# F. Conclusions

## 1. Where Do We Stand

This study highlights significant challenges and unresolved issues surrounding the Eurodac and Interoperability Regulations, particularly concerning data subjects' rights to information, access to and rectification and erasure of data, alongside effective remedies. These rights are based, at their core, on the respect for human dignity. They are rooted in EU fundamental rights and data protection law. Furthermore, they are central pillars that enable data processing within an interoperable EU information system, e.g., Eurodac, to be considered lawful.

The right to information emerges as a critical concern, with frequent violations and limited enforceability exacerbating risks within expanding interoperable information systems. As information systems grow in complexity and scope, ensuring data subjects are informed about data usage becomes increasingly crucial. Addressing these challenges demands robust mechanisms that guarantee transparency and empower data subjects to understand and protect their rights effectively.

Access to data and information presents another formidable hurdle, complicated by procedural barriers and the absence of a unified access portal. This disparity disproportionately affects individuals outside the Schengen Area, underscoring the need for enhanced accessibility and a broad interpretation of transparency principles. The chapter on access further underscores the intricate interplay between access rights and rights to rectification, erasure, and restriction of processing. Despite legal provisions, practical implementation of the right to access data and information remains challenging. Particularly in security-related contexts, where the right can be severely restricted, the consequences for data subjects may be far-reaching and thus data accuracy is paramount.

The right to an effective remedy emerges as pivotal in safeguarding data subjects' interests, yet it also faces limitations due to procedural complexities, evidentiary challenges, and the principle of mutual trust. The Eurodac and Interoperability Regulations currently fall short in providing an effective remedy concerning Eurodac data. EU law, particularly the AMMR, does offer avenues for redress, albeit with practical limitations. Significant uncertainties persist regarding the objects or acts that can be contested, com-

pounded by the intricate nature of migration and asylum procedures across multiple jurisdictions. The scarcity of judicial scrutiny concerning data rights and access to justice made possible under the Eurodac Regulation (and depending on the national structure of legal remedies) underscores the need for enhanced legal clarity and protection, especially for vulnerable data subjects.

As interoperability is deployed, addressing these limitations will be crucial to ensure equitable legal protections for all data subjects. Whilst data volumes and processing operations increase, prioritising procedural fairness, accuracy, and transparency becomes even more critical to mitigate errors and ensure proportionality.

Furthermore, the application of the Eurodac and Interoperability Regulations in Schengen/Dublin-associated countries such as Switzerland highlights significant complexities arising from the intricate interpretation of bilateral law and the divergences between Union and Swiss national law. These discrepancies, particularly concerning data subjects' access to justice rights, suggest a need for clearer legal alignment. Ensuring compliance with human rights standards remains crucial amidst these legal intricacies. This seems all the more important when one considers how interoperable systems, and Eurodac in particular, are being expanded beyond the borders of EU or Schengen/Dublin-associated countries.

What, then, do these challenges imply for the realisation of the rights examined in this study? The regulations analysed here have not yet been implemented, and case law exists only in relation to the current, "old" Eurodac system. This makes it difficult to anticipate how the rights in question will be applied under the revised framework. One conclusion, however, is already evident: the data subjects concerned – children and adults migrating to Europe – are not afforded the same privacy and data protection rights as EU citizens. They are required to provide significantly more sensitive data, which are processed and cross-checked extensively, while exercising very limited autonomy over them. In light of the challenges identified in this study, it is likely that these individuals will be unable fully to realise even the limited data protection rights formally available to them within the interoperable Eurodac system.

A decisive factor, therefore, lies in the implementation process. This may create opportunities to uphold, as far as possible, the rights of these data subjects. In the longer term, it will be essential to develop case law that affirms the equality and equal worth of EU citizens and third-country nationals.

