Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement
Working Paper Series

Digitalization in Dutch and EU Migration Law
Individual Rights in the Blind Spot

Bahija Aarrass & Lynn Hillary*

Keywords:

Dutch migration law; EU Migration law; Digitalization

* Dr. B. Aarrass works as an Assistant Professor at the department of Constitutional and Administrative Law at the VU University Amsterdam. Dr. L. Hillary works as an Assistant Professor of the Europeanization of Constitutional and Administrative Law at the University of Amsterdam.

DIGITALIZATION IN DUTCH AND EU MIGRATION LAW
Individual Rights in the Blind Spot

Bahija Aarrass & Lynn Hillary

Dr. B. Aarrass works as an Assistant Professor at the department of Constitutional and Administrative Law at the VU University Amsterdam.

Dr. L. Hillary works as an Assistant Professor of the Europeanization of Constitutional and Administrative Law at the University of Amsterdam.

Keywords:

Dutch migration law; EU Migration law; Digitalization

I Introduction

Digitalization is becoming increasingly important in migration law, both on the EU and on the national level. Many national migration systems are heavily automated and as such they are a test bed for the digitalization in other fields of national administrative (procedural) law. EU migration law has also employed automated systems for border controls abundantly, and the use of digitalization and AI seems to even be turned up a notch in the EU Pact on Migration and Asylum. We believe that studying these tendencies towards digitalization in national and EU migration law teaches us valuable lessons for other areas of public law in light of the implications of digitalization trends on human rights and access to justice.

This article employs a broad notion of digitalization, based on an understanding of digitalization by the Dutch Council of State: '[Digitalization] refers to a large number of technologies, such as algorithms, big data, digital platforms, artificial intelligence, robotics, biometrics, persuasive technologies, augmented reality and virtual reality. Digitalization concerns […] not only collecting and exchanging data […]. Much broader, it concerns the replacement of existing instruments, methods and organizational forms by new digital modes of operation with often-drastic consequences'.[1]

In our article, we will map several digitalization developments in national and EU migration law. As to the former, we will discuss the Dutch example of appeal proceedings in asylum cases, which is part of the national project to digitalize the administrative judicial process. As to the second part of the paper, we will display the information systems currently used in the EU system of controlling the external borders. Additionally, we will discuss several new proposals on the EU level that would facilitate the use of cross-border information exchange between the national decision-making authorities in the field of migration law. When discussing these topics of digitalization in national and EU migration law, we will identify several problems that such digitalization may entail and its implications for individual rights protection and access to justice. Doing so will lead us to a bottleneck analysis that serves as lessons for the digitalization in other areas of public law.

II Migration law as a testing ground for digitalization in Dutch public law

2.1 Introduction

Digitalization has been used in different areas of law, but in the Netherlands the legal field that has known a long history of digitalization is national migration law. For example, in asylum and migration detention cases, there is an obligation to litigate digitally. But digitalization has also made its appearance in other sub-areas of migration law. For example, since March 1st 2021, the possibility to litigate digitally on a voluntary basis exists in other subareas of immigration law as well, such as in family reunification cases. Digital or automated systems have also been integrated into the decision-making process in migration law for some time now. For example, the integration exam, which is a prerequisite for family members to attain a residence permits taken on a computer, even if an integration exam has to be taken abroad.[2] In the context of labor migration, employers who wish to attract an employee from abroad are subject to an online procedure to be designated as a recognized sponsor by the Immigration and Naturalization Service (hereinafter: INS).[3] Finally, in the so-called immigration chain, automation and exchange of data have been taking place on a large scale for a long time.[4] Within that a specific program was introduced, the Chain Computerization Program, which focused on optimizing the information flows within the entire immigration chain, including the INS, the Return and Departure

[1] *Parliamentary Papers II* 2017/18, 26643, 557, at 3-4, also available at www.raadvanstate.nl/@112661/w04-18-0230/

[2] Press release 1 March 2021, 'Lawyers can voluntarily litigate digitally in regular immigration cases', www.rechtspraak.nl; Central government, 'Complication in implementation of new integration law', 27 January 2022, consulted via www.rijksoverheid.nl/actueel/nieuws/2022/01/26/complicatie-in-uitvoering-nieuwe-inburgeringswet.

[3] In the context of a procedure to obtain a temporary residence permit (MVV), an obligation that applies in most proceedings in regular immigration law, subject to exceptions, see art. 16 paragraph 1 under a, jo 2p Dutch Immigration Act.

[4] IND.nl/portaal Business.

Service (DT&V) and the organization responsible for reception, the Central Reception of Asylum Seekers (COA). [5] Lastly, the recent online and other forms of remote hearing in judicial asylum cases may be added to these developments.

This part of the contribution only discusses digitalization in the judicial procedure (and not the primary decision-making process). In particular, two current issues are discussed: the digitalization of the appeal procedure in asylum and detention cases and remote hearing in judicial cases. To this end, we first briefly describe the procedure, because it appears that the intertwinement of procedural rules and automated processing contributes greatly to turning a blind eye on individual rights to access to justice and transparent and fair procedures.

2.2 The Dutch asylum and migration detention procedure: *lex specialis and lex generalis*

Immigration law is a sub area of Dutch administrative law. This means that general administrative norms such as the General Administrative Law Act and other administrative material and procedural standards apply to decisions on migration issues. This also means that, in principle, the administrative courts have jurisdiction to review these decisions. An immigration law procedure can relate to different phases in the procedure: the admission and expulsion of the alien, as well as to the deprivation of liberty (migrant detention) . The main rules of national immigration law are laid down in the Aliens Act 2000 (AA), the Aliens Decree 2000, and the Aliens Regulation 2000. At the same time, Dutch immigration law is strongly governed by rules of the international and European legal order.

The conditions for an asylum status are set out in article 29 Aliens Act. A rejection of an asylum application means that the asylum seeker must leave the Netherlands immediately. The asylum seeker may appeal against the rejection of an asylum application. In contrast to the ordinary administrative procedure, there is no possibility of official objection to the decision authorities, but merelya pronouncement procedure exists, in which the asylum seeker is given the opportunity to submit an opinion against the intention to reject or grant the application. After such a decision, the asylum seeker may then lodge a direct appeal with the administrative court. In comparison to the general administrative procedure, shorter time limits apply for lodging an appeal in the asylum procedure: one week (General Asylum Procedure) and four weeks (Extended Asylum Procedure) respectively, as opposed to six weeks in the general administrative procedure.[6]

If a rejection of an asylum application becomes irrevocable in court, a departure obligation immediately applies. In addition, if it is otherwise established (outside the asylum procedure) that an alien is not lawfully staying in the Netherlands, is refused entry to the Netherlands or (forcibly) has to leave, there is illegal residence, and an obligation to leave the Netherlands applies as well. Immigration detention is the most infringing measure to effectuate departure. Detention is only justified for the purpose of preparing the return or carrying out the removal and if less coercive means would not be sufficient. Article 6(1) of the AA provides a general basis for immigration detention in the border procedure. The conditions under which migrant detention is possible if someone is already in the country are set out in Articles 59 to 60 AA. Migrant detention is permitted as long as there is a prospect of expulsion and the other conditions are met, as codified in Article 5 European Convention on Human Rights and Article 47 EU Charter of Fundamental Rights. [7] The retention period is at maximum six months. A possibility to appeal against the detention (i.e. the return decision) is limited to twenty-eight days.

