rejected asylum seekers more quickly cannot justify such intensive legal intervention. In several decisions, the Federal Constitutional Court has emphasized that state access to IT systems is not permitted for just any political purpose, but only for the protection of outstandingly important legal interests.[8] Migration policy objectives cannot be put on the same level as the prevention or prosecution of the most serious crimes.

The law also lacks the procedural regulations which secure fundamental rights and which are required according to settled case law when accessing personal data.[9] The requirement that only fully qualified lawyers within the BAMF are allowed to release the results report for use in asylum proceedings does not guarantee the necessary independent control of the legality of the measures.

In conclusion, data processing by the BAMF thus also runs counter to various data protection regulations, such as the adequacy and minimization of data, but also the transparency and traceability of data processing.

---

[6] Fundamental to this is the Federal Constitutional Court's "census judgement", BVerfG, NJW 1984, 419.

[7] Fundamental to this is BVerfG, NJW 2008, 822 <827>.

[8] BVerfGE 141, 220 <304 f.> .

[9] BVerfGE 65, 1 <46>; 113, 29 <57 f.>; 120, 351 <361>.

The legal foundation: How far-reaching are the BAMF's powers?

Despite this, the Bundestag, the German Federal Parliament, has further developed legislation surrounding the evaluation of data carriers. In July 2017, the "Gesetz zur besseren Durchsetzung der Ausreisepflicht" (Law on Better Enforcement of the Obligation to Leave the Country) came into force. Among other things, this law broadened the provisions on detention pending deportation and custody of persons leaving the country, as well as the powers of the BAMF to pass on data to other authorities.

In addition, the legal option of reading out refugees' data carriers was added. For this, § 15 of the Asylum Act (Asylgesetz, AsylG) was amended, which regulates the duty of an asylum seeker to cooperate with establishing the facts within the framework of the asylum procedure. Asylum seekers who are unable to produce a valid passport or replacement passport are now obligated to submit, hand over and surrender all data carriers that may be of relevance for establishing their identity or nationality on request. However, this data carrier analysis is only permissible insofar as this is essential for the determination of identity and nationality, "and the purpose of the measure cannot be achieved by milder means" (§ 15 AsylG).

The legal regulations do not restrict the measure to smartphones, the term "data carrier" allows the evaluation of a large number of other devices, such as simpler models of mobile phones referred to as feature phones, but also USB sticks, hard disks, laptops or even fitness wristbands. Data carriers may only be evaluated if there are no actual indications for the assumption that "only knowledge from the core area of private life would be obtained". Nevertheless, knowledge gained in this sphere may not be used and must be deleted (§ 48 para. 3a sentences 2-4 AufenthG). In addition, the data carriers may only be evaluated "by a staff member who is qualified for judicial office" (§ 48 para. 3a sentence 5 AufenthG) – a regulation based on the construct of judicial reservations.

The law obliges those concerned to provide any login data that is needed to evaluate the data carrier. If this does not occur, the respective authorities may request information about the corresponding access data from the telecommunications service providers, such as PIN and PUK codes for SIM cards or passwords (§§ 48 para. 3a sentence 3, 48a para. 1 AufenthG).

In the explanatory memorandum to the Federal Government's draft bill, it is assumed that data carrier evaluation would be an appropriate measure for 50 to 60 percent of the applicants as part of the compliance effort. Based on the number of 280,000 registered asylum seekers in 2016, the Federal Government assumed that 150,000 persons per year would be considered for a data carrier readout.[10]

[10] Bundestags-Drucksache 18/11546: Draft Bill of the Federal Government, Act to Improve the Enforcement of the Obligation to

The BAMF, an office under pressure

Nearly half a million refugees submitted their initial asylum application in Germany in 2015, more than twice as many as in the previous year. By the end of that year, 337,331 initial proceedings were still pending, with an average process duration of almost 8 months.[11] The outstanding cases piled up. At the same time, the BAMF came under pressure from media reports that portrayed it as an overburdened Office: "Chaos and loss of control for asylum applications" – that was the tenor of headlines over many months.[12] The Federal Office's staff councils wrote an open letter to the Head of the Office, in which they excoriated the lack of qualification exhibited by hastily trained new personnel, as well as "systemic deficiencies".[13]

In addition to this, there were cases such as that of Franco A., a German soldier who in 2016 posed as a Syrian asylum seeker and was granted protection status. The lieutenant colonel in the German Armed Forces was allegedly planning a right-wing terrorist attack.[14] The fact that such a deception was possible caused widespread doubt in large parts of the public about the quality of asylum decisions.[15]

The BAMF was under pressure to act. The introduction of various IT assistance systems was intended to speed up decisions and increase their quality.[16] Automatic photo matching, dialect and name analysis as well as data carrier evaluation were introduced and presented at the Bamberg branch office in July 2017 – about two months before the upcoming federal elections.[17] "A case like Franco A. can no longer happen", BAMF Vice President Dr. Markus Richter summed up in November 2018 in an interview with the Frankfurter Allgemeine Zeitung (FAZ).[18] The Office is nowadays presenting itself as a pioneer in authority digitization.[19]

Exit, March 16, 2017, p. 15.

[11] BAMF (2016): The Federal Office in Numbers 2015.

[12] See for example J. Bock: Chaos und Überforderung bei der Annahme von Asylanträgen, Stuttgarter Nachrichten, December 21, 2015.

[13] Gesamt-Personalrat und Örtlicher Personalrat des BAMF (2015): Offener Brief an den Leiter des BAMF, published on tagesschau.de.

[14] Generalbundesanwalt: Anklage wegen des Verdachts der Vorbereitung einer schweren staatsgefährdenden Gewalttat, December 12, 2017.

[15] See for example A. Reimann: Wie leicht kann man sich ins Asylverfahren einschleichen?, Spiegel, May 17, 2019.

[16] Federal Ministry of the Interior: Press Release: Neue IT-Assistenzsyteme im BAMF, December 6, 2017.

[17] BAMF: Press Release: Moderne Technik in Asylverfahren, July 26, 2017.

[18] B. Beeger, T. Neuscheler: „Ein Fall wie Franco A. kann nicht mehr passieren", Frankfurter Allgemeine Zeitung, November 6, 2018.

[19] BAMF: Press Release BAMF-IT: Am Puls der Zeit, July 17, 2019.

In practice: How the BAMF reads out and analyses data carriers belonging to refugees

The regulations in the Law on Better Enforcement do not contain any precise specifications on the process of reading out and evaluating the data carriers. A glance at the BAMF's internal instructions on "identity verification"[20] and "reading mobile data carriers"[21] as well as at manuals and training documents provides insight into this subject.[22]

Even though the BAMF is legally authorized to evaluate data carriers of all kinds, the authority is currently only analyzing smartphones and so-called feature phones, simpler mobile phones with a smaller range of functions. The data carrier evaluation process can be separated into three phases: The readout, the automatic analysis and the evaluation of the analysis results.

Whether a data carrier will be read out is usually decided right when the applicants register – so before the asylum hearing. If a refugee is not able to produce a passport or passport replacement documents, a readout may be considered. The mobile devices of children can also be read out, especially if no one else in their family is in possession of such a device, so the official orders. "The extraction of mobile devices has no age limit", the instruction states.

The registered person is requested by employees of the Asylum Procedures Secretariat to hand over their device and is made aware of their legal obligation to do so. Their consent is documented by a signature.[23] The person concerned must participate in this process and unlock the device as well as change certain device settings that make the readout possible.

The data is then extracted in the applicant's presence and hooked up to a special computer for this purpose. If the readout is successful, the extracted data is automatically combined into a results report and stored in a so-called "data safe". The BAMF employee cannot view the report at this time. According to BAMF, the raw data is deleted immediately after the results report has been created, and the device is returned to the applicant.

Should the asylum decision-maker conclude that they do not need the data analysis results because the applicant's identity could be sufficiently established by other indications, they will then have the report deleted via a ticket system. If they do want to use the report, however, they need to apply for its release.[24]

---

[20] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

[21] BAMF: Dienstanweisung für das Asylverfahren – Auslesen von mobilen Datenträgern.

[22] BAMF: Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität, Sicherheitsaspekte. Einführung in die neuen IT-Tools, August 30, 2017.

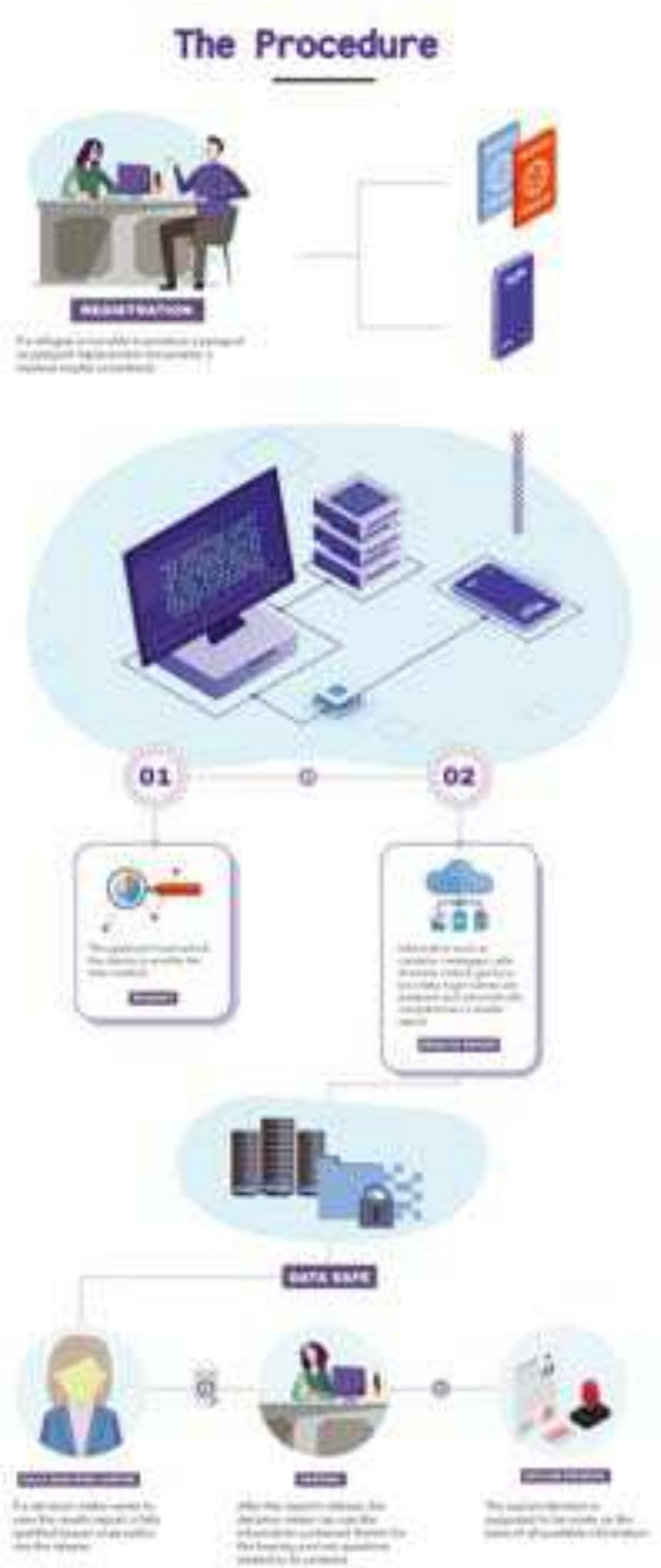
[23] BAMF: Form D1705.