The following two sections examine the findings of this study in greater depth: Section Two considers the meaning and implications of human dignity in the context of the interoperable Eurodac system, while Section Three analyses where and how the implementation of the Eurodac and Interoperability Regulations could strengthen the rights of data subjects. Section Four will then consider potential future developments concerning the interoperable Eurodac system and propose ways of reframing migrant data processing towards a more humane and rights-oriented approach. The chapter concludes with final reflections by the author.

## 2. The Dignity of the Data Subject

Human dignity stands as a cornerstone of the European human rights framework, deeply embedded in the EU's CFR and the ECHR. This principle underpins many other rights, including privacy, data protection, access to justice and procedural rights. The GDPR acknowledges human dignity as a critical aspect in safeguarding personal data. It highlights its role in ensuring transparency, fairness and lawfulness, as well as data accuracy and purpose, data and storage limitations. The EDPS stresses the intrinsic link between privacy and dignity, arguing that protecting human dignity can counterbalance the pervasive surveillance and power asymmetries prevalent in modern digital landscapes.[2268]

In order to clarify whether dignity, as it is conceived in this study, is granted to the migrant data subjects recorded by Eurodac, we must briefly recall what dignity means in this context. The philosophical examination of human dignity and its implications for privacy and data protection reveals a nuanced and multifaceted landscape. The first chapter's exploration of philosophical and judicial traditions, both European and non-European, emphasises the centrality of human dignity in human rights discourse. Philosophers such as Kant, with his focus on autonomy and self-determination, and African concepts like *Ubuntu*, which foregrounds the interconnectedness of persons, highlight the diverse yet convergent views on the inherent worth of individuals. Essentialist views that pit 'Western' and 'non-Western' thought traditions against each other misunderstand that the idea of human dignity has a universal core and is shaped by diverse cultural and political inputs. For instance, indigenous resistance, feminist and

2268 EDPS 'Opinion 4/2015 Towards a New Digital Ethics - Data, Dignity and Technology' (n 85) 12.

LGBTQAI+ movements, as well as judicial contributions from all around the world, have been decisive in shaping and advancing human rights and dignity. While human dignity is understood differently across cultures and legal systems, common elements emerge, such as the recognition that each individual has a right to self-determination, the prohibition of instrumentalising human beings, and the respect for the interconnectedness and the relational aspect of human existence.

In the context of data protection, human dignity emerges as a form of privacy protection conceived as a personal right. Privacy is vital for personal identity and personal data can be understood, in many cases, as parts of one's own body or one's own history rather than possessions. This perspective underscores the ontological impact of privacy breaches, suggesting that dehumanisation occurs when individuals lose control over their data. Protecting privacy is essential for maintaining human dignity and enabling individuals to contribute to their narratives. The implications of these thoughts for this study are profound. Data are not mere objects or property; they are constitutive of personal dignity. Therefore, the collection and processing of data must always have a justified reason. Individuals must have rights to know and control their data.

The metaphor of people as travelling entities, used by Floridi, can be understood literally in this study: it refers to people on the move, who have embarked on a long and often life-changing journey. Many of these travellers are not met with hospitality in Europe and most of them lose control over their data. To a certain extent, this leads to a visible dehumanisation in the interoperable Eurodac system. Of course, it must be emphasised that granting asylum – and Eurodac also serves this purpose – is an act of humanisation. Still, as this study has demonstrated, Eurodac serves a range of additional purposes, including the compilation of extensive statistics and analyses aimed at controlling migration, as well as facilitating the fight against crime – a function embedded in Eurodac in a manner that presupposes that migration as such, and migrants in particular, pose a threat to Europe's public security. With respect to data processing for statistical purposes, data subjects have virtually no means by which to ensure that the principle of proportionality is respected. Likewise, only limited instruments provide adequate safeguards against access to their by law enforcement authorities.

