Doing refugee right(s) with technologies? Humanitarian crises and the multiplication of "exceptional" legal states

Twigt, M.A.

Refugee Survey Quarterly, 2023, **00**, 1–21
https://doi.org/10.1093/rsq/hdad020
Article

Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of "Exceptional" Legal States

Mirjam Twigt *

ABSTRACT

Like borders, refugee protection settings beyond the EU often serve as testing grounds for technologies. This article takes a socio-legal perspective to show how humanitarian experimentation in these contexts is made possible through different, interacting challenges to sovereignty. It argues that the understanding that actors or their positions are "exceptional" allows for and justifies data practices that would otherwise not be legally permissible. Examples of data practices in refugee protection settings are connected to work in geopolitics, science and technology studies, and sociology of law.
The article shows how the position of the United Nations High Commissioner for Refugees (UNHCR) as negotiator on behalf of refugees and an emergency-driven techno-solutionism not only interacts with the already precarious legal context most people seeking refuge find themselves in. It coincides with the legal positioning of International Organisations and with citizenship-oriented conceptions of privacy, further constituting people seeking refuge as (digital) rights optional. This is problematic not least because of concerns about adequate data protection or the implications of bias. Data flows and algorithms are generative of the politics of contemporary societies, implying that the structural undermining of digital rights of people seeking refuge in the present can also hinder their access to rights in the future.

KEYWORDS: refugee protection, digital rights, automation, International Organisations (IOs), international law, sovereignty, accountability

* Institute for History, University of Leiden, The Netherlands. Email: m.a.twigt@hum.leidenuniv.nl. The research was carried out whilst the author was a Postdoctoral Fellow for REF-ARAB: Refugee Protection and the Arab Middle East at the Faculty of Law, University of Oslo, Norway.

The author is grateful to Maja Janmyr, Nora Milch, Sanjeeb Hossain, Anna Kvittingen, Charlotte Lysa, Helene Gundhus, Katja Franko, Kristina Bergtora Sandvik, Andrea Grønningsæter, Lewis Turner, Stephan Scheel, and Nina Amelung. Gratitude also goes out to participants of the Forced Displacement Workshop series for Junior Scholars, specifically David Hughes, Ghuna Bdiwi and Eliza Bateman for their kind and thorough feedback on earlier versions of this article and to the anonymous peer reviewers for their helpful response.

The research was supported by the Research Council of Norway's Independent Projects (FRIPRO) programme under project number 286745.

1. INTRODUCTION

"When refugees flee war, they become citizens of a country called UNHCR until they return to their country or are resettled. Does this country UNHCR not have the right to own the data of its citizens?"[1] With these words Imad Malhas, the founder of IrisGuard, seeks to legitimise the registration of "iris-scanning fraudproof biometrics" by the United Nations High Commissioner for Refugees (UNHCR).[2] Back in 2013, the technology his company developed was key in trialling the capturing of biometric data upon registration for refugee protection with UNHCR Jordan. These days, obtaining biometric data by drawing on developments in Artificial Intelligence (AI) is standard UNHCR registration practice. The UN refugee agency has obtained the biometric information of at least 8 million people, which was supposed to be stored on a single database by the end of 2019.[3]

Much of the reasoning behind UNHCR's biometric registration procedures is grounded in the conflation of a person's digital identity with their legal identity. The emphasis is put on Sustainable Development Goal 16.9 – universal access to a legal identity – and the desire that "no one should be left behind".[4] The problem is, however, that the registration of biometric information by UNHCR does not guarantee legal recognition or access to rights. Contrary to the assertion by Malhas in the above quote, UNHCR is neither a country nor a State. It is an international organisation (IO) with a legal mandate to provide protection and assistance to the world's refugees.[5] In this article, an IO is understood to be "an organization established by agreement under international law, with at least one organ with a will of its own (*volonté distincte*) and which possesses international legal personality".[6] As such, UNHCR is subject to international law and bears international human rights responsibilities.[7] But it has legal immunity regarding domestic and regional legislations. And it is well known that UNHCR and other organisations involved in refugee governance have problems with accountability. There are ample legal, political, and practical reasons why accountability towards people it is mandated to protect tends to fall short.[8]

UNHCR has positioned itself as negotiator of "protection space", especially in States that are geographically located in South-East Asia and the Middle East and are non-signatory to the 1951 Refugee Convention and its 1967 Protocol.[9] In this capacity, the UN refugee agency along with other UN agencies is deeply involved in governing practices that are generally associated with responsibilities of sovereign States. The ways these organisations

[1] C. Nedden, & A. Dongus, "Getestet an Millionen Unfreiwilligen tested on millions of non volunteers)", *Die Zeit*, 17 Dec. 2017, available at: https://www.zeit.de/digital/datenschutz/2017-12/biometrie fluechtlinge-cpams-iris-erkennung-zwang (last visited 19 Jan. 2023).

[2] United Nations High Commissioner for Refugees – Innovations (UNHCR – Innovations), *Using Biometrics to Bring Assistance to Refugees in Jordan*, Geneva, UNHCR, 30 Aug. 2016, available at: https://www.unhcr.org/innovation/using-biometrics-bring-assistance-refugees-jordan (last visited 19 Jan. 2023).

[3] M. Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, 20(6), 2021, 581–599.

[4] B. Manby, "Preventing Statelessness among Migrants and Refugees: Birth Registration and Consular Assistance in Egypt and Morocco", *LSE Middle East Centre Paper Series*, No. 27, 2019; K. Sandvik, "Is Legal Technology a New "Moment" in the Law and Development Trajectory?" *Antipode