[24] BAMF: Form D1735.

In this case, a fully trained lawyer with qualifications for judicial office working at the BAMF makes the decision after carrying out a "necessity and proportionality" examination and, where appropriate, releases the report for evaluation. If the result of this examination is negative, however, the report must be deleted.[25]

If the decision-maker happens to be a fully qualified lawyer themselves, they can decide independently on the release. However, this scenario would be the exception rather than the rule, as decision-makers are not required to have a law degree. Rather, the minimum requirement is a Bachelor's degree in a field that falls under the specifications for nontechnical intermediate civil service.[26]

Once the report is released, it is imported from the data safe into the electronic file system MARiS (which stands for Migration Asylum Reintegration System), after which it is deleted from the data safe and added to the respective asylum case file. It can now be used to prepare for the asylum hearing. Depending on the report's contents, the decision-maker can classify the results into one of three categories: Firstly, the report supports the information provided by the applicant; secondly, the report does not support the information provided by applicant; and thirdly, no usable results. As soon as a report has been added to an asylum file, it will no longer be



[25] BAMF: Form D1706.

deleted, even if the results turn out to be unusable. From then on, the regular deletion periods for asylum files apply. According to § 7 para. 3 of the Asylum Act (AsylG), asylum case files must be destroyed at the latest ten years after the conclusion of the asylum procedure and deleted from the data processing systems of the Federal Office. Shorter deadlines only apply in exceptional cases; for example, in cases of naturalization.

During the hearing, the interviewer – who is not always the same person as the decision-maker – may use the results report to ask the applicant questions about possible contradictions to the indications of identity or origin they provided. However, the interviewer is not supposed to hand over the report to the asylum seeker.

No passport, no ID: who is affected?

According to statistics compiled by the Federal Ministry of the Interior, 54.2 percent of applicants were unable to submit identification papers in 2018;[27] in the first quarter of 2019, the figure was as high as 55.4 percent.[28] This rate varies considerably depending on the country of origin. The majority of refugees from Syria presented identification papers in 2018, with only 19.2 percent being unable to do so. In contrast, 86.8 percent of applicants from Nigeria and 96.5 percent of refugees from Somalia had no form of passport, passport replacement or identification card.[29] If an applicant does not present valid passport or passport replacement, their smartphone may be subject to a readout if there are no milder means to determine identity and origin. However, according to the guiding instructions on identity verification, only documents "which can prove identity by means of a photograph and which can be checked for authenticity by the Federal Office" are considered to be milder means for establishing identity. Passport replacements include refugee IDs or identity cards, but civil status documents such as birth or marriage certificates can also be used to confirm an identity.

However, even some asylum seekers who have valid documents from their country of origin also have to hand over their devices. Internal BAMF instructions show that it is sufficient for another authority to withhold these documents in order to read out mobile phone data when registering for identity verification.

[26] Bundestags-Drucksache 18/10786: Temporary employment at the Federal Office for Migration and Refugees, December 30, 2016, answer to question 6.

[27] Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 8.

[28] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to questions 5 and 6.

[29] Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 8.

Registered first-time asylum applicants older than 18 from January to December 2018

Source: Bundestags-Drucksache 19/8701; Supplementary information on asylum statistics for the year 2018, answer to question 9 a), answer to question 8.

In addition, the passports of some states are not recognized in Germany; citizens of these countries must always expect their data carriers to be read out.[30] The Federal Ministry of the Interior, in agreement with the Federal Foreign Office, regulates which passports and replacement documents are recognized in Germany in constantly updated general decrees. Suitability as proof of identity is also gauged on the basis of "an assessment of state structures and documentary systems with regard to the corruption index of the respective issuing country".[31] These general decrees show, among other things, that Somali passports and passport replacement papers issued or renewed after 31 January 1991 are not recognized.[32] The same is true for documents issued after 2015 in IS-occupied areas of Iraq or passports and passport replacement papers issued by Taliban offices in Afghanistan, for example.

Moreover, for technical reasons, the validity of the passports of some countries cannot be determined directly on the spot; in these cases, too, the BAMF reads the data carriers of the persons concerned: Passports and passport replacements are checked for authenticity by means of a physical-technical examination (PTU). There is a total of three levels of verification, as can be seen from the instruction "Asylum procedure – certificate and document verification".[33] The first step is to conclusively establish a document's validity or authenticity on the spot. If this cannot be done, the BAMF will consider reading the data carriers of the applicants on the second level. According to the instructions, documents that can be examined on the spot include machine-readable documents from all countries of origin, as well as all other documents from Syria, Iraq, Iran, Eritrea, Ukraine, Afghanistan and the Russian Federation.

Refugees with any other type of documentation are subject to an immediate readout of their devices. In addition, their documents are sent to an external testing center, which constitutes the second level of testing. If the authenticity of the documents still cannot be confirmed by this, or if manipulation is suspected, the PTU department in Nuremberg carries out the final evaluation as the third test level. If a document turns out to be genuine in the second or third examination level, thereby making the data carrier readout superfluous, the justification of the asylum decision ought to refer only to the indication of origin proven from the identity document.[34] In the central asylum hearing however, the results report might have already been in

[30] BAMF: Dienstanweisung Asylverfahren – Urkunden- und Dokumentenprüfung.

[31] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

[32] Bundesministerium des Innern, Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes from April 6, 2016, BAnz AT 25.04.16 B1. Passport types after 2013 are exceptions, see Bundesministerium des Innern, Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes from April 5, 2018, BAnz AT 13.04.18 B7.

[33] BAMF: Dienstanweisung Asylverfahren – Urkunden- und Dokumentenprüfung.

[34] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

the hands of the decision-maker. To summarize, it is a realistic scenario that a refugee is in possession of a valid identification document and might have even presented this, but that this fact is simply not put under consideration during registration, leading to a data carrier readout nevertheless.

Personal account: worrying about private photos and readouts that are never used

At the BAMF branch office at the Welcome Center in Bielefeld, applications and hearings often take place on the same day. A procedural consultant spoke with the GFF about her experiences. She accompanied a Nigerian asylum seeker in his early twenties to the BAMF. The applicant had no passport, only a newspaper clipping with his picture in it from his country of origin. Between the application and the hearing that followed on the same day, his phone was read out. An interpreter and the person who received his asylum application were present and explained that his smartphone was now going to be read out. He was asked where he got the device from, but was not informed on the details of this process.

The applicant reported being worried because his device also contained private photos and videos. During the situation, he was too shy to even voice his concerns and only told his procedural consultant about them in the waiting room afterwards. His smartphone was connected to a computer, it took about five to ten minutes to read it out, and then he received his phone back. It was not clear to him that BAMF employees could not also see his photos or the content of messages. In the hearing, which was conducted by another BAMF employee, the findings from his phone were not discussed. It is also unclear whether obtaining the necessary authorization from a fully qualified lawyer in this short time period would have been possible.

What does the results report contain?

The results report contains summarized, mainly statistical information. Saved contacts, incoming and outgoing calls as well as text messages from various messenger services as well as call duration, all of which are evaluated according to country codes. As a country indicator, the top-level domains of visited internet domains are also statistically processed and displayed in tables and pie charts.

At a glance: what sort of data can the BAMF read?[35]

- Country codes of contacts in the address book
- Incoming and outgoing calls by duration and country code
- Incoming and outgoing SMS and messages by country code
- Language used in incoming and outgoing SMS and messages
- Browsing history according to country endings of visited web sites
- Login names and email addresses used in apps
- Location data from photos, possibly also from apps

Geodata: where were you?

Aside from contact information and call logs, the BAMF also uses geolocation data. The decision-maker is shown this location data as points on a map, albeit without any time allocation or source. The decision-maker knows that this geographical location is derived from data on the mobile phone, but not from where or when this information exactly originates. In his interview with the Frankfurter Allgemeine Zeitung (FAZ), BAMF Vice President Dr. Markus Richter stated that geodata from photo files is being taken into account as well.[36] An evaluation protocol known to the authors confirms this statement and names photos as a source for found location information. It is not known at this point whether app information, known wifi networks or recorded GPS data are evaluated as well, as the BAMF refuses to divulge information on this matter.

[35] BAMF: Training manual for BAMF employees, 2017 edition, pp. 78 and 104.

[36] B. Beeger, T. Neuscheler: „Ein Fall wie Franco A. kann nicht mehr passieren", Frankfurter Allgemeine Zeitung, November 6, 2018.

The Results Report

01

02

03

04

05

Speech analysis of text messages: which language(s) do you write?

The analysis of text messages goes beyond just compiling statistical information. In the results report, the interviewer can see the frequency of languages used for incoming and outgoing messages; for messages in Arabic, the dialects used are noted as well. According to a reply from the Ministry of the Interior in December 2018, the software can currently differentiate between 170 languages and dialects.[37] Evaluation reports, for example from October 2019, note that "although more than 90 languages are recognized, not all existing languages are supported by the system. If a language is not known, the system will recognize one of the most similar languages." It is not possible to judge the reliability of the language module used by the BAMF.

The Federal Office refuses to disclose any information about the training data set and algorithms on which the speech recognition program is based and what its error rates are. Precisely because of the multitude of Arabic dialects and a large variation of inconsistent spellings, particularly in chat dialects, precise language identification is likely to be a challenge. It can at least be inferred that some languages can be correctly identified more often than others. Such discrepancies can lead to discrimination because native speakers of some languages are more likely to be affected by inaccurate results. Research projects on automated language identification systems that were supposed to differentiate between Modern Standard Arabic and Egyptian dialect at the sentence level achieved accuracy rates of 85.5 percent.[38]

In conclusion, as long as data on the reliability of speech recognition in the BAMF's cell phone evaluations does not exist, it is impossible for the Office's employees and also judges to correctly assess the probative value of this test. This poses a constitutional problem.

[37] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 15.

[38] H. Elfardy, M. Diab (2013): Sentence Level Dialect Identification in Arabic, Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, ACL 2013.