Within the interoperable Eurodac system, it can only to a limited extent be assumed that data subjects contribute to their own narratives, that is, that they are treated as "authors" of their lives. The rights examined in

this study are precisely those intended to enable data subjects to control, understand, and intervene in the construction of such narratives. Yet, as this study has demonstrated, these rights are designed and embedded within the information system(s) in such a way that they cannot be fully realised or effectively exercised. Moreover, it cannot be assumed that data subjects will gain a meaningful overview or understanding of what happens to their data before – or even after – they provide them to European authorities. They possess no genuine control over their data – data which, moreover, are not merely peripheral but include highly sensitive information such as biometric identifiers, as well as intimate personal details relating to origin, family, and aspects of their journey.

Thinking carefully about what human dignity means in the context of data collection and processing is an important step that is often neglected in the development of new information systems. Recognising the dignity of the data subjects who are subject to the interoperable Eurodac system is therefore a first step towards guaranteeing their rights. A second step is to understand that not all of the challenges and restrictions to the rights examined in this study are irreversibly anchored in the Eurodac and Interoperability Regulations. Certain obstacles to the fulfilment of these rights could be overcome in the implementation process. Some technical adjustments would also help facilitate the enforcement of rights and thus facilitate access to justice. The following section outlines what could and should be taken into account in the coming months and years in order to guarantee that the rights of data subjects who enter the Schengen Area as irregular migrants and asylum seekers are safeguarded as far as possible.

## 3. Opportunities in the Implementation Process

Looking ahead, the implementation of interoperability and the expanded Eurodac system presents an opportunity to clarify legal ambiguities and strengthen protections under EU data law. It is imperative that developments in the realm of information systems prioritise the legal rights of data subjects, ensuring their protection remains commensurate with that of EU citizens.

To address the challenges and obstacles highlighted in the previous chapters, several measures can be taken during the implementation process of the Eurodac and Interoperability Regulations to guarantee that the rights to information, access to and rectification and erasure of data, and an effective remedy can be exercised more effectively.

The Commission may issue guidelines, communications, and interpretative notes to clarify as well as facilitate the application of EU regulations.[2269] Various specialised EU agencies along with committees can provide guidance and technical advice on the interpretation of certain regulations. In addition, practical and technical measures may be adopted, including the training of personnel and the enhancement of specific tools analysed in this study, such as the web portal. Finally, a clarification and extension of rights can be achieved through case law. Some of these measures already exist. For example, the EDPB has issued guidelines on the right to access data as quoted in this study.[2270] The following section does not deal with individual existing instruments and cases but provides an overview of the options that exist to safeguard rights discussed in this study.

### a) *Implementing the Right to Information*

As mentioned in the chapter on the right to information, the Eurodac Regulation lacks some clarity in what specific information has to be provided regarding the purposes of data use, security flags, recipients, and data transfers to third countries. The Interoperability Regulations further complicate this landscape, introducing new systems and automated processes that require detailed and comprehensible communication to data subjects. However, the main problem with the right to information is its implementation. Studies have shown that a significant number of data subjects are either unaware of, or misinformed about, the reasons for which they are required to provide biometric data. The new purposes for which Eurodac data will be used and the introduction of interoperability will exacerbate this problem. The expansion of so-called 'border procedures' is likely to further undermine the right to information, as these procedures are considerably shorter than ordinary asylum processes. Moreover, the accelerated handling of asylum procedures generally restricts the effective exercise of information rights.[2271]

During the implementation of the EU Asylum Pact, particular attention should be given to ensuring the effective realisation of the right to information. This entails the development and provision of clear and encompassing

2269 cf European Union, 'Communication from the Commission – EU Law: Better Results through Better Application' (2017) OJ C 18/10.
2270 EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (n 553).
2271 cf Asylum Procedure Regulation, Art 43ff.

information materials for data subjects. The material should be available in multiple languages and not merely distributed in written form, but also communicated directly and in a culturally sensitive manner, so as to take into account the diverse backgrounds of data subjects. Also, Member States should, besides providing information on government websites and leaflets, utilise social media to support access to truthful information.

