*German Law Journal* (2024), pp. 1–27
doi:10.1017/glj.2023.112

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

# When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis

Francesca Palmiotto

Hertie School, Centre for Fundamental Rights, Berlin, Germany
Email: f.palmiotto@hertie-school.org

(Received 10 July 2023; accepted 07 November 2023)

**Abstract**

This Article addresses the pressing issues surrounding the use of automated systems in public decision-making, specifically focusing on migration, asylum, and mobility. Drawing on empirical data, this Article examines the potential and limitations of the General Data Protection Regulation and the Artificial Intelligence Act in effectively addressing the challenges posed by automated decision-making (ADM). The Article argues that the current legal definitions and categorizations of ADM fail to capture the complexity and diversity of real-life applications where automated systems assist human decision-makers rather than replace them entirely. To bridge the gap between ADM in law and practice, this Article proposes to move beyond the concept of "automated decisions" and complement the legal protection in the GDPR and AI Act with a taxonomy that can inform a fundamental rights analysis. This taxonomy enhances our understanding of ADM and allows to identify the fundamental rights at stake and the sector-specific legislation applicable to ADM. The Article calls for empirical observations and input from experts in other areas of public law to enrich and refine the proposed taxonomy, thus ensuring clearer conceptual frameworks to safeguard individuals in our increasingly algorithmic society.

**Keywords:** automated decision-making; EU Law; Fundamental Rights; Artificial Intelligence; Migration; Asylum; GDPR; AI Act

## Introduction

Between 2015 and 2020, the UK Home Office deployed an automated system to support visa decision-making. The so-called "visa streaming" tool classified applicants based on three risk levels, considering nationality as a factor. Based on the risk assessment, applicants would be subject to more or less scrutiny by public officers. The practice remained unknown until 2020 when the Joint Council for the Welfare of Immigrants (JCWI) and the law firm "FoxGlove" challenged the use of the tool because of its discriminatory effects and lack of transparency.[1] The two civil society organizations argued that the visa streaming algorithm was discriminatory by design: applicants from nationalities identified as suspect nationalities received a higher risk score and, thereby, a higher level of scrutiny by officers. In their defense, the Home Office claimed that

[1]Jack Maxwell & Joe Tomlinson, *Experiments in Automating Immigration Systems* 51 (2022); Derya Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, 21 (2023), https://hertieschool-f4e6.kxcdn.com/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/automating-immigration-and-asylum_final_afar.pdf (last accessed Feb. 27, 2024).

the tool was "only used to allocate applications, not to decide them" and that it complied with the Equality Act 2010.[2] Before the case could be heard in court, the Home Office pledged a review of the visa streaming tool and the termination of its use in August 2020. Despite no longer being used, the full details of the algorithm remain unknown.[3]

This case shows, in an exemplary manner, three key issues that permeate the use of automated systems in public decision-making. Automated decision-making (ADM) is 1) opaque, 2) complex and diverse, and 3) has the potential to affect fundamental rights.[4] First, notwithstanding the increasing use of ADM by public administrations across Europe, these tools still lack transparency. In most cases, the public becomes aware of automated systems when infringement of fundamental rights occurs and receives attention from the media or thanks to the efforts of civil society organizations. Second, how automated systems are used in practice is often unclear and complex. Rather than making the final decisions autonomously, automated systems assist, inform, and support decision-makers in a wide range of possibilities. When concerns for fundamental rights arise, public administration and governments justify themselves by arguing that the tool does not make the final decision, as in the case of the UK visa algorithm. Yet, automated systems can lead to violations of fundamental rights even if the decision-making process is not fully automated. Consider the Dutch childcare benefit scandal, which led the Dutch Government to resign in 2021 and to publicly declare that their algorithm for allocating childcare benefits was "institutionally racist." Even if the system was not taking the decision, as a result of the racial risk assessment, thousands of families went into debt, ended up in poverty, and more than one thousand children were taken out of their homes and placed in care as a result of the accusations.[5]

ADM is used to identify asylum seekers without valid documents, allocate social benefits, detect tax fraud, and support decision-makers with relevant information. In light of the multitude of uses of ADM in practice, it is important to know when a decision is automated from a legal perspective. Do regulatory definitions of ADM reflect and account for their empirical differences, and what legal protection is afforded to individuals affected by it?

This Article addresses these questions by taking the field of migration, asylum, and mobility as a case study, drawing on the empirical research conducted for the AFAR project by Derya Ozkul. In light of the lack of transparency from public administrations, her research is a unique occasion to analyze an entire sector of public law and investigate how ADM is used in a whole spectrum of activities and processes. This Article aims to contrast how ADM is used on the ground with how it is legally conceptualized under EU law. Sections *I* and *II* closely examine the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) to assess how the law defines and categorizes ADM. It shows how the legal protection for ADM is based on the concept of solely automated in the GDPR and on the definition of "high-risk AI" systems in the AI Act. Following this legal analysis, the Article shows how the

[2]Ozkul, *supra* note 1, at 20.

[3]Id.

[4]*See generally* Council of Europe Committee of Experts on Internet Intermediaries, *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications* (2018), https://rm.coe.int/algorithms-andhuman-rights-en-rev/16807956b5 (last accessed Jan. 22, 2019); Council of Europe Committee of Experts on Internet Intermediaries, *Algorithms and Human Rights*, (2018), https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (last accessed Feb. 27, 2024); AI Now Institute, *Litigating algorithms: Challenging government use of algorithmic decision systems* (2018), https://ainowinstitute.org/litigatingalgorithms.pdf (last accessed Jun. 3, 2019); Fundamental Rights Agency, *#BigData: Discrimination in data-supported decision making* (2018), https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making (last accessed Jun. 3, 2019); Fundamental Rights Agency, *Getting the future right – Artificial intelligence and fundamental rights* (2020), https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights (last accessed Jun. 3, 2019).

[5]European Parliament, The Dutch childcare benefit scandal, institutional racism and algorithms (2022), https://www.europarl.europa.eu/doceo/document/O-9-2022-000028_EN.html (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

legal categories fail to grasp most real-life cases where automated systems segment decision-making but do not replace humans entirely.

Existing legal scholarship has focused on the limited protective function of the GDPR in relation to ADM, contending that Article 22 GDPR is too narrow in scope,[6] needs further authoritative interpretation,[7] does not provide rights and protection,[8] and suffers from significant weaknesses.[9] Drawing on examples from different fields, Veale and Binns show how decision-making based on profiling can challenge the applicability of Article 22 GDPR.[10] Similarly, Hänold argues that "Art. 22 GDPR in reality only achieves a limited protective function"[11] because its scope of application does not cover situations where profiling supports a decision. Finally, legal scholars[12] and civil society organizations[13] have criticized the Commission's proposal for an AI Act for the lack of new rights for individuals harmed by AI systems. This Article takes a step further and contends that legal protection in the automation age requires a fundamental rights approach[14] based on an empirical and legal understanding of how automation segments decision-making.

The Article proposes a taxonomy to understand, explain, and classify automation in decision-making to bridge the gap between ADM in law and practice. This taxonomy allows us to 1) bring theoretical clarity where regulatory categories fail to grasp the reality of ADM, 2) pinpoint what rights are at stake for individuals affected by ADM, and 3) identify the sector-specific laws applicable to ADM systems.[15] As ADM poses issues that transcend data protection (GDPR)[16] and internal market legislation (AI Act), the proposed taxonomy can inform a legal analysis based on fundamental rights and sector-specific legislation to fill the gap in protection. This Article invites experts in other areas of public law to observe ADM and empirically enrich the proposed taxonomy. As public administrations continue to introduce new forms of ADM, it is crucial to have clear conceptual frameworks to safeguard individuals in our increasingly algorithmic society.

[6]Stefanie Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, *in* Robotics, AI and the Future of Law 123–153 (Marcelo Corrales, Mark Fenwick & Nikolaus Forgó ed., 2018).

[7]Frederike Kaltheuner & Elettra Bietti, *Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR*, 2 J. Info. Rights, (2018).

[8]Céline Castets-Renard, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, *in* Constitutional Challenges in the Algorithmic Society 93–110 (Amnon Reichman et al. ed., 2021).

[9]Lee Bygrave, *Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision-Making*, *in* Algorithmic Regulation 248–262 (Karen Yeung & Martin Lodge ed., 2019).

[10]Reuben Binns & Michael Veale, *Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR*, 11 Int'l Data Priv. L. 319–322 (2021).

[11]Hänold, *supra* note 6, at 147.

[12]In this sense see Lilian Edwards, *Regulating AI in Europe: Four Problems and Four Solutions*, Ada Lovelace Institute (2022), https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/ (last accessed Feb. 27, 2024); Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act,* ArXiV (2021), https://osf.io/38p5f; *Cfr.* Vera Lúcia Raposo, *Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence*, 30 Int'l J Law Info Tech 88–109 (2022).

[13]Algorithm Watch and Others, Open letter (2022), https://algorithmwatch.org/en/fundamental-rights-protections-in-the-council-position-on-the-ai-act/ (last accessed Feb. 27, 2024).

[14]*See generally* Malcolm Langford, *Taming the Digital Leviathan: Automated Decision-Making and International Human Rights*, 114 Am. J. Int'l L. 141–146 (2020) in migration management, *see specifically* Petra Molnar, *Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective*, 8 Cambridge Int'l L. J. 305–330 (2019).

[15]*See generally* M. Fink & M. Finck, *Reasoned A(I)Dministration: Explanation Requirements in EU Law and the Automation of Public Administration*, 47 Eur. L. Rev. 376–392 (2022); Jennifer Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, 39 Legal Stud. 636–655 (2019).

[16]Elizabeth M. Renieris, Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse (2023); Alessandro Mantelero, Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI (2022).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

## A. ADM in the GDPR: Solely Automated Decisions

Automated decision-making is not a recent concept in law. In 1995, the Data Protection Directive (DPD)[17] provided individual natural persons with a qualified right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data" (Article 15 DPD).[18] The more recent GDPR[19] is closely based on its predecessor, Article 15 DPD, and enshrines a narrow concept of ADM, considering only decisions without human involvement.[20]

### *I. The Function and Rationale of Article 22 GDPR*

Article 22(1) GDPR generally prohibits solely automated decision-making.[21] The policy underpinning this provision is the fear that fully automated processes can be detrimental to human dignity and lead to an abdication of accountability and responsibility by human decision-makers.[22] Concerns about fully automated decision-making are echoed in Recital 71, which considers risks of inaccurate personal data, security, and discriminatory effects. The rationale of Article 22 GDPR is to provide protection for individuals against the detrimental effects of automated profiling or processing of their agency and participation in decisions affecting them.[23] Nonetheless, the GDPR allows for exceptions to the general prohibition in three limited cases. More specifically, automated decision-making is permissible only if 1) it is strictly necessary for contractual purposes, 2) it is authorized by Union or Member State law, or 3) it is based on the data subject's explicit consent (Article 22(2) GDPR).

When exceptions apply, the GDPR provides for specific safeguards to ensure that data subjects are not at the mercy of opaque ADM without human intervention and have the possibility to exercise their rights. Therefore, the data controller must implement specific safeguards such as the right to obtain human intervention, to express their point of view, and to contest the decision (Art. 22(3) GDPR). Moreover, in order to minimize discriminatory effects on the basis of protected characteristics such as ethnic origin, political opinion, religion, or beliefs, Art. 22(3) GDPR restricts the use of sensitive data in ADM. Data related to protected characteristics (that is, special categories of personal data under Art. 9 GDPR) can be processed, but only if it is based on explicit consent or a substantial public interest is involved.