Arabizi, chat dialects in the Arabic language

In German as well, the language we use in short text messages differs from the formal language in written texts or documents, in particular through the frequent use of abbreviations. In Arabic-speaking countries there is an added factor in that this language is often phonetized with Latin characters in text messages. There are different ways of doing this and, in a way, different "chat dialects" have developed, which are gathered under the name "Arabizi".

These dialects consist of a combination of Latin letters and characters representing Arabic sounds that have no phonetic equivalent in English or French.[39] A variety of spellings exist for a single Standard Arabic word. Thus, the term تحرير (liberation), can be expressed with the character combinations ta7rir, t7rir, tahrir, ta7reer or tahreer.[40] In addition, there are considerable differences between Arabic dialects, which might use totally different words or just pronounce the same word differently, which would affect the way these words are then phonetized. There is no standardization, Arabic words are mixed with English or French expressions and abbreviations.

Indications of identity: who are you?

At the end of a results report, possible indications of identity are listed. These include user profile names from apps, other user identities, stored information and email addresses that can be assigned to the device owner. This information may come from Google or Apple accounts, from dating apps like Tinder or from Facebook profiles linked to other applications. It is not known from which applications the system is able to extract this data.

However, the BAMF's training manuals name some examples and estimate that information derived from travel sites such as Booking.com is more reliable than that from, for instance, dating profiles. Google accounts and the messenger service Viber are also explicitly named in these documents, and the results reports available to the GFF lists Facebook and WhatsApp as well.

[39] M. A. Yaghan (2008): "Arabizi"": A Contemporary Style of Arabic Slang. published in: Design Issues, Vol 24. Issue: 2.

[40] K. Darwish (2013): Arabizi Detection and Conversion to Arabic.

C. Criticism: what is the issue at stake?

Serious invasion of privacy

Electronic devices, smartphones in particular, can connect large amounts of personal information and contain a person's entire "digital household": Text messages to family members, contact data including lawyers' information, account and payment data, access to email accounts, search engine history, residence data, intimate photos. Mobile devices are full of memories and often the only bridge refugees have to their old home. Smartphone data can be used to construct movement profiles and social networks[41] and to create detailed personality profiles of their users.[42] The German Federal Commissioner for Data Protection and Freedom of Information also emphasized this during the legislative process.[43] The reading, analysis and evaluation of mobile data carriers encroaches deeply on the privacy of refugees and violates the right to informational self-determination and, in particular, the confidentiality and integrity of information technology systems.[44]

"By systematically reading out mobile phone data, the bill creates the 'transparent refugee'", criticised Pro Asyl in a statement on the Law on Better Enforcement of the Obligation to Leave the Country.[45] The human rights organization, like many data protection experts and legal scholars, expressed considerable constitutional concerns during the legislative process. Among these critical voices are criminal law expert Nikolaos Gazeas[46] and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) at the time, Andrea Voßhoff, as well as the Deutscher Anwalt Verein (DAV), an association of lawyers.[47] The central points of criticism are the lack of protection of the core areas of private life, the lack of effective oversight and objection mechanisms as well as suitability and general proportionality. The lack of transparency of the BAMF's approach is to be deplored as well.

---

[41] T. W. Boonstra, M. E. Larsen, H. Christensen (2015): Mapping dynamic social networks in real life using participants' own smartphones.

[42] C. Stachl, S. Hilbert, J.-Q. Au, D. Buschek, A. De Luca, B. Bischl, H. Hussmann, M. Bühner (2017): Personality Traits Predict Smartphone Usage. Eur. J. Pers., 31: 701– 722.

[43] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)831, March 23, 2017.

[44] BVerfG, NJW 2008, 822.BVerfG, NJW 2008, 822.

[45] Pro Asyl: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)825 A, March 22, 2017.

[46] See K.Schuler, T. Schwarze: Asylpolitik: "Mit dem Grundgesetz nicht vereinbar", Zeit Online, February 20, 2017 and T. Podolski: Sicherheitsrechtler zum Gesetzentwurf über Auslesen von Handys bei Asylsuchenden: "Kann nicht schaden, die Daten zu haben", Legal Tribune Online, February 22, 2017.

[47] Deutscher Anwalt Verein: Stellungnahme SN 39/17 zum Gesetz zur besseren Durchsetzung der Ausreisepflicht, May 12, 2017.

Who is in charge of protecting the most private information? Lack of core area protection

The general right of privacy obliges the state to protect the basic conditions of free personality development and self-determination (Article 2 para. 1 in conjunction with Article 1 para. 1 GG). As early as 1957, the Federal Constitutional Court stated that there must be an "inviolable area of human freedom", referring in particular to human dignity.[48] Later, it also conceptually introduced the "absolutely protected core area of private life".[49] Article 48 para. 3a of the Residence Act (AufenthG) states that an evaluation of data carriers is inadmissible if there are factual indications for the assumption that "only knowledge from the core area of private life would be obtained" and that any knowledge thus gained cannot be exploited and must be deleted immediately. Case constellations in which "solely", i.e. exclusively knowledge from the core area of private life would be obtained are difficult to imagine with a mobile phone. In practice, this exception is therefore empty – because it does not protect against data that "also" relates to the core area of private life being read and evaluated. Even if the raw data is deleted after the results report has been created, through its evaluation, the intervention has already taken place. As long as the login names and email addresses used in apps are also listed in the results report, which can also touch upon linked dating apps, an intervention in the core area is at least conceivable here as well. The legal scholar Prof. Tarik Tabbara considers the inadequate core area protection to be one of the biggest problems of data carrier evaluation. He describes the proposed solution for the theory-practice problem of core area protection in the Asylum and Residence Act as "a downright cynical solution", as the reservation applies only to the evaluation, but not to the readout that preceded it.[50]

No effective control mechanism: authorization by BAMF-internal lawyers

For especially serious encroachments on basic rights, in particular surveillance measures, a judicial reservation applies. According to the Federal Constitutional Court, the basic rights also give rise to procedural requirements if their effective protection can only be ensured in this way. An encroachment on a basic right can therefore only be permissible if an external supervisory body carries out a legality audit.[51] A court approval offers special protection, precisely because it is granted by an independent and neutral entity.[52] There is much to suggest that a judicial reservation is therefore also necessary for the evaluation of refugees' data carriers.

[48] BVerfGE 6, 32 <41>.

[49] BVerfGE 80, 137 <153>.

[50] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Issue 227.

[51] BVerfG, NJW 2011, 2113 <2118>.

[52] BVerfG, NJW 2018, 2619 <2623>.

However, this reservation is not precisely legally defined. It merely needs to be authorized by a BAMF employee qualified for judicial office, i.e. a fully qualified lawyer. While clearly inspired by the mechanism of judicial reservation, it cannot be compared to the former. Prof. Tabbara notes that a "'fully qualified lawyer reservation' does not fulfill more than the minimum requirements of a true judicial reservation." The fully qualified BAMF lawyers are firmly integrated into the BAMF's chain of command, therefore this oversight mechanism cannot "even remotely fulfill the function of protecting basic rights that a judicial reservation is meant to secure."[53]

What if you refuse? How voluntary are data carrier evaluations really?

The BAMF emphasizes that applicants must activate their devices and possibly also adjust the system settings themselves so that data can be extracted. In addition, the person concerned must sign a form confirming that they have ceded their device.

Data processing may be allowed under Articles 6 and 7 of the European General Data Protection Regulation (GDPR) if the data subject gives his consent. Such consent must be given voluntarily and informed (Recital 32 of the GDPR). The form to be signed does not contain information on what data will be read from the data carriers, how they will be processed and to whom, if any, they may be disclosed. According to the descriptions given by both the persons concerned and their lawyers, there is also no verbal explanation of what happens with the data. There is also a lack of voluntariness: Even from a formal point of view, it can be denied that the signature expresses consent; according to its wording, it merely confirms the hand-over of the device. Nor can it be considered voluntary because the refugees are in a subordinate relationship to the authority. In the form to be filled out they are also informed on their legal obligation to hand over their data carriers to be read out.[54] A refusal to do so constitutes a violation of this obligation – with grave consequences. Benefits in accordance with § 11a para. 5 of the Asylum Seekers Benefits Act (Asylbewerberleistungsgesetz, AsylBLG) may be reduced; in the worst case, an asylum application in accordance with § 33 para. 2 of the Asylum Act (AsylG) may be considered withdrawn. Internal BAMF regulations state that applicants should be expressly informed of this fact if they initially refuse to surrender their device.

Due to the threat of consequences in the case of a refusal to hand over the device, there is a considerable power imbalance between the BAMF and the asylum seekers who are in need of protection and dependent on the Federal Office's decision. However, an act by which the applicants fulfill an (alleged) legal obligation cannot be regarded as voluntary.

---

[53] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Issue 227.

[54] BAMF: Form D1705.

Milder means and necessity? No chance.

The right to confidentiality and integrity of IT systems may only be restricted in cases of necessity and proportionality, in order to achieve overriding important and legitimate objectives. However, data carrier readouts purely serve migration policy objectives: This measure is intended to help the prevention of unjustified asylum grants or for the faster deportation of rejected asylum seekers. That this objective is sufficiently important to justify such an intensive, sweeping and groundless violation of people's private lives is doubtful under constitutional law, in view of the case law of the Federal Constitutional Court to date. For example, it is precisely not comparable with a measure taken to prevent serious criminal offenses and on the basis of concrete suspicions.

Part of proportionality is also that intensive legal interventions are only to be used if there are no other possibilities with which the desired objective can be achieved. § 15a of the Asylum Act (AsylG) also states that data carrier evaluation may only be carried out if there are no milder means of determining the origin or identity of applicants. However, if the conditions for the basis of the intervention are fulfilled, i.e. the applicant cannot present a valid passport or passport replacement document, the BAMF does not provide for any other milder means at all. Language biometrics, as well as name transliteration and analysis are also mentioned as milder means in the training guidelines. Apart from the question of whether these means actually are milder and therefore less transgressive, the BAMF does not actually use them as alternative measures. As internal BAMF documents reveal, these measures are applied at the same time and in addition to the data carrier readout.[55] As a result, their findings are not taken into account prior to the readout and automatic analysis of a device.

It was already noted during the legislative process by Pro Asyl that it was precisely the questioning of asylum seekers by qualified staff during the asylum hearing that was a less invasive and more reliable means of indicating origin and identity.[56] Information provided during the hearing can be checked very reliably on the basis of precise enquiries. Both the Federal Data Protection Commissioner and the Deutscher Anwalt Verein (DAV), an association of lawyers, also doubted the necessity of interfering with the fundamental right of the confidentiality and integrity of IT systems. The Deutscher Anwalt Verein (DAV) also described the proceedings as disproportionate in the final analysis.[57]

[55] Both name transliteration and dialect analysis are only an option for Arabic-speaking applicants, according to the BAMF.

[56] Pro Asyl: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)825 A, March 22, 2017.