Because of the infringing character of this instrument on the habeas corpus principle, specific legal terms apply in the case of detention of foreign nationals. This is why specific guarantees are in order such as the right to (be able to) subject such deprivation of liberty to prompt judicial review. This means that a hearing should take place no later than fourteen days after the lodging of an appeal or the

[5] *Parliamentary Papers II* 2013/14, 19637, no. 1822.
[6] Article 42 and 69 Vw AA. See 3.113 and further Aliens Decree.
[7] Article 51 paragraph 2 and 3 AA. Article 62(1) of the AA applies to this period of 28 days.

sending of a notification. The court normally calls on the alien to appear in person for a judicial review, as this is one of the rights that is inherent in the habeas corpus principle.[8]

2.3 Digitalization of the appeals procedure in asylum and migrant detention cases

Since June 12, 2017, asylum and detention cases have been subject to the obligation to litigate digitally. In the meantime, this has led to experiences of the various actors (lawyers, INS and judiciary) which resulted in several rulings on this issue. Before discussing the status quo of the digitalization and grassroots experiences, we first touch upon the origins and content of the digitization project that made this possible, called the Quality and Innovation Program (hereafter: QIP).[9] The experiences gained with this are then discussed, and finally we discuss the new plan for digitalization, the ambition of which is to increase the scope of this plan to Dutch general administrative law.

2.3.1 The digital litigation project

The obligation to litigate digitally in asylum and detention cases was part of the broader program, QIP. The aim was to digitize the judiciary in the Netherlands and thus improve the judicial process. In 2017, section 8.1.6a of the GALA (Traffic by electronic means within administrative law) was established. This created a general possibility for actors in administrative law to litigate digitally, but for asylum and detention cases this was from then on not just an option anymore. In this field actors were obliged to digitally conduct an appeal procedure before the administrative court.[10] The choice for this jurisdiction is largely due to the automated exchange of data of the various actors in the immigration chain. In the Dolmatov case, it became painfully clear how inadequate (automated) data exchange could lead to far-reaching consequences for the individual.[11] Dolmatov was a Russian national who requested asylum in the Netherlands, which was refused. He stayed in Detention Center Rotterdam with the aim of deportation to Russia. After Dolmatov's asylum application was rejected, his lawyer appealed on the last day of the deadline. In accordance with Article 82 AA, the appeal had suspensive effect and Dolmatov was allowed to await the hearing of the appeal in the Netherlands. However, two days later, an automatic change took place in INDiGO – the information system used by the INS – as a result of which the system indicated that Dolmatov did not reside lawfully in the Netherlands and was therefore to be expelled. This was because the INS had failed to put a check mark in the system that the appeal had suspensive effect. This information was accessible to various chain partners. In the meantime, he was placed in detention in Rotterdam where he made several suicidal attempts. The appeal lodged by his lawyer was communicated by the court to the INS, but because there was no link in the system between the registration and the status of the foreign national, Dolmatov remained wrongly registered as 'not lawfully resident in the Netherlands'. He committed suicide on January 17th, 2013.

These events illustrate the consequences of the exchange of information between crucial actors in a chain not (or incorrectly) being processed.. An Inspection Report following the Dolmatov case also showed that it had been known for some time that the different automated systems did not connect with each other or contained outdated information due to a delay in processing time. Therefore, the Dolmatov case was a reason for the Dutch judiciary to start mandatory digital litigation in asylum and detention cases, thereby referring to the need to repair this problem. An additional reason for opting for these cases was that litigants in such cases are usually assisted by a lawyer. A number of practical reasons were also mentioned: the relatively short procedure terms, the fact that no court fee is levied and that there is only one governemental representative authority in this area(the INS). were These were the main reasons to select migration law as a test bed for digital litigation.[12]The rules in the new section in

[8] Article 94 AA, paragraph 4.
[9] *State Official Journal (herafter: Stb)* 2016*,* 174 (as amended by decree of 31 May 2017 (*Stb.* 2017, 230).
[10] This obligation also applied in certain civil cases from 1 September 2017. In the second phase, the proposal enters into force for claims in the canton sector and for decisions to which Chapter 7, section 3 or section 7 of the Aliens Act 2000 apply, *Parliamentary Papers II* 2014/15, 34059, no. *3.*
[11] Report of the Inspection Security and Justice (a brach of the Ministry of Justice), 'De dood van Dolmatov' (trans: The death of Dolmatov), annex to *Parliamentary Papers II 2*012/13, 19637, no. 1648.
[12]L. Hesselink, 'Experiences with digital litigation on asylum and detention' (trans.), *A&MR* 2016, nr. 2, at 74-76.

the GALA relate to how the digital traffic with the administrative court should take place.[13] It provides that the lodging of an appeal by electronic means is mandatory.[14], The term 'electronic means' refers only to the digital data processing system of the administrative court concerned. The administrative court has the power to determine that documents do not have to be submitted electronically or that a party may continue to litigate non-digitally (paragraphs 2 and 6).[15] For deadlines and other issues, the usual general administrative procedural rules apply, in addition to the fact that the time of receipt and transmission of messages in the digital system is further specified in Article 8:36c. A message is qualified as received, once it has reached the administrative court's digital data processing system.Under paragraph 3, other parties receive a notification from the administrative court outside the digital system (notification message) showing that a new message has become accessible in their case. In order to be able to take note of the content, the digital system must be consulted. Finally, the aforementioned court decision may lay down further rules, such as the requirements to be met by the digital system for data processing of the courts. This should ensure that it is possible to identify who is using the system, that documents are only accessible to authorized persons, when messages have been received or sent out and to ensure that system malfunctions are tracked.

Theobligation to digitally litigate in asylum and detention cases would soon apply to the entire administrative law. However, it has not yet come to that while it is constantly being pushed forward (see below).[16] In other administrative cases before Dutch courts, however, a digital path can be chosen voluntarily. For these reasons, the experience gained in asylum and detention cases is of great importance nonetheless.