In addition to affording protection against discriminatory decisions, the GDPR aims to foster transparency and fairness in the decision-making process. Recital 71 of the GDPR states that the data subjects "should have a right to obtain an explanation of the decision reached after such

[17]Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281).

[18]Lee Bygrave, *Article 22 Automated Individual Decision-Making, Including Profiling*, in THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY, 522–542 (Cristopher Kuner et al. ed., 2020).

[19]Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016 O.J. (L 119).

[20]For a comprehensive analysis of Article 22 GDPR see Bygrave, *supra* note 18; Maja Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, 27 INT'L J. L. INFO. TECH. 91–121 (2019); Gianclaudio Malgieri, *Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations*, 35–61 COMPUTER L. SEC. REV. (2019); Isak Mendoza & Lee A. Bygrave, *The Right Not to Be Subject to Automated Decisions Based on Profiling*, *in* EU INTERNET LAW: REGULATION AND ENFORCEMENT 77–98 (Tatiana-Eleni Synodinou et al. ed., 2017).

[21]In an Opinion from 2018, the EDPB took the view that Article 22 provides for a prohibition by endorsing Article 29 WP Guidelines stating that: "The term right in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data".

[22]Bygrave, *supra* note 18, at 526. For an analytical overview of normative concerns see Karen Yeung, '*Why Worry about Decision-Making by Machine?*', ALGORITHMIC REGULATION 21–48 (Karen Yeung & Martin Lodge ed., 2019).

[23]Bygrave, *supra* note 18, at 526.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

assessment," a provision which gave rise to a fervent debate among legal scholars.[24] The possibility of obtaining an explanation for the automated decision must be read in light of the connected transparency rights in Articles 13 and 15 GDPR. These provisions grant the data subject the right to know whether they are subject to ADM and to receive meaningful information about the logic involved and the envisaged consequences before (Art. 13(2)(f) GDPR) and after a decision is reached (Art. 15(1)(h) GDPR). Finally, ADM, which involves systematic and extensive evaluation of data subjects, is explicitly subject to a Data Protection Impact Assessment (DPIA) pursuant to Article 35(3)(a) GDPR.[25]

Similarly, the Law Enforcement Directive (LED) prohibits solely automated decisions in Article 11 LED, albeit with some differences – especially in terms of lower transparency standards and the data subject's rights – compared to the GDPR. While the latter generally applies to ADM in migration and asylum governance, where ADM is used for law enforcement purposes, the LED applies as *lex specialis*. As the empirical cases will show, automation is largely used with the promised benefits of increasing security, preventing threats, and minimizing document fraud. When migrants are perceived as security threats, the line between migration and criminal law blurs,[26] and the use of automated systems has the potential to erase these boundaries even further.[27] Therefore, it is important to be aware of cases where the applicability of the LED can be triggered and the different protection that is afforded to data subjects. In the following analysis, I will generally refer to Article 22 GDPR and call into question Article 11 LED in specific cases where doubts arise.

## II. When is a Decision Solely Automated?

Under the first paragraph of Article 22 GDPR, an automated decision has to be 1) individual with legal or significant effects on the data subject and 2) based solely on automated processing or profiling.

First and foremost, the outcome has to be an individual decision. According to Bygrave, the term "decision" should be broadly interpreted and include a "particular attitude or stance is taken towards a person" with binding effects.[28] National Data Protection Authorities (DPAs) and courts have considered cases where an automated system was used by public administrations[29] or private companies, especially in the gig economy sector.[30] Under Article 22 GDPR, whether the decision-maker is public or private is irrelevant. Instead, what is crucial is whether the decision has legal or similarly significant effects on the individual.

Even if the GDPR does not define "legal effects," the Guidelines on Automated Individual Decision-making and Profiling from WP29 (hereafter, "Guidelines") clarify that the automated decision must affect someone's legal rights, legal status, or their rights under a contract.[31] Some

[24]Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7 In'l Data Priv. L. 243–265 (2017); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 In'l Data Priv. L. 76–99 (2017).

[25]Heleen L. Janssen, *An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making*, 10 In'l Data Priv. L. 76–106 (2020).

[26]Valsamis Mitsilegas, The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law (2015).

[27]*See extensively* Teresa Quintel, Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond (2022).

[28]Bygrave, *supra* note 18, at 532.

[29]Consiglio di Stato [Italian Higher Administrative Court], Case No. 2270/2019, (Apr. 8, 2019), https://www.medialaws.eu/wp-content/uploads/2019/11/Consiglio-di-Stato-sez.-VI-8-aprile-2019-n.-2270.pdf (last accessed Feb. 27, 2024).

[30]*See among others*, Garante per la Protezione dei Dati Personali [Italian Data Protection Authority], Decision No. 9675440, (Jun. 10, 2021) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440 (last accessed Feb. 27, 2024).

[31]Article 29 Working Party, Guidelines on Automated Individual decision-making and profiling, https://ec.europa.eu/newsroom/article29/items/612053 (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

examples mentioned involved refusals to admit entry into a country or denial of citizenship.[32] In any case, as explained in the Guidelines, even where there is no change in data subjects' legal rights or obligations, individuals could still be impacted sufficiently to seek out the protections under this provision when the decision has "significant effects." According to the Guidelines, for data processing to significantly affect someone, the decision must have the potential to significantly affect the circumstances, behavior, or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or, at its most extreme, lead to the exclusion or discrimination of individuals.[33] Some examples mentioned in Recital 71 GDPR include the automatic refusal of an online credit application and e-recruiting practices without any human intervention.

The second requirement set by Article 22 GDPR is that the decision has to be solely based on automated processing, including profiling. The use of the word "solely" means, according to the Guidelines, that a decision is taken without "meaningful human intervention."[34] Assessing the threshold of "meaningfulness" is arguably the most challenging criterion to interpret in Article 22 GDPR and is the most contested aspect in the case law.[35] The Guidelines specify that the human involved should not simply accept the automated output but have the authority and competence to influence the decision, considering all the relevant data.[36] Therefore, mere human involvement does not exclude the applicability of Article 22 GDPR *a priori* but needs to be assessed on a case-by-case basis.

Looking at the emerging case law from national courts and DPAs, recent research shows how interpreting the meaningful human involvement requirement depends on the context.[37]

In the first landmark judgment on Article 22 GDPR by the CJEU,[38] the Court adopted a highly context-dependent approach in interpreting "solely automated decision". The case concerned the compatibility of data processing by SCHUFA, a German credit agency, with the GDPR. More specifically, the Court was asked to interpret whether the decision by a bank to deny credit based on SCHUFA credit scoring is an automated decision under Article 22 GDPR. In C-634/21, The Court held that, since the automating scoring plays a "determining role" in credit granting, it is an automated decision.[39] While the judgment must be welcomed, as the Court expanded legal protection for data subjects in the banking sector, it has not fully clarified the interpretative doubts exposed in the literature on the legal boundaries of Article 22 GDPR. As I have argued elsewhere, while the SCHUFA case was clear-cut, based on factual evidence proving the lack of human discretion on the bank's side, it will be more challenging to apply the concept of "determining role" in other areas of decision-making.[40] In my view, the judgment confirms the difficulties in having an abstract definition of "automated decision", and opts for a more contextual approach, taking into account the concrete roles of the automated systems and the human in the loop. For this purpose, national DPAs have already developed a sophisticated set of criteria to analyse the margin of human discretion left.

[32]*Id.*

[33]*Id.*

[34]*Id.*

[35]Sebastiao Barros Vale & Gabriela Zanfir-Fortuna, Automated Decision-Making Under the GDPR - A Comprehensive Case-Law Analysis, (Future of Privacy Forum) https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/ (last accessed Feb. 27, 2024).

[36]Article 29 Working Party, *supra* note 31, at 21.

[37]Barros Vale & Zanfir-Fortuna, *supra* note 35, at 28.

[38]C-634/21, Schufa Holding, ECLI:EU:C:2023:957, (Dec. 7, 2024).

[39]*Id.* para 50.

[40]Francesca Palmiotto, Scoring for Data Protection Rights: The Court of Justice's First Judgment on Article 22 GDPR (Case C-634/21 and Joined Cases C-26/22 and C-64/22), EU Law Live, (2024) https://eulawlive.com/op-ed-scoring-for-data-protection-rights-the-court-of-justices-first-judgment-on-article-22-gdpr-case-c-634-21-and-joined-cases-c-26-22-and-c-64-22-by/ (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

Factors to be considered include whether the human took into account other elements to make the final decision, their competence, training, and authority. National courts and DPAs apply a sophisticated set of criteria, looking at the entire organization structure, reporting lines, chains of approval, effective training of staff, as well as internal policies and procedures.[41] Moreover, the application of Article 22 GDPR does not rely on the type of the system but on *how* it is used in a concrete case. In the field of migration and asylum, a clear example of automated systems that fulfill the requirements of Article 22 GDPR are those that make positive decisions for visa, residency, and citizenship applications.

Visa decision-making in the EU is undergoing a radical digital turn through the use of interoperable databases powered by AI systems, which raised several concerns highlighted by legal scholars and human rights organizations.[42] Visa applicants' fingerprints are introduced into the Visa Information System (VIS), which stores information on short-term visa applicants during the application procedure and is verified against the database for possible duplicates or matches.[43] In July 2021, the legal framework was revised,[44] extending the scope to include long-term visa holders, lowering the age for fingerprints, and promoting automation in decision-making.[45] Individual risk assessment is an aspect of visa decision-making considered particularly suitable for computation. In 2009, the Visa Code[46] provided for an individual assessment of the risk of illegal immigration and security; AI systems now automate this process, as proposed in a 2019 study for the European Commission.[47] The proposed amendments in the 2021 VIS Regulation introduce new specific risk indicators "applied as an algorithm enabling profiling" (Article 9j VIS Regulation 2021). Similarly, in the context of the European Travel Information and Authorisation System (ETIAS),[48] which will become operational in mid-2025, visa-exempt third-country nationals will be assessed against the risk of irregular migration, security, or public health (Article 1 ETIAS Regulation). The data will be checked against all other EU systems, Europol data, Interpol databases, the new ETIAS watchlist, and specific risk indicators. Screening rules will be built into an algorithm to identify travellers fitting pre-defined risk profiles (Article 33 ETIAS Regulation).

VIS and ETIAS pre-screen applicants based on automated risk assessment. While in VIS, a human caseworker will manually process every visa application (Article 9c VIS Regulation 2021).

[41] *Id.*

[42] *See among others* Evelien Brouwer, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, 26 EUR. PUB. L. 71–92 (2020); Niovi 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*, 45 E.L. REV. 348 (2020); Charly Derave, Nathan Genicot & Nina Hetmanska, *The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System*, 13 EUR. J. RISK REGUL. 389–420 (2022); Valsamis Mitsilegas, *Interoperability as a Rule of Law Challenge*, EUPLANT (May 6, 2020).

[43] Costica Dumbrava, *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, EUROPEAN (2021), https://data.europa.eu/doi/10.2861/91831 (last accessed Feb. 27, 2024).

[44] Regulation 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, 2021 O.J. (L 248).

[45] *See in particular* Niovi Vavoula, Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism, 23 European Journal of Migration and Law 457–484 (2021).

[46] Regulation 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas, 2009 O.J. (L 243).

[47] Deloitte and Directorate-General for Migration and Home Affairs (European Commission), *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security*, (2020), https://data.europa.eu/doi/10.2837/923610 (last accessed Feb. 27, 2024).