[57] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)831, March 23, 2017; Deutscher Anwaltverein (2017): Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht zum Entwurf eines Gesetzes zur besseren

Personal account: the BAMF will still read out phone data even in the face of conclusive evidence regarding indications of origin

In October 2019 the BAMF read out the smartphone belonging to a Cameroonian refugee who was unable to show the Federal Office any identity papers, but instead presented a medical certificate detailing her reasons for fleeing, her personal history and the resulting psychological stress. The woman is a victim of forced prostitution and was severely and repeatedly raped , which also led to physical symptoms such as a chlamydia infection with resulting sterility. The attending psychotherapist attested to a post-traumatic stress disorder with suicidal thoughts, depression and a dissociative disorder. Despite the detailed descriptions of her origin and history in the certificate, BAMF had the woman's mobile phone handed over anyway and performed a data readout, with the requested evaluation being approved by a fully qualified lawyer. The informational value of the result report is limited, but outgoing calls to Cameroonian dialing codes, contacts in the refugee's address book and the language analysis of text messages make the information provided by the refugee appear plausible.

Data transfer: who else receives the data?

The Law on Better Enforcement of the Obligation to Leave the Country not only introduced the legal basis for data carrier evaluation, but also extended the legal possibilities of transmitting data to other bodies, such as security authorities or intelligence services. As a result, asylum seekers no longer have an overview of who can access their data.

According to the Federal Ministry of the Interior, there are no statistics on how often data from device analyses is passed on to security authorities.[58] The persons affected are not informed of this, which makes it impossible for them to check whether the transfer was permissible in terms of data protection considerations.

In general, data transfers from the BAMF to other government agencies have increased substantially in recent years; it is not possible to trace whether transmitted data originates from

Durchsetzung der Ausreisepflicht (Bundestags-Drucksache 18/11546).

[58] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 30.

data carrier evaluations or was otherwise collected as part of asylum proceedings. In 2015, there were 517 transmission cases from the BAMF to the domestic secret service, the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV). This number rose to 2,418 in 2016 and to 10,597 in 2017, while the total number of asylum applications fell significantly during this period.[59] According to the Ministry of the Interior, MSAB itself, the producer of the readout and evaluation system, has no access to personal data, neither from BAMF employees nor from asylum seekers. However, BAMF administrators do have access to the "data safe" for maintenance purposes or in order to forward data to the courts, and thus to unaudited reports of the data evaluations.[60]

[59] Bundestags-Drucksache 19/3840: Exchange of data between police and intelligence services in Germany, 16.08.2018.

[60] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 28.

The BAMF's attitude towards proportionality and its secret data protection impact assessment

According to Article 35 of the General Data Protection Regulation (GDPR), the persons responsible for data processing are obliged to carry out a data protection impact assessment if it "is likely to present a high risk to the rights and freedoms of natural persons". This is the case for automated processing operations in particular, which involve a "systematic and comprehensive" assessment of "personal aspects" of individuals and on the basis of which decisions concerning them are to be taken. Personal aspects also include the behavior, whereabouts or movement of a person. Data processing can be said to be systematic and comprehensive when large amounts of personal data are processed (Recital 91 of the Regulation), which concerns, for example, profiling operations. However, these requirements are also met in the case of an automated analysis of mobile phone data on calls and messages, browser behavior and location data, the results of which can influence the asylum application decision.

A data protection impact assessment must, among other things, describe the planned processing operations, specify the purpose pursued therein and assess their necessity and proportionality. A freedom of information request on the BAMF's data protection impact assessment of the data carrier evaluation was rejected with a delay of nine months with reference to security concerns.[61] The BAMF argued that possible security gaps in the system could be identified and exploited by third parties.

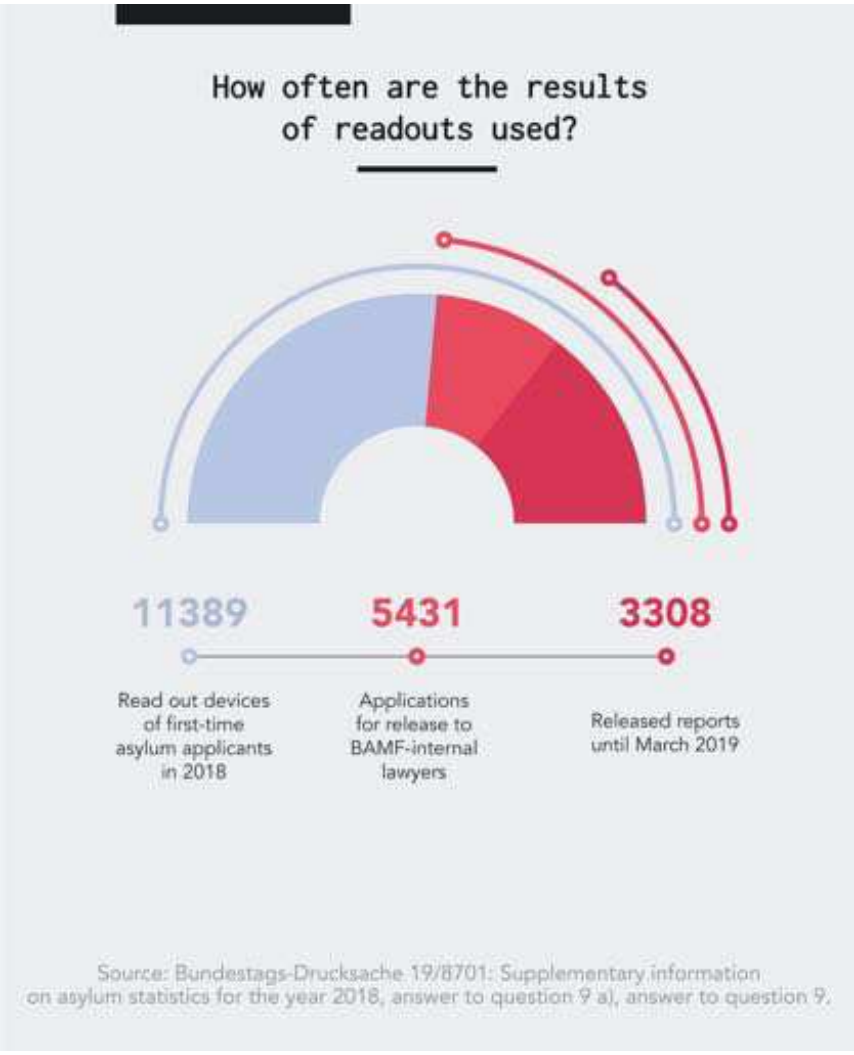
Is it worth it? How conclusive are the results reports?

Even before the adoption of the Law on Better Enforcement of the Obligation to Leave the Country, some organizations doubted the efficacy of data carrier analysis. One of the aims of the law was to speed up deportations: Data carrier analyses were to verify identity, origin and grounds for protection. However, statistics confirm that these reports rarely proved useful for this purpose: They are easy to circumvent, fail frequently on the technical level and are unusable in most cases. The results that actually are usable largely confirm the information provided by asylum seekers; only in rare exceptional cases do they uncover contradictions to the information provided.

[61] Request according to the Freedom of Information Act request on the data protection impact assessments of the BAMF, rejected on May 13, 2019.

Circumventing the measure is as easy as just denying that one owns a smartphone or other data carrier. It can be presumed that word about the BAMF's habitual readouts has spread among asylum seekers.

A significant proportion of the readouts, namely 23 percent in the first quarter of 2019[62] and 26 percent in 2018[63], already fail on the technical level. According to the BAMF's own data, even if the readout itself is successful, the results are largely unusable: In the first quarter of 2019, 55 percent of the evaluated reports contained no useful findings.[64] In 2018 this figure rose even higher, to 64 percent.[65]



There is a wide variety of reasons that can lead to unusable outcomes: For example, the data base may be too small because a mobile phone has not been used for a long time. Or the data may be contradictory because the mobile phone was used by several people, simultaneously or consecutively, without all content being deleted when the device was passed on. If an asylum seeker has only bought a smartphone in Germany, then obviously geodata on it is worthless for the BAMF because no location outside Germany will be determinable.

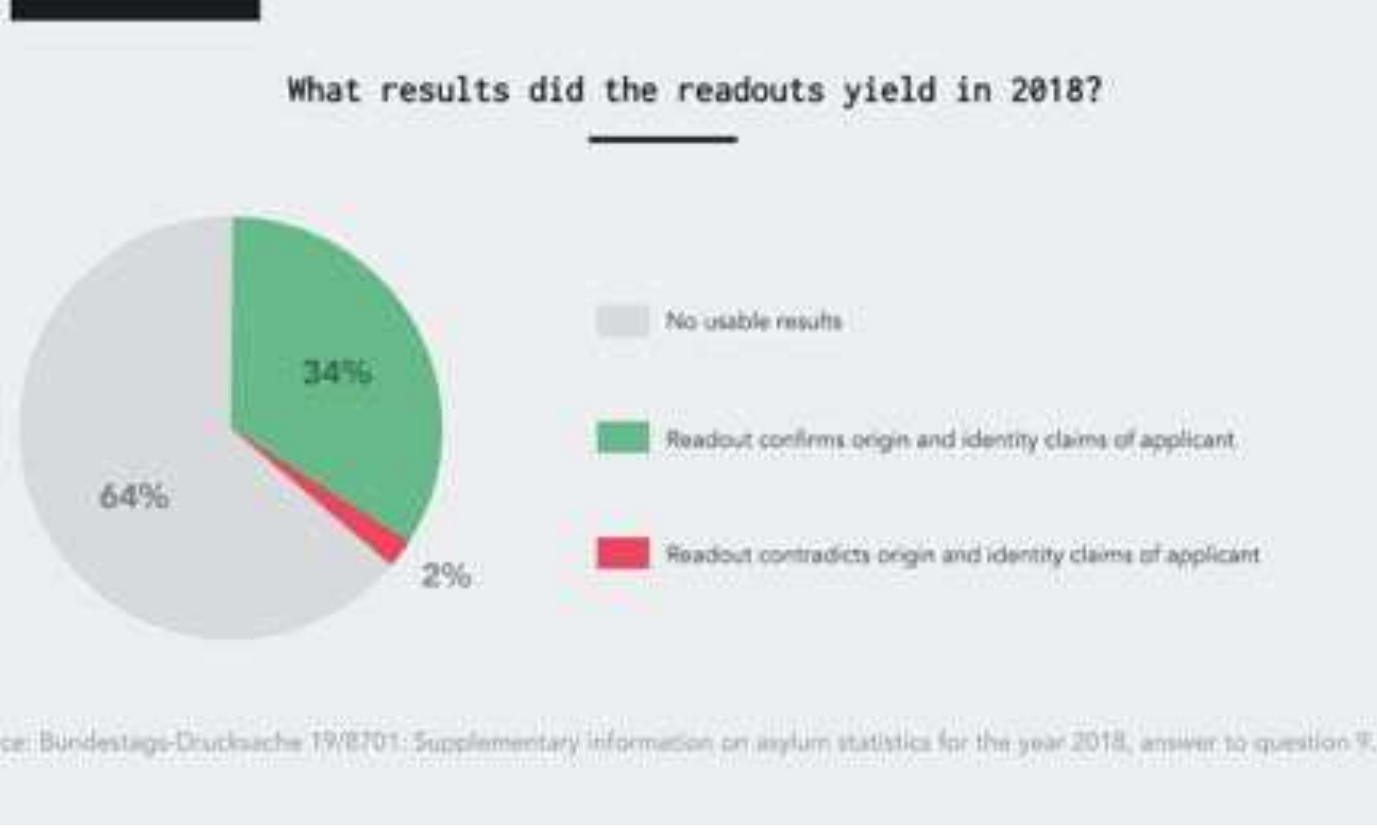
In one of the results reports available to the GFF, it is additionally noted under the section about location data that "due to the highly dynamic nature of the app data" it cannot be guaranteed in every case that the device was also located at the detected location. Or possibly, the

[62] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to questions 5 and 6.