2.3.2 Experiences with digital litigation in migration cases

The ambitious digitalization project in the Dutch judicial system has had major financial and organizational consequences. This is in stark contrast to the expectation in the first phase of this project that the required changes to administrative procedural law (in contrast to civil law) would be less extensive and would relate in particular to an extension of digital communication between the litigant and the court. However, the Council of State had already been critical of the project's aim to link both digitization and uniformity (of the processes) and to take it as a starting point for the process.[17] Moreover, the Council of State also questioned the feasibility of this endeavor, given the dependence on automation, the success of which was not certain. These reservations were confirmed, because due to these problems, the digitalization project has been stopped within administrative law and in other areas of law.[18] In this context, an evaluation committee has determined that the digitalization of the judiciary is a large organizational and ICT program, which is of extraordinary complexity within an extraordinarily complex environment. However, the Council was satisfied with the results in asylum and detention cases.[19]

---

[13] Prior to the entry into force of this section, art. 8:40a GALA as a legal basis for digital litigation before the administrative court, which declared the provisions 2:13-2:17 GALA (traffic between citizen and administrative body) to apply mutatis mutandis.
[14] Art. 8:36a paragraph 1 GALA.
[15] *Stb.* 2020, 410. Until 31 December 2020, this followed from the Decree on digitalisation of civil procedural law and administrative procedural law (*Stb.* 2016, 292).
[16] *Parliamentary Papers* II 2012/13, 29279, no. 490. As of 15 April 2020, the obligation also applies in administrative cassation proceedings of which the Tax Chamber of the Supreme Court takes cognizance (*Stb.* 2020, 99).
[17] *Parliamentary Papers II* 2012/13, 29279, no. 164, p. 4.
[18] *Parliamentary Papers II 2014/15, 34059, nr. 3, MvT.*
[19] Note 'Lawyers can voluntarily litigate digitally in regular immigration cases', https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Advocaten-kunnen-vrijwillig-digitaal-procederen-in-reguliere-vreemdelingenzaken.aspx#:~:text=Advocaten%20kunnen%20vrijwillig%20digitaal%20procederen%20in%20reguliere%20vreemdelingenzaken,-Utrecht%2C%2015%20februari&text=Vanaf%201%20maart%202021%20kunnen,gedaan%20in%20th%20existing%20systems.

That being noted, the case law in asylum and detention cases shows that problems regularly arise with digital litigation in these cases, with the consequence of inadmissibility before the administrative court. The vast majority of judicial rulings on digital matters relate to inadmissibility issues due to not filing an appeal in due time. This is not surprising given the (sometimes very) short appeal periods in asylum and detention cases, as discussed above and given the system malfunctions. Dutch case law therefore shows a certain judicial flexibility in admissibility matters if evidence problems arise with regard to (for example) the timely digital submission of procedural documents.

A subject that regularly occurs in case law of the highest Dutch administrative court is the (timely) submission of documents by litigants. In several rulings, this court seems to give delegates the benefit of the doubt in the event of evidentiary problems because the reliability and unambiguity of the operation of the systems was insufficient. For example, in one case, an alien's appeal was dismissed as inadmissible because the grounds of the appeal had been filed too late. The Council of State ruled that the lower court should not have ignored the fact that the digital system did not send acknowledgements of receipt at the time the grounds were filed. As a result, the alien could not prove that he had submitted the grounds on time. The appeal had therefore been wrongly dismissed as inadmissible.[20] Other judgments in which similar technical problems or ambiguities occurred also assumed an excusable delay. [21]

It is also striking that in this context, the Council of State regularly uses ICT experts to explain the operation of the systems at the hearing. However, this does not mean that the judiciary is flexible in all cases.22For example, the Highest administrative court applied a strict approach with the legal representative who did not act expeditiously after an ICT problem. And also in a case in which the attorney claimed not to have received a notification of the placement of the judgment in the digital system (and therefore appealed too late), this court relied on the investigation submitted (regarding log messages) by the lower court and declared this appeal unfounded.[23] In the meantime, a period has passed in more recent cases in which various actors have been given the opportunity to remove the initial problems from the systems. This also has consequences for the flexibility that the administrative judge exercises in this regard. Several statements about the requirement of signing statements illustrate this. In a ruling in 2019, the Council of State considered that the method used by the court of The Hague when digitally signing judgments did not meet the legal requirements in some cases. As a result of this ruling, the court has adjusted its working method. In the beginning, judgments were signed with real-time 'wet' signatures again, but since the end of September 2019, the courts have signed rulings digitally again. In some detention cases, the Council of State subsequently ruled that the new method of digital signing — two factor authentication in which statements can be validated by contacting the registry to request a certified copy of the ruling — met the legal requirements. The first obstacles to user-friendliness experienced by lawyers in particular also seem to have been resolved afterwards.[24]

However, this does not mean that digital litigation is now running smoothly, on the contrary: now that a new plan has been launched for administrative law, the impact of such shortcomings on the right of access to justice must be explicitly taken into account.

2.3.3 Basic plan for digitalization

After it became clear that the QIP program would not be continued, a basic digitalization plan was launched. With the basic plan, the judiciary is now digitizing in small steps and has one main goal: digital accessibility for litigants and professionals. This should not only lead to better digital access to

[20]Administrative Court (Council of State) 31 March 2017, ECLI:NL:RVS: 2017:888, *AB* 2017/191.
[21] See Administrative Court (Council of State) 6 August 2018, ECLI:NL:RVS:2018:2614; Administrative Court (Council of State) 27 February 2019, nr. 201803139/1; Administrative Court (Council of State) 19 February 2019, 201806508/1/V3, ECLI:NL:RVS:2019:554. See also Albers 2002, at 6-7.
[22] Administrative Court (Council of State) 30 April 2019, 201804030/ 1/V3.
[23] Administrative Court (Council of State) 30 April 2021, ECLI:NL:RVS:2021:942, *JV* 2021/123.
[24] Administrative Court (Council of State) 30 april 2019, ECLI:NL:RVS:2019:1400. Administrative Court (Council of State) 20 december 2019, ECLI:NL:RVS:2019:4375; Administrative Court (Council of State) 2019, E CLI:NL:RVS:2019:4375.

justice, but also contribute to timeliness and predictability of justice and support cooperation in the chains and networks. Part of this is the Digital Access project. Digital Access consists of a digital mailbox for litigants, a digital mailroom for the registries and a digital file accessible to the participants in the proceedings. External parties gain access by logging in with, for example, a lawyer's card.[25]

It is clear that digitalization within the judiciary is inevitable in view of the digitalization of society. Other countries also use digital systems in appeals in asylum cases, either via a portal or via e-mail systems.[26] But it seems that the ambitious plans to introduce digitalization everywhere still pose a risk. In addition, for asylum and detention cases, the current systems has to comply with much more guarantees, both technical and legal before it can be qualified as a sufficiently accessible and fair procedure..