[48] Regulation 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 O.J. (L 135).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

By contrast, in ETIAS, travel authorizations will be automatically issued if the system does not report a hit (Article 21(1) ETIAS Regulation). If the automated processing results in a hit, the application will be processed manually by the ETIAS National Unit of the responsible Member Stats (MS), which will decide whether to issue the travel authorization (Articles 21(2) and 22 ETIAS Regulation). Therefore, in ETIAS, only positive decisions will be automated, while denials of travel authorization will require human intervention. A further example of positive automated decisions comes from Norway, where the Norwegian Directorate of Immigration (UDI) automated the processing of residency applications for family immigration and citizenship applications. Like ETIAS, only those that receive a positive response are fully automated; a human caseworker will assess the others.[49]

Visa and residency decisions undoubtedly have legal effects, such as authorizing admission to a country or acquiring citizenship. Moreover, as shown above, they do not involve human intervention. The compelling question is whether Article 22 GDPR applies to positive automated decisions. The answer can be found by contrasting the GDPR with the LED, which, in Article 11 LED, provides that the twin provisions of Article 22 GDPR explicitly mention decisions with "adverse" legal effects. According to Veale and Binns, this contrast between data protection instruments serves as an indicator of the legislator's will to expand the scope of the GDPR to all legal and significant effects "regardless of their valence."[50] Including positive ADM under Article 22, GDPR has important consequences for automated systems used in migration management: the prohibition and safeguards apply irrespective of the positive or negative outcome. There is, however, a second caveat.

While automated decisions in citizenship and residency clearly fall within the scope of the GDPR, automated risk assessment may trigger the applicability of the LED when used to assess risks to security. Depending on the authorities processing the data, these cases could fall within the scope of the GDPR or the LED, with different standards of protection. Yet, delineating between the two instruments is a challenging exercise, as the research by Quintel shows.[51] She argues that in light of the blurred line between EU law enforcement agencies and migration agencies, the unclear delineation between the different data protection instruments leads to lowering data protection standards, particularly purpose limitation.[52] This is the case with the ETIAS regulation, where many provisions remain unclear and do not sufficiently draw a clear line between criminal law enforcement and migration law enforcement processing of personal data.[53]

In sum, this Section has focused on the interpretation of Article 22 of GDPR. In the decision-making process considered by the GDPR, the human is not present or simply accepts the automated output as a "token gesture" without considering other relevant factors for the decision. Automated decision-making in migration and asylum governance relates solely to positive decisions. While all the general provisions of the GDPR still apply to cases where automated systems aid, support, or assist humans in decision-making processes,[54] the specific guarantees, the prohibition of Article 22, and the connected transparency rights in Articles 13 and 14 apply to a narrow set of cases where a decision, with legal or significant effects, is solely based on automated processing or profiling. As Section III will show, in real life humans retain discretion in decision-making processes that have legal or significant effects on groups of people who are already vulnerable and disenfranchised, such as migrants and asylum seekers.

[49]Ozkul, *supra* note 1, at 23–37.
[50]Binns and Veale, *supra* note 10, at 328.
[51]Quintel, *supra* note 27.
[52]*Id.*
[53]*Id.* at 39.
[54]Hänold, *supra* note 6.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

## B. ADM in the AI Act: A Risk-Based Approach

### *I. The Function and Aims of the AI Act*

Next to data protection law, a crucial source of EU regulation for ADM systems is the Artificial Intelligence Act (AI Act).[55] Proposed in April 2021, the AI Act will be the first comprehensive regulation of AI systems at a supranational level.[56] At the heart of the proposal is the idea of co-regulation through standardization based on harmonized rules for development, placement on the market, and the use of AI systems within the EU.[57] Two key objectives drive the AI Act: 1) improving the functioning of the internal market by laying down a uniform legal framework for the development, marketing, and use of trustworthy artificial intelligence (AI) while 2) ensuring a consistent and high level of protection of overriding reasons of public interest such as health, safety, and fundamental rights.

Although the AI Act shares similar objectives with the GDPR, particularly the protection of fundamental rights, it is primarily an internal market instrument based on 114 TFEU. The nature of the AI Act as an internal market regulation is reflected in the overall structure of the legislation, inspired by product safety regimes. AI systems are "products" that must undergo conformity assessment and comply with specific requirements. The proposal follows a risk-based approach, with certain particularly harmful AI practices restricted or subject to mandatory horizontal requirements and conformity assessment procedures before they can be placed in the market. To minimize risks to the protection of fundamental rights, the AI Act focuses on the quality of training, validation, and testing data sets of AI systems. Additionally, it places a clear set of horizontal obligations on providers of high-risk AI systems, ranging from document keeping to the duty of information and collaboration in case of risks. Once in compliance with the legal requirements, AI systems must undergo a conformity assessment procedure based (in the large majority of cases) on internal control. Providers themselves assess the compliance of their systems with legal requirements, draw up a declaration of conformity, and affix a CE marking.[58] The final step is the registration of the AI system in the EU database, which is accessible to the public and contains important information such as the system's intended purpose, information about the provider, and instructions for use.

Unlike the GDPR, which sets requirements for solely automated decisions, the AI Act primarily concerns AI systems that pose an unacceptable or high risk, considering AI-driven decision-making as a potential source of risk. Even if the legislation does not provide a definition of AI decision-making, the role of AI systems in influencing decisions is a core concept in the classification rules for high risk AI set in Article 6 of the AI Act (see below sub-section II). Additionally, the AI Act acknowledges the potential role of AI for decision-making systems in different provisions. Article 14 on human oversight,[59] for instance, refers explicitly to the issue of

[55]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 (Apr. 21, 2021), hereinafter AI Act.

[56]For a comprehensive analysis see Lilian Edwards, *Expert Opinion: Regulating AI in Europe*, ADA LOVELACE INSTITUTE, (2022), https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/ (last accessed Feb. 27, 2024); Veale and Zuiderveen Borgesius, *supra* note 12; Martin Ebers, *Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act*, SSRN, (2021), https://Articles.ssrn.com/abstract=3900378 (last accessed Feb. 27, 2024); Martin Ebers et al., *The European Commission's Proposal for an Artificial Intelligence Act - A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, 4 J 589 (2021). On the importance of the AI Act for the EU and the rule of law see Mireille Hildebrandt, *The Artificial Intelligence of European Union Law*, 21 GERMAN L. J. 74–79 (2020).

[57]Ebers, *supra* note 56, at 2.

[58]Luciano Floridi et al., *CapAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act*, SSRN, (2022), https://Articles.ssrn.com/abstract=4064091 (last accessed Feb. 27, 2024).

[59]On the role of the human in ADM see, among others, Reuben Binns, *Human Judgment in Algorithmic Loops: Individual Justice and Automated Decision-Making*, 16 REGUL. & GOVERNANCE 197–211 (2022); Marco Almada, *Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems*, PROCEEDINGS OF ICAIL 2019, (2019);

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

"automation bias,"[60] in particular, high-risk AI systems used to "provide information or recommendations for decisions to be taken by natural persons" (Article 14(4)(b) AI Act). The provision also echoes Article 22 GDPR, which states that no decision can be made on the basis of biometric identification unless the result is verified by at least two natural persons (Article 14(5) AI Act). Moreover, in the context of regulatory sandboxes, the Act prohibits the processing of personal data that leads to "decisions affecting the data subjects" (Article 54(1)(f) AI Act). Three sets of requirements are particularly relevant for AI-driven ADM:[61]

1. Article 10 on data governance sets rules on how training data sets must be designed and used to reduce error and discrimination generated by inaccurate or historically biased data.
2. Article 11 on transparency requires AI systems to be designed and developed "to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately."
3. Article 14 on human oversight requires that systems must be designed and developed in such a way that they can be "*effectively overseen by [a] natural person,"* allowing the user to spot anomalies, be aware of automation bias, correctly interpret the input, and eventually disregard or override the system.

Contrary to the GDPR, where the data subject is a key subject of rights and beneficiary of information, the original proposal did not enshrine new rights for individuals affected by AI systems (or "end-users"). After all, the AI Act was originally designed as an internal market regulation where the core idea was that "obligations for ex-ante testing, risk management, and human oversight will facilitate the respect of other fundamental rights by minimizing the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary". Throughout the legislative process, however, the Parliament successfully strengthened the role of individuals affected by AI Systems. Following the recommendations of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), the Parliament intervened by granting individuals a new cornerstone right: a right to explanation of individual decision making using a high-risk AI system (Article 68c AI Act).The right applies to decision taken on the basis of an output from an high-risk AI system, which produces legal or similarly significantly adverse effects. In these cases, individuals can request from the deployer "clear and meaningful explanations on the role of the AI systems in the decision-making procedure and the main elements of the decision taken" (Article 68c(1) AI Act). In other words, rather than granting individuals access to information on the system, this new right demand decision-makers to explain how they have used an AI system to reach a decision. Despite this notable addition, the overall focus of the AI Act still remains on the role of the provider, protecting the fundamental rights of individuals with ex-ante requirements when the system is classified as "high risk".

## *II. When is an AI System "High-Risk"?*

The requirements set in the AI Act, including human oversight and data quality mentioned above and the right to an explanation, apply to automated decision-making, broadly defined as long as the decision is taken, supported, or aided by 1) an "AI system" and 2) it poses a "high risk."

Ben Wagner, *Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems*, 11 Policy & Internet 104–122 (2019).

[60]Raja Parasuraman & Dietrich H. Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration,* 52(3) Human Factors 381–410, (2010); Linda J. Skitka, Kathleen L. Mosier & Mark Burdick, *Does Automation Bias Decision-Making?*, 51 Int'l J. Human-Comput. Stud. 991–1006 (1999).

[61]See more specifically Edwards, *supra* note 12.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

First, "AI systems" are defined as "machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Article 3(1) AI Act). This definition is relatively broad and open. It aims to be "technological neutral" to keep up with ongoing technological changes,[62] and it was one of the most debated aspects of the original proposal.[63,64]

Second, if a system fulfills the definition in Article 3(1) of the AI Act, the provider must assess its risk as low, high (Article 6 AI Act), or unacceptable (Article 5 AI Act). Article 6 identifies two main categories of high-risk systems: 1) AI systems intended to be used as safety components of products subject to third-party ex-ante conformity assessment and 2) stand-alone AI systems listed in Annex III. AI systems for decision-making can be found predominantly in the second category, including, inter alia, AI systems for assessing students, managing work relationships, or assessing the eligibility of individuals for welfare benefits (Annex III AI Act). The risk for stand-alone AI systems lies in identifying areas where the task performed or the purpose of the AI system poses a threat to fundamental rights.[65] In the original proposal, systems listed in Annex III (amendable by the Commission[66]) were automatically considered high-risk. For instance, the use of AI systems in migration, asylum, and border control management is explicitly identified as high risk in light of the impact on "people who are often in [a] particularly vulnerable position" (Recital 39 AI Act). Annex III specifically refers to systems used to detect individuals' emotional states, assess risks, verify the authenticity of documents, and assist public authorities in examining asylum, visa, and residence permit applications (Annex III point 7 AI Act).