Border officials, police officers, and migration and asylum authorities should be trained to ensure that the right to information is fully respected. They must be trained in what the digitalisation of the European migration and asylum framework entails, in order to be able to convey what is at stake. Authorities must furthermore be aware that information needs to be provided to data subjects before biometric data are collected.

It is to be hoped that civil society will increasingly bring cases before the courts to clarify the scope of the information to which data subjects are entitled. Such litigation could foster a broad interpretation of information rights, including the requirement that data subjects be informed of sharing of their data with third countries and access by law enforcement authorities, thereby enhancing the justiciability of the right to information.

### b) *Making the Right to Access Data and Information Robust*

To enhance access to justice and practical efficiency of the right to access data and information in the Eurodac and Interoperability Regulations, several measures can be considered. Communications and interpretative notes could be issued, suggesting a broad interpretation of the right of access to data, ensuring data subjects have comprehensive access to information about how their data are used, by whom, and for what purposes.
On a national level, Member States ought to, as much as possible, simplify the process for submitting and processing access requests, providing model requests, reducing procedural complexities and ensuring timely responses. The latter can also be claimed by legal action, demanding that the interpretation of Art. 43 Eurodac Regulation must always take place in light of Art. 12 GDPR and therefore, e.g., the time limits for a response to a request must be applied.

Another measure that would require some new technical advancement is the development of a unified, user-friendly web portal for submitting access requests. This web portal should provide a single point of access for data subjects, streamlining the process and reducing the complexity associated

with multiple authorities and systems. The web portal should be designed to ensure accessibility for all users, including persons with disabilities and children. It should include assistance services for individuals who may encounter difficulties in its use. Such measures could also help address the particular challenges faced by persons outside the Schengen Area, who face additional complexities related to providing biometric identification and a legal address.

### c) *Facilitating the Right to Rectification and Erasure*

Similar to the right to access data, the right to rectify and erase data could be clarified and potentially broadened with guidelines, communications and interpretative notes. On the national level, it will be crucial to establish clear, efficient procedures for data rectification and erasure requests, ensuring that data subjects can easily request rectification and erasure of inaccurate or outdated data. Member States should develop standardised forms and guidelines to support data subjects in submitting rectification or erasure requests, thereby reducing the burden of providing extensive claims and evidence. Moreover, national courts must ensure that the principle of mutual trust does not impede the safeguarding of data accuracy.

Measures to ensure data accuracy – such as regular audits, verification processes, and monitoring for inaccuracies – must not exclude data subjects. They must always retain the opportunity to review and control their own data and their processing. The law establishes data security and monitoring mechanisms, which must remain verifiable by data subjects. As currently framed, the Eurodac Regulation provides sufficient flexibility to enable data subjects to exercise greater control over, and gain a clearer understanding of, the accuracy of their personal data.

### d) *Ensuring an Effective Remedy*

Finally, enhancing the provision of the right to an effective remedy within the implementation process of the Eurodac and Interoperability Regulations depends significantly on how national legal systems design remedies for requests for access, rectification, or erasure of Eurodac data or information. For example, the stage at which judicial review is possible may partially determine the duration of proceedings – an important factor in

ensuring accessibility. To ensure accessibility, data subjects should not be required to initiate multiple parallel procedures to obtain access to their data across different information systems.

Furthermore, it is essential to adopt a critical approach to the use of biometric data and data-processing operations, and to engage seriously with the legal issues that arise in connection with them. Advancing the right to a fair hearing and ensuring thorough and effective review mechanisms are central to this endeavour. Strengthening the training of civil servants – particularly those in asylum and migration authorities who work with EU information systems – as well as enhancing the training of courts and law enforcement authorities, would make a significant contribution. The recruitment of data and data-protection experts within these bodies would likewise assist in managing new technologies responsibly and competently. Taken together, such measures could reduce the risk that mutual trust degenerates into blind trust. In individual cases, courts should also consider granting suspensive effect to appeals, thereby ensuring that data subjects have sufficient time to seek redress and that their rights remain protected throughout the appellate process.

