EJLT European Journal of Law and Technology

Technology-related Risks to the Right to Asylum: Epistemic Vulnerability Production in Automated Credibility Assessment

Frida Alizadeh Westerling*

Abstract

This paper examines the risks that artificial intelligence may incur for the enjoyment of the fundamental right to asylum. It examines at a theoretical level how understandings of digitally acquired data produce vulnerability in the asylum procedure. The EU Commission's draft AI Act has been criticised for having a weak understanding of fundamental rights, although this regulation aims to minimise risks to such rights when AI systems are used. The paper attempts to provide the missing understanding of the negative implications that AI can have for the right to asylum. This analysis is pivotal if we want to implement the safeguards proposed in the AI Act in a meaningful way. The paper argues that the way of giving meaning to digitally acquired data is something of an implicit and collective practice that is characterised by overconfidence in such data. This may in practice lead to a heightened burden of proof on the asylum applicant.

Keywords: asylum procedure, automated decision-making, credibility assessment, vulnerability, AI regulation, oversight

* PhD Researcher in Law, University of Helsinki, Finland. Many thanks to the two anonymous reviewers and my supervisors Riikka Koulu and Kati Nieminen for their constructive advice.

1. Introduction

Assessing evidence is difficult. This is particularly true in the case of the asylum procedure, which is one of the more inherently complex administrative procedures. The task of credibility assessment is an essential part of examining an asylum claim, as there is seldom verifiable evidence to base the decision upon. In practice, the procedure is time-consuming and demanding in terms of human resources. Automating the tasks of the asylum official in the name of efficiency can therefore be a tempting measure to take. Not only can automation make the procedure more efficient, but the use of advanced technology also has the potential to deal with some of the criticism that asylum decisions have received in terms of lacking transparency and argumentation. In order for this to happen, however, responsible digitalisation of the procedure is needed that takes into account the challenges inherent in the procedure.

In spring 2021, the EU Commission released its proposal for the first regulation on the use of artificial intelligence, the AI Act (AIA).[1] As proposed in Article 14(2) of the AIA, the requirement of human oversight is particularly pivotal in minimising risks to protecting fundamental rights in high-risk sectors such as the asylum field.[2] More specifically, it is proposed that AI systems that are intended to 'assist in the examination of asylum applications' are high-risk systems.[3] Examples of high-risk AI systems are those implemented in biometric identification, public authorities' use of tools to detect emotional state, and risk assessments in managing migration.[4]

The AIA has been criticised for not reflecting a basic understanding of what these risks to the enjoyment of fundamental rights entail.[5] As the regulation aims to minimise violations to fundamental rights, it is crucial to understand what these

---

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, *EUR-Lex*, April 21, 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, accessed 19 November 2022. Hereafter referred to as 'the AI Act', 'the AIA' or 'the proposed Regulation'.
[2] Art 14(2) of the AI Act: 'Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.'
[3] Art 7(d), Annex III, the AIA.
[4] Annex III, the AIA.
[5] Smuha, N. et al., 2021. How the EU can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, LEADS Lab, University of Birmingham, pp. 8–9, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991, accessed 19 November 2022.

technology-related risks really are. The use of artificial intelligence in examining asylum cases may impact the enjoyment of different fundamental rights, such as the right to privacy and integrity, the principle of non-discrimination, and the right to life. However, the paper aims to analyse the technological change in the context of the asylum procedure in order to understand the risks that the use of AI may pose specifically to the right to asylum.

This paper takes a socio-legal perspective when answering the research question: What risks does the use of AI pose to the enjoyment of the right to asylum? Using the heuristic tool of epistemic vulnerability production, the paper more specifically asks the question: What impact does AI have on institutional and epistemic vulnerability production in asylum decision-making? In order to develop meaningful safeguards, we ought to make sense of how legal practice is being shaped by new tools for producing and assessing evidence.

This paper looks at the effects of the use of AI in credibility assessments, which are at the core of refugee determination. The study focuses on technology used for assisting the asylum decision-making process. Examples of such technologies are voice biometrics and technologies used for digital forensics. Credibility assessment is broadly understood here as the assessment of the credibility of the asylum claim as a whole, meaning the analysis of the applicant's statements in conjunction with other internal and external evidence, such as digitally acquired data. The paper therefore deals with augmented decision-making, which means a process of decision-making that is in part automated or accompanied by technological recommendations for the human decision-maker.[6]

International human rights law (IHRL) has been recommended by scholars as a useful framework for recognising the risks of AI, including in the field of migration management.[7] The IHRL framework offers substantial and procedural rights to assess the risks against harm, and enables legal obligations (positive and negative), such as oversight mechanisms and a system of redress.[8] The IHRL framework may

---

[6] This broad definition of augmented decision-making covers a variety of different practices of automated decision- making, in which the level of assistance (or augmentation) from the technology differs greatly. Note that the proposed AIA does not differentiate between the levels of augmentation, or rather 'assisting'.

[7] Molnar, P., 2019. Technology at the Margins. *Cambridge International Law Journal* 8(2), 305–330;
McGregor, L., Murray, D., Ng, V. 2019. International Human Rights Law as a Framework for Algorithmic Accountability*, International and Comparative Law Quarterly* 68(2), 309-343;
Beduschi, A., 2020. International Migration Management in the age of artificial intelligence, *Migration Studies* 9(3), 576–596; Rayfuse, R., 2018. Public International Law and the Regulation of Emerging Technologies. In *The Oxford Handbook of Law*, *Regulation and Technology*. R. Brownsword, E. Scotford and K. Yeung (Eds), pp. 500–521. OUP, Oxford, UK.

[8] McGregor et al., 2019 (8).

rule out the use of a certain technology, require modification or additional safeguards, and add responsibility to actors.[9] Nevertheless, there are also limits to this framework, for example when it comes to the status of businesses in human rights law, the particular nature of AI and questions of accountability.[10] Going beyond the debate on IHRL as a framework to assess AI risks, there is a need to concretise a human rights-based approach to manage AI challenges.[11] In addition, more focus on oversight mechanisms is needed.[12]

Following these pleas, this paper seeks to contribute to the development of meaningful oversight mechanisms. At the intersection of technology, human rights and migration, previous research has mainly focused either on the impact of technology on different human rights and/or in particular on issues related to privacy and discrimination.[13] For this reason, the effects of these technologies on data protection and the right to privacy will not be covered in this paper. In contrast, this paper approaches the human rights risks of AI from a wide range of technologies used in a particular legal context – the asylum decision-making procedure. Further, the emphasis is on the socio-technical use of AI rather than on the risks that lie in the technicalities of artificial intelligence. Moreover, the focus of the paper is on European asylum practices.

---

[9] Ibid.

[10] Liu, H., 2018. The Power Structure of Artificial Intelligence. *Law, Innovation and Technology* 10(2), 197–229, pp. 209–210; Liu, H. et al. 2020. Artificial intelligence and the Legal Disruption: a New Model for Analysis. *Law, Innovation and Technology* 12(2) 205–258, p. 215; Smuha, N. A., 2021. Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea. *Philosophy & Technology* 34(1), 91–104.

[11] Smuha (10); Molnar, P., 2021. Robots and refugees: the human rights impacts of artificial intelligence and automated decision-making in migration. In: *Research Handbook on International Migration and Digital Technology*. M. McAuliffe (Ed.), Edward Elgar Publishing, Cheltenham, United Kingdom, p. 139.

[12] McGregor et al. (8) 314; Molnar (7); Molnar (11) 145.

[13] Molnar (7); Molnar, P. and Gill, L., 2018. *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*. U. o. T. Citizen Lab and International Human Rights Program, Faculty of Law; Brouwer, E., 2011. The use of biometrics at the borders: A European policy and law perspective. In: Innovating Government: Normative, Policy and Technological Dimensions of Modern Government. Van der Hof, S. & Groothuis, M. M. (Eds.), T.M.C. Asser Press, The Hague, Netherlands; Vavoula, N., 2021. Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism. *European Journal of Migration and Law 23*(4), pp. 457–484; Jasmontaite-Zaniewicz, L., Zomignani Barboza, J., 2021. Disproportionate Surveillance: Technology-Assisted and Automated Decisions in Asylum Applications in the EU? *International Journal of Refugee Law 33*(1), pp. 89–110; Kinchin, N., 2021. Technology, Displaced? The Risks and Potential of Artificial Intelligence for Fair, Effective, and Efficient Refugee Status Determination. *Law in Context* 37(3).