This automatic approach to risk classification was highly debated during the legislative process. The Council and the Parliament proposed amendments to Article 6 of the AI Act, introducing two different risk assessment mechanisms *in concreto*. On the one hand, the Council proposed a presumption of high risk for AI systems listed in Annex III unless "the output of the system is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to the health, safety or fundamental rights" (Article 6, Council compromise text). On the other hand, the Parliament proposed to consider AI systems as falling in the critical areas or use cases in Annex III as high risk if "they pose a significant risk of harm to the health, safety or fundamental rights of natural persons" (Article 6 Parliament text). Despite the criticism raised by the EDPS on the proposed amendments,[67] during the trilogue, the three institutions finally found an agreement on Article 6, whereby the concept of automated decision-making now plays a crucial role in the high-risk classification rules. Under the new Article 6(2) and (2a) of the AI Act, the provider shall check the list in Annex III and perform a risk assessment. An AI system is classified as "high-risk" only when it does not pose "a significant risk of harm to the health, safety or fundamental rights", including "by not materially influencing the outcome of decision-making". In this way, the EU legislator linked the concept of high risk to AI-driven decision-making, although with unclarity and uncertainty. When

[62]Kees Stuurman & Eric Lachaud, *Regulating AI. A Label to Complete the Proposed Act on Artificial Intelligence*, 44 COMPUT. L. & SEC. REV (2022).

[63]On a critique to the definition of AI see Joanna J. Bryson, *Europe Is in Danger of Using the Wrong Definition of AI*, WIRED, https://www.wired.com/story/artificial-intelligence-regulation-european-union/ (last accessed Feb. 27, 2024); Stuurman and Lachaud, *supra* note 62.

[64]Before opening the trilogue, both the Council and Parliament proposed a narrower version of Article 3 by introducing the requirement of "autonomy."

[65]Stuurman and Lachaud, *supra* note 62.

[66]The list can be amended by the Commission if a high-risk system intended to be used in the areas listed in Annex III "poses a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights" (Article 7(1) AI Act).

[67]EDPS Opinion 22/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments (23 October 2023), https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2023-10-23-edps-opinion-442023-artificial-intelligence-act-light-legislative-developments_en (last accessed Feb. 27, 2024), at 11.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

does an AI system "materially influence" a decision? Article 6(2a) suggests that this should be the case when AI systems only perform a narrow procedural task, a preparatory activity or when they are intended to improve the result of a completed human activity. The new Article, at least, clarifies that such exceptions do not apply when the AI systems perform profiling of natural persons, which will always be considered high risk. Apart from AI profiling systems, however, it will be up to the provider to determine when their AI systems pose a risk to fundamental rights, health and safety and, therefore, whether they fall in the scope of the regulation.

Undoubtedly, interpreting this provision will be a challenging task for providers. While AI systems that fulfil the "solely automated decision" definition under Article 22 GDPR clearly present a high risk for individuals, a risk assessment may be less straightforward when they partly automate decision-making. Does an AI system for triaging cases pose a risk to fundamental rights? What about AI systems that provide information to decision-makers who take (and are responsible for) the final decision? Worryingly, the new version of the AI Act seems to suggest that fundamental rights are unaffected when AI systems do not have a prevalent role in decision-making. Many real life examples of ADM have, however, already proven the contrary, as Section III will show.

## III. ADM in EU Law: Key Takeaways

The GDPR and the AI ACT both regulate ADM but with different scopes and types of protection. Article 22 GDPR contains a micro-charter for automated decisions to limit automated processes detrimental to human dignity and enhance the accountability and responsibility of human decision-makers. While generally prohibited, automated decisions that fulfill Article 22(2) conditions are exceptionally allowed, provided additional safeguards are present, including the right to contest the decision and obtain human intervention. Compared to the general provision on special categories of data (Article 9 GDPR), more stringent rules for processing sensitive data apply. Finally, specific transparency rights are enshrined in Articles 13 and 15 GDPR, allowing the data subject to obtain information about the automated decision system's use, logic, and consequences. Legal protection against the adverse effects of ADM depends on whether the decision is "solely" automated. In the silence of the CJEU, national DPAs and courts have adhered to the guidelines on Article 22 GDPR by the WP29 (now European Data Protection Supervisor (EDPS)), which is interpreted solely as a "lack of meaningful human intervention." Suppose an automated system supports decision-makers, but humans consider other elements to make the final decision and have the competence, training, and authority to disregard the system's recommendation. In that case, the specific safeguards and rights for data subjects will not be applicable. The recent SCHUFA case has shed new light and shadows on the interpretation of Article 22 GDPR. In C-634/21, the Court held that credit scoring is an automated decision when the decision-maker "draws strongly" on it to establish, implement or terminate a contractual relationship. With this judgment, the Court suggests focusing on the relationship between the human and the machine, analyzing, on the one hand, the margin of discretion left on the side of the decision-maker and, on the other, the concrete role of the automated systems within the decision-making process.

The AI Act adopts a different approach. The core idea is to "minimize"[68] (not eliminate) risks of erroneous or biased AI-assisted decisions with ex-ante requirements and conformity assessment procedures. AI is a product that must comply with specific design requirements before being put on the market, which includes data quality, risk management, transparency, and human oversight (Chapter III AI Act). Such requirements apply when AI systems – defined in the proposed regulation – pose a high risk to safety, health, or fundamental rights. Unlike the GDPR, where the data subject is a key actor, the AI Act is primarily concerned with the provider and the deployer of the AI system. Thanks to the efforts of the European Parliament, the individual

[68]AI Act, *supra* note 55, at 11.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

affected by AI systems finally found a space in the AI Act in Article 68c, which grants a right to an explanation for AI driven decision-making.

| | Scope of Protection | Definition | Type of Protection |
|---|---|---|---|
| GDPR | • Solely automated decisions with legal or significant effects<br>• Legal protection applies regardless of the type of technology used | • Solely means "without meaningful human involvement" (Guidelines by Article 29 WP)<br>• Automated credit scoring is an automated decision when it plays a determining role in credit granting (C-634/21) | • Prohibition with exception<br>• Rights for data subjects<br>• Restrictions on the use of sensitive data<br>• Transparency and information to data subjects |
| AI ACT | • High-risk AI systems<br>• Legal protection applies only to AI systems defined in Article 3 of the AI Act | • High risk AI systems listed in Annex III (Article 6 AI Act) if they pose a significant risk of harm to the health, safety and fundamental rights of natural persons (except for profiling AI systems, which are always high risk) | • Requirements for high risk AI systems<br>• Obligations for providers and users<br>• Conformity Assessment Procedure<br>• Right to an explanation for AI-driven decision-making |

In conclusion, legal protection for ADM systems under the GDPR and the AI Act essentially rely on two legal questions: (1) Is the decision solely automated, that is, is the role of the human insufficiently meaningful, and (2) does the system (if AI) present a significant risk of harm for fundamental rights? In the following sections, I will address these questions by empirically observing how automated systems are used in the whole sector of migration and asylum.

## C. ADM in Real Life: A Taxonomy for a Fundamental Rights Analysis

### *I. Dissecting ADM: A Brief Note on Methods*

The AFAR project started two years ago with an ambitious working package: a mapping of the current uses of new technology in European migration and asylum governance.[69] The mapping report was not easy: the security, privacy, and proprietary information rules hampered the public administration's investigation of new technologies. After one year of intense research, questionnaires were submitted to the EU and national Parliaments, thanks to the help of interested MPs, interviews with public officials, requests for information from private companies, informal meetings, and freedom of information requests, Derya Ozkul published her report in January 2023.[70] Her research revealed that ADM systems were used in diverse and complex ways – from triaging applications to language recognition in asylum procedures – with some forms of human involvement in most cases. After reading her research, I wanted to resolve the puzzle of how to classify such systems where automation segments decision-making without replacing humans. Are these automated decisions?

Legal scholars have commonly termed these types of systems as "semi-automated decision-making,"[71] "decision-support systems,"[72] or "mixed algorithmic decision-making."[73] By including

[69]For an overview of the project see AFAR Project, https://www.hertie-school.org/en/research/research-directory/afar (last accessed Feb. 27, 2024).

[70]Ozkul, *supra* note 1.

[71]Simona Demkova, *The Decisional Value of Information in European Semi-Automated Decision-Making*, 2 Rev. Eur. Admin. L. 29–50 (2021).

[72]Among others Brkan, *supra* note 20, at 10.

[73]Danielle Keats Citron, *Technological Due Process*, 85 Wash. Univ. L. Rev. 1249–1313 (2008); Madalina Busuioc, *Accountable Artificial Intelligence: Holding Algorithms to Account*, Pub. Admin. Rev. 1–12 (2020).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

the concept of "decision," these definitions recognize, in the words of Demkova, the "decisional value"[74] of automated processing on the process, even when a human is involved.[75] Yet, not every semi-automated decision-making process is the same. Automatically assigning cases to human case workers differs from flagging applicants as potential security threats: the outcomes and fundamental rights involved differ. To better grasp and account for these differences, it is necessary to question what exactly is automated and for what purposes. What is the role of the automated system in the broader process? The following Section builds on these leading questions to dissect automated systems in migration and asylum governance. By focusing on what is automated and for what purpose, I identify three ways in which automated systems are used: internal case management, flagging potential suspects, and generating evidence in administrative and judicial proceedings.

## II. Automated Triage

After Brexit, the UK had to deal with a massive number of residents applying to the EU Settlement Scheme (EUSS). Under the EUSS, individuals from EEA countries and Switzerland could apply for indefinite or time-limited permission to enter or remain in the UK, provided that certain requirements were fulfilled. As of 31 March 2023, more than 7.2 million applications had been received,[76] making it extremely difficult for the UK public administration to manage such an unprecedented number of cases. The solution was found in the use of automated tools to speed up and make case management more efficient. Automated systems were used, in particular, to categorize the applications and assign them to caseworkers "according to their skills, profile, and experience."[77] The caseworker would then take the final decision for the applicants automatically assigned to them by a "triaging system."

In medicine, triaging refers to sorting patients according to the urgency of their need for care. Upon an initial assessment by the medical staff in an emergency room, patients are labelled and categorized in color codes based on the severity of their conditions. Similarly, so-called "triaging systems" assess and categorize individuals applying for visas, residency, citizenship, settlement, and asylum. Veale and Binns conceptualize these technologies as "multi-stage profiling systems triaging human decisions."[78] In triaging systems, "new cases are profiled and categorized," determining "the future decision pathway that the case continues along."[79] While humans make the final decision, the automatically generated classification determines the next steps in the decision-making process.

In some cases, the classification simply determines the internal workflow: the system assesses and assigns a new case to human case workers. The main objective is to help officials and the public administration manage cases more effectively. For example, in the EU settlement scheme, the application is assessed according to its complexity and is assigned to human workers. As reported by Ozkul, "The more complex the case is, the more highly graded the officer examining it."[80] A second example is the automated triaging of appeal cases in the Netherlands to determine which lawyer will work on the relevant appeal case.[81] Moreover, in asylum procedures, the Dutch

[74]Demkova, *supra* note 71.

[75]For a definitory proposal of ADM see Rashida Richardson, *Defining and Demystifying Automated Decision Systems*, (2021), SSRN, https://Articles.ssrn.com/abstract=3811708 (last accessed Feb. 27, 2024).

[76]GOV.UK Official Statistics, EU Settlement Scheme quarterly statistics (2023), https://www.gov.uk/government/statistics/eu-settlement-scheme-quarterly-statistics-march-2023/eu-settlement-scheme-quarterly-statistics-march-2023 (last accessed Feb. 27, 2024).

[77]Ozkul, *supra* note 1, at 32.

[78]Binns and & Veale, *supra* note 10, at 321.

[79]*Id.* at 322.

[80]Ozkul, *supra* note 1, at 32.