2.4 'Digital' Hearing facilities

In legal proceedings, the hearing of parties is an important element that should guarantee the right to a fair hearing. Due to the Covid-19 measures, video and audio connections have been used in asylum hearings and court cases from April 2020 to allow asylum seekers, INS staff, interpreters, agents and judges to communicate with each other. This is also called tele-hearing. With this way of working, an (asylum) hearing could still take place remotely at the INS and court cases didn't have to be postponed. This is an example of 'digitization' in which the exercise of a right or depends greatly on digital systems, such as (internet) connection, secure audio and video systems and other software.

The need to use 'telehoren'/online hearing arose due to the Covid 19 measures. Until then, in particular in detention cases, it seemed inconceivable that a person in immigration detention would not be heard promptly in legal proceedings. The use of videoconferencing or teleconferencing was considered as a solution because it made the process less location-based and to some extent more flexible. But it soon became clear that these methods could not always offer a solution. In a ruling by the Dutch Council of State, it expressed practical objections to making a hearing possible during the Covid pandemic. In a number of cases, attempts had been made to work with videoconferencing. However, the Division did not consider it justified to continue with this. The rooms at detention centers that had been set up for this purpose were very small. As a result, it was impossible for strangers, interpreters, supervisors and regular agents to keep a distance of one and a half meters from each other. In addition, detention centers in principle no longer allowed interpreters and authorized representatives within the buildings. The other option, namely bringing the foreigner to court, meant that many people still had to come to court (parties, interpreters, judges, clerks, security guards, cleaners, etc.). At that time, when everyone was advised to stay at home as much as possible, this was out of the question. The Division ruled that temporary waiving of hearings of foreign nationals in detention cases is permitted, but that it should not be on an automatic basis. It is justified only when a clear individual consideration of all the interests involved can be found in the judgment.

In addition to the practical objections to 'telehearing' mentioned, there are also more fundamental disadvantages. For example, the literature has mentioned that it is associated with less human interaction that can be crucial for a complete picture as regards the fact finding. This might beespecially of importance when it comes to hearings in asylum or humanitarian procedures, where intimate and traumatic events are often discussed. In addition, it is questionable whether tele-hearing or the waiver of hearing is compatible with the right to a fair trial. It follows from settled case-law of the ECtHR that Article 6 ECHR, including the right to be heard, may be restricted if those restrictions are (1) foreseeable, (2) meet the public interest objectives pursued by the measure, and (3) are proportionate and do not affect the core of the fundamental right. Whether there is a violation of the alien's rights is assessed on the basis of the specific circumstances of the case. When assessing the admissibilit' of a

[25]Basic plan 2018 (available on rechtspraak.nl), p. 31; 'Digital access to civil law and administrative law is taking shape', 3 February 2021, which can be consulted via www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Digitale-toegang-civiel-recht-en-bestuursrecht-krijgt-vorm.aspx.

[26] Amongst others: Finland, Germany, Sweden, Hungary, France and Switzerland. See European Council of Refugees and Exiles, *Digitalisation of asylum procedures: risks and benefits* 2022.

restriction, consideration is given to whether compensatory measures have been taken to mitigate the adverse effects of not hearing as much as possible.[27]

In a case against the Netherlands, in which an asylum seeker had lodged an appeal against a decision to detain foreigners, the ECtHR ruled on this. The administrative judge's hearing in this case was supposed to take place on March 19, but on March 17, the courts closed their doors due to the first Covid 19 lockdown. Attempts to hear the asylum seeker via tele/video conference failed due to the covid measures in the detention centers. However, his lawyer was heard by telephone. The ECtHR considers it justifiable that the complainant was not heard in person, partly because of the unexpected lockdown, public health, the limited consequences for the asylum seeker and the fact that it was not a procedure within the meaning of Article 6 ECHR (immigration law procedures do not fall under 'civil rights' nor under 'criminal prosecution' within the meaning of Article 6 (1) ECHR.

2.5 Concluding remarks

Digitalization is already having a major impact on Dutch national migration law. The mandatory digital litigation in some cases is an example of this. Digitalization has accelerated during the Covid pandemic. This brings important advantages in terms of efficiency, as the relevant litigants indicate, such as the timely availability of documents. In the asylum procedure, it proved difficult, but not impossible, to work remotely and thus to comply with an important element of the appeal procedure – hearing. But in our opinion, the experiences in migration law should not lead to a blind focus on the positive experiences of digitalization. Through a flexible approach, the administrative court may have been able to avoid major obstacles caused by the inadequate functioning of digital systems. However, it must be borne in mind that digitalization also entails risks and cannot be seen as a fully-fledged replacement for human interaction, which may be jeopardized in migration cases. Moreover, digital litigation can only remain mandatory if access to justice is guaranteed. After all, accessibility to the judiciary should not be made dependent on the functioning of automatic systems.

III Digitalization in EU Migration Law

3.1 Introduction

In addition to the previously discussed developments on the national Dutch level, this section of our article discusses the EU level. For a while now, and increasingly, EU migration law makes use of digitalization. A recurrent theme of digitalization in EU migration law is the fixation on collecting data of third country nationals and attaching consequences to data hits. Notably, these digitalization tendencies in migration law run parallel to another development in the EU polity. In recent years, there has been an increased awareness and focus on privacy and, generally, the protection of individual rights in the context of digitalization, for example, in the General Data Protection Directive (GDPR)[28] and the proposal for the AI Act.[29] The focus on individual rights in the GDPR and the AI Act stand in stark contrast to the digitalization taking place in EU migration law. As we will discuss, the protection of individual rights remains in a blind spot in the digitalization trend in EU migration law.

Digitalization tendencies can especially be observed at the external borders of Europe,[30] as we will discuss below. In the context of external border control, the question that is sought to be answered is twofold. Firstly, does the person trying to gain access to the territory have access in the form of a residence permit? If so, they will be granted access. In that case, it does not yet matter what the grounds are for that permit, be it their nationality, a short-term visa, long term residency, etc. However, only if the answer to the previous question is negative and the person trying to gain access to the territory does not have a residence permit, the question of international protection comes into play. If they apply for

[27] ECHR Guide on article 6 ECHR, available on: Guide on Article 6 - Right to a fair trial (criminal limb) (coe.int).
[28] Regulation 2016/679.
[29] COM/2021/206 final.
[30] External borders are defined in Art. 1(1)-(2) Regulation 2016/399 (Schengen Borders Code)).

international protection, they will enter the asylum procedure in one of the Member States. If they do not, the third country national will be denied access and returned to their country of origin.

In this article, we do not discuss the substantive requirements for acquiring access to the territory and the related EU legislation.[31] Rather, we focus on the digitalization developments in the context of controlling the external borders. In the remainder of this section, we provide an overview of several EU databases that help us understand digitalization tendencies in EU migration law. These instruments offer this insight because they facilitate the cross-border information exchange between the Member States' decision-making authorities. Firstly, we discuss the Schengen Information System (SIS), the Visa Information System (VIS) and the Eurodac database. Secondly, we look into the Entry and Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). Lastly, we discuss digitalization developments in external border management that are aimed specifically at refugees. For each instrument, we identify its purpose and discuss, wherever applicable, the related national Dutch case law.[32] We conclude this section by exploring if and how digitalization fulfills those purposes effectively while also mapping the potential risks involved in the digitalization of EU migration law.