The asylum procedure has certain characteristics and structures that lead to a power imbalance between the official and the legal subject. Therefore, computational automation and streamlining of the process are challenging and may have dire consequences as people's lives are at stake. This article addresses the technology-related risks by looking at how vulnerability is produced in the procedure in conjunction with the use of new technologies. Even though human vulnerability is a constant that cannot be eradicated,[14] we can reduce certain procedural and institutional 'pain points' that work against the legal subject's enjoyment of rights by looking at how legal practices give rise to vulnerability. The asylum procedure can be described as producing different types of vulnerabilities: linguistic, psychological, and epistemic. This categorisation is based on Määttä et al.'s article 'Linguistic, psychological and epistemic vulnerability in asylum procedures: An interdisciplinary approach'.[15] Here, I will focus on epistemic vulnerabilities, even though all of the categories are linked to each other. I look in particular at how technology plays a role in institutional and epistemic vulnerability production, namely at how social constructions and understandings of digitally acquired data produce vulnerability.

This framework is useful as it helps to provide an understanding of how knowledge has traditionally been produced in the asylum procedure. This, I argue, is pivotal if we want to understand the context in which AI enters the decision-makers' minds. This analysis duly provides a sounding board against which safeguards against fundamental rights violations can be assessed. This socio-legal and contextual analysis of AI risks is essential if we want to understand how to implement and make the requirement of human oversight proposed in the AIA meaningful in practice. Combined with the analysis of vulnerability production, the study makes use of research on automating public administration, and reports on the technology-related risks and rights violations in the asylum procedure to gain a broader understanding of the common characteristics of such risks.

I argue that the risks posed by technology in the procedure are linked to highly contextual understandings of what kind of information is valuable, and hence produced in the refugee status determination (RSD) process. From the perspective of epistemic vulnerability production, the technology-related risks seem to share two overarching characteristics: they stem from collective and implicit knowledge production related to digitally acquired data, which increases the asylum seeker's burden of proof.

---

[14] Fineman, M. A., 2018. Introducing vulnerability. In: *Vulnerability and the legal organization of work*. M. A. Fineman & J. Fineman (Eds.), pp. 1–10. Routledge, Oxon, UK, pp. 4–5, 8.
[15] Määttä, S. M., Puumala, E., Ylikomi, R., 2021. Linguistic, Psychological and Epistemic Vulnerability in Asylum Procedures: An interdisciplinary Approach. *Discourse Studies 23*, 46–66.

The paper starts with a brief overview of the asylum procedure, followed by an explanation of the link between the AI Act and the asylum procedure (Section 2). It then explores how and what kind of epistemic vulnerabilities are produced in the asylum procedure (Section 3). This is followed by an analysis of the risks that the use of technologies incurs for the procedural aspects of the asylum decision-making process (Section 4). The paper then discusses the possible implications that the findings may have for the effective exercise of the right to asylum, and what this means for developing legal safeguards (Section 5).

2. The asylum procedure and the AI Act

The asylum apparatus emanates from the 1951 Refugee Convention and its 1967 Protocol. The definition of a refugee therein sets the foundational goal for the examination of the asylum claim. The right to international protection is stipulated in the EU Statute, and according to Article 18 of the EU Charter of Fundamental Rights, the right to asylum is a fundamental right.[16] In the EU, this fundamental right has been complemented by the larger EU asylum *acquis*, which includes legislation such as the Qualification Directive and the Procedure Directive.[17]

In order to determine whether a person is a refugee or in need of international protection, several elements need to be taken into consideration in their entirety. The initial burden of proof lies with the asylum applicant, who needs to substantiate his/her claim. When this has been complied with, the burden of proof shifts to the state party, who is required, according to the case law of the European Court of Human Rights (hereinafter ECtHR), to 'dispel any doubts' about the person not being in need of protection.[18] National praxis, however, adopts slightly different views on how the burden of proof in asylum cases is distributed.[19] According to the

[16] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
[17] Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (recast) OJ L. 337/9-337/26 (hereinafter 'the Qualification Directive'); Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection.
[18] *Saadi v. Italy* [GC], no. 37201/06, §129, 28 February 2008; *N.A. v. the United Kingdom*, no. 25904/07, §111, 17 July 2008; R.C. v. Sweden, no. 41827/07, § 50, 9 March 2010.
[19] See 'Evidence and credibility assessment in the context of the Common European Asylum System', European Asylum Support Office, Luxembourg: Publications Office of the European Union, 2018, pp. 43–44, available at:

Qualification Directive, it is nevertheless the duty of the Member State, in cooperation with the applicant, to assess the relevant elements that the applicant has presented.[20] The ECtHR has in more recent case law redistributed the burden of proof, and ruled that in reference to the general situation of the country of origin, the burden of proof falls on the state party.[21] It is arguable that the directive and the recent case law of the ECtHR push for a rather low burden of proof on the asylum seeker. The low burden of proof in asylum law compared to criminal law is linked to the fact that the asylum procedure combines elements of both an inquisitorial and an adversarial procedure. In this sense, it can be described as a 'double hybrid'.[22]

Even though digitalisation is nothing new in the asylum procedure, IT systems are becoming more advanced and influential in nature, extending technology as a tool to manage caseloads towards something that helps in gathering information.[23] Behind this technological change are security and efficiency interests spurred by the lack of evidence in the procedure.[24] In short, technology is increasingly being deployed to datafy[25] the asylum seeker for the purposes of augmented decision-

---

https://euaa.europa.eu/sites/default/files/EASO%20Evidence%20and%20Credibility%20Assesment_JA_EN_0.pdf, accessed 19 November 2022.

[20] Art 4(1) The Qualification Directive.

[21] J. K. and others v. Sweden [GC], no. 59166/12, §97-98, 23 August 2016. This is also the case if the state party claims cessation or exclusion of asylum.

[22] Noll, G., Introduction: Re-mapping Evidentiary Assessment in Asylum Procedures. In: Noll, G. (Ed.), Proof, Evidentiary Assessment and Credibility in Asylum Procedures, Leiden, Martinus Nijhoff, 2005, pp. 1–10, p. 3.

[23] See Dijstelbloem, H., 2009. Europe's New Technological Gatekeepers – Debating the Deployment of Technology in Migration Policy. *Amsterdam Law Forum* 1(4), pp. 11–18; and Molnar, P. and Gill, L., 2018. *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*. U. o. T. Citizen Lab and International Human Rights Program, Faculty of Law, p. 14.

[24] See e.g. Sadık, G. & Kaya, C., 2020. The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management. *Uluslararası İlişkiler Dergisi, Special Issue: Revisiting Migration in International Relations* 17(68), pp. 145–160; and Vavoula, N., 2021. Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism. *European Journal of Migration and Law 23*(4), pp. 457–484.

[25] Datafication refers to the collective use of different types of data, which is rooted in the assumption of data being objective and the self-evident link between data and people. See Van Dijck, J., 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12(2), 197–208, p. 199. As Hintz et al. stress, datafication should be understood not only as a technical development, but as a contemporary societal trend, "advanced by the amalgamation of different cultural, political and economic forces that both shift and entrench power relations". The datafication of people, such as migrants, follows the thought that data is able to objectively represent social life. See Hintz, A., Dencik. L., Walh-Jorgensen, K., 2019. Digital Citizenship in a Datafied Society, Polity Press, Cambridge, UK, pp. 45–49.

making.[26] According to the General Data Protection Regulation, asylum decisions may not be completely automated without the explicit consent of the data subject.[27] Nevertheless, automated decision-making systems can either augment or replace parts of the asylum decision-making process, for example with the help of digitally acquired data, including big data analytics.