[81]*Id.* at 56.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

Ministry of Justice and Security is evaluating whether text mining can support them in triaging appeal cases, including asylum claims.[82] Finally, the study commissioned by the European Commission in 2020 analyses the opportunities of triaging systems in visa decision-making, long-term migration processes, Schengen border crossings, the operational management of services at eu-LISA, and for granting international protection.[83]

Automated case management does not qualify as solely automated decisions as humans are too meaningfully involved in the process: the system only assigns an application to human caseworkers. Moreover, they don't qualify as "high-risk" AI systems (provided that the system fulfils the technical requirements of Article 3 AIA), as Annex III does not list this type of system. In a presentation by the Commission, they explicitly consider automated case management systems as low risk, claiming that "if the triaging would be wrong, officials would receive cases that do not match their experience, interest, capacities. They would re-direct the cases manually".[84] Nonetheless, even if automated case management is not a final decision, the influence of the output on the decisional outcome cannot be overlooked. Recalling the example of triaging in hospitals, it is clear that a wrong categorization can have adverse consequences. Being assigned a green rather than a red code can put a patient in need of urgent care at significant risk. Automated systems based on biased, racialized data and assumptions can lead to discriminatory treatment. Consider the case of the UK visa streaming algorithm case, where applications for visas made by individuals of certain nationalities were more likely to be refused and took longer to determine.

In other cases, the automated triage triggers follow-up actions by human case workers. Such follow-up activities range from higher scrutiny by officials, or further data collection, to intrusive investigations on individuals' private lives. The purpose of automated systems here is different. Instead of determining the internal workflow, the classification flags individuals as potential suspects that require further investigation.

### III. Automated Suspicion

Since 2019, the Home Office has deployed an automated system to "triage" applicants into green and red categories based on risk assessments. The tool was designed to detect sham marriages. Once registration was assessed as high risk, the Home Office investigated the applicants' story through interviews and house visits or delayed the nuptials for up to seventy days to allow for further investigations. Maxwell and Tomlinson, who thoroughly studied the practices of the Home Office in their recent book, describe such follow-up activities as "grueling."[85] Officials interrupted wedding ceremonies to ask questions about the couple's sex lives, raided houses to check if they shared the same bed, and showed nude photographs sent years before to their ex-partner.[86] As this case shows, automated systems can trigger follow-up activities that have significant adverse effects on individuals, reaching the most private aspects of their lives in ways that can be humiliating and degrading.

Based on a risk assessment, an individual may be categorized as a suspect, which justifies follow-up actions by the competent authorities. The 2020 EC report, for instance, explicitly states that "to avoid suspicion, some travelers take convoluted routes to avoid attention from authorities

[82] *Id.*

[83] Deloitte & Directorate-General for Migration and Home Affairs (European Commission), *supra* note 45.

[84] European Commission DG Home, Rules on migration, Asylum, and Border Management in the AI proposal, https://www.statewatch.org/media/3074/eu-council-ai-act-com-presentation-borders-migration.pdf (last accessed Feb. 27, 2024).

[85] Maxwell & Tomlinson, *supra* note 1, at 1.

[86] Diane Taylor & Frances Perraudin, *Couples Face "insulting" Checks in Sham Marriage Crackdown*, THE GUARDIAN (Apr. 14, 2019), https://www.theguardian.com/uk-news/2019/apr/14/couples-sham-marriage-crackdown-hostile-environment (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

(for example, going from Egypt to Belgium through Japan)."[87] AI systems could monitor, search, and combine data from different sources such as VIS and EES (and also Passenger Name Record (PNR) data collected by airlines) to detect possible "irregular travelling patterns." The outputs of this analysis could prompt a human to investigate further or to ask the applicant for further information/documentation.[88] Eu-LISA, the agency for the operational management of large-scale IT systems, indicated that machine learning could be used "when dealing with *suspicious* applications" (emphasis added) to support caseworkers with risk assessments.[89]

Interestingly, the term "triaging" is used by the authorities deploying these systems; for example, the Home Office in the case illustrated above and by the European Commission in their 2020 report referring to automated risk assessment. This terminology risks diverting attention from the nature and purposes of these automated systems. Rather than simply "triaging" applications, they provide hints for further investigations, which can have a range of adverse consequences on individuals' fundamental rights, particularly their right to a private life (not just data protection). Framing these tools as "automated suspicion" better captures the crucial difference between triaging systems from a legal perspective.

Automated suspicion lies at the crossroads between criminal and migration law, where third-country nationals are increasingly perceived as suspects of crimes and "potential security threats."[90] A clear example is the use of travellers' data to prevent, detect, investigate, and prosecute terrorist offenses and serious crimes. Directive 2016/681 (the PNR Directive) regulates the use of PNR data from passengers in extra-EU flights to prevent, detect, and prosecute terrorist offenses and crimes. For this purpose, the PNR data of passengers are analyzed by automated means to identify persons who require further examination by the authorities (Article 6 PNR Directive).

Akin to automated case management, automated suspicion is not a decision within the meaning of Article 22 GDPR. A public official takes both the final decision (such as delaying the nuptials) and intermediate decisions (such as investigating the couple with a house search). The system provides hints and creates suspicion, but it is at the officer's discretion to decide whether or not to take action (at least formally).[91] Regarding the AI Act, provided that the definition of AI in Article 3 is fulfilled, automated suspicion systems are high-risk when assessing the risk of offending, security risks, risks of irregular immigration, or health risks (Annex III 7.b). Automated suspicion raises several issues that threaten fundamental rights, including the right to non-discrimination and private life.

First, when the triaging system flags a case, humans are justified in taking follow-up actions based on an automated classification. However, how the system generates such classifications is often unclear. The system could account for protected characteristics such as age and ethnicity but has the potential for discrimination.[92] As scholarly literature shows, "risk analysis largely builds

[87]Deloitte and Directorate-General for Migration and Home Affairs (European Commission)Deloitte and Directorate-General for Migration and Home Affairs (European Commission), *supra* note 47, at 90.

[88]*Id.*

[89]Publications Office of the European Union, European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom & Aleksandrs Cepilovs; Publications Office of the European Union, *Artificial Intelligence in the Operational Management of Large-Scale IT Systems: Research and Technology Monitoring Report : Perspectives for EU LISA* (2020), https://data.europa.eu/doi/10.2857/58386 (last accessed Feb. 27, 2024) at 30.

[90]Bruno Oliveira Martins & Maria Gabrielsen Jumbert, *EU Border Technologies and the Co-Production of Security 'Problems' and 'Solutions,'* 48 J. Ethnic Migration Stud. 1430–1447 (2022).

[91]Empirical studies have shown the propensity of humans to adhere to algorithmic suggestions. See among others Parasuraman and Manzey, *supra* note 59; Kate Goddard, Abdul Roudsari & Jeremy C. Wyatt, *Automation Bias: Empirical Results Assessing Influencing Factors*, 83 Int'l J. Med. Informatics 368–375 (2014); see, on the contrary, Saar Alon-Barkat & Madalina Busuioc, *Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice*, 33 J. Pub. Admin. Rsch. Theory 153–169 (2023), (showing that Dutch civil servants had enhanced awareness of algorithmic bias in the aftermath of the child benefit scandal).

[92]See generally on border control and discrimination E. Tendayi Achiume, *Digital Racial Borders*, 115 Am. J. Int'l L. 333–338 (2021).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

upon gendered and racialized assumptions."[93] For instance, the Home Office in the UK has shared that the system detecting potential sham marriages considers, as a risk factor, the age difference between partners.[94] Furthermore, automated systems could be based on methods lacking scientific validity. In the words of Hildebrandt: "Reliable AI can only be developed if it is based on a sound and contestable research design anchored in the core tenets of reproducible open science."[95] For some ADM systems, the opposite is true. Consider the case of iBorderCtrl, an EU-funded project developing a technology for lie detection based on emotion recognition. The project envisaged a two-step procedure. Before travelling to Europe, people would be asked to answer questions in front of a video camera. On arrival at the EU borders, their recorded facial expressions would be compared with pictures from the previous border crossing. Based on the video recording, the system was supposed to detect whether travellers were lying.[96] Travellers receiving a high score would be subject to more investigations by border officers.[97] The project was criticized by civil society organizations and academics and was challenged by Patrick Breyer before the CJEU.[98] Among other issues, the main criticism was the ability of the technology to infer human behavior from facial movements. No evidence proves that this method is scientifically sound.[99]

Finally, the system can lack individual accuracy when based on statistics and correlations, raising the question of whether a non-individualized classification can justify taking individual decisions at all.[100] When the Public Law Project analyzed the automated risk assessment of applicants for marriage in the UK, they found that couples were referred to the system when one or both came from outside the European Economic Area. Rather than on causality, these risk factors are based on the discriminatory assumption that the sole aim of a marriage with a non-EU citizen is to obtain migration status.[101] Moreover, in the case of iBorderCtrl, researchers made clear that emotion recognition cannot account for individual characteristics; how people communicate emotions varies substantially across cultures, situations, and even people within a single situation.[102] Legal scholars who researched AI systems in criminal law enforcement have warned against the use of predictive policing from the perspective of the right to be presumed innocent.[103] Rich argues that automated suspicion algorithms are insufficient to generate individualized suspicion. Therefore, officers should not be allowed to base arrest or search decisions on automated systems' predictions alone.[104]

The AI Act can help address some of these issues by establishing standards and requirements for AI systems that generate suspicion. Nevertheless, the AI Act does not answer fundamental questions about what system can generate accurate and non-discriminatory suspicion. Should suspicion be individualized even when automated? What safeguards and remedies do individuals need in case of errors, inaccuracy, and biased outcomes? Interestingly, the CJEU addressed these questions in three instances where they considered the compatibility of risk assessment with

[93]Niels van Dijk, Raphaël Gellert & Kjetil Rommetveit, *A Risk to a Right? Beyond Data Protection Risk Assessments*, 32 Comput. L. Sec. Rev. 286–306 (2016).

[94]Ozkul, *supra* note 1, at 31.

[95]Hildebrandt, *supra* note 56, at 78.

[96]Ozkul, *supra* note 1, at 27.

[97]*Id.* at 26.

[98]Case T-158/19, *Breyer v. REA*, ECLI:EU:T:2021:902, (Dec. 15, 2021), (currently under appeal in C-135/22 P).

[99]See, among others, Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, Psych. Sci. Pub. Int. (2019); Inioluwa Deborah Raji et al., *The Fallacy of AI Functionality*, 2022 ACM Conference on Fairness, Accountability, and Transparency 959–972 (2022), http://arxiv.org/abs/2206.09511.

[100]Alexandra Hall, *Decisions at the Data Border: Discretion, Discernment and Security*, 48 Sec. Dialogue 488–504 (2017).

[101]Ozkul, *supra* note 1.

[102]Barrett et al., *supra* note 99.

[103]Athina Sachoulidou, *OK Google: Is (s)He Guilty?*, 30 J. Contemp. Eur. Stud. 284–296 (2022); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, Univ. Pennsylvania L.Rev. 327–410 (2015).

[104]Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. Pa. L. Rev. 871–929 (2015).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

fundamental rights: Opinion 1/15, *La Quadrature du Net and Others v Premier ministre*, and *Ligue de droit humains ASBL Conseil des ministres*.[105]

In 2015, the European Parliament requested an Opinion from the Court on the compatibility of the envisaged agreement between Canada and the EU on the transfer and processing of PNR data (hereafter "Agreement") with the provisions of the Treaties (Article 16 TFEU) and the CFREU (Articles 7, 8 and Article 52(1)).[106] The envisaged Agreement concerned, *inter alia,* the transfer and use of PNR data to prevent, detect, investigate, or prosecute terrorist offenses and other serious transnational crimes (Article 3 of the Agreement). More specifically, the envisaged Agreement allowed PNR data to be analyzed by automated means before the arrival of the aircraft in Canada. The automated analyses could "give rise to additional checks at borders in respect of air passengers identified as being liable to present a risk to public security and, if appropriate, on the basis of those checks, to the adoption of individual decisions having binding effects on them."[107] The European Parliament raised doubts as to the compatibility of automated analysis with the principle of proportionality, underlying, in particular, the lack of a link between PNR data and the potential existence of a threat to public security. The Court shared the European Parliament's views with regard to the automated risk assessment and the lack of sufficient safeguards in the envisaged Agreement.