[63] Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 9 a).

[64] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to question 6.

[65] Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 9.



applicant mainly uses apps that cannot be evaluated by the BAMF systems. In addition, refugees often use pseudonymous identities because they fear surveillance – both in their countries of origin and during their flight.[66] Therefore, it cannot be assumed that a Facebook profile name also corresponds to the refugee's real name.

Not nearly all test reports will actually be used by the BAMF in the end. Of the 3,502 data carriers successfully read out, the BAMF reported 1,538 applications from decision-makers to BAMF-internal lawyers for the release of the result reports in the first quarter of 2019; in 1,236 cases these have already been released. It is unclear how many of the remaining applications have actually been rejected and how many have not yet been processed. In the course of 2018, about 5,400 clearance applications regarding about 11,400 read-out data carriers were received.[67]

Moreover, the results of the test reports reveal contradictions to the applicants' submissions in only the rarest cases. In the first quarter of 2019, this was true in only one percent of the evaluations, so 12 cases. In the course of the year 2018, contradictions arose in two percent of cases, which corresponds to 66 cases of approximately 3,300 approved evaluations.

[66] M. Gillespie, L. Ampofo, M. Cheesman, B. Faith, E. Iliadou, A. Issa, S. Osseiran, D. Skleparis (2016): Mapping Refugee Media Journeys – Smartphones and Social Media Networks.

[67] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to question 6; Bundestags-Drucksache 19/8701: Supplementary information on asylum statistics for the year 2018, answer to question 9.

In all other cases, the reports confirmed the statements made by applicants. In the first quarter of 2019 this was the case with 44 percent and in 2018 with 34 percent of the evaluated results reports.[68] According to its own testimony, the Federal Government is aware of at least individual cases in which applicants have presented manipulated mobile devices.[69] It can therefore be concluded that the relationship between the encroachment of the affected asylum seekers' fundamental rights and the usefulness of the procedure is clearly imbalanced.

Finally, it is striking that asylum seekers from different countries of origin are affected to very different degrees by data carrier readouts. Most of the asylum seekers affected in the first quarter of 2019 were Afghan citizens with 952 cases, followed by 285 Georgians. Equipment belonging to asylum seekers from Syria, who still constituted the largest group of asylum seekers in this period with 3,454 persons, was read out only 101 times.[70]

To summarize, data carrier evaluations serve the legislative goal of preventing asylum abuse and accelerating deportation only very rarely. If measures promise very little success, the question then arises as to whether they are permissible. Prof. Tabbara also raises this question and points out that in the case of criminal law measures such as police searches, the case-law of the Federal Constitutional Court recognizes that their presumed inefficacy makes the measure disproportionate and thus inadmissible.[71]

But even without deliberate avoidance actions by the applicants, the evaluations can be useless: Dr. Matthias Lehnert, lawyer for residence and asylum law, also notes that the results of the analysis have no probative value in court proceedings if the methods cannot be reviewed by the court or if it turns out that the evaluation is prone to error.

[68] Ibid.

[69] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 3.

[70] Bundestags-Drucksache 19/11001: Supplementary information on asylum statistics for the first quarter of 2019, answer to question 6.

[71] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Issue 227.

Personal account: text messages in Modern Greek, Esperanto and Finnish? Imprecise language analyses

In June 2019, the BAMF read out an Iraqi asylum seeker's smartphone. He stated that he had owned the device since about March 2019 – which was confirmed by the BAMF's analysis. Accordingly, only an insignificant amount of information was gained from the results of the smartphone evaluation. For the majority of the analyzed country codes for outgoing (42 percent) and incoming (57 percent) telephone calls, no valid country assignment could be determined. Most of the allocated calls were said to originate from Greece, which is consistent with the refugees statement of having received the telephone in Greece. The results of the analyzed text messages are even less usable. 100 percent of outgoing messages and 97 percent of incoming messages could not be attributed to any country. Regarding the contacts in the address book of the person seeking protection, 44 could not be assigned at all, 22 percent of the remaining contact numbers were assigned to Turkey and Greece respectively and 6 percent to Iraq and Japan respectively.

Finally, the evaluation of the language used in the text messages is completely implausible: Most of the outgoing messages are said to have been written in English or Italian, namely 33 percent each. However, according to the analysis, 75 percent of the incoming messages were written in modern Greek – followed by Chinese, Japanese, Esperanto, Finnish and Dutch. As per the results report, no useful location data, browser data or identity information was found on the device. According to the lawyer of the person concerned, neither the hearing nor the asylum decision referred to the results of the analysis.

BAMF employees are left to interpret the meaning of results on their own

The majority of the results are unusable. It is up to the decision-makers and interviewers to recognize this – and to reject reports or resolve contradictions by asking specific questions. For this, they need information to help them classify the results. The training guidelines, however, only contain rudimentary points of orientation. They state, for example: "The longer the device has been used, the more meaningful the report." "The more data that could be read out, the more valid the report." In addition, possible reasons are provided for why a device has "a large number of device downtimes", i.e. was switched off. This may indicate that the device has been used or resold by different users. It is not specified what amount of data can be assumed to lead to a reliable result.

A further error source is that despite a sufficient amount of data on a smartphone, only a subsection of this data can actually be evaluated by the BAMF. One example would be if the applicant uses apps for the majority of their communication that are not supported by the BAMF's system. Another, if the country codes of incoming messages are analyzed, but an applicant communicates via messengers that do not use a telephone number as an identification feature and therefore do not contain a country code. So, because only part of the communication is then evaluated, the results can easily be distorted.

In regard to the language identification analysis of text messages, the guidelines provide no information on the analysis software's error rates to the decision-makers. Without this information, decision-makers cannot assess the uncertainty inherent in the analysis results. If a language is not known to the system, it is meant to recognize the language that appears most similar to it, but whether this is always a language spoken in a region that is geographically close to the country of origin is not certain. With regard to the quality of the login data, the training guides point out that, for example, booking.com login names are more meaningful than those of dating apps. Again, it is not known which applications are used to determine profile information. Similarly, the training guidelines do not list the exact sources of the geoinformation used in the evaluation of location data.

The decision-makers are obliged to decide the asylum case while taking all available information into account. However, computer-generated results, backed up by statistical data, convey a sense of objectivity and accuracy that can be misleading. If a decision-maker misinterprets the results, puts trust in them and therefore accuses the applicant of having provided false information on origin and identity, this may lead to an asylum application being erroneously rejected as "manifestly unfounded".

"Manifestly unfounded" – A rejection with consequences

§ 30 of the Asylum Act (AsylG) regulates when an asylum application can be rejected as "manifestly unfounded". This is the case, for example, if "key aspects of the foreigner's statements are unsubstantiated or contradictory, obviously do not correspond to the facts or are based on forged or falsified evidence" or " the foreigner misrepresents or refuses to state his identity or nationality in the asylum procedure". If an application for asylum is rejected on such a basis, there are immediate consequences. The applicant is requested to leave Germany within one week (§ 36 para. 1 AsylG). If they do not fulfill the obligation to leave the country, they can be deported.

The applicant has only one week to file an action against the BAMF's rejection. Within this period, an application for summary proceedings must also be filed, as the deportation decision can be executed immediately.

In connection with other IT assistance systems, namely dialect analysis, individual cases are known in which the rejection of an asylum application was essentially based on their results, although other factors confirmed the information provided by the applicant.[72] There is no data on how many asylum rejections are pending before courts that are primarily based on the results of the IT tools. According to the Federal Ministry of the Interior, there are no findings on this.[73]

Is the cost worth it?