The legal framework for augmented decision-making in the administrative sector is practically non-existent in the EU at present. However, the AI Act will to some extent clarify the legal playground of AI systems in use. The proposed regulation prohibits certain types of AI systems,[28] and imposes more extensive requirements on AI systems used in high-risk sectors. These requirements are proposed to include conformity assessments and the obligations of human oversight over AI. Human oversight in particular is given a pertinent role in minimising risks to fundamental rights. According to Article 14 of the draft AIA, human oversight should be made possible by having the provider incorporate the measures of oversight into the technology itself, when technically feasible.[29] Alternatively, or additionally, the provider should identify appropriate oversight measures to be implemented by the user to control the AI system.[30] These measures will enable the overseer to take on a diverse set of responsibilities and capabilities, such as understanding, monitoring and addressing the AI system, remaining aware of automation bias, interpreting the system's outcome, disregarding or reversing the AI system, and intervening through a stop button or similar. These measures are comprehensive, requiring a wide range of competence from the user. In the context of the asylum procedure, the user would be the caseworker. Asylum caseworkers are unlikely to have a technical background.

In her policy analysis of the EU's upcoming AI regulation, Koulu analysed the problematisation behind the development of the notion of human oversight. She found that the underlying assumption behind technology problematisation in the EU's policy documents on AI regulation is the idea of human versus technology. This dichotomy functions as a basis for stressing the importance of humans exercising control over technology, wherein the threat is assumed to lie. Koulu's analysis

---

[26] Nielsen, T. R. and Møller, N. H., 2022. Data as a Lens for Understanding what Constitutes Credibility in Asylum Decision-making. *Human-Computer Interaction* 6, pp. 1–20, p. 5.
[27] Art 22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[28] For example, 'real-time' remote biometric identification of natural persons for the purpose of law enforcement (Art 18, the AIA).
[29] 'Provider' means a natural or legal person, public authority or other body that develops AI systems or that plans to place an AI system on the market, whether for payment or free of charge (Art 3, the AIA).
[30] Art 14(3), the AIA.

further reinforces the need to move on from the human versus technology dichotomy towards a more nuanced understanding of human-technology interaction.[31]

It is noticeable that this idea of human versus technology can be observed in the draft Article 14, which seems to be both techno- and user-centric as to the suggested measures. This calls for taking a step back, and asking a more fundamental question: What are the actual risks to be managed in respect of the enjoyment of fundamental rights? In order to minimise violations of fundamental rights, we need to understand what the risks related to the use of technology entail. Before examining this question in the following section, the type of technology that the EU Commission aims to regulate will be addressed.

Simply put, the AIA will regulate the use of AI systems. Defining artificial intelligence is nevertheless a challenging task as technology is constantly developing along with the understanding of what is perceived as 'intelligent'. The proposed regulation defines AI broadly as certain categories of software[32] that can 'generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with'.[33] All software falling under this definition of AI which assists in the examination of asylum applications is categorised as high risk.[34]

Does this mean that all technology used in the asylum procedure would be classified as high risk? This will depend on the degree of integration of technology with the administrative decision-making process. It is not always clear, however, what the technology's degree of integration is. This depends on the role that the technology is assigned by the user (the asylum decision-maker) but also on the broader practices of the organisation in question. Nevertheless, if the tool falls under the scope of the AI definition and in some way assists in the examination of the asylum claim, then the requirements intended to be applied in high-risk sectors should be implemented.

What then are the technologies that are being used in the asylum procedures, particularly for augmenting credibility assessments? In the EU, large-scale IT systems such as Eurodac, the Visa Information System (VIS) and the Schengen Information System (SIS) use fingerprints and faces for identity-verification purposes using so-called 'biometrics' (biometric capture), which refers to the 'automated recognition

---

[31] Koulu, R., 2020a. Human Control over Automation: EU Policy and AI Ethics. *European Journal of Legal Studies* 12(1), pp. 9–46.

[32] Annex 1 of the AIA lists the following categories of software as AI: machine learning approaches, logic- and knowledge-based approaches but also statistical approaches, Bayesian estimation, search and optimization methods.

[33] Art 3(1), the AIA.

[34] Annex III, point 7(d), the AIA.

of individuals based on their physical and/or behavioural characteristics'.[35] In addition, new information systems are under development.[36] As proposed by the EU Commission, the AI Act will not apply to AI systems that are components of these large-scale IT systems in the Area of Freedom, Security and Justice as long as they have been placed on the market or put into service before one year has elapsed from the date of application of the AI Act, with the exception of significant changes taking place in the design or intended purpose of the AI system(s).[37]

The use of biometrics is expanding throughout the asylum procedure, and it is becoming an increasingly important tool in assessing the credibility of the applicant. For example, the Federal Office for Migration and Refugees (BAMF) in Germany uses a type of voice biometrics in the asylum procedure that digitally recognises Arabic dialects and is used to assist officials through recommendations in establishing the identity of the asylum applicant.[38] This system compares the voice of the asylum seeker with other voice recordings of persons from the same area in order to decipher whether the applicant's accent matches that of the reference group.[39]

---

[35] Kloppenburg, S. and van der Ploeg, I., 2020. Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences, *Science as Culture* 29(1), pp. 57–76.

[36] The new Entry-Exit System for Registering Third Country Nationals (EES) and the European Travel Information and Authorization System (ETIAS) as well as the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN) are planned to come into operation in 2023. For an overview of these information systems, see Vavoula, N., 2021. Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism. *European Journal of Migration and Law 23*(4), pp. 457–484.

[37] Explanatory Memorandum of the AI Act, para 1.2.

[38] European Migration Network 2022. The use of digitalisation and artificial intelligence in migration management, The European Commission, 10.2.2022, available at https://emn.ie/publications/the-use-of-digitalisation-and-artificial-intelligence-in-migration-management/, accessed 13 November 2022, pp. 9, 12. Six Member States use AI for the purpose of language identification (Germany, Finland, Hungary, Lithuania, Latvia and the Netherlands), including assessment (Germany and Latvia). Hungary is also planning to use a speech recognition system to establish identity. However, it remains unclear from the EMN's rapport whether these systems are or will be used for the examination of asylum applications. See also Tangermann, J., 2017. *Documenting and establishing identity in the migration process. Challenges and practices in the German context. Focussed Study by the German National Contact Point for the European Migration Network (EMN)*; Working Paper 76 of the Research Centre of the Federal Office for Migration and Refugees, Nuremberg: Federal Office for Migration and Refugees, p. 50, available at: https://ec.europa.eu/home-affairs/system/files/2020-09/11a_germany_identity_study_final_en.pdf, accessed 19 November 2022.

[39] Jasmontaite-Zaniewicz & Zomignani Barboza (n 13) 94.

Additionally, technologies used for automating credibility interviews are coming onto the scene, with more advanced ones asking follow-up questions.[40] The programme developed for BAMF offers information about the asylum seeker's region and country of origin to the interviewer during the interview. This assists in asking targeted questions about the applicant's place of origin in order to establish his/her identity.[41]

Technologies deployed in border procedures are relevant for the assessment of asylum claims. Data that is gathered on a person when entering a country can be used for assessing the overall credibility of his/her asylum claim. Moreover, the core of the asylum claim is often related to the asylum seeker's identity. One automated credibility assessment tool used at the borders of the United States is Automated Virtual Agent Truth Assessment in Real Time (AVATAR). AVATAR uses a virtual agent to automate screening, interviews and credibility assessments by detecting 'potential anomalous behaviour' through analysis of data streams from sensors such as cameras, microphones, and eye-tracking systems.[42] This predictive system has been tested in the EU by Frontex, resulting in a field test at an airport in Bucharest, Romania in 2013.[43] Connected to this project is the EU-financed project known as iBorderCtrl, which was used during 2016–2019 as a pilot for detecting deception at borders in the EU. The project is currently being tested in Greece, Hungary and Latvia. It includes one AI-powered module where an avatar asks passengers a series of filtered questions at the border crossing.[44]

---

[40] Tangermann (n 38) 37. See also Research Innovation Action iBorderCtrl Intelligent Portable Control System, D7.3 Dissemination and communication plan, European Commission, Ref. Ares (2017) 4690395 - 26/09/2017, available at https://netzpolitik.org/wp-upload/2021/04/17_D7_3_Dissemination_and_communication_plan_legible.pdf, accessed 8 November 2022.

[41] Tangermann (n 38) 37.