More specifically, the Court underlined two key issues. First, the automated risk assessment was not sufficiently individualized when based on pre-established models and criteria. Consequently, follow-up actions or decisions based on risk assessments were taken "without there being reasons based on individual circumstances that would permit the inference that the persons concerned may present a risk to public security."[108] Second, the Court considered the significant margin of error of automated analyses when based on non-verified data and pre-established models and criteria.[109] Therefore, the Court concluded that the envisaged Agreement was incompatible with Articles 7 and 8 of the CFREU and listed the safeguards that need to be added.

First and foremost, the Court stated that the pre-established models and criteria must be reliable, specific, and non-discriminatory to target only individuals "under a reasonable suspicion."[110] Additionally, the method implemented in the system had to be reliable and topical, taking into account international research.[111] Second, the Court considered the rights of data subjects and transparency. While the Agreement already provided for a right to access and correct PNR data, those provisions did not require that passengers be notified of the transfer of their PNR data to Canada.[112] Consequently, the Agreement must provide a right to individual notification for air passengers whose data has been transferred or used, only when such notification is no longer liable to jeopardize the investigations.[113]

The Court also considered the right to non-discrimination in La Quadrature du Net and Others v Premier ministre. The judgment originates from requests for a preliminary ruling from the French Conseil d'État and the Belgian Constitutional Court on the compatibility of national

[105]Opinion 1/15 of the Court, ECLI:EU:C:2017:592, (Jul. 26, 2017); Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others, ECLI: EU:C:2020:791, (Oct. 6, 2020); Case C-817/19, Ligue des droits humains ASBL v Conseil des ministres, ECLI: EU:C:2022:491, (Jun. 21, 2022).

[106]For a detailed analysis of Opinion 1/15, *supra* note 105, see Christopher Kuner, *International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15, EU-Canada PNR*, 55 Common Mkt. L. Rev. (2018); Monika Zalnieriute, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, 81 Mod. L. Rev. 1046–1063 (2018).

[107]Opinion 1/15 at para.131.

[108]*Id.* at para. 132.

[109]*Id.* at para. 170.

[110]*Id.* at para. 172.

[111]*Id.* at para. 174.

[112]*Id.* at para. 221.

[113]*Id.* at para. 224.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

legislation with Directive 2022/58 and the CFREU.[114] Among other aspects, the Court considered the compatibility of automated traffic and location data analyses within Articles 7, 8, and 11 of the CFREU and the right to an effective remedy, highlighting the discrimination risks in the context of automated decision-making. Similar to the use of PNR data in the EU-Canada agreement, national law allowed for automated analyses of traffic and location data retained by providers of electronic communication services to detect links to terrorist threats. Automated risk assessment presented similar issues, as highlighted by the Court in Opinion 1/15 – the lack of individualized suspicion justifying an interference with the right to privacy and the compatibility with the principle of proportionality and effective review. In the ruling, the Court recalls the requirements set in Opinion 1/15, particularly the reliability and specificity of pre-established models and criteria, "making it possible to achieve results identifying individuals who might be under a reasonable suspicion of participation in terrorist offences."[115] Moreover, to ensure that risk assessments do not result in discrimination, pre-established models and criteria cannot be based on that sensitive data in isolation.[116] Finally, the Court recalls the issue of potential errors in automated analysis. It reiterates that "any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the persons concerned is adopted."[117]

Finally, in *Ligue de droit humains ASBL Conseil des ministers*, the Court ruled on the interpretation and validity of Directive 2016/681 regarding the use of PNR data for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime (PNR Directive), vis-à-vis Articles 7 and 8 of the CFREU.[118] Thus, the PNR Directive regulates the use of PNR data from passengers in extra-EU flights to prevent, detect, and prosecute terrorist offenses and crimes. For this purpose, the PNR data of passengers is analyzed by automated means to identify persons who require further examinations by the authorities (Article 6 PNR Directive). In the judgment, the Court recalled Opinion 1/15 and the requirements set for the risk assessment of PNR data, particularly the principles of non-discrimination, reliability, and specificity of pre-established models and criteria; the need for a connection between the use of data; the objectives pursued; and the requirement of reasonable suspicion to justify follow up actions.[119] In this sense, the Court also clarified that the reliability of pre-established models and criteria means taking into account both incriminating and exonerating circumstances.[120] The Court also highlighted that the obligation to provide an individual review by non-automated means requires Member States to provide their national authorities with the materials and human resources to carry out such reviews.[121]

The case law of the CJEU on risk assessments in border controls is an important reminder of the role of fundamental rights beyond data protection law in the automation era. It shows that fundamental rights can provide normative grounds to set limits to new tech and justify additional safeguards for individuals and precautions. What is also worth noting is that the Court approaches the compatibility of risk assessment with fundamental rights without attempting to qualify these systems as automated or part-automated systems. On the contrary, the Court focuses on the (analogical) concept of suspicion, arguing that, even when automated, suspicion must be

[114]For an overview of *La Quadrature du Net and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, see Xavier Tracol, *The Two Judgments of the European Court of Justice in the Four Cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre Des Barreaux Francophones et Germanophone and Others: The Grand Chamber Is Trying Hard to Square the Circle of Data Retention*, 41 Comp. L. Sec. Rev. (2021).

[115]*La Quadrature du Net and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, para para. 80.

[116]*Id.* para. 181.

[117]*Id.* para. 182.

[118]For an overview of the case, see Sophie Duroy, *Case C-817/19, Ligue Des Droits Humains v. Council of Ministers (C.J.E.U.)*, Int'l Legal Materials 1–3 (2023).

[119]*Ligue des droits humains ASBL*, Case C-817/19, paras 118 and 219.

[120]*Id.* para. 200.

[121]*Id.* para. 180.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

individualized and reasonable. This reasoning allows the court to set limits and requirements for automated systems, such as the right to human revision of positive outputs, reliability, topicality, and specificity of models, and the need for a connection between the automated processing of data and the objectives pursued.

Sections *I* and *II* focused on automated systems operating at the initial decision-making stage. Unlike triaging systems that determine the internal workflow, automated suspicion triggers follow-up actions by public authorities. A final way automated systems are deployed nowadays is to offer sources of information to human decision-makers to prove relevant facts or provide expert analysis. I refer to these systems as "automated evidence."

## IV. Automated Evidence

Asha Ali Barre and Alia Musa Hosh are two sisters who fled Somalia and sought asylum in Canada based on a fear of sectarian and gender-based violence from militant Islamist groups. Two years after they were recognized as refugees, the Refugee Protection Division (RPD) vacated their status. According to the RPD, Asha, and Alia were not Somalis but Kenyan citizens who entered Canada with a study permit using a different identity. In the view of the RPD, the fact that they lied about their country of origin was a crucial element affecting their credibility for fearing persecution. A photo comparison generated using facial recognition software was the primary evidence against them.[122]

In this example, the automated system did not make the final decision; it aided the RPD in their decision-making. Legal scholars often define these systems as "decision-support systems".[123] As the human in the loop "reviews and takes into account other factors in taking the decision"[124] next to the automated output, these systems do not qualify as automated decisions under Article 22 GDPR. In the words of Veale and Binns, decision-support systems aid human decision-makers by providing "one source of information amongst others under consideration."[125] Among other examples, Veale and Binns considered a system used by an employer to score candidates for job openings, where the score was not used to sift applications but to provide additional information. In some cases, though, automated systems do more than just provide "information." In the case of Barre and Hosh, the RPD used the photo comparison to prove the unreliability of the asylum seekers' claim, which was a crucial element for revoking their status. In this case, the facial recognition software generated *evidence*.

With the term automated evidence, I refer to cases where the output of an automated system is used to prove a fact that is relevant to the final decision.[126] The concept of evidence encompasses both judicial and administrative proceedings in line with the terminology used by CJEU in their

[122]Federal Court of Canada, Asha Ali Barre and Alia Musa Hosh v. The Minister of Citizenship and Immigration, Case No. 2022 FC 1078, para. 54 (Jul. 20, 2022), https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/521971/index.do (last accessed Feb. 27, 2024) [when Asha and Alia applied for judicial review, the court found the decision to vacate their status unreasonable and in breach of procedural fairness].

[123]*See among others* Johan Schubert, *Artificial Intelligence for Decision Support in Command and Control Systems*, in the 23rd International Command and Control Research & Technology Symposium Multi-Domain C2, 15 (2019); Michael Veale, Max Van Kleek & Reuben Binns, *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 1–14 (2018); Marijn Janssen et al., *Will Algorithms Blind People? The Effect of Explainable AI and Decision-Makers' Experience on AI-Supported Decision-Making in Government*, SOC. SCI. COMPUT. REV. (2020).

[124]Article 29 Working Party, *supra* note 31.

[125]Binns and Veale, *supra* note 10, at 322.

[126]Several examples of automated evidence can also be found in the criminal justice sector. See Francesca Palmiotto, *Artificial Intelligence and the Transformation of Criminal Trials : Preserving Fairness in Europe*, EUI PHD THESIS (2023), https://cadmus.eui.eu/handle/1814/75243 (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

case law, where the Court derived from Articles 47 and 41 CFREU a right to access and comment on the evidence, which also applies to administrative decisions.[127]

Next to automated biometric identification, several examples of automated evidence can be considered. In Germany, the immigration authority (BAMF) uses a tool for name transliteration to convert asylum applicants' names into the Latin alphabet. The BAMF also claims this technology "helps identify the applicant's country of origin" and supports the plausibility check of origin.[128] The BAMF also uses the "dialect identification assistance system" (DIAS) for language identification of asylum seekers. As the AFAR report explains, the tool assesses an audio recording with a probability calculation (for example, 60% Arabic Levantine, 20% Arabic Gulf), which is compiled into a PDF form and added to the applicant's case file.[129] According to BAMF, the automated output is used for identification, fraud detection of ID documents, narratives in asylum procedures, and even in return decisions "as origin countries do not accept rejected asylum seekers without reliable evidence."[130] A second example is the automated analysis of mobile phone data in asylum procedures. In some European states, including Germany, the Netherlands, Norway, Denmark, and the UK, asylum seekers' mobile phones can be seized to extract data. Such data are then processed by software that generates a report that can be used "for identity determination and/or the assessment of the applicant's submission."[131] A further example relates to automated fraud detection. At the borders, some European states use or are piloting the use of fraud detection systems for travellers' identities and forged documents.[132] In visa decision-making, fraud detection systems could provide evidence of false, counterfeit, or forged travel documents, which justifies the refusal of entry visas into EU Member States (Article 32 of the Visa Code). Moreover, visa applications are automatically assessed and categorized into risk levels in the EU and the UK, which hitherto had implemented a "visa streaming tool" until 2020, when the practice was halted.[133] Automated risk assessment can be used to prove that an individual poses a threat to public security, which constitutes a ground for a refusal decision (Article 32 Visa Code).