3.2 SIS, VIS and Eurodac

For a while now, SIS, VIS, and Eurodac have been the centralized information databases in EU migration law. The operational management of all three systems lies with eu-LISA, the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.[33]

3.2.1 SIS

The Schengen Information System came into existence in 1995 as a remedy against the abolition of internal borders by means of the Schengen zone.[34] More specifically, SIS aims to contribute to 'maintaining a high level of security within the area of freedom, security and justice of the Union by supporting operational cooperation between national competent authorities, in particular border guards, the police, customs authorities, immigration authorities, and authorities responsible for the prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties'.[35] Vavoula describes SIS' purpose as 'keeping away the unwanted'.[36] With that goal in mind, SIS facilitates the exchange of information between the Member States by means of 'alerts', which are defined in the SIS Regulation as 'a set of data entered into SIS allowing the competent authorities to identify a person with a view to taking specific action'.[37] Thus, for these alerts, SIS employs digital modes of operation for collecting and exchanging data.

Specifically relevant to our article is the chapter of the SIS Regulation on 'Alerts for Refusal of Entry and Stay on Third-Country Nationals'. Article 20 provides an exhaustive list of data that an alert 'shall' contain – and thus *must* contain, but at the same time is *only allowed* to contain. An alert contains identification details of the person concerned but also their residence status, the reason for the alert, and the action to be taken in case of a 'hit'. A 'hit' is understood as a match between data that were previously issued by a Member State and the newly entered data. In 2018, a functionality was added to

[31] For an example of issues related to the substantive requirements for entering the territory, see District Court The Hague 22 September 2021, ECLI:NL:RBDHA:2021:10283.
[32] Case law review was updated until February 1, 2023.
[33] Art. 1(3) Regulation 2018/1726 (eu-LISA Regulation).
[34] E. Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (diss. Leiden), at 47-57.
[35] Consideration 1 of the Preamble of Regulation 2018/1861 (SIS Regulation).
[36] N. Vavoula, 'The "puzzle" of EU large-scale information systems for third-country nationals: surveillance of movement and its challenges for privacy and personal data protection', *European Law Review* 2020, No. 3, at 351.
[37] Art. 3(1) Regulation 2018/1861 (SIS Regulation).

SIS, enabling authorities to automatically search fingerprints[38] and new functionalities, including the storing and automatic search of palm prints, were added in March 2023.[39]

While the SIS Regulation gives rise to a broad scope in terms of the data to be stored and searched for, this is not unlimited. In Articles 21-26 of the SIS Regulation, the entry of alerts of third country nationals into the Schengen Information System is restricted. One example is the requirement that alerts are to be preceded by 'an individual assessment which includes an assessment of the personal circumstances of the third-country national concerned and the consequences of refusing him or her entry and stay'.[40] Moreover, the principle of proportionality generally limits digitalization in SIS: The Member States are required to 'determine whether the case is adequate, relevant and important enough to warrant an alert in SIS'.[41]

Legal remedies are in theory available based on Article 54 of the SIS Regulation: 'any person may bring an action before any competent authority, including a court, under the law of any Member State to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her'. In practice, however, a SIS alert is not easily challenged. The review of SIS alerts depends largely on an active stance of the national (data protection) authorities or judges of the Member States. Brouwer argued that this may be problematic in case of alerts that are challenged in another Member State than the issuing Member State.[42] Moreover, the person concerned may not be aware of the alert because individuals do not have access to SIS. This means that one may only find out that a SIS alert exists by the time there is already a hit. By then, the original data entry may contain obsolete information that has become difficult to challenge. Karanja even argued that 'once a person is registered in the SIS, it is not easy to exonerate oneself because the safeguards that exist are full of obstacles that make it difficult for the person to exercise the rights accorded'.[43]

Interestingly, no Dutch national migration case law exists to the best of our knowledge in which a third country national successfully relies on the disproportionality of a SIS alert.[44] This could be explained by the accuracy of the proportionality check by the issuing Member States, imposing no need to litigate. Alternatively, an explanation could be found in the difficulties of accessing legal remedies, in combination with a very cautious review by the national courts. This has been supported by a 2008 study focused on proportionality in SIS.[45]

Our study of the national case law also confirms the image that, even when an individual does litigate against a SIS alert, courts are rather lenient towards the authorities on their decision to enter information into SIS.[46] For example, in four similar cases at the end of 2022 and beginning of 2023, a third country national who had been declared an undesirable foreign national – leading to a SIS alert – challenged not only the declaration of undesirability but also the proportionality of the corresponding

[38] Automated Fingerprint Identification System (AFIS), see https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/alerts-and-data-sis_en
[39] Art. 37b(5) Regulation 2022/1190 (altering the SIS Regulation); https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en
[40] Art. 24(1)(a) Regulation 2018/1861 (SIS Regulation).
[41] Art. 21(1) Regulation 2018/1861 (SIS Regulation).
[42] Dutch Council of State 25 June 2012, ECLI:NL:RVS:2012:BX0048; E.R. Brouwer, 'Slimme grenzen. Het gebruik van EU-databestanden voor migratiecontrole', *Asiel- en migrantenrecht* 2013, No 9, at 463.
[43] S.K. Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-Operation*, Martinus Nijhoff Publishers (2008), at 393.
[44] National case law inquired upon at www.rechtspraak.nl with keyword 'SIS' in combination with the filter 'migration law'. Further selection was done based on the reliance of individuals on the disproportionality of the decision and whether the litigation was actually targeted at the SIS alert.
[45] S.K. Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-Operation*, Martinus Nijhoff Publishers (2008), at 392-393.
[46] E.g. District Court The Hague, Haarlem (preliminary relief) 19 December 2022, ECLI:NL:RBDHA:2022:13652, par. 6-7; District Court The Hague 19 December 2019, ECLI:NL:RBDHA:2019:14323, par. 6.1-6.2; Dutch Council of State 31 January 2018, ECLI:NL:RVS:2018:347, par. 5.2.

SIS alert. The first instance courts focused solely on the proportionality of the undesirability without considering the proportionality of the SIS alert.[47]

The hurdles in challenging a disproportionate SIS alert in combination with the lack of successful litigation, point to our observation that third country nationals who are the subject of a SIS alert are not necessarily protected in practice by the principle of proportionality. Arguably, it is up to the national courts to ensure effective judicial protection in case an individual does bring forward a proportionality-based claim against a SIS alert. This would require full judicial review. However, since individuals may also have a hard time finding their way to court in the first place, the authorities of the Member States must be wary when entering and extracting data in and from SIS. They must abide by the restrictions in Articles 21-26 of the SIS Regulation, most notably the proportionality requirement.