[42] Nunamaker, J. F., Golob, E., Derrick, D. C., Elkins, A. C., & Twyman, N. W., 2013. *Field tests of an AVATAR interviewing system for trusted traveler applicants*. The University of Arizona, available at: https://eller.arizona.edu/sites/default/files/FieldTestsofanAVATARInterviewingSystemforTrustedTravelerApplicants.pdf, accessed 19 November 2022.

[43] Aaron Elkins, Elyse Golob, Jay Nunamaker, Judee Burgoon, and Douglas Derrick, 2014. *Appraising the AVATAR for Automated Border Control*, BORDERS – University of Arizona, available at: https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/002653/P9_RE(2019)002653(ANN3)_XL.pdf, accessed 19 November 2022.

[44] European Migration Network 2022. The use of digitalisation and artificial intelligence in migration management, The European Commission, 10.2.2022, available at https://emn.ie/publications/the-use-of-digitalisation-and-artificial-intelligence-in-migration-management/, accessed 13 November 2022, p. 10.

Furthermore, asylum seekers' digital data in social media accounts and devices is extensively used as evidence in the asylum procedure. Searching digital personal data has two purposes: to establish the identity of the applicant and to assess the asylum claim further, but also to check whether the asylum seeker is a potential security threat.[45] Intelligent digital forensics analyses the digital data for the purpose of presenting certain information to the caseworker, who then assesses the relevance of the data as evidence and its probative value in the asylum case at hand. It can help increase accuracy and reduce processing times by analysing digital data.[46] For example, countries such as Norway, Denmark and Belgium are practising or seeking to legitimise the practice of searching through asylum seekers' mobile devices and digital accounts.[47] Similarly, the BAMF has been testing different technical methods to analyse data carriers for the purpose of establishing the identity of asylum applicants.[48]

To conclude, the asylum procedure is undergoing rapid change as new tools are being deployed to augment credibility assessments. What these tools have in common is the underlying rationale to establish the real 'truth' about individuals.[49]

3. Datafication and epistemic vulnerability production

Technological tools are added to existing legal practice and are hence an extension and a part of the continuous development of already existing practices.[50] They bring

---

[45] Gabrielsen Jumbert, M., Bellanova, R. and Gellert, R., 2018. Smart Phones for Refugees: Tools for Survival, or Surveillance?, *PRIO Policy Brief*, 4. Oslo: PRIO, available at: https://www.prio.org/Publications/Publication/?x=11022, accessed 19 November 2022.
[46] Kinchin, N. 2021. Technology, Displaced? The Risks and Potential of Artificial Intelligence for Fair, Effective, and Efficient Refugee Status Determination. *Law in Context* 37(3), section 2.4.
[47] Gabrielsen Jumbert et al. (n 45). Comparing the asylum applicant's information with social media and other sources against the information given by the applicant is also the practice in the United States, albeit limited to certain populations of asylum seekers. See Patel, F. et al., 2019. *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security*, Brennan Center for Justice, 22 May 2019, available at: https://www.brennancenter.org/our-work/research-reports/social-media-monitoring, accessed 19 November 2022.
[48] Tangermann (n 38) 35.
[49] Gabrielsen Jumbert et al. (n 45).
[50] Sismondo, S., 2010. *An introduction to science and technology studies*, 2nd ed., Blackwell Publishing Ltd., Malden, USA, pp. 57–71; Boelie E., 2005. Taking the Socio-Technical Seriously: Exploring the Margins for Change in the Traffic and Transport Domain. In: *Inside the Politics of Technology, Agency and Normativity in the Co-Production of Technology and Society*, H. Harbers (Ed.), pp. 171–197, Amsterdam University Press, Amsterdam, the Netherlands; Edwards, P. N.,

data to the attention of the decision-maker, who makes sense of it and determines its value for his/her task. As new technological tools are added to existing practices, the challenges and weaknesses found in those practices play a part in how humans use and understand technology.[51]

The administration of asylum can be considered a knowledge-producing field,[52] which establishes and develops discourses of truth. This is linked to the very nature of the asylum procedure: the impossibility of ever knowing the truth based on verbal accounts and other non-verifiable evidence combined with a future risk assessment.[53] As Poertner puts it, for this reason there is a 'fundamental unknowability' inherent in asylum decision-making.[54]

Refugee status determination (RSD) is based on responses to questions that provide the knowledge needed for handling the casework and assessing evidence.[55] Staffans describes this as a 'debate about the correct way to perceive and de-construct reality'.[56] RSD is a practice of constructing a specific version of reality that is based on cultural norms.[57] To put it differently, the asylum process becomes a performance both for the applicant and the decision-maker.[58] The asylum seeker's performance is assessed and mirrored in an assumed 'real' story, namely the narrative of the so-called 'authentic' refugee who is expected to present a certain level of vulnerability and victimhood.[59] One recognised pattern of assessing the

---

2001. From 'Impact' to Social Process: Computers in Society and Culture. In: *Handbook of Science and Tech Studies*. S. Jasanoff et al. (Eds.) SAGE Publications, Inc., California, USA.

[51] Oster, J., 2021. Code is Code and Law is Law—the Law of Digitalization and the Digitalization of Law. *International Journal of Law and Information Technology* 29(1), pp. 101–117. See pp. 106–107, 115.

[52] Schittenhelm, K. and Schneider, S., 2017. Official Standards and Local Knowledge in Asylum Procedures: Decision-making in Germany's Asylum System. *Journal of Ethics and Migration Studies* 43*(10)*, pp. 1696–1713, p. 1707.

[53] Määttä et al. (n 15) 48, 53.

[54] Pörtner, E., 2021. *Re-Cording Lives Governing Asylum in Switzerland and the Need to Resolve*. transcript Verlag. https://doi.org/https://doi.org/10.14361/9783839453490, accessed 16 May 2022, p. 289.

[55] Schittenhelm and Schneider (n 52) 1707; and Staffans, I., 2012. *Evidence in European Asylum Procedures*. Brill, Leiden, the Netherlands, p. 36.

[56] Staffans, I., 2012. *Evidence in European Asylum Procedures*. Brill, Leiden, the Netherlands, p. 36.

[57] Wikström, H. and Johansson, T., 2013. Credibility Assessments as 'Normative Leakage': Asylum Applications, Gender and Class. *Social Inclusion* 1(2), pp. 92–101, p. 94.

[58] Bodström, E., 2020. Asylum Decisions as Performances: Intertextuality in Internal Credibility Assessment. *International Journal of Refugee Law* 32(4), pp. 623–644, p. 654.

[59] See Schittenhelm and Schneider (n 52) 1702, Bodström (n 58) 654 and McFadyen, G., 2019. Memory, Language and Silence: Barriers to Refuge Within the British Asylum System. *Journal of Immigrant & Refugee studies* 17(2), pp. 168–184, p. 174.

credibility of an asylum applicant is to construct an understanding of what is told and what presumably 'really' happened.[60]

Knowledge represents a view, or a vision, from somewhere, and looking at the epistemics of knowledge acknowledges that our understandings are shaped by our location, situating, and positioning. Haraway calls this *situated knowledges*.[61] Määttä and Ylikomi understand epistemic vulnerability as symbolising an institutional disposition towards knowledge that affects the kind of information that becomes valued as knowledge.[62] I understand this production of epistemic vulnerability as both institutional and collective, that is, vulnerability shaped daily by the organisation and its people producing knowledge. The disposition towards knowledge is understood here as institutional in a broad sense. What is *viewed* as knowledge concerns practices of power. Haraway writes that vision is always a question of the power to see, and perhaps a question of the implicit violence in our visualising practices.[63] Power dictates what can be known, namely what can be viewed as truth. Thus, knowledge supports power in action.[64]

The institutional disposition towards knowledge concerns the question of who the subject of law, the asylum applicant, is in the eyes of the state party. The institutional disposition is characterised by a strong view of knowledge as objective and neutral.[65] This is where vulnerability theory begins its engagement with law, by understanding the 'idealized ordinary', in this case the 'authentic' refugee.[66] Fineman writes that the laws we make will reflect 'the assumed needs, capabilities, and characteristics of that contrived subject and will form the social institutions and relationships that meet those needs'.[67] For the asylum applicant, this means that whether or not they will be considered credible or non-credible depends on how they as a subject are constructed by law and legal practice, namely how 'authentic' they are perceived to be.