In the future, both national and EU courts can be expected to issue an increasing body of case law, particularly in the field of data protection. This development will also encompass specific issues arising from the digitalisation of administrative processes, including evidentiary standards for certain types or uses of biometric data and for legal decisions supported by automated systems. Such case law may help to clarify some of the questions raised in this study and, ideally, to safeguard the rights of data subjects. The challenge, however, will be to ensure that these protections are applied equally to third-country nationals. As this study has shown, data protection for non-EU citizens is already limited, a situation that must be addressed to prevent the further consolidation of a two-tier system in data protection law.

One essential dimension of ensuring access to the right to an effective remedy, not addressed in this study, concerns the availability and accessibility of legal support. Providing accessible legal support services for data subjects, particularly vulnerable individuals who may face challenges navigating the legal system, strengthens this right. This includes offering free or low-cost legal assistance and/or representation and promoting awareness of available legal remedies and support services through information that is accessible to data subjects.

By implementing these measures, the EU can enhance the protection of data subjects' rights under the Eurodac and Interoperability Regulations, ensuring individuals are informed, empowered, and able to exercise their rights effectively. A commitment to transparency, accuracy, and accessibility will be crucial in overcoming identified obstacles and fostering a fairer and more just data protection framework across Europe.

## 4. Looking Ahead: Rethinking Migrants' Data in Europe

As was discussed in the chapter on Balkandac, in examining the implementation of the Eurodac and Interoperability Regulations, along with the challenges that may hinder the realisation of data subjects' rights, it is crucial to recognise that these systems will further develop. Legislative developments are paralleled by ongoing technical enhancements that will continue in the coming years. Understanding the broader security and migration context, particularly the expansion of Eurodac and interoperability beyond the EU and Schengen Area, is essential for assessing the significance of human dignity within this security, surveillance and administrative framework. The urgent need for transparency and the realisation of the rights examined in this study, regarding data sharing and processing, cannot be overstated.

The most prominent example of this expansion is the development of the Balkandac system and related initiatives, highlighting the future trajectory of interoperable information systems. The Western Balkan states, key transit countries along the Balkan route, have seen increased EU engagement, including the deployment of EBCG Agency staff and financial resources to manage movement and fortify borders. This has led to the development of biometric data collection systems modelled on Eurodac, ensuring future interoperability. These countries have been equipped to enhance data collection and sharing, aimed at avoiding multiple asylum applications and facilitating the deportation of irregular migrants.

Expansion efforts are not exclusive to the Balkan region. In an IOM data briefing in 2018, the organisation suggested that UNHCR should be included as one of the entities able to access the data collected in Eurodac.[2272] The briefing further states that "[t]his recommendation would

2272 International Organisation for Migrants (IOM) and UK Aid, 'Registration and Identity Management of Irregular Migrants in the EU' (Global Migration Data Analysis Centre 2018) ISSN 2415-1563.

also be justified if the recent proposals declared in the meeting between European Union and African leaders[2273]– held in Paris on 28 August 2017 to establish decentralised transit centres in Niger and Chad, where the identification and registration of asylum seekers would be carried out under the supervision of UNHCR – come to fruition".[2274] These specific proposals have not yet materialised. Still, the EU makes high monetary investments in programmes that shall improve data registration of asylum seekers in Africa.