3.2.2 Eurodac

In 2013, the Eurodac system was introduced in order to store the fingerprints of third country nationals in a centralized database.[48] Originally, Eurodac was aimed solely at supporting the existing Dublin system for determining which Member State is responsible for an application for international protection made in Europe.[49] By taking and registering fingerprints in a database, the Member States can determine whether a third country national has, for example, entered the EU in a certain Member State and that that Member State, based on the Dublin Regulation,[50] should be held responsible for the assessment of the application for international protection of that third country national. Later, the scope of Eurodac was enlarged to include 'purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences'. This entails that police forces and authorities responsible for internal security have access to Eurodac, too.[51]

Based on Article 23 of the Eurodac Regulation, the responsibility for data processing lies with the Member States. This includes *inter alia* the lawfulness of taking the fingerprints and the accuracy of the data. As a result, the correction or erasure of data in Eurodac must also be managed by the Member State that had originally entered the data into the database.[52] Contrary to SIS, individuals must be informed when their data are entered into Eurodac.[53]

With almost 645,000 annual registered sets of fingerprints even in COVID year 2020,[54] it is clear that Eurodac is a considerable database, depending on a vast registration practice. Such practice has, however, not lead to an equally vast successful body of case law. We believe this can be explained by the cross-border, fragmented character of Eurodac and the limited possibilities for challenging the Eurodac registration in and by itself. As argued by Vavoula, these characteristics of Eurodac are intensified by the Dublin system, which is designed for efficiency and less so for effective judicial protection.[55]

3.2.3 VIS

[47] District Court The Hague, Rotterdam 6 January 2023, ECLI:NL:RBDHA:2023:105, par. 7-7.2; District Court The Hague, Rotterdam 23 December 2022, ECLI:NL:RBDHA:2022:14655, par. 6-6.2; District Court The Hague, Rotterdam 22 December 2022, ECLI:NL:RBDHA:2022:14204, par. 6-6.2; District Court The Hague, Rotterdam 12 December 2022, ECLI:NL:RBDHA:2022:14655, par. 8-8.2.
[48] Regulation 603/2013 (Eurodac Regulation).
[49] Art. 1 Regulation 603/2013 (Eurodac Regulation).
[50] Art. 13 Regulation 604/2013 (Dublin Regulation).
[51] Consideration 10-14 of the Preamble of Regulation 603/2013 (Eurodac Regulation); N. Vavoula, 'The "puzzle" of EU large-scale information systems for third-country nationals: surveillance of movement and its challenges for privacy and personal data protection', *European Law Review* 2020, No 3, at 355.
[52] Art. 27 Regulation 603/2013 (Eurodac Regulation).
[53] Art. 29 Regulation 603/2013 (Eurodac Regulation).
[54] eu-LISA (March 2021), *Eurodac – 2021 statistics*, at 5. No data on 2021 and 2022 were available at the time of writing.
[55] N. Vavoula, 'Information sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust', *German Law Journal* 2021, at 414.

In addition to SIS supporting the Schengen system and Eurodac supporting the Dublin system, VIS supports the European visa policy. In that sense, VIS is targeted purely toward migration management. It does so more than SIS and Eurodac. As opposed to VIS, SIS and Eurodac also facilitate information exchange on criminal offences, not just information exchange in *migration* law.

VIS supports the European visa policy by facilitating the exchange of data on visa applications and decisions but also by combatting 'visa shopping' and fraud. Additionally, VIS aims to identify third country nationals who do not fulfill the substantive residence requirements.[56] To achieve this goal, Member States have to register various data when a visa application is filed but also when they issue, refuse, annul, or extend a visa.[57] To that end, Article 5 of the VIS Regulation exhaustively lists the categories of data to be registered in VIS, including photographs and fingerprints of the applicant and information on the issued/refused/annulled/revoked/extended visa. All visa applications that are filed by one person are linked to one another, regardless of the Member State they filed the application with.[58]

The responsibility for the proper use of VIS is laid down with the Member States. Based on Article 7 of the VIS Regulation, the national authorities are required to ensure that they use VIS in a way that is non-discriminatory and 'necessary, appropriate and proportionate to the performance of the tasks of the competent authorities'. We have found no national migration case law on these limitations on VIS registration.[59] On the contrary, we submit that the CJEU considers VIS as best practice. We deduct this from a case concerning Turkish workers who had to have a facial recording and their fingerprints taken in order to work in the EU. The CJEU did not find this disproportionate, partly because of the similar practice of data storing in VIS.[60] As a result, we believe that the CJEU also views the amount of data stored in VIS as proportionate.

3.2.4 In Sum

SIS, VIS and Eurodac are the current central databases that facilitate interstate information exchange in EU migration law. We have observed that, while information exchange may lead to efficiency on migration management and border control, the individual rights of third country nationals remain in a blind spot. While legal remedies, for example, are available in theory, in practice their effectiveness could be challenged. Lastly, proportionality assessments of the processing of the data are required. However, it remains unclear to what extent national authorities and judges actually take this into account.

3.3 EET and ETIAS

The discussed Schengen Information System, Eurodac database, and Visa Information System are tailored for the exchange of information on third country nationals. However, the Commission has acknowledged the flaws in the EU's architecture of data management and that gaps would need to be addressed to register data on visa-exempt third country nationals. In 2016, the Commission therefore proposed additional instruments: the Entry-Exit System and the European Travel Information and Authorisation System.[61] Generally speaking, the initiative focused on the interplay of migration management, on the one hand, and the combat against terrorism and organized crime, on the other

[56] Consideration 5 of the Preamble of Regulation 767/2008 (VIS Regulation).
[57] Art. 8-15 Regulation 767/2008 (VIS Regulation).
[58] Art. 5 Regulation 767/2008 (VIS Regulation).
[59] National case law inquired upon at www.rechtspraak.nl with keyword 'VIS' in combination with the filter 'migration law'. Further selection was done based on the reliance of individuals on the disproportionality of the decision or the discriminatory character of the decision, and whether the litigation was targeted at the registration of data in VIS. For example, see District Court The Hague, Middelburg (preliminary relief) 27 September 2016, ECLI:NL:RBDHA:2016:11574, par. 4-6, in which the accuracy of the data stored in VIS were challenged.
[60] CJEU Case C-70/18 *Staatssecretaris van Justitie en Veiligheid /A, B, P* [2019] par. 59. See also AG Pitruzzella's conclusion to the case, par. 29.
[61] Note that the European Criminal Records Information System (ECRIS-TCN) falls outside of the scope of this article because, while it may be focused on third country nationals, it is not a part of digitalization trends in *migration* law.