In the asylum procedure, knowledge production is constant and entails both authorised and informal knowledge.[68] In fact, explicit and implicit assumptions play an important part in how – and what kind of – knowledge is produced in the RSD

---

[60] Schittenhelm and Schneider (n 52) 1703.
[61] Haraway, D., 1988. Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. *Feminist Studies*, *14*(3), 575–599.
[62] Määttä et al. (n 15) 48.
[63] Haraway (n 61) 585.
[64] Wickham, G., 2013. Foucault and Law. In: *Law and Social Theory*, R. Banakar & M. Travers (Eds.), 2nd ed., pp. 217–232, Hart Publishing, Oxford, United Kingdom, p. 226.
[65] Määttä et al. (n 15) 51–59.
[66] Fineman (n 14) 4.
[67] Ibid.
[68] Schittenhelm and Schneider (n 52) 1702.

process, particularly in the context of credibility assessment.[69] The metaphor 'normative leakage', which Wikström and Johansson use, entails the implicit reasonings about class, religion, culture, gender norms and so on that, in practice, are not only part of, but also play a significant role in the asylum decision-making process.[70] The implicit reasonings which are not acknowledged as such in the procedure constitute the leakage here. The implicitness can be deciphered in the way that decision-makers find it difficult to put the reasonings behind the outcome of an asylum decision into words.[71]

Vulnerability can be found in these practices of knowledge production. Fineman writes that rather than using vulnerability as a comparative concept (someone is more or less vulnerable than someone else), spaces, positions or relationships can be indicators of exposure to or the probability of vulnerability.[72] These spaces can be thought of as sites for the production or reduction of resilience, which is strongly linked to vulnerability in vulnerability theories. According to Fineman, the inequality of resilience is what is often produced within and through social institutions and relationships of privilege defined and reinforced by law.[73] Assessing the different elements of produced vulnerabilities allows us to expose assumptions and biases that are shaping the use of technology in the asylum procedure.[74] If we want to understand what the risks to fundamental rights in this procedure are, contextualised questions of how knowledge is produced, and the vulnerability therein, are highly relevant as they concern how sense is made of digitally acquired data.

Assessing evidence is not a neutral process. Nor is it an individual process. In fact, the practice of knowledge production in the asylum procedure is highly collective, as the working conditions of asylum authorities influence considerably, and politically, how applications are dealt with on a daily basis.[75] This collectiveness stems partly

---

[69] Spijkerboer, T., 2005. Stereotyping and acceleration: Gender, procedural acceleration and marginalised judicial review in the Dutch asylum system. In: G. Noll (Ed.), *Proof, Evidentiary Assessment and Credibility in Asylum Procedures*. Martinus Nijhoff, Leiden, the Netherlands; and Campbell, J. R., 2020. Examining Procedural Unfairness and Credibility Findings in the UK Asylum System. *Refugee Survey Quarterly* 39(1), pp. 56–75, pp. 65–70.

[70] Wikström and Johansson (n 48) 100. See also Johannesson, L., 2012. Performing Credibility: Assessments of Asylum Claims in Swedish Migration Courts, *Nordisk Juridisk Disskrift* 35(3), 69–84.

[71] Liodden, T. M., 2020. Who Is a Refugee? Uncertainty and Discretion in Asylum Decisions. *International Journal of Refugee Law* 32(4), pp. 645–667, p. 656; Jubany, O., 2011. Constructing Truths in a Culture of Disbelief: Understanding Asylum Screening from Within, *International Sociology* 26(1), pp. 74–94, pp. 86–87.

[72] Fineman (n 14) 8.

[73] Ibid., p. 9.

[74] Ibid., p. 4.

[75] Schittenhelm and Schneider (n 52) 1710.

from the fact that an asylum decision is not made in a vacuum, but reflects a comparison with, or even depends upon, the case set as a whole, both that of the individual asylum official and that of the asylum authority. Creating ways to categorise and compare asylum claims is a practice of discretionary power, as it functions as a benchmark for assessing asylum cases.[76] In other words, the methods of collective categorisation may play an important role in how individual cases are examined and assessed.

In the context of the asylum procedure, the discourse of knowledge becomes visible in the ways that questions are posed and evidence is framed and evaluated.[77] As such, technological tools used for credibility assessment are a part of the production of knowledge. The existing practice of knowledge production affects the value and meaning that are attached to digitally acquired data or automation at large. In other words, questions of epistemic vulnerability remain relevant in the technology-enhanced asylum procedure.

The technological tools used for credibility assessments come with their own affordances and may strengthen and weaken certain aspects of the existing processes of knowledge production. The necessary prerequisites for establishing a standardised process are centralisation as well as standardisation of work practices, which can then be automated.[78] Hence, streamlining or automating the asylum procedure with the help of technology strengthens the perspective, or the 'gaze', of the organisation. Automation results in decision-making being moved upstream, further away from the 'street-level bureaucrats'.[79] As such, automation may be used as a method for categorisation practices that are already in place, but may also increase such practices as new ways to create and mediate categorisations of people become possible.

At the same time, automating decision-making procedures can be a means of limiting the use of discretionary power exercised by the individual official. This may lead to fewer individual assessments and a more collective or organisational discourse on credibility assessment. In the asylum field, this categorisation and standardisation of human behaviour raises particular concerns. Firstly, the legal subjects have very different cultural and societal backgrounds and secondly, the claims for international protection vary to a considerable degree. This becomes

---

[76] Liodden (n 71) 653.
[77] Määttä et al. (n 15) 48.
[78] Koulu, R., 2020b. Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy. *Maastricht Journal of European and Comparative Law*, *27*(6), pp. 720–735, p. 731.
[79] Alkhatib, A. and Bernstein, M., 2019. Street-Level Algorithms: A Theory at the Gaps Between Policy and Decisions, in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, pp. 1–13, Association for Computing Machinery.

problematic, for example, when asylum interviews are augmented. A set of recommended questions (outputs of algorithms) entail reasonings about how and what people are expected to explain when they recall personal events or describe their place of origin, for example. The autobiographical memory, which is activated during asylum interviews, is a social-cultural-cognitive system.[80] There are differences, for example, in terms of the level of detail in how people from interdependent cultures recall and tell personal stories compared with people from independent cultures.[81] This needs to be taken into consideration when assessing credibility in legal settings and when developing technology for its augmentation.

On the other hand, standardised and collective decision-making is nothing new. Manuals and country of origin-specific policies have long been directing and steering asylum officials towards consistent decision-making. Indeed, they play a role in reducing the risks of subjectivity when discretionary power is used. However, discretionary power and practice are essentially both individual and collective.[82] Automation strengthens the collective use of discretion as decision-making processes are standardised, but it also changes the nature of collective discretion. Behind the technological interfaces are systems analysts and software designers creating ways to analyse data (evidence), which in some respects broadens but also anonymises the group(s) of people practising collective discretion. Hence, it transfers and distributes discretion to a larger group of people.[83]

It is important to remember that the underlying interests behind automation play a role in how technology affects knowledge production. Scholars in the field of science and technology studies have long rejected the view of technology as something neutral and 'apolitical', and stress that technologies do not follow predetermined, neutral trajectories.[84] Moreover, scholars of critical data studies problematise the dominant narratives of data as something neutral and objective, and the way in

---

[80] Basu-Zhark, J., 2011, Effects of Collectivistic and Individualistic Cultures on Imagination Inflation in Eastern and Western Cultures, *Inquiries Journal* 3(2).
[81] Jobson, L., 2009, Cultural Differences in Specificity of Autobiographical Memories: Implications for Asylum Decisions, *Psychiatry, Psychology and Law*, 16(3), pp. 453–457, pp 455–456.
[82] Petersen, A., Christensen, L. R. & Hildebrandt, T., 2020. The Role of Discretion in the Age of Automation. *Computer Supported Cooperative Work* 29, pp. 303–333, pp. 304, 327.
[83] See Bovens, M. and Zouridis, S., 2002. From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control. *Public Administration Review* 62(2), pp. 174–184.
[84] Sismondo, S. 2010. An introduction to science and technology studies. 2nd ed, Blackwell Publishing Ltd, West Sussex, UK; Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). 2012. The social construction of technological systems, anniversary edition: New directions in the sociology and history of technology. MIT Press. Cambridge, USA; Feenberg, A., 2002. Transforming technology: a critical theory revisited. Oxford University Press, New York, USA.

which it changes thought and knowledge production.[85] Technological tools are not neutral as such, as they are both impacted by and impact the values and behaviours of their developers, and of those who use the technology. The fact that a technological tool affects its user's behaviour and thought has to be reflected in the way oversight mechanisms are developed.