In these cases, automated systems generate evidence that supports or denies claims made by migrants, people on the move, or asylum seekers, leading to the "constitution of novel regimes of proof."[134] Automated evidence can affect the reliability of asylum seekers' claims and can be used to prove that they are not credible. Even if the final decision is not solely automated, the use of new technologies for evidentiary purposes raises relevant issues for the protection of individuals. Similar to triaging systems, the accuracy and validity of the system are crucial to generate reliable evidence. In the case of Barre and Hosh, the claimants challenged the facial recognition software,

[127]Case T-232/00, Chef Revival USA Inc. v. Office for Harmonisation in the Internal Market, 2002 E.C.R. II-02749, paras 41–42 [on translation of evidence in administrative phase before an EU institution]; Case C-300/11, ZZ v Secretary of State for the Home Department, EU:C:2013:363, para. 54–59 (Jun. 4, 2013) [on disclosure of evidence for a decisions refusing entry to the territory]; Joined Cases C-225/19 and C-226/19, R.N.N.S. and K.A. v Minister van Buitenlandse Zaken, ECLI:EU:C:2020:951, (Nov. 24, 2020) [on disclosure of evidence in common visa policy]; Case C-28/05, G. J. Dokter, Maatschap Van den Top and W. Boekhout v Minister van Landbouw, Natuur en Voedselkwaliteit, 2006 E.C.R. I-05431, para. 75 (Jun. 15, 2006) [in connection with the control of foot-and-mouth disease, where the Court stated that the addressees of such decisions must be placed in a position in which they may effectively make known their views on the evidence on which the contested measure is based]; Case C-277/11, M. M. v Minister for Justice, Equality and Law Reform and Others, ECLI:EU:C:2012:744, para. 89 (Nov. 22, 2012) [on the applicability of the right to be heard to decisions taken by national authorities in asylum procedures]. In the literature see Madalina Moraru, *The European Court of Justice Shaping the Right to Be Heard for Asylum Seekers, Returnees, and Visa Applicants: An Exercise in Judicial Diplomacy*, 13 Eur. J. Legal Stud. 21–62 (2021); Marcelle Reneman, EU Asylum Procedures and the Right to an Effective Remedy 93(2014).

[128]Ozkul, *supra* note 1, at 41.

[129]*Id.* at 44.

[130]*Id.* at 45.

[131]*Id.* at 50.

[132]*Id.* at 25.

[133]*Id.* at 20.

[134]Matthias Leese, Simon Noori & Stephan Scheel, *Data Matters: The Politics and Practices of Digital Border and Migration Management*, 27 Geopolitics 5–25, 13 (2022).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

relying on research showing the increased risk of misclassification for black women and other women of color.[135] In the UK, the Home Office accused tens of thousands of students of cheating in a government-approved English language test based on an automated voice recognition system.[136] For students with invalid test results, the Home Office cancelled their visas and refused any pending applications; others were taken into immigration detention in the UK and subsequently deported.[137] As it was later proven through several audits and expert opinion, the system was riddled with errors and lacked accuracy in generating evidence.[138] The quality of input data – processed by the system to generate evidence – represented a further issue. If data are not correct, up to date, and relevant, the evidence generated will be inaccurate. In the context of mobile phone data processing, civil society organizations have pointed out how mobile phones are often used by multiple people, leading to contradictory and wrong assessments. Finally, it is questionable whether speech or dialect recognition is a suitable method to prove "fraud of ID documents and narratives"[139] in asylum procedures, as it currently is in Germany.

Resorting to the concept of evidence has relevant legal consequences for two reasons. First, the law sets admissibility standards and rules to collect evidence that applies to automated evidence. For instance, in the context of asylum procedures, the Qualification Directive[140] sets out evidence rules for assessing facts and circumstances in applications for international protection. More specifically, Article 4 of the Qualification Directive requires evidence to be assessed individually and in cooperation with the applicant.[141] These rules shall be respected even when evidence is automatedly generated. Moreover, even when automated, evidence must comply with the relevant admissibility and exclusionary rules of evidence. Concerning phone data analysis, civil society organizations have criticized the practice for violating privacy and data protection rights and challenged this practice in different countries.[142] If automated systems process data collected in breach of data protection laws, the legality of the evidence generated based on such processing will also be impacted. In a case brought before the German Federal Administrative Court, denying international protection for asylum seekers was annulled because it was based on illegally collected mobile phone data.[143]

Second, the concept of evidence triggers the procedural rights of the individual affected by the decision, including the right to access and challenge the evidence against them. Granting procedural rights to challenge automated evidence is particularly important in asylum proceedings where inaccurate automated evidence can have a snowballing effect on the applicant's credibility. Under EU law, procedural rights are enshrined in Articles 47 and 41 of the

[135]Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *in* Proceedings of the 1st Conference on Fairness, Accountability and Transparency 77–91 (2018).

[136]Maxwell and Tomlinson, *supra* note 1, at 6.

[137]*Id.*

[138]Finally, the Upper Tribunal concluded that no weight at all can now be placed on the ETS evidence. See *id.* at 30.

[139]Ozkul, *supra* note 1, at 45.

[140]Directive 2011/95/EU, of the European Parliament and of the Council of December13, 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), 2011 O.J. (L 337).

[141]Gregor Noll, *Evidentiary Assessment in Refugee Status Determination and the EU Qualification Directive*, 12 Eur. Pub. L. (2006).

[142]*See among others*, High Court of Justice Queen's Bench Division, R(HM and MA and KH) v Home Dep, Case No. CO/4793/2020 and CO/577/2021, (Mar. 25, 2022), https://www.bailii.org/ew/cases/EWHC/Admin/2022/695.html (last accessed Feb. 27, 2024).

[143]Verwaltungsgericht Berlin [VG Berlin] [Administrative Court of Berlin], Case No. 9 K 135/20.A, (Jun. 1, 2021), https://www.asyl.net/fileadmin/user_upload/29743.pdf (last accessed Feb. 27, 2024) and Bundesverwaltungsgericht [BVerwG] [German Federal Administrative Court], Febr. 16, 2023, AsylMagazine 9/2021, 338. For an analysis of the judgments see Francesca Palmiotto & Derya Ozkul, *"Like Handing My Whole Life Over": The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures*, VerfBlog (Feb. 28, 2023), https://verfassungsblog.de/like-handing-my-whole-life-over/ (last accessed Feb. 27, 2024).

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

CFREU. More specifically, the Court has derived the right to access the case file and the right to comment on evidence from the principle of equality of arms under Article 47 CFREU.[144] Additionally, the Court clarified that the right to be heard, which derives from Article 41 CFREU, requires that the addressees of a decision that significantly affects their interests must be in a position whereby they may effectively make known their views on the evidence upon which the decision was based.[145] This right implies that the parties concerned must be informed of the evidence adduced against them.[146] These procedural rights also apply to asylum procedures[147] and common visa policies.[148] As explained by Moraru, the Court recognized a high threshold of disclosure of evidence by public authorities in common visa policies and the refusal of entry decisions in the cases *ZZ* and *R.N.N.S. and K.A.*,[149] developing "a constitutional view of a common principle of *audiatur et altera pars* which applies to all cases where the legal status of an individual is rejected or denied based on threats to public policy or national security."[150]

Interestingly, in *Ligue de Droit ABSL*, the Court refers to their judgments in *ZZ* and *R.N.N.S. and K.A.* when considering the compatibility between automated analyses based on AI systems and the right to an effective remedy. According to the judgment, the issues are twofold. First, using artificial intelligence technology in self-learning systems ("machine learning"), which can be modified without human intervention, does not provide sufficient certainty for the human reviewer and the data subject and should, therefore, be precluded. Second, opacity in AI systems prevents understanding the reasons why a given program arrived at a positive match, hence depriving data subjects of their right to an effective judicial remedy enshrined in Article 47 of the Charter.[151] In this regard, the Court sets transparency rights for data subjects to foster their right to an effective remedy against decisions based on automated analyses. First, in administrative procedures, the person concerned must be able to "understand how those criteria and those programs work, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress."[152] Second, in the context of judicial redress, the person and the court involved "must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken *including the pre-determined assessment criteria and the operation of the programs applying those criteria*."[153]

One should note that neither the GDPR nor the AI Act provides this level of transparency to the individual (end-user or data subject). Nonetheless, by assessing the use of automated evidence under the right to an effective remedy, the Court was able to derive specific transparency rights for individuals, including the possibility to understand and examine the criteria and operations of the programs.

## V. Overview of Categories and Guiding Questions

While the general provisions of GDPR cover every type of automated decision, the specific safeguards enshrined in Article 22 apply only to cases where the decision is solely automated. In practice, most automated systems do not make final decisions but rather assist and support

[144]*See among others*, Case C-450/06, Varec SA v Belgian State, 2008 E.C.R. I-00581, para. 47; Case C-199/11, Europese Gemeenschap v Otis NV and Others, ECLI:EU:C:2012:684, para. 71 (Nov. 6, 2012).

[145]*See G. J. Dokter*, Case C-28/05 and cited case law at para. 74.

[146]Case Case C-32/95 P, *Commission* v. *Lisrestal and Others*, 1996 E.C.R. I-5373, para. 21.

[147]*See M. M.*, Case C-277/11. In the literature see RENEMAN, *supra* note 127, at 86 and 95.

[148]*R.R.N.S. and K.A.*, Joined Cases C-225/19 and C-226/19, para. 43.

[149]Case C-300/11, ZZ, ECLI:EU:C:2013:363, (4 June 2013); C-225/19, R.N.N.S. and K.A., ECLI:EU:C:2020:95, (24 November 2020).

[150]Moraru, *supra* note 127, at 45.

[151]*Ligue des droits humains ASBL*, Case C-817/19, para.195.

[152]*Id.* para. 210.

[153]*Id.* para. 211.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

human decision-makers. How can automated systems be defined as such when the outcome is a decision and the level of human intervention is sufficiently "meaningful"? This Section provides a conceptual framework to categorize new technologies used in migration and asylum decision-making in Europe. In addition to solely automated decisions, I have illustrated three further categories of ADM: automated triage, suspicion, and evidence.

These categories focus on the outputs of the automated system; they do not define the overall decision-making process and are not isolated in watertight compartments. In some cases, the same system performs more than one role in the decision-making processes. Regarding visas, automated systems classify the application, make positive decisions if no issue arises, or flag it to a human case worker when assessed as suspicious. Likewise, the fraud detection system detecting "sham marriages" in the UK primarily flags cases requiring further investigation. At the same time, the risk assessment will be "available to the caseworker if an application for permanent residence is submitted and is considered as part of that decision," hence it is usable in evidence.[154] Therefore, automation can serve different purposes within the same decision-making process involving different rights that deserve equal protection. As the previous sections have shown, the classification of ADM systems always requires an analysis *in concreto,* focusing on the following guiding questions.

### *Is the outcome a decision?*

First and foremost, the requirement of an individual decision sets the boundaries between automated decision-making from other practices emerging from the increasing digitalization of border and migration management.[155] It is only in the first case that the decision has legal or significant effects on the data subject.

### *What is the role of the human in relation to the outcome?*

The GDPR takes a step further, narrowing down the scope of application of Article 22 GDPR to only those decisions taken "without human involvement."[156] The second step requires focusing on the role of the human in relation to the outcome. A decision is solely automated when the human is absent, or their intervention is not meaningful. Only positive decisions in visas, residency, and citizenship decision-making are automated. When the human involvement is sufficiently meaningful to exclude the applicability of Article 22 GDPR, the next step is to analyze the role of the automated output in the process.