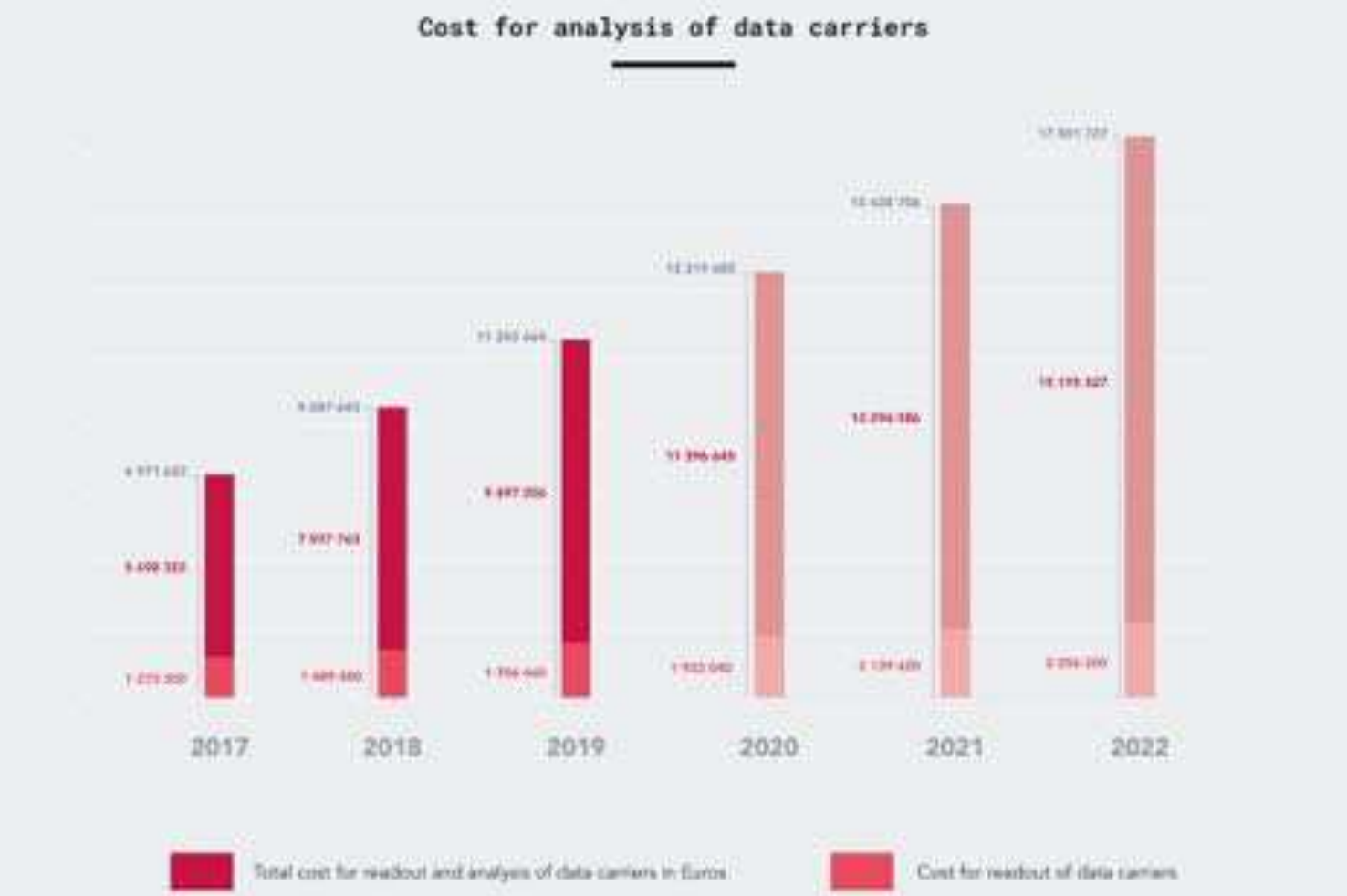
In relation to the limited benefit of the data carrier evaluation, the costs for the system are disproportionate. They clearly exceed the original expectations of the bill at its introduction. In February 2017, the Federal Ministry of the Interior stated that one-off installation costs of 3.2 million euros were to be expected for the reading devices.

One year later, the Ministry corrected its calculation to 4,788,507.60 euros spent in 2017 and a further 1,596,169.20 euros by April 2018.[74] These amounts relate only to the hardware and

[72] A. Biselli: Eine Software des BAMF bringt Menschen in Gefahr, Motherboard/VICE, August 20, 2018.

[73] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 23.

[74] Bundestags-Drucksache 19/1663: Use of voice recognition software by the Federal Office for Migration and Refugees, April 16, 2018, answer to question 13.



Source: The displayed cost consists of the total cost up to now for purchase and support. The cost of 2017 contains purchase and support for the hard and software used to read out data carriers, from 2018 onwards it is support cost. The cost 2020 is an estimation based on former cost. Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 15.

software for the reading process. In order to analyze the data, further expenses were due: 1,070,000 euros in 2017 and an additional 182,000 euros by April 2018. Together, this amounts to around 7.6 million euros by the end of 2018 – and thus more than twice as much as originally estimated.

According to information from the Federal Ministry of the Interior dating from December 2018, the system is expected to cost a total of 11.2 million euros by the end of 2019. The total expenses will continue to rise; support and licenses are expected to cost around 2.1 million euros annually. In addition, licenses must also be purchased annually for each reading device.[75]

[75] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 15.

In contrast, according to the explanatory memorandum to the law, 300,000 euros per year were earmarked for these items. The total costs also include the expenses incurred during the project's test phase totaling 585,480 euros. At that time, the BAMF was testing systems from MSAB, T3K and Cellebrite.[76]

Black box smartphone evaluation: Intransparent software and algorithms

Obtaining information on the BAMF data carrier evaluation is an arduous process. The BAMF released information only piece by piece and with sometimes considerable delays. In some instances, the answers are so incomplete that they can hardly be classified as truthful. So, the BAMF responded to a press enquiry in April 2018 about the manufacturers of hardware and software for reading out and evaluating mobile devices belonging to refugees: "ATOS provides the necessary software and hardware for reading out and evaluating data carriers".[77] The BAMF did not reveal that ATOS was only the supplier of the overall system and that the individual components come from manufacturers such as MSAB and T3K. The Office also only responded to inquiries under the Freedom of Information Act after long waiting periods and regularly exceeds all legal deadlines. The statutory period of one month may only be deviated from by the authorities in unusual circumstances, for example in particularly labor-intensive requests. The training guidelines were only transmitted by the BAMF after almost four months, and the request for the data protection impact assessments was completely rejected after nine months.

But the BAMF also concealed information from parliamentary inquiries. In June 2018, for example, the Federal Ministry of the Interior, which is superordinate to the BAMF, answered a written question from the Bundestag, the German Federal Parliament, to the effect that it had (only) tested or procured products from ATOS, MSAB and T3K for data carrier analysis.[78]

It was only in December 2018, in response to a later Minor Interpellation, that the Federal Ministry of the Interior added that Cellebrite technology had also been tested.[79] The algorithms and database on which the products are based, the applications which they are able to evaluate and the error rates to be expected are still not public knowledge. The BAMF refuses to answer questions about these topics, its reasoning being that conclusions might be drawn about the way the technology works, which could potentially impede its effectiveness. Even with re-

[76] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 25.

[77] Anna Biselli: Handys von Asylbewerbern zu analysieren, kostet viel mehr als geplant, Motherboard/VICE, April 17, 2018.

[78] Bundesministerium des Innern: Schriftliche Frage Monat Juni 2018, Arbeitsnummer 6/225.

[79] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 25.

gard to the error rate of language analysis for text messages, the Office refuses to provide any information. Yet, a lot of this knowledge is crucial in order to assess the reliability of the system.

Therefore, many questions remain unanswered: (How) Does the BAMF prevent, for example, geodata from photos sent to a refugee by another person from being included in the evaluation? Which languages can the text analysis module recognize? If a refugee writes text messages in Kurmanji, will this language be recognized? If not, is it then at least assigned to another Kurdish language or will it be completely mischaracterized? What are the error rates in language recognition, and do they differ between languages?

In its final report, the Data Ethics Commission appointed by the Federal Government drew up recommendations for the use of algorithmic systems by state actors.[80] In this report, the Commission's experts also formulated transparency requirements. These include that state decisions for which algorithmic systems were used must remain transparent and justifiable. In addition, the Data Ethics Commission refers to a position paper of the Freedom of Information Commissioners in Germany. According to this paper, public bodies should be in possession of "meaningful, comprehensive and generally understandable information regarding their own data processing" and if possible make this information public. In this, the position paper expressly includes the data categories being processed, as well as the underlying logic, including calculation formulas, and the weighting of the input data.[81] The BAMF does not fulfill any of these transparency criteria.

Only the beginning? Expanding data carrier evaluation is a technical possibility

In view of the introduction of this new state authorization for data carrier analysis and the correspondingly broad and – above all – cost-intensive technical upgrades, the question arises as to whether these means will in future be used in cases other than those currently provided for by the legal basis in the Asylum Act. MSAB's readout and evaluation system is technically capable to do more than the BAMF is legally allowed to do. So far, the results report provided to BAMF employees mainly contains overview information on how the data carrier was used, but no communication content, with the exception of login names used in apps. However, this is not because it is not technically feasible.

It would take little effort to match time stamps to geodata. Contact information could be checked for connections to persons known to the police or intelligence services. The company

[80] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission, October 23, 2019.

[81] 36. Konferenz der Informationsfreiheitsbeauftragten in Deutschland: Position paper „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar", October 16, 2018.

T3K, whose language recognition software is currently used to evaluate text messages, also offers image recognition technology that can allegedly automatically search stored photos for images of drugs, weapons, or terrorist propaganda.[82] The XRY software used by the BAMF can also recover deleted data from iCloud backups[83] and, according to the manufacturer, is also capable of "Android exploits", i.e. the possibility of exploiting weak points in Android devices' software to circumvent security mechanisms.[84] A further technical possibility is the analysis of text messages' content, for instance by keywords. The result for refugees registering in Germany would be to increasingly become victims of measures that are otherwise only permissible on concrete suspicion of criminal offenses.

This is not just a theoretical scenario – rather, it is a reflection of concrete demands that have already been voiced. The former head of the BAMF, Jutta Cordt, informed the Südwestrundfunk (SWR) in November 2017 that she wanted to have access to photos.[85] One year later, in December 2018, the Federal Ministry of the Interior declared that the technical and legal possibilities of extending smartphone evaluation were currently being examined.[86]

There is a simple explanation for the BAMF's eagerness to extend data readouts: Already today, the Office is trying to find out whether an asylum seeker has had contact with traffickers or terrorist groups, both as a victim or a perpetrator. The BAMF regularly forwards information about refugees to the Federal Constitutional Protection Agency if it is suspected that the person is planning a serious crime or might be of interest to the secret service.

A pilot project by the BAMF on "profile analysis" uses artificial intelligence for analyzing hearing protocols, in an attempt to automatically identify security-relevant content. Through this, the Office wants to "comply more easily and quickly with the BAMF's legal reporting obligations to security authorities".[87]

Finally, conclusions in regard to the escape route are also of interest: In Austria, the determination of travel routes is an explicit goal of the data carrier evaluation, in order to obtain clues as to the state through which the refugee entered the EU. The Dublin III Regulation stipulates that

---

[82] T3K-Forensics: Analyse von Smartphones in der Mobilforensik (last downloaded on December 7, 2019).

[83] MSAB: XRY v7.3 upgrade tackles implications of iOS 10.3 (last downloaded December 7, 2019).

[84] MSAB: XRY (last downloaded December 7, 2019).

[85] SWR: Interview der Woche – Jutta Cordt, Präsidentin Bundesamt für Migration und Flüchtlinge (BAMF), November 2017 (no longer accessible).

[86] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 27.

[87] R. Böcker: KI-Anwendungen im Einsatz, Newsletter des Behörden Spiegel "E-Government, Informationstechnologie und Politik", Ausgabe Nr. 938, March 21, 2019 and A. Biselli: Asylbehörde sucht mit Künstlicher Intelligenz nach auffälligen Geflüchteten, netzpolitik.org, July 19, 2019.

the EU member state that a refugee entered first is the one responsible for that person's asylum case. In the so-called "Dublin procedure", asylum seekers can be deported if it can be proven that they entered through another EU member state. Another conceivable gateway to more surveillance is the identity information already available in the results report, such as Facebook profile IDs or email addresses. They could serve as a starting point for further investigations. So, decision-makers could manually search the Facebook profile of asylum seekers for further information.