In November 2015, the EU Emergency Trust Fund for Africa (EUTF for Africa) was launched by European and African partners at the Valletta Summit on Migration.[2275] In 2017, Oxfam looked at the specific programmes financed by the EUTF for migration management. The organisation found that of the 400 million euros allocated, most projects were designed to restrict and discourage irregular migration through migration containment and control (55% of the budget allocated to migration management); raising awareness about the dangers of irregular migration (4%) and implementing policy reforms for returns (25%); improving the identification of countries' nationals (13%).[2276] Data collection was part of many of these programmes.[2277] Countries have been equipped, e.g., with technology and technical support as well as specialised training for border surveillance.[2278] According to a European Commission paper, the EU's Sub-Saharan Africa Regional Migration Support Programme (RMSP) "will facilitate a balanced, coherent, coordinated and comprehensive approach to support

2273 'Déclaration Conjointe - Relever Le Défi de La Migration et de l'Asile' (*Élysée*, 28 August 2017) <https://www.elysee.fr/emmanuel-macron/2017/08/28/declaration-conjointe-relever-le-defi-de-la-migration-et-de-l-asile>.

2274 IOM and UK Aid, 'Registration and Identity Management of Irregular Migrants in the EU' (n 2273) 5ff.

2275 'Emergency Trust Fund for Africa' (*European Union* 10 April 2024) < https://trust-fund-for-africa.europa.eu/our-mission/objective-and-governance_en>.

2276 Elise Kervyn and Raphael Shilhav, 'An Emergency for Whom? The EU Emergency Trust Fund for Africa – Migratory Routes and Development Aid in Africa' (Oxfam 2017) 4.

2277 ibid.

2278 E.g., Border Management Programme for the Maghreb region (BMP-Maghreb) in Morocco and Tunisia, 6 Jul 2018 - 17 Aug 2024, with 65 million Eurodac from the EU, via the ETFA at: 'Border Management Programme for the Maghreb Region (BMP-Maghreb)' (*EU - Emergency Trust Fund for Africa*) <https://trust-fund-for-africa.europa.eu/our-programmes/border-management-programme-maghreb-region-bmp-maghreb_en>.

the implementation of the political objectives of the Union."[2279] One of these objectives is "strengthening migration governance and management, fostering cooperation on return and readmission" and seeking "synergies […] with actions linked to the external dimension of relevant Commission funding instruments for migration and of EU agencies, such as [the EBCG Agency] and Europol."[2280] The RMSP foresees "digital support to migration management in relevant countries, such as readmission case management systems, their interoperability with biometrics databases and strengthened administrative capacity building".[2281] The EU also provides concrete and far-reaching support in connection with data collection about migration to various North African countries.[2282] Matching EU and Western African databases will allow the EU to find out about people's journeys before they enter Europe and facilitate their deportation.[2283]

These efforts to collect more data on migrants and migration movements in Africa are not yet as concrete as in the Balkans,[2284] but the goals are the same. Like in the Balkans, the EU exports its policy goals, involving its agencies such as the EBCG Agency and Europol, and supports the digitalisation and interoperabilisation of data collection in order to manage migration flows and facilitate returns. It can be expected that these efforts grow during the next years.

What is more, some EU Member States are trying to outsource asylum procedures by means of bilateral agreements.[2285] Although the biometric

2279 European Commission, 'Sub-Saharan Africa: Multi-Annual Indicative Programme 2021-2027' 43.

2280 ibid 44.

2281 ibid 46.

2282 E.g., Paula García Andrade, Eleonora Frasca, 'The Memorandum of Understanding between the EU and Tunisia: Issues of Procedure and Substance on the Informalisation of Migration Cooperation' (*European Law Blog*, 26 January 2024) at <https://eumigrationlawblog.eu/the-memorandum-of-understanding-between-the-eu-and-tunisia-issues-of-procedure-and-substance-on-the-informalisation-of-migration-cooperation/>; European Union, 'EU Migration Support in Morocco' (2023).

2283 See Alizée Dauchy 'Dreaming biometrics in Niger: The security techniques of migration control in West Africa' (2023) 54(3) Security Dialogue 213ff.

2284 See regarding the challenges in Westafrica Philippe M Frowd 'The Promises and Pitfalls of Biometric Security Practices in Senegal' (2017) 11 International Political Sociology 343ff.