### *What is the role of the human in relation to the output?*

Within the umbrella term of part-ADM, the role of the automated system's output in the process and how humans use it largely differs. In automated triage, the system classifies a new case or application based on the automated assessment; the human can get a case assigned or be required to take follow-up actions. Examples include the "visa streaming algorithm" and automatic detection of "sham marriages" in the UK, the risk-assessment tool used in the Netherlands to screen employment sponsorships, the EU-funded project iBorderCtrl, and the automated case-management system for the EU settlement scheme. In automated evidence, the system provides information or an expert assessment humans use to prove a fact relevant to the decision. Systems generating evidence assess the reliability of asylum seekers' claims and include language categorization, mobile phone data analysis, and biometric identification.

[154]Ozkul, *supra* note 1, at 30.

[155]*See generally* Jean-David Ott & Eleonora Testi, Digitalisation of Asylum Procedurs: Risks and Benefits, AIDA 34 (2022), https://asylumineurope.org/wp-content/uploads/2022/01/Digitalisation-of-asylum-procedures.pdf (last accessed Feb. 27, 2024).

[156] Article 29 Working Party, *supra* note 31, at 20.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

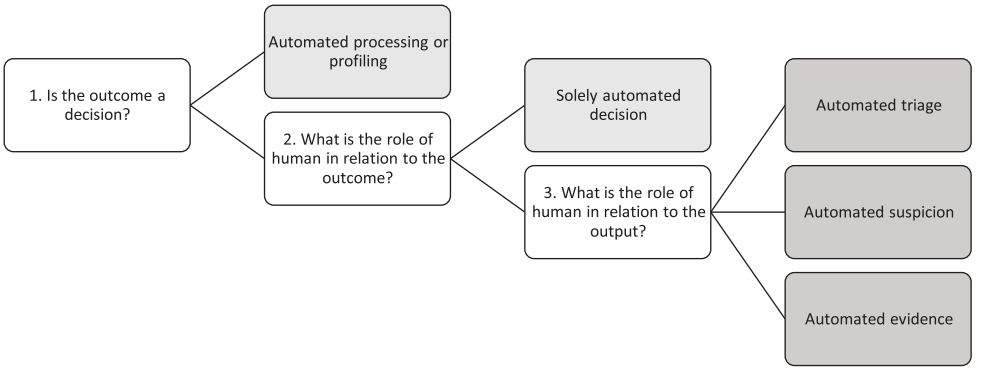


**Figure 1** - Guiding questions and classification of ADM systems.

### *What fundamental rights are at stake?*

Every typology of ADM systems can have adverse effects on individuals. Scholars have analyzed the consequences that automated systems can have for migration and border management,[157] refugee procedures,[158] and governance,[159] leading to new forms of surveillance,[160] discrimination,[161] and stigmatization[162] of migrants, asylum seekers, and refugees. Defining and classifying ADM systems is the first crucial step to investigating each system's legal challenges to fundamental rights. A solely automated decision, for instance, raises issues of the right to have a reasoned decision and the right to be heard; automated triage poses risks, among others, to the right to non-discrimination; automated evidence is strictly linked to procedural fairness and the right to a fair trial. Contrary to what Article 6 of the AI Act suggests, automated systems presents a risk of harm to fundamental rights, even when triaging applications, flagging individuals or providing evidentiary elements to decision-makers. Dissecting decision-making allows us to identify what fundamental right is at stake and what tools can be used to safeguard individuals.

In the field of migration and asylum, it is worth highlighting two important concerns. The first is how the safeguards stemming from fundamental rights, such as the right to a reasoned decision or access to the file, should be interpreted in the face of *new* challenges raised by automation. For this purpose, the CJEU case law on risk assessment represents an important point of reference. Further, technical solutions proposed in the literature, such as algorithmic fairness, explainability, and other design approaches for automated systems,[163] need to be analyzed in the specific context of migration and asylum governance from an interdisciplinary perspective that takes into account the law and computer science behind these systems and also the perspectives of migrants and

[157]See among others Ana Beduschi, *International Migration Management in the Age of Artificial Intelligence*, 9 MIGRATION STUD. 576–596 (2021); Leese, Noori & Scheel, *supra* note 134; RESEARCH HANDBOOK ON INTERNATIONAL MIGRATION AND DIGITAL TECHNOLOGY, (Marie McAuliffe ed., 2021); Petra Molnar, *AI and Migration Management*, in THE OXFORD HANDBOOK OF ETHICS OF AI (Markus D. Dubber, Frank Pasquale & Sunit Das ed., 2020).

[158]Niamh Kinchin, *Technology, Displaced? The Risks and Potential of Artificial Intelligence for Fair, Effective, and Efficient Refugee Status Determination*, 37 L. CONTEXT (2021).

[159]Kristin Bergtora Sandvik, *The Digital Transformation of Refugee Governance*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL REFUGEE LAW 1007–1026 (Cathryn Costello, Michelle Foster & Jane McAdam ed., 2021).

[160]Raluca Csernatoni, *Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management*, 27 EUR. SEC. 175–200 (2018).

[161]Achiume, *supra* note 92.

[162]Achraf Farraj, *Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers.*, 42 COLUM. HUM. RTS L. REV. 891–941.

[163]See among others, Veale, Van Kleek, and Binns, *supra* note 123; Jon Kleinberg et al., *Algorithmic Fairness*, 108 AEA ARTICLES AND PROCEEDINGS 22–27 (2018); Matt J. Kusner et al., *Counterfactual Fairness*, ARXIV:1703.06856 (2018), http://arxiv.org/abs/1703.06856.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

asylum seekers. The second concern addresses the risk that automation may exacerbate old migration and asylum governance issues. For instance, using automated systems to flag individuals as suspicious further blurs the boundaries between migration and criminal enforcement. Moreover, automated evidence risks creating non-refutable sources of evidence against asylum seekers in already "deeply dysfunctional" procedures, even without automation.[164] Whether EU asylum and migration law is sufficiently equipped to face the new challenges that automation brings remains a crucial question that requires further research.

## D. Conclusions: Beyond Automated Decisions

ADM in the public sector is a complex phenomenon. Automated systems flag applications, profile individuals, determine the workflow, and provide expert assessments, but they rarely replace humans. In this complexity, understanding when a decision was automated is the puzzle that prompted this work. In light of the lack of public information about ADM systems, the mapping report by Derya Ozkul represented a much-needed empirical study that made the analysis possible.

This Article combined empirical findings with a legal analysis of ADM under EU law and showed how the concept of "solely automated decision" fails to grasp the reality of ADM in practice. Moreover, it has also claimed that an ex-ante risk-based approach at the heart of the AI Act provides limited protection to individuals.[165] Despite the welcomed addition of the right to explanation the AI Act, in order to address the harm caused by ADM, design requirements must be coupled with ex-post rights, remedies, and transparency towards end-users. Finally, while it is acknowledged that algorithmic decision-making has implications for human rights[166] regardless of their technical characteristics, the AI Act regulates only systems that fulfill the definition of AI in Article 3. To address this gap, this Article proposes to move beyond the concept of "automated decisions" and complement the legal protection in the GDPR and AI Act with a taxonomy that can inform a fundamental rights analysis.

The proposed approach has a theoretical, doctrinal, and normative value. First, it brings conceptual clarity where regulatory categories fail to grasp the reality of ADM. It allows us to analyze the complex ways in which automation augments decision-making and accounts for their differences.

Second, it pinpoints what general laws apply beyond tech regulation. Focusing on the overall decision-making process and the role of automation therein allows us to shed light on the applicable legal framework. Beyond the legal definition of automated decisions, the Article has classified automated systems into three categories: automated triage, suspicion, and evidence. The proposed categorization allows us to uphold automated systems to the same standards required for human decision-making.[167] Also, in the automation age, suspicion must be reasonable. Even when automated, evidence must comply with the rules on its collection and admissibility. While automation brings new challenges, it must also follow "old" rules governing human decision-

[164]Gregor Noll, *Credibility, Reliability, and Evidential Assessment*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL REFUGEE LAW 607–626 (Cathryn Costello, Michelle Foster & Jane McAdam ed., 2021); HILARY EVANS CAMERON, REFUGEE LAW'S FACT-FINDING CRISIS: TRUTH, RISK, AND THE WRONG MISTAKE (2018).

[165]The lack of rights and remedies for the end-user in the AI Act was criticized in the EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (last accessed Feb. 27, 2024) and by scholars including Nathalie A. Smuha et al., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, SSRR, (2021), https://Articles.ssrn.com/abstract=3899991 (last accessed Feb. 27, 2024) and Veale & Zuiderveen Borgesius, *supra* note 10.

[166]Council of Europe's, Algorithms and Human Rights, supra at 4.

[167]On the application of administrative law principles to ADM in the UK see Cobbe, *supra* note 15.

https://doi.org/10.1017/glj.2023.112 Published online by Cambridge University Press

making. In this sense, one has to acknowledge the limited function of the GDPR as a data protection framework; it is not a panacea for any issue raised by automation.[168]

Third, it provides normative arguments to delimit their employment or require additional safeguards for fundamental rights-compliant use. For instance, transparency in automated evidence – which goes beyond "the logic involved" and requires understandability and access to the criteria and operations of the programs – can be derived from the right to an effective remedy. The case law of the CJEU on risk assessments in border control is an important reminder of the role of fundamental rights beyond data protection law in the automation era. In all three cases, the Court was asked to assess the compatibility of EU law (Opinion 1/15 and Ligue de Droit) or national law (La Quadrature du Net) with the right to privacy and data protection enshrined in Articles 7 and 8 of the CFREU. In addressing these questions, the Court derived additional safeguards for part-ADM from the Charter's fundamental rights, including the right to non-discrimination and an effective remedy (Articles 21 and 47 CFREU). In the case law on risk assessment, the CJEU provided legal protection for part-ADM from a fundamental rights-oriented interpretation of EU law. To do so, the Court unpacked automated decision-making in various phases, considering how automation affects fundamental rights involved in each segment. When considering risk assessment to flag individuals as "suspicious," the Court derived design requirements for automated systems – such as reliability, topicality, and specificity of models and criteria – from Articles 7, 8, and 21 of the Charter. When considering automated risk assessment providing evidence for decision-makers, the Court derived transparency rights from Article 47 CFREU.

In conclusion, this Article has attempted to draw a clearer picture of ADM in the field of migration and asylum law. As public administrations keep introducing automated systems in decision-making, it is crucial to conceptualize ADM in other public law areas. Moreover, for the effective applicability of the high-risk classification rules in the AI Act, it is crucial to have a clear conceptual framework to understand, analyze and assess when, how and which fundamental rights are at stake when AI systems support decision-making in critical areas, such as migration and asylum, education or criminal justice. The guiding questions in Section III can be useful for researchers in other fields to theorize new categories of ADM or borrow the proposed ones.

**Acknowledgements.** I want to thank the AFAR team and all Centre for Fundamental Rights members at the Hertie School for their support and feedback throughout the research. A special thanks goes to Prof. Cathryn Costello and Dr Derya Ozkul for the fruitful discussions and comments. I would also like to thank Prof. Sean Rehaag and Dr Simona Demkova for their feedback on an earlier version of this Article.

**Funding Statement.** This research is part of the Algorithmic Fairness for Asylum Seekers and Refugees (AFAR) Project, funded by the Volkswagen Foundation under its Challenges for Europe Programme.

**Competing interests.** The author declares none.

[168]On the limitation of data protection frameworks, see in particular the brilliant work by Renieris, *supra* note 16.

**Cite this article:** Palmiotto F (2024). When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis. *German Law Journal*, 1–27. https://doi.org/10.1017/glj.2023.112