D. More than smartphone data: automation of migration control in Germany

In parallel to the data carrier evaluation, the BAMF introduced further, so-called IT assistance systems, for identity verification. The IT systems are grouped under the name "Integrated Identity Management – Plausibilization, Data Quality and Security Aspects (IDM-S)" and, in addition to data carrier evaluation, also include procedures for image biometrics, voice biometrics and for the transliteration and analysis of Arab names.[88]

Biometric images and automatic database comparison

In addition to fingerprints, refugees' biometric facial images are captured at each initial registration. They serve to identify asylum seekers who have already been registered and to so avoid double registrations. Biometric facial images and fingerprints are also used to compare them with those in other databases. For example, a comparison with the EU's EURODAC database is used to determine whether a registration has already taken place in another EU country. The images and fingerprints are then stored in a chip of the electronic residence permit.

Transliteration assistant TraLitA

When BAMF transliterated Arabic names into the Latin alphabet, inconsistencies repeatedly occurred as a uniform transliteration did not take place. An automatic transliteration program is therefore used to transfer applicant's entries at registration from Arabic characters into the Latin alphabet in a standardized way.

In addition, an analysis is carried out to determine how frequently a name occurs in certain regions of origin in order to assess how plausible the provided information is. According to the instructions for the determination of identity, this country of origin prognosis takes the following format: "The name is [rare/very rare] in the specified country [Syria]. In [the country/the countries] [Libya, Egypt/Morocco] is more common."[89] According to the Federal Ministry of the Interior, the system is based on a database of one billion names from all over the world; for each Arabic-speaking country, the system has been tested with 20,000 real names. Nevertheless at times, the error rates are high. In the case of Syrian or Iraqi nationals, the system is said to be correct in 85 to 90 percent of cases, but with applicants from the Maghreb regions, only a success rate of 35 percent is recorded, "[which] could be due to the historical mixture with

[88] BAMF: Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität, Sicherheitsaspekte. Einführung in die neuen IT-Tools, August 30, 2017.

[89] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

the French and Italian languages."[90] Therefore, when the system suggests that a name originates from the Maghreb region, it is therefore far more likely that this assessment is incorrect.

Dialect as a characteristic of origin

Arabic-speaking applicants may also be subjected to a dialect analysis when they first register. For this, they must submit a two-minute language sample, which is then analyzed by a system that indicates probabilities for possible languages and dialects. This also is intended to check the plausibility of indications of origin. According to current information provided by BAMF, the error rate of this software is currently at 15 percent, with variations depending on the mother tongue and region of origin. In December 2018, the German government reported a success rate of over 90 percent for the Arabic-Levantine dialect spoken in Lebanon, Jordan, Syria, Israel and Palestine. The BAMF determines the error rate via both validated speech samples and random samples from its own speech and dialect recognition, which were additionally verified by "technical experts and language experts".[91]

The Arabic-Levantine dialect is supposedly developed the most in the language model used. For this, the BAMF purchased an Arabic-Levantine language package from the Linguistic Data Consortium of the University of Pennsylvania for 3,721.62 euros.[92] Queries on the error rates for the other dialects remained unanswered by the BAMF. The extent of the training data sets for a particular dialect is a decisive factor for failure rates. There is confirmation that by December 2018, a total of 8,000 validated speech samples had been fed into in the system. The number of language samples per dialect and language is not specified, however. In its reply, the German government points out that this information is classified as "classified information – for official use only", since otherwise deliberate acts of deception take place during asylum proceedings and language recognition could be manipulated.[93] In fact, the conclusion to be drawn above all is that the susceptibility to errors has never been checked by a specialist supervisory control and cannot be understood by external actors with no recourse to the algorithms used. Various linguists have voiced doubts as to the reliability of language determination.[94] A proper assessment of the reliability and indicative effect for all persons party to the proceedings, from the BAMF staff to the judges, is therefore impossible.

[90] Bundestags-Drucksache 19/6647: Use of IT assistant systems at the Federal Office for Migration and Refugees, December 19, 2018, answer to question 34.

[91] Ibid., answer to question 11.

[92] Ibid., answer to question 14.

[93] Ibid., answer to question 16.

[94] See, among others P. Hummel: Software soll Dialekt von Asylbewerbern untersuchen, March 17, 2017, Welt; A. Biselli: Software, die an der Realität scheitern muss, March 17, 2017, Zeit Online; A. Biselli: Eine Software des BAMF bringt Menschen in Gefahr, August 20, 2018, Vice/Motherboard.

For an affected person, it is very difficult to challenge an inaccurate result. And in practice, the main danger is that the results will be assigned a degree of reliability that they do not deserve.

Since 2015: data carrier evaluation in the Foreigners' Offices

Foreigners' Offices had already been allowed to access data carriers two years before the BAMF. The latter, as the Federal Authority for refugees is responsible for carrying out asylum proceedings. But the Foreigners' Offices are usually located at county level and responsible for all people without German citizenship. They decide, among other things, on residence permits, settlement permits or the execution of deportations. As a result of an amendment to § 48 of the Residence Act (Aufenthaltsgesetz, AufenthG), they have been able to access foreigners' devices if they are unable or unwilling to prove their identity ever since July 2015. According to amended § 48 AufenthG, this can be done in order to establish identity and nationality and for the purpose of enforcing deportations, unless milder means are available.

Little is known about the exact practice and frequency of use by the Foreigners' Offices throughout the country, since their responsibilities are regulated by state law. In an answer to a written question posed by representative Niklas Schrader (LINKE) in the Berlin House of Representatives from August 2018, the Senate Administration for Internal Affairs and Sport stated that in Berlin, the information was viewed and evaluated exclusively by a fully qualified lawyer employed by the Foreigners' Office.[95] According to the Senate Administration, the information includes "telephone numbers with area codes, with their corresponding names, possibly also addresses, phone logs, SMS messages, WhatsApp messages and those from comparable messenger apps, emails and photos".

In the period from July 2015 to August 2018, a total of 40 devices were evaluated in the state of Berlin. In individual cases, the login data had been requested from a provider, but the Office does not compile any statistics on this.

[95] Abgeordnetenhaus Berlin Drucksache 18/15903: Zugriff auf private Datenträger durch die so genannte Ausländerbehörde, August 16, 2018.

E. Beyond borders: refugee data carrier evaluation in Europe

Germany was not the only country to react to the increase in asylum seekers from 2015 on with the introduction of new powers and technologies for the evaluation of data carriers. In December 2017, the European Migration Network coordinated by the EU Commission reported that the evaluation of smartphones and other data carriers was planned as a standard measure in asylum proceedings only in Germany and, at that time, the Netherlands and Estonia.[96] In addition, data carrier evaluation is obligatory in Latvia, but only on the basis of criminal law. Further, the report goes on, data carrier evaluation is also planned as a possible measure in Italy, Lithuania, Norway and Croatia. Moreover, migration and security authorities have also been granted additional powers in Austria, Denmark and Belgium.

The purpose for which the data is used, the frequency with which the measures are implemented, the extent to which the data is read and the authority responsible for reading the data carriers vary considerably between countries. Also, that police authorities are confiscating and evaluating devices is more common than readouts by migration authorities. It is noticeable, however, that in all countries little or no information on this practice is public.

Denmark and Norway

Denmark and Norway were among the first countries to evaluate refugees' data carriers. According to the Danish daily newspaper Dagbladet Information, the Danish police began reading and storing data from smartphones, SIM cards and other data carriers in 2015, as part of asylum procedures and without suspicion of crimes.[97] The Danish national police's response to a freedom of information request, the contents of which are known to the GFF, shows that this measure was only actually applied to a comparatively small proportion of refugees. From May to December 2016, 383 mobile phones were read, compared to 503 in all of 2017. In these cases, the police confiscated the devices, read them out and then passed the information over to the immigration authorities. Like the BAMF's measures in Germany, the permissible aim of the measures is to obtain information on refugees' identity and origin. However, should the police have reason to suspect a crime, they also use these chance findings.[98] According to Richard Østerlund la Cour, superintendent at the National Aliens Center at the Danish Police, the data carrier readout consists of an almost complete copy of the contents of the device, which also

[96] European Migration Netzwork (2017): EMN Synthesis Report for the EMN Focussed Study 2017 – Challenges and practices for establishing the identity of third-country nationals in migration procedures.

[97] M. K. Stræde, S. Gjerding: Hundredvis af asylansøgeres mobiler kopieret af politiet, Dagbladet Information, February 17, 2016.

[98] Ibid.

includes photos and videos. The daily newspaper Politiken quotes la Cour as follows: "If you come into the country and say you come from Syria but have nothing but your face to prove it, the mobile phone is the best way to determine whether you are telling the truth or if actually all calls go to Ghana."[99]

The preconditions for implementing the action have been further lowered. Initially, the legal basis provided for a readout of data carriers if this was considered important for determining origin and identity. After an amendment to the law in 2017, this is now already permissible if the assumption can be made that the data might be of significance for the asylum procedure (§ 40 para. 10 of the Danish Aliens Act, Udlændingeloven).[100] Jesper Lund, chairman of IT-Politisk Forening, a Danish NGO for digital rights, reports that the legal basis is interpreted broadly and that the evaluations include mobile phones, tablets and other devices. In principle, the evaluation without the consent of the person concerned is only permissible with a judicial reservation, but this can be waived in case of imminent danger (§ 806 para. 4 Retsplejeloven). "The clear intention of the Danish government was to confiscate refugees' mobile phones in more cases, undoubtedly to find more reasons for rejecting asylum applications," says Lund.

Like the BAMF in Germany, the Danish police use MSAB's XRY system to extract information from mobile phones, which is knowledge gleaned from another for freedom of information request in possession of the GFF. In addition to establishing identity and origin, the data can also be used to assess the motive for the asylum application, to determine possible reasons for rejecting the asylum application and to examine whether the asylum seeker poses a threat to Danish national security (§ 40 para. 10 Udlændingeloven).[101]

In Norway, the practice of data carrier evaluation was under media discussion in 2016, because the police confiscated the telephones of several unaccompanied underage refugees.[102] In October 2017, the Norwegian daily Aftenposten reported on plans for new Arrival Centers in which the Immigration Directorate UDI and the Police Immigration Service PU would be permitted to use GPS paths, pictures, apps, internet activities, messages and contacts to examine asylum seekers' applications.[103] Data extraction already takes place during the registration process, analogous to German practice. Social media information was also systematically ana-

[99] F. Hvilsom, M. Gram: Politiet tager asylbørns mobiler ved ankomst, Politiken, February 15, 2016.

[100] Author's own translation. Original: „Dokumenter og genstande, der må antages at være af betydning for at fastslå en udlændings identitet eller tilknytning til andre lande, eller som må antages at være af betydning for sagens oplysning, kan tages i bevaring, hvis det skønnes fornødent."

[101] Udlændinge- og Integrationsministeriet: Forslag til Lov om ændring af udlændingeloven, April 5, 2017.