2285 cf Colleen Barry, Llazar Semini, 'The EU is Watching Albania's Deal to Hold Asylum Seekers for Italy. Rights Activists Are Worried' *Associated Press News* (Milan, 22 February 2024); Thorsten Frei, 'Das individuelle Recht auf Asyl muss ersetzt werden' *Frankfurter Allgemeine Zeitung* (18 July 2023).

and biographical recording of asylum seekers would legally remain within the competence of these countries, the process would be facilitated in another country.

Further developments may also be seen in security cooperation. As previously discussed, security-focused initiatives like the expansion of data collection through Europol and the Prüm II framework contribute to the interoperability of migration and security data. Especially the Prüm II framework facilitates cross-border data exchange, enhancing biometric data sharing capabilities among Member States and third countries. Also, Europol's and Interpol's databases, linked to the interoperability system, are integral to EU migration and security operations. With the growing possibilities and efforts to collect and process data, the opportunities for international data exchange in the security realm are increasing and will certainly continue to be utilised in the future.

Against this background, it is important to realise the narrative with which the EU approaches migrants' data. These policies' aim is to collect and process as much data as possible and, if necessary, to exchange them with other countries. The migrants themselves are not taken into consideration. As mentioned above, they are not perceived as subjects, as people who have a right to write their story. The indissoluble migration-security nexus reinforces this view: the notion that anyone other than the state – which requires security-related data to prevent crime – could have a right to access, manage, or rectify such data seems inconceivable. However, Eurodac ultimately manages digital identities that are composed of the most personal data, facial images and fingerprints, along with a range of biographical data. A lot of thought is currently being given in the EU – with EU citizens in mind – to how digital identities can be managed and how people can maintain their autonomy and overview over their data in an increasingly digital world. For example, the EU has launched a proposal for a digital identity wallet. The EU praises the wallet to be "a secure and easy way for European citizens, residents and businesses to prove who they are when accessing digital services."[2286] The wallet app will "enable you to safely obtain, store and share important digital documents about yourself."[2287] The question of whether migrants also have a right to manage their data is rarely raised in connection with the information systems analysed in this study. The data subjects are, to a certain extent, granted access to

2286 European Commission, 'A Digital ID and Personal Digital Wallet for EU Citizens, Residents and Businesses' (n 233).

2287 ibid.

their data. Control over their data lies, however, very clearly with the EU and its Member States. There are some justifiable reasons for this, as the identification of asylum seekers is crucial to the asylum process. Nonetheless, less opaque and intrusive technical solutions do exist and could have been deployed. It would be highly desirable – and indeed necessary from a human rights perspective – for the data-protection standards applied to EU citizens to be extended to migrants. Extending these safeguards is essential not only to close the existing gap in equal treatment but also to ensure full compliance with data-protection principles and to strengthen migrants' access to justice. Only by affording migrants the same level of protection can the EU and associated states uphold the fundamental values that underpin their legal orders.

## 5. Final Thoughts

The issue of an increasingly digitalised asylum and migration system in Europe (and beyond) will remain highly relevant in the future. Neither Eurodac nor interoperability are finalised projects – neither at the technical nor the legal level – and will (have to) continue to engage us. The topic of digitalisation in administration, the use of biometric data and algorithms will continue to raise important legal along with practical questions. This study hopefully serves to highlight some aspects in this area. It should furthermore be understood as an appeal, despite all the technical possibilities, not to forget the human side of "administering", "controlling", and "managing" migration and migrants, people on the move, travellers who are trying to write their story. Technical innovations often compel the legal system to adapt more swiftly than it typically would. Amid these upheavals, it is essential not to overlook the core principles of law that ensure order is just and beneficial for the coexistence of individuals. The individual's dignity must be the foundation for legal innovation. In addition to theoretical insights, this study hopefully provides practical arguments that can be useful in future legal cases to help data subjects assert their rights. The expansion of the EU's information systems has been taken almost to the limits of technical possibilities. Now, it is important to protect people's rights in these systems as far as still possible.