The tension between the state's interest to grant asylum to refugees and the interest to protect the state from people abusing paths of migration is a constant factor playing a part in how border and migration procedures are managed, and where technology comes into play.[86] In Europe, the different interests involved in the bigger migration management picture are characterised by strong security incentives,[87] which can be noticed in the increasing use of technological tools for gathering data about the physical elements of people on the move, particularly in border procedures.[88]

In addition, the more intelligent the technology is perceived to be, the more the view of technology as something neutral may intensify.[89] For example, surveillance systems follow the premise of producing 'pure information' about the individual and the body through the process of abstracting data and reassembling it.[90] The data about the individual turns into an individual object itself. As Käll puts it, in this construction of data as an individual object, it is dematerialised from the processes that are needed for its production.[91] This can be observed, for example, in the

---

[85] Hintz, A., Dencik, L., and Wahl-Jorgensen, K., 2018. *Digital Citizenship in a Datafied Society*. Polity Press, Cambridge, UK, pp. 6–7; D'Ignazio, C., Klein, L. F., 2020. Data Feminism. The MIT Press, Cambridge, USA.

[86] For example, 'fast track' procedures and quick transnational processing at the border are a means of accelerating case management based on profiling. See e.g. Doornbos's discussion on the impacts of fast tracks on the asylum seeker. Doornbos, N., 2005. Evidentiary Assessment through asylum interviews. In: G. Noll (Ed). Proof, Evidentiary Assessment and Credibility in Asylum Procedures, Martinus Nijhoff Publishers, Leiden, the Netherlands.

[87] Huysmans, J., 2000. The European Union and the Securitization of Migration. *Journal of Common Market Studies*, 38(5), 751–777, Dijstelbloem, H., 2009. Europe's New Technological Gatekeepers Debating the Deployment of Technology in Migration Policy. *Amsterdam Law Forum*, 1(4), 11–18; Farzamfar, M., 2021. The Implications of the Securitisation of Immigration upon the Right to Seek Asylum in the European Union: An Interdisciplinary Legal Analysis. Doctor of Law Thesis, Department of Law, University of Helsinki, Helsinki.

[88] Elrick, L. E., 2021. Finding the Balance between Security and Human Rights in the EU Border Security Ecosystem. *European Journal of Law and Technology* 12(1,) 1–41, p. 11.

[89] Corple, D. J. and Linabary, J. R., 2020. From Data Points to People: Feminist Situated Ethics in Online Big Data Research. *International Journal of Social Research Methodology* 23(2), pp. 155–168, p. 160.

[90] Haggerty, K. D. and Ericson, R.V., 2000. The Surveillant Assemblage. *British Journal of Sociology* 51(4), pp. 605–622, p. 6.

[91] Käll, J., 2020. The Materiality of Data as Property. *Harvard International Law Journal Frontiers* 61, p. 6.

underlying presumption behind digital forensics that data obtained from digital devices or online accounts is highly reliable evidence. Hildebrandt writes that the result of a new form of data-driven agency, which puts emphasis on the data itself, is a collective digital unconsciousness which renders us manipulable.[92]

To conclude, the discourses of credibility produce epistemic vulnerability in the asylum procedure.[93] The assumptions and normative understandings about human behaviour and societies affect how evidence is produced and assessed with the help of technological tools.

Additionally, the datafied asylum processes give rise to a new assumption, or rather strengthen the view of data produced or gathered by the state party as something neutral and objective. This view of technology as neutral, whether it concerns information about bodies, mobile devices, or online content, leads to over-reliance on digitally acquired data. Implicit knowledge production is particularly problematic as the informal production and practice of knowledge remain hidden from the public. The mismatch between the institutional disposition towards knowledge as objective and neutral, and its implicit practices, leads to a situation whereby the asylum seeker cannot understand and question the implicit reasonings and assumptions upon which the interview to a certain degree unfolds, and the decision is finally made. In the asylum procedure, implicit reasonings are particularly problematic since the legal subjects often do not have the language and cultural skills to understand the bureaucracy of the procedure, which affects the resources to appeal against a negative asylum decision. In the next section, I analyse technology-related risks to the right to asylum in the light of datafied practices of knowledge production.

4. Technology-related risks

The centralisation and spread of collective discretion in the asylum procedure is an interesting side of the coin when it comes to new technologies related to identifying age and dialects, for example, as well as truth assessment tools. The assessments are becoming extensively corporal, as micro gestures, pulse, teeth and so forth become a means of measuring the body of the asylum seeker, and of gathering further evidence. Along with automation's centralisation of practice, and creating distance between the decision-maker and the asylum seeker, technology offers a

[92] Hildebrandt, M. 2015. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Edward Elgar Publishing, Cheltenham, UK., pp. 41–46, 56–59, 66–67.
[93] Määttä et al. (15) 59; see also Bodström (n 58) 639, 641.

means to increasingly 'penetrate' and assess the bodies of asylum seekers, both for security reasons and for assessing the overall asylum claims. These technologies create a twofold movement – one that moves away from individualised assessments towards mainstream decision-making, and one that moves into the highly personal sphere, where bodily data from the asylum seeker is gathered. Procedurally, technology decreases individual assessment, but substantively accentuates individuality and distinctiveness through the increased examination of the asylum seeker's body.

As the highly individual and personal corporal measurements are built upon standardisations of human behaviour, they give little room for individual interpretations. The conundrum follows that due to limited possibilities to interpret differences in voice, narrative, personality, culture, and so on, the assessment remains at the standardised level of the organisation, even though detailed individual measurements of bodies are under scrutiny. For example, voice biometrics are based on generalisations of dialects, and their assessment in the asylum procedure is based on the assumption between language and geographical places.

Truth detectors and other credibility assessment tools on the other hand are based on assumptions about human behaviour that are culture-specific as well as situational. Lie detectors cannot differentiate between cultural differences in human behaviours and may easily flag traumatised and nervous people as exhibiting 'abnormal' behaviours. People applying for asylum have often experienced severe trauma before and/or during the journey to the country of asylum, putting them at higher risk of being falsely flagged as a security threat. In the European context, not only the use, but also the initial development and deployment of technology is based on Western-centred individualised assumptions about human behaviour. The collective or standardised practices of giving meaning to corporal data, which are eventually used as material facts in the case at hand, are therefore problematic. The risk here lies in evidence assessments being too standardised, leaving little room for case-by-case assessment.

Moreover, underlying the challenges of the standardised yet personal decision-making systems are more fundamental problems related to epistemological and ontological premises concerning data gathering and the datafied subject. As mentioned earlier, one issue in respect of the use of digitally acquired data as evidence, such as social media data, relates to a general problem of overconfidence in such data. In a procedure characterised by a lack of verifiable information, it is particularly easy from the organisation's point of view to cling to digital or big data

analytics as a way to get closer to the 'truth'.[94] Here, technology can reflect the existing search for denotational accuracy in the RSD, namely the urge to give probative value to data/evidence that is perceived to be easily 'digestible' and regarded as something that can be taken as given.[95] Hence, overconfidence in digitally acquired data constitutes an implicit way to give meaning to data, and can be described as a new form of the already existing normative 'leakages' in the asylum procedure.