hand.[62] EET and ETIAS have not yet entered into force. The date of entry into force has been pushed back a couple of times.[63] At the time of writing, however, EET and ETIAS are expected to be added to the plethora of digitalized EU migration management systems by the end of 2023.[64] Eu-LISA will also be responsible for the operational management of EES and ETIAS, in addition to the management of SIS, VIS and Eurodac.[65]

3.3.1 EES

The idea behind the Entry-Exit System is to remedy the shortcoming that VIS does not register visa-exempt third country nationals. According to the Commission:

> The objectives of the EES are (a) to improve the management of external borders, (b) to reduce irregular migration, by addressing the phenomenon of overstaying and (c) to contribute to the fight against terrorism and serious crime, thereby contributing to ensuring a high level of internal security.[66]

The EES Regulation therefore requires the registration of travel documents, facial images, biometric data, allowing for the calculation of the duration of authorized stay and automatic alerts to the Member States when a third country national has overstayed.[67] Similarly to the information exchange systems that are already in place, the use of EES must be 'necessary, appropriate and proportionate'.[68]

At the time EES will be employed, a communication channel to VIS will be set up: this 'Secure Communication Channel' facilitates that '[t]he retrieval of visa-related data from the VIS, their importation into the EES and the updating of data from the VIS in the EES' will be 'an automated process'.[69] A similar communication channel will be established between EES and ETIAS as soon as they enter into force, as we will discuss under paragraph 3.4.

3.3.2 ETIAS

Parallel to the EES, the European Travel Information and Authorisation System was proposed. ETIAS would require visa-exempt third country nationals to register information about their travels to Europe, like the ESTA system for short-term stays in the US of *inter alia* EU citizens. This would enable the 'consideration [at the external borders] of whether the presence of those third-country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic risk'.[70] More specifically, applicants have to submit various personal data and answer questions on criminal offences, previous travel to war or conflict zones and return decisions that were issued against them.[71] Such data and information, once entered into ETIAS, would automatically be compared to other EU data management systems that are discussed in this article, such as the SIS, EES, VIS, and Eurodac.[72]

3.3.3 In Sum

The entry into force of EET and ETIAS would broaden the scope of data processing *ratione materiae* in the sense that visa-exempt third country nationals would also fall under the digitalization trend in EU

---

[62] COM(2016) 205 final, p. 4-5.
[63] For example, at the time of writing of a previously published book chapter Mid 2022, EES and ETIAS were still expected to enter into force by the end of 2022. See Bahija Aarrass and Lynn Hillary, *Digitalisering in Het Migratierecht. Lessen Voor Het Overige Bestuursrecht*, ed. by Bahija Aarrass, Rolf Ortlep, and Karianne Albers (2022), 220–21.
[64] https://travel-europe.europa.eu/ees/general-information_en for EES and https://travel-europe.europa.eu/etias_en for ETIAS.
[65] Art. 1(4) Regulation 2018/1726 (eu-LISA Regulation).
[66] COM(2016) 205 final, at 12.
[67] Article 1(1) and Article 3(1) Regulation 2017/2226 (EES Regulation).
[68] Article 10 Regulation 2017/2226 (EES Regulation).
[69] Article 8(1) Regulation 2017/2226 (EES Regulation).
[70] Article 1(1) Regulation 2018/1240 (ETIAS Regulation).
[71] Article 17 Regulation 2018/1240 (ETIAS Regulation).
[72] Article 20 Regulation 2018/1240 (ETIAS Regulation).

migration law. As with SIS, VIS, and Eurodac, data processing under EET and ETIAS would require a proportionality test. However, like with SIS, VIS, and Eurodac, we wonder whether this proportionality test would also remain a paper tiger under EET and ETIAS.

3.4 Interoperability between EU Information Systems

As the VIS, SIS, Eurodac, and later also EES and ETIAS, are not an integral, interconnected system, the body of information on (border crossings by) third country nationals – while vast – is still fragmented. Such fragmentation will be remedied by a Regulation establishing a framework for interoperability between EU information systems.[73] According to the Interoperability Regulation, the interoperability between VIS, SIS, Eurodac, EES, and ETIAS would serve the effectiveness and efficiency of external border checks, the combat against illegal immigration, the implementation of the common visa policy and the assistance in the examination of applications for international protection, but also the maintenance of public order in Europe.[74] As with the use and storage of data in the underlying EU information systems it aims to connect, the interoperability itself should be proportional.[75] As we have argued in paragraph 2 on the Dutch procedure in asylum and migrant detention cases following the *Dolmatov* case, the interoperability between information systems might seem beneficial at first glance, but also involves risks that would push the protection of individual rights even further away from the mind's eye.

3.5 New Pact on Migration and Asylum 2020

The previously discussed instruments and EU information systems are all centered on streamlining legal pathways and/or fighting illegal migration. In addition, we discuss developments that are also more focused on identifying applicants for international protection at the external borders. In that area of migration law, a digitalization trend is taking place as well. In recent years, this has been prompted by the 2020 Commission proposals for a New Migration and Asylum Pact.[76] In this section, we focus on the proposal to establish a screening procedure at the external borders.[77]

The aim of the screening procedure is twofold: Firstly, to distill asylum seekers with likely unsuccessful cases, and secondly, to direct third country nationals to the relevant procedures, be it the asylum procedure or the return procedure.[78] The screening procedure would be applicable to third country nationals who have crossed the border in an unauthorized manner, who have applied for international protection at the external borders without fulfilling entry conditions, or who have been disembarked after a search and rescue operation.[79] As noted in the 2020 proposal for the Screening Procedure Regulation, the screening at the external border would consists of:

> '(a) A preliminary health and vulnerability check;
>
> (b) An identity check against information in European databases;
>
> (c) Registration of biometric data (i.e. fingerprint data and facial image data) in the appropriate databases, to the extent it has not occurred yet; and

[73] Regulation 2019/817 (Interoperability Regulation).
[74] Article 2(1) Regulation 2019/817 (Interoperability Regulation).
[75] Consideration 19, 30 and 68 of the Preamble of Regulation 2019/817 (Interoperability Regulation). See also Cristina Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU', Human rights law review, 21, 21/2 (2021), 433–57.
[76] COM(2020)609 final.
[77] COM(2020)612 final.
[78] Joana Abrisketa Uriarte, 'The European Pact on Migration and Asylum: Border Containment and Frontline States', European Journal of Migration and Law, 24, 24/4 (2022), 469.
[79] COM(2020) 612 final, p. 3 and Art. 1 of the proposal.

(d) A security check through a query of relevant national and Union databases, in particular the Schengen Information System (SIS), to verify that the person does not constitute a threat to internal security.'[80]

Such screening at the external border would result in a debriefing form that dictates the further procedure to be followed. Once the screening ends, the third country national is referred to either the return procedure or the asylum procedure, or they receive a refusal of entry.[81] We argue that this debriefing form is an important point to consider both in terms of human involvement and in terms of judicial review options.

As acknowledged in the proposal for the Screening Procedure Regulation, 'the debriefing form filled out by the end of the screening contains information that is necessary to enable the Member States' authorities to refer the persons concerned to the appropriate procedure.'[82] Based on this phrasing, it is not to be excluded that the debriefing either automatically leads to a decision on, for example, the refusal of entry – or else that it would be quite influential with only limited scrutiny by decision-making authorities at the external borders. Based on the wording of the Pact and the proposal for the Screening Procedure Regulation, it remains unclear to what extent there will be human involvement in the decision after debriefing. Because the aforementioned health, identity and security checks during the screening procedure all constitute forms of 'automated processing' in the sense of the Article 22(1) of the GDPR, which requires that a decision should not be based *solely* on automated processing when that decision produces legal effects or similarly significantly affects them.[83] We therefore argue that the decision-making authorities should merely view the debriefing form, i.e. the outcome of the screening procedure, as a starting point and that they should always exercise full scrutiny of the debriefing form with the aim of making the decision on a case-by-case basis.

Moreover, we observe that the proposal for a Screening Procedure Regulation does not consider the screening procedure – and thus the debriefing form it results in – as entailing 'any decision affecting the rights of the person concerned' and therefore 'no judicial review is foreseen regarding the outcome of the screening'. The proposal considers the subsequent judicial review against the decision in the asylum procedure or the return procedure as sufficient.[84] We believe this would only be the case if the judicial review during the asylum or return procedure would indeed include the possibility to challenge the debriefing form, the data registered, and the checks conducted during the screening procedure. It seems to us that the Member States may stumble into the same pitfalls as they initially did with the judicial review of Dublin decisions. Similar to the judicial review of the decision on the Member State responsible for an asylum application made in Europe,[85] we expect the CJEU to also require full judicial review of the outcome of the screening procedure.

Lastly, it must be noted that the Screening Procedure Regulation has generally been criticized because it poses risks to the protection of human rights.[86] Cornelisse and Reneman, for example, draw parallels between the proposed screening procedure at the external borders and the issues that have risen in Moria and other so-called hotspots. They particularly point out the potential violations of the right to liberty.[87] As noted, too, by Brouwer and others, '[u]nfortunately, the proposal does not address the main

[80] COM(2020) 612 final, p. 2.
[81] COM(2020) 612 final, p. 13 and Art. 13 of the proposal.
[82] COM(2020) 612 final, p. 12.
[83] Art. 22(1) Regulation 2016/679: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'
[84] COM(2020) 612 final, p. 12-13.
[85] CJEU Case C-63/15 *Mehrdad Ghezelbash* [2016] para. 61.
[86] Abrisketa Uriarte, 'The European Pact on Migration and Asylum: Border Containment and Frontline States' 468–74.
[87] Galina Cornelisse and Marcelle Reneman, 'Border Procedures in the Commission's New Pact on Migration and Asylum: A Case of Politics Outplaying Rationality?', European law journal: review of European law in context, 26, 26/3–4 (2021), 181–98

bottlenecks of the approach as identified by existing evaluations and scholarly research on its implementation, but rather further reinforces these.'[88] Additionally, the screening procedure would not only constitute a pre-entry procedure, but in effect also a procedure preceding the asylum/return procedure. We signal that this could raise the question of how this integrates with the Dublin procedure, which is also a procedure that precedes the asylum procedure. While the integration with the envisioned relocation mechanism in the new Dublin Regulation is made clear in the proposal for the Screening Procedure Regulation,[89] the consistency of this proposal with the rest of the criteria for responsibility under the Dublin Regulation remains underexplored.

3.6 Concluding remarks

Based on the foregoing, we observe a growing use of digitalization in EU migration law. This trend not only consists of introducing new databases, as has been done over the past decennia, but also of connecting existing databases or even integrating them. Moreover, we observe that Member States are more willing to attach automatic consequences to the gathered information. While this may be beneficial to the efficiency of European migration policies, digitalization may also impose risks on the safeguarding of human rights of mostly third country nationals. Indeed, individual rights protection finds itself in the blind spot of digitalization. This was already the case before the creation of the current databases, which allow for a vast registration practice. Later, these risks were heightened by not only using the registered data for border control and determining which Member State was responsible for which asylum application, but also for investigative purposes. As to the most recent developments, we observe a trend towards an increased scale in the exchange of data and an incline in interconnectedness. Finally, we argue that this trend may also entail an increase in the risks for the access to justice and the proportionality of the storage and automated use of data.

IV Conclusion: Migration Law as a Test Bed for Digitalization and Lessons Learned

Digitalization plays a major role in national and European migration law, and this has been the case for much longer than in other areas of law. In this contribution, we first described the digitalization developments in Dutch national migration law, in particular in the appeal procedure in asylum and detention cases and remote hearing in migration cases. These developments have been accelerated by the covid pandemic. Within European migration law, we described, secondly, the already existing, but also some new proposals for information systems that facilitate the cross-border exchange of information between the authorities of the Member States that take decisions in migration cases. In European migration law, digitalization has existed since the 90s, but the new proposals intensify the use of digital practices. While European law is often invoked for legal protection in national law to challenge the consequences of digitalization, EU law itself offers opportunities to deploy digital systems on a large scale for border control and other purposes.

On the one hand, we recognize that there are certain advantages to digitalization trends in migration law, in particular in terms of effectiveness and efficiency. On the other hand, we believe there are disadvantages to replacing human interaction with digitalization. Consider, for example, the inadequate functioning of national systems for digital litigation in migration cases. Digitalization also poses risks to human rights and legal protection, for example when digitalization hinders access to justice or when digitalization is at odds with the right to privacy.

The migration law systems discussed here are often relatively unknown to general public law lawyers. However, it is not inconceivable that such developments in national and European migration law could be precursors to digitalization trends in other areas of public law. We believe that the findings on these developments should be closely monitored, taking into account, in particular, the impact on the

<https://www.narcis.nl/publication/RecordID/oai:research.vu.nl:publications%2F28d99d47-3fc7-41b8-8bc5-21a1e67a2867>.

[88] Evelien Brouwer and others, 'The European Commission's Legislative Proposals in the New Pact on Migration and Asylum Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE', 53.

[89] COM(2020) 612 final, p. 7 and Art. 14(3) of the proposal.

protection of individual rights, which are in a blind spot in many instances. We therefore argue, firstly, that a thorough consideration at the development, whereby both ICT experts and (practicing) lawyers provide input for the digital systems, is necessary. Secondly, the signaling function of actors in the implementation should not be underestimated. Finally, access to an effective legal remedy against decisions based on digitalization must be ensured.