[102] NTB: Norsk politi beslaglegger asylsøker-mobiler, February 16, 2016.

[103] T. Olsen: Listhaugs nye ankomstsenter: Vil tappe mobiler og bruke avansert datainnsamling for å sjekke asylsøkere, October 26, 2017.

lyzed in connection with asylum applications.[104] In January 2017, the Norwegian government submitted a proposal for an amendment to the Aliens Act (Utlendingsloven), which would give the police further powers to search the phones and devices of asylum seekers.[105] Until then, data carriers were seized on the basis of § 10 of the Police Act (Lov om politiet) in order to obtain information on the identity of refugees. In the future, potential information on travel routes or a possible security risk are also supposed to constitute grounds for a data evaluation.[106]

Belgium

An amendment to the law in 2017 allows asylum authorities in Belgium to demand the surrender of refugees' digital media and the ability to analyze it.[107] However, in practice this has not been implemented yet. The measure is permitted by law if it can be assumed that an applicant is withholding information. There is no restriction on the types of digital media covered; even private email exchanges can be evaluated. If applicants refuse to surrender information, they are seen to violate their obligation to cooperate, which can result in the rejection of their asylum application. The Belgian Data Protection Commissioner criticized the legislative initiative and stated that the digital information should only be requested when needed, rather than systematically.[108] He pointed out that the Belgian Migration Authorities' employees were not trained to carry out such invasive interventions. Further, the assessment as to whether there is reason to believe that the asylum seeker is withholding information was subjective and difficult to verify.

He also points out that the draft law does not protect the rights of the person concerned and does not exactly regulate how the data should be treated. Opposition also came from NGOs such as the Association pour le droit des étrangers (Association for the Right of Foreigners), which criticized the fact that refugees' consent was not voluntary, as they were under pressure for fear of having their asylum applications rejected.[109]

---

[104] T.Olsen, L. L. Dragland: Slik kan Facebook avdekke løgn: Disse avslørte seg selv, July 12, 2017 and T. Olsen: Asyladvokat: – Facebook er et sted mange driver med tull og fanteri, July 13, 2017.

[105] Norwegian Ministry of Justice: Høringsnotat-Forslag til endring i utlendingsloven og utlendings-forskriften–visitasjon og undersøkelse av asylsøkere ved registre-ringmv, January 11, 2017.

[106] Ibid.

[107] Original: "Loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demanders d'asile et de certaines autres catégories d'étrangers".

[108] Commission de la protection de la vie privée (2017): Avis d'initiative relatif au projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement e l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres ca (CO-A-2017-047).

[109] V. Henkinbrant: D'une curieuse idée du consentement : une plongée sans fond dans la vie privée des demandeurs d'asile, September 2017.

These powers have not been used since the law came into force. In 2018, a complaint against the law was lodged with the Belgian Constitutional Court.[110] A hearing of the complaint has not yet taken place, as the lawyers working on the case informed the GFF.

Austria

Just as in Belgium, data carrier evaluation in Austria is legally supported but not yet implemented. Since September 2018, public security organs in Austria have been permitted to remove and evaluate data carriers from refugees in order to clarify their identity or determine escape routes within the framework of asylum proceedings.[111] The reason for the latter is to transfer asylum seekers to other EU states, as far as possible: If the data evaluation shows that the refugee has entered Austria through another EU member state, this state is obliged to allow them entrance under the EU Dublin III Regulation.[112]

The security authorities are allowed to forward the result of the evaluation and the backup copy to the Federal Office of Foreign Affairs and Asylum. According to a reply to an inquiry by the Austrian Ministry of the Interior in July 2019, it is partly due to data protection reasons that the measures have not yet been applied.[113] In its explanatory memorandum, the Austrian government states that geolocalization data stored on mobile phones, but also photographs of documents that have not been presented in a physical form, are of particular interest. A judicial or other reservation is not provided for, nor is there any restriction on the use of data from the core areas of private life. Moreover, milder means are not explicitly defined in the text of the law.

The Austrian digital rights NGO epicenter.works criticizes the fact that the police can make complete backup copies of data carriers of any kind without subsequently having to delete data that does not serve the intended legal purposes.[114] Epicenter.works also criticizes a violation of the principle of equality, because the stricter conditions, which even apply to criminal investigations, cannot be applied to asylum seekers – "even though the persons concerned are neither suspects nor defendants, nor in any other way connected with crimes". The UN Refugee Organization UNHCR condemned the fact that security authorities in Austria are al-

[110] Ciré: Un recours contre des lois liberticides et contraires à la Constitution, September 12, 2018.

[111] The Fremdenrechtsänderungsgesetz two new parts to the Fremdenpolizeigesetz 2005 regarding the evaluation of data carriers; see: Bundesgesetzblatt für die Republik Österreich: 56. Bundesgesetz: Fremdenrechtsänderungsgesetz 2018 – FrÄG 2018 (NR: GP XXVI RV 189 AB 207 S. 36. BR: 9998 AB 10020 S. 883.), August 14, 2018.

[112] Bundesministerium für Inneres: Erläuterungen zur Regierungsvorlage zum Fremdenrechtsänderungsgesetz, 2018.

[113] Bundesminister für Inneres Dr. Wolfgang Peschorn: Entscheidungen des BFA und Evaluation aktueller Maßnahmen im Bereich des Asylwesens, 3614/AB XXVI. GP, July 23, 2019.

[114] A. Adensamer, A. Hanel, L. D. Klausner, H. R. Pecina: Stellungnahme zum Fremdenrechtsänderungsgesetz von epicenter.works, May 15, 2018.

lowed to evaluate data carriers on a blanket basis, even though Migration Authorities are responsible for asylum proceedings.[115]

Great Britain

In Great Britain, the Data Protection Act of 2018 contains far-reaching exceptions to data protection safeguards under the General Data Protection Regulation when processing data for the purpose of maintaining effective immigration control. This condition has come under criticism from human rights organization Privacy International, as large amounts of data are being collected at borders and beyond to track and identify people. The NGO Platform for International Cooperation on Undocumented Migrants has therefore lodged a complaint with the European Commission.[116] In addition, the reading of data carriers by the police is generally widespread, not only among suspects of criminal offenses, but also among witnesses.[117] The human rights organization Privacy International has investigated this practice and found that there is often a lack of a legal basis and basic protective mechanisms regarding this practise.[118] The extent to which refugees are affected by such readouts, for example during police checks at borders, is not known.

In Great Britain, however, there are even more far-reaching powers: A legislative change to the Police Act in 2013 gave not only police officers but also British immigration officers the right to interfere with mobile phones and other technical devices belonging to asylum seekers.[119] This goes far beyond the mobile phone evaluation allowed in Germany, and makes it possible to carry out secret surveillance measures, place bugging devices and to hack and search phones and computers. The change in law and accompanying new practice went largely unnoticed until The Guardian Observer reported it in 2016.[120] According to a briefing document from the Home Office addressed to immigration officers, it was intended "to ensure that immigration officers can deploy a full range of investigative techniques to deal effectively with all immigration crime". A representative of the UK Home Office confirmed that the measure had prevented the distribution of forged travel documents. In response to a request from the Labour Party in the House of Commons, James Brokenshire, then Minister of Security and Immigration in the

[115] UNHCR: UNHCR-Analyse des Entwurfs für das Fremdenrechtsänderungsgesetz 2018, May 9, 2018.

[116] PICUM: PRESS RELEASE – Advocates bring first GDPR complaint to EU against UK data protection law for violating data rights of foreigners, July 1, 2019.

[117] Big Brother Watch UK (2019): Digital Strip Watch. The Police's Data Investigation of Victims.

[118] Privacy International (2018): Digital stop and search: how the UK police can secretly download everything from your mobile phone.

[119] With the "Crime and Courts Act 2013" § 93 para. 5 of the 1997 Police Act was changed and migration officers were added to the list of those authorized to intervene with property and wireless communication.

[120] M. Townsend: Revealed: Immigration officers allowed to hack phones, The Guardian, April 10, 2016.

Home Office, stated that since 2013, immigration officials had been authorized to investigate and prevent serious crimes relating to immigration or nationality offenses only – which they had been doing ever since.[121] It is not yet known whether the procedure was also used to review the statements made by asylum seekers during the asylum proceedings.

There are grounds to believe that that the responsible authorities are using hardware and software produced by the Israeli mobile forensics manufacturer Cellebrite: The latter made a delivery to the "UK Immigration Enforcement" department, and in May 2018 a payment of 45,000 pounds from the British Ministry of the Interior for "laboratory and scientific equipment" was entered in the UK Home Office's Transparency Index.[122]

[121] Written Question by Andy Slaughter, MP : Immigration Officers: Surveillance, answer from March 22, 2016.

[122] UK Home Office: Transparency data – Home Office spending over £25,000, May 2018.

F. Conclusion

With the data carrier and smartphone analysis, the BAMF deeply violates refugees' privacy in a moment in which they are particularly vulnerable: They fear negative consequences for their asylum procedure if they refuse to surrender their data and are under pressure, they can barely assess the consequences of this evaluation and do not know exactly what will happen to their data. The protection of proceedings through internal BAMF controls of legality is inadequate and subsequent legal protection is difficult to access and not promising in the short-term.

In view of the intransparent approach and the unknown evaluation procedures (algorithms) being used, neither the general public nor decision-makers or judges can properly assess the reliability of the results. Asylum application decisions are thus becoming more and more dependent on the results of error-prone IT systems. The benefits of this multi-million-euro technology are few in comparison: In less than half of the cases, an evaluation provides even usable information; contradictions to the information provided by refugees were only discovered in the rarest of cases: From about 20,000 devices read out by the end of 2019, this applied to a low three-digit range of cases. The main beneficiaries are the manufacturers of monitoring technology who are making a decent profit from their products.

The BAMF's approach must be understood as part of a national and international trend, in which new controlling and monitoring technology is being tested and used on refugees. Further, the expansion of these technologies for other purposes and to other parts of the population remains a threat. Germany is not the only country to rely on data carrier evaluation. In recent years, asylum and police authorities in other European countries have also begun to confiscate and analyze the digital household of refugees. Asylum procedures are increasingly being digitized – be it automatic data comparison with growing databases, mobile forensics as heretofore only used in criminal proceedings, or artificial intelligence to search for suspicious refugees. The human being with their personal history of flight fades into the background and turns into a collection of pure data.

Every refugee has the right to a fair asylum procedure. This also includes that its outcome does not depend on an automated and hard-to-verify decision of whether protection is to be granted or not. Refugees, too, have a right to informational self-determination and to the confidentiality and integrity of information technology systems. They must not be subject to second-class data protection. Their particular vulnerability and defenselessness must not be exploited to test new control and monitoring technology.

All in all, this shows that a comprehensive – also legal – review of the BAMF's data carrier evaluation is necessary.