This relates to the normative assumption and the narrative about the asylum organisation being objective (see Section 3). It has been observed in a study that asylum claims that are deemed non-credible are due to a perceived divergence across different types of data, such as the applicant's disclosed 'raw' data and the legal authorities' 'clean' data, or the applicant's disclosed data and technology-induced data.[96] It seems that technological tools for credibility assessment strengthen this dichotomy between the state party's 'clean' data and the applicant's 'raw' data. The assessment of data duly takes on the initial position that the raw data is suspicious and needs to be assessed in the light of the clean data. In addition to the problem of overconfidence, the datafication and categorisation of asylum claims seems to be a rather complex practice, meaning that the decision-making and the argumentation behind evidence assessments become blurred.[97]

What kind of effects does overconfidence in digitally acquired data and the complexity of datafication have on the right to asylum? I claim that the implicit epistemics about the 'real refugee' combined with complexity and overconfidence in datafication may potentially have significant effects on the asylum seeker's burden of proof. This is more specifically a consequence of the difficulty in questioning the data, and the asylum seeker's ability to 'overrule' the output of the technology – in other words, to prove that the data is flawed, misleading, low in probative value, or inapplicable to the case at hand. The complexity of datafication is particularly problematic in the asylum context as it puts the asylum seeker in an even more vulnerable situation vis-à-vis the state party. How can an asylum seeker know how much weight an AI system such as voice biometrics has been given as evidence in his/her case? This poses the following problem: how does the asylum seeker know which facts need to be further substantiated?

---

[94] See Kitchin, R., 2014. Big Data, New Epistemologies and Paradigm Shift. *Big Data & Society* 1(1), pp. 1-12; Van Dijck, J., 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2), pp. 197–208.
[95] Jacquemet, M., 2015. Asylum and Superdiversity: The Search for Denotational Accuracy During Asylum Hearings. *Language and Communication* 44, pp. 72–81.
[96] Nielsen and Møller (n 26) 12.
[97] Ibid., p. 20.

Even though digitalised evidence can offer more effortless ways for the asylum seeker to substantiate his/her case, I claim that the effects of datafication of the case assessment are more problematic than opportunistic in terms of the asylum seeker's procedural status. The fact that technologies for credibility assessments are often deployed with security interests in mind leads to a situation whereby the technological change strengthens the view of asylum seekers as threats, and so the task of the asylum seeker to be perceived as a person in need of international protection becomes increasingly challenging. For example, a questionable and misinterpreted social media post might have dire effects on the outcome of the case. Thus, the overconfidence and complexity related to datafication, in combination with the increased acquisitorial nature of RSD due to security interests, challenges the collaborative aspirations of EU asylum law when it comes to the asylum seeker-official collaboration in substantiating and examining the claim, and may severely affect the division of the burden of proof between the state and the asylum applicant. This complexity may in practice lead to situations where the asylum seeker does not have enough information about how to argue his/her case.

The consequence is a heightened burden of proof on the asylum seeker to challenge a decision of non-credibility that is based on or augmented by digitally acquired data. This may constitute a new procedural risk spurred by augmented asylum decision-making systems.

A feature of this risk of a heightened burden of proof is its comprehensiveness. In the light of knowledge production and practices in the asylum procedure, I suggest that the practice of giving meaning to data in the asylum procedure is happening largely at an organisational level rather than at an individual level. By this, I mean that the decisions about which data to gather, and how to gather and assess it, are taken collectively. This should be accounted for when developing oversight mechanisms, namely when deciding who the overseer is. That the practices of giving meaning to digitally acquired data would become highly individualised is questionable, as asylum decision-makers tend to acquire an 'institutional habitus', which is strongly linked to, and dependent on, the collective practices and ideologies of the communities of asylum officials and the organisation.[98] This indicates an important feature of technology-related risks in this context, namely that the implications are collective. As decision-making and knowledge production are automated at an institutional level, this has impacts on the larger group of asylum applicants. This is the case particularly when the risks are inherent in the deployment of the technology itself, and where the mere deployment of the technology for augmenting credibility assessment (and not a technical fault in the

[98] See e.g. Affolter, L. 2021. *Asylum Matters On the Front Line of Administrative Decision-Making*. Palgrave Macmillan (eBook), available at: https://doi.org/10.1007/978-3-030-61512-3, accessed 15.4.2022.

tool) constitutes a risk to the enjoyment of the right to international protection. In relation to personal corporal measurements, the epistemic risks therein are collective rather than individual. In other words, the risks related to giving meaning to data affect the group of applicants collectively, even though the examination of asylum claims is increasingly entering the personal sphere.

In sum, this analysis suggests that the technologies that are used to augment credibility assessments contribute to producing epistemic vulnerability through the way in which they contribute to collective and implicit practices of knowledge production. Even though automation bias and overconfidence in data are general phenomena, they may be particularly problematic in the context of asylum decision-making where epistemic vulnerabilities are highly produced. The risks that technological tools for credibility assessment incur seem to stem from institutional overconfidence in digitally acquired data and the neutrality of the organisation's production and gathering of data. In practice, this leads to the burden of proof falling increasingly upon the asylum applicant in terms of challenging the state party's perception of non-credibility. As the right to asylum is dependent on effective procedural operations being in place, these procedural risks in the RSD process may have significant ramifications for the effective exercise of the right to asylum, and as such also for other fundamental rights such as the right to life, liberty and security.

5. Discussion

As the risks to the right to asylum are analysed in this paper through the practices of epistemic vulnerability production, it means that there are other elements of risk that fall outside the scope of this analysis. Nevertheless, it is useful to understand the context in which technological change is happening, and particularly how meaning is created in the more complex legal decision-making environments. Automation shines a new light on knowledge production; it makes legal reasoning visible to some extent as one can analyse concrete decision-making tools, their underlying rationales and, perhaps most importantly, the way they are understood and implemented. However, the analysis in this paper should not be viewed as comprehensive as I aimed to understand the risks that technology can pose to the right to asylum in view of how the asylum procedure produces knowledge and epistemic vulnerability. Nevertheless, the analysis highlights important implications of automation, and calls for a clear legal framework as well as a larger political debate about the datafication of the asylum procedure.

A key implication of automating the assessment of asylum claims seems to be the heightened burden of proof on the asylum seeker. This is particularly alarming in a legal procedure characterised by power imbalance and doubt vis-à-vis the legal

subject. As explained earlier, the asylum seeker needs to substantiate his/her claim, that is, present evidence to the asylum organisation, and so the initial burden of proof falls on the applicant. After the applicant has substantiated his or her claim, the assessment of the material facts should be conducted as a collaboration between the asylum seeker and the state party according to the Qualification Directive. Since the standard of proof in asylum cases is relatively low,[99] the shift from the asylum applicant's initial burden of proof to a shared burden of proof should take place relatively early on in the procedure.

What the use of technological tools for credibility assessment seems to do is increase the applicant's burden of proof during this stage of exploring and assessing evidence, after the initial burden of proof that rests with the applicant has shifted to a shared burden of proof. In practice, this division and shifting of the burden of proof is often difficult to indicate over time. Nevertheless, the idea that it would be the applicant's task to dispel doubts about digitally acquired data pointing to their non-credibility is at odds with the principle of burden of proof in asylum law.

This procedural risk in the RSD process jeopardises the effective exercise of the right to asylum, as the latter is dependent upon the procedural operations in place.[100] It is noteworthy that the procedural risk of a heightened burden of proof may also have ramifications for the prohibition of discrimination, which is linked to the fundamental right to asylum. Certain groups of people on the move, such as children, disabled people, and elderly people may be particularly affected by the datafied asylum assessments, and so their specific position in the asylum procedure needs to be considered. For example, applying digital forensics to minors requires an understanding of children's use of devices and online behaviour.[101]

---

[99] European Asylum Support Office 2015, *Practical Guide: Evidence Assessment*, available at: https://euaa.europa.eu/sites/default/files/public/EASO-Practical-Guide_-Evidence-Assessment.pdf, accessed 19 November 2022, p. 21; ECtHR 2016, *Article 3 The Court's approach to burden of proof in asylum cases*, Research Division, Council of Europe, available at: https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf, accessed 15 April 2022. For national differences on the burden of proof, see EASO 2018, *Judicial analysis: Evidence and credibility assessment in the context of the Common European Asylum System*, Publications Office of the European Union, Luxembourg, pp. 80–81, available at: https://euaa.europa.eu/sites/default/files/EASO%20Evidence%20and%20Credibility%20Assesment_JA_EN_0.pdf, accessed 15 April 2022.

[100] Some suggest that Article 18 of the European Charter of Fundamental Rights entails the right to have access to effective procedures for assessing asylum claims. See Nicolosi, S. F., 2017. Going Unnoticed? Diagnosing the Right to Asylum in the Charter of Fundamental Rights of the European Union: The Right to Asylum in the EU Charter. *European Law Journal* 23(1–2), pp. 94–117, pp. 116–117.

[101] Joint General Comment No. 4 of the CMW and No. 23 of the CRC in the context of International Migration: States parties' obligations in particular with respect to countries of

What then do these findings about technology-related risks add to the discussions and ongoing regulatory drafting of the EU's AI regulation? When it comes to developing and implementing legal safeguards, an important question arises from this analysis: How are augmented decision-making systems recognised and understood by the organisation and the asylum officials? New technological tools do not change the fundamental nature of evidence assessment in the asylum procedure. Nevertheless, they force decision-makers to constantly reconsider which data can be used as evidence and what kind of probative value the data can bring to the case examination. This is where the epistemic risks to the asylum seeker lie. In order for the AIA to serve its purpose and minimise violations of fundamental rights, its measures need to reflect a realistic understanding of how humans interact with technology and the role that technology is given in the respective contexts.

As mentioned at the beginning of this paper, human oversight deserves particular attention as it is considered to have great significance in minimising fundamental rights violations. The level and content of human oversight remains ambiguous, jeopardising legal certainty as to the responsibilities of the user. The vagueness of terms (such as 'monitoring', 'understanding', 'reversing') is a result of the legislator's decision to make the AI Act a horizontal regulation and to apply the principle of technological neutrality (as opposed to a sectoral and technology-specific regulation).[102] This balance of legal certainty and future-proofing in a legislation is inevitably difficult to set.

Some of the issues emerging from the findings in this paper are particularly problematic in relation to the technocentricity of the requirement of human oversight proposed by the EU Commission. What is noteworthy is that the proposed technocentric and user-centric human oversight mechanism does not correspond to the more complex readings of automated decision-making, and the risks to the enjoyment of fundamental rights that datafication incurs. The current requirement of oversight is built upon the assumption that the risks reside in the technological features, for example when there is a malfunction of some sort. What is overlooked are situations of user-machine interaction where the well-functioning technology itself plays a part in the violation of a right in certain contexts.

Additionally, it is problematic to assign the user, such as the asylum official, the task of overseeing his/her own automation biases and epistemic assumptions about the

---

transit and destination, CMW/C/GC/4-CRC/C/GC/23, 16 November 2017, point 13. See also Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021, points 10, 119–120.

[102] See Koulu, R., Hirvonen H., Sankari S., Heikkinen, T. (forthcoming 2023). Artificial intelligence and the law: Can and should we regulate AI systems? [Manuscript in preparation] In: *Research Handbook on Law and Technology*. Brożek, B., Kanevskaia, O. and Pałka, P. (Eds.), Edward Elgar Publishing Ltd, Cheltenham, UK.

use of the data. Furthermore, assigning the task of overseeing the technology to caseworkers who do not have the professional experience needed for monitoring and understanding the output of the technology at hand is problematic. Giving the task to the user to oversee his/her own use of an AI system as the primary means to protect fundamental rights is also contrary to the principle of impartial and independent oversight in IHRL. Whether this responsibility of oversight would empower the user, or the asylum official, is doubtful. The interplay between an AI system and its user is more nuanced than that.[103] As Bijker puts it, technologies not only assist, but are 'powerful forces acting to reshape human activities and their meanings'.[104]

In short, the problem of human oversight as proposed in the AI Act lies in who the overseer is, but also what and who the target of oversight is. What is needed are safeguards that are not only directed at loss of control due to faults in the technology itself, such as malfunctions, security breaches or faulty programming, if rights violations are to be minimised. This would entail oversight mechanisms proposed in the AIA that further monitor how humans in the procedure understand and work together with the technology in use. Considering my claim that the overconfidence in digitally acquired data in the asylum procedure is a collective practice, an organisational oversight mechanism in the asylum context will hardly serve the purpose of minimising risks to the right to asylum. In other words, viewing the risks of AI also as problems of power is called for when developing oversight mechanisms.[105] One complementary solution to the techno- and user-centric human oversight requirement could be involving external, independent bodies with the authority and resources to oversee ex ante the causes of technology-related collective challenges and risks.[106]

This, I believe, is needed if the EU's goal to protect fundamental rights through the regulation will not remain an unsubstantiated claim of 'human rights washing' in an

---

[103] See e.g. Veale, M., Van Kleek, M. and Binns, R., 2018. Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). New York, Association for Computing Machinery, 1–14, available at: https://doi.org/10.1145/3173574.3174014, accessed 19 November 2022.

[104] Bijker, W. E., 2009, How is technology made? - That is the question. *Cambridge Journal of Economics* 34(1), 63–76, p. 20.

[105] Liu 2018 (n 10).

[106] Ex ante safeguards also proposed by McCarroll, E., 2020. Weapons of Mass Deportation: Big Data and Automated Decision-Making Systems in Immigration Law. *Georgetown Immigration Law Journal* 34(3) pp. 706–731, p. 729; and Smuha et al. (n 5) 56. On collective redress in the form of ex ante protection, see Hakkarainen, J., 2021. Naming Something Collective Does Not Make It So: Algorithmic Discrimination And Access to Justice. *Internet Policy Review* 10(4), pp. 1–24, p. 18.

attempt to protect so-called European values.[107] Hence, legal safeguards in the AIA need to have an impact on the underlying causes of rights violation risks that are rooted in the practices of knowledge production and overconfidence in datafication. In order to minimise the risks to fundamental rights, the oversight mechanisms would need to tackle the collective underlying problems of knowledge production and the epistemics of datafication. Yet this begs the question of whether oversight mechanisms are able to do that.

6. Conclusions

The asylum procedure is a particularly complex administrative procedure. The lack of information and its intercultural nature renders the asylum decision-making process prone to the particular influence of implicit knowledge production and biases. Alongside this, technological change is leading to increased automated credibility assessments. This change is spurred by new ways of gathering and analysing data in an administrative procedure which is in general characterised by lack of evidence. As the use of technologies has an impact, whether direct or indirect, on the examination of facts, it has implications not only for the status and procedural rights of the asylum seeker, but also for the enjoyment of the fundamental right to asylum and international protection, not to mention the right to life.

If fundamental rights safeguards in technology regulation are to be effective, critical analysis of their workings in specific contexts is expressly called for. The main objective of this paper has been to understand the nature of the risks that technology poses to the applicant's right to asylum. I explored how the asylum procedure produces epistemic vulnerability and how technological tools for credibility assessments take part in this context of knowledge production. In doing so, I identified two important elements of technology-related risks. First, the risks stem in particular from the implicit ways of giving meaning to digitally acquired data. Second, the production of knowledge with the help of digitally acquired data is something of a collective practice. This collectiveness is both a source of risk (less individualised assessments), and a feature of risk (implications are collective). I furthermore found that the implicitness and collectiveness of giving meaning to digitally acquired data in the procedure is characterised by overconfidence in such data. This overconfidence in digitally acquired data may lead to a heightened burden of proof on the asylum applicant.

[107] See the Explanatory Memorandum of the AIA.

As the asylum procedure is characterised by a power imbalance and institutional vulnerability, it is important to ensure that the increasing use of technology in this procedure does not further undermine the asylum seeker's procedural agency and rights. One current legislative pursuit to tackle risks related to technology is the EU Commission's proposed regulation on artificial intelligence, the AI Act. The requirement of human oversight is currently given a pertinent role in minimising risks to the enjoyment of fundamental rights. The findings in this paper are nonetheless problematic in relation to the techno- and user-centricity of the proposed requirement of human oversight, as it does not correspond to the more complex readings of automated credibility assessments and the risks to the enjoyment of fundamental rights that datafication poses.

Hence, we need to develop safeguards that can be implemented in a meaningful way. In addition to targeting technocratic risks, safeguards need to respond to the causes of technology-related risks to the enjoyment of rights. That said, the findings in this article may help us to understand how to develop meaningful legal safeguards that actually have a more comprehensive impact on minimising risks to the rights of the asylum seeker. For this to take place, further research that considers how the asylum official envisages and understands automated processes is called for, but also how asylum seekers perceive the use of technologies. Knowing the everyday risks that occur helps create meaningful oversight and control mechanisms over the datafication of the decision-making process. This can help align technology regulation with the nature of asylum decision-making in action, and with the challenges that augmented decision-making systems pose to this administrative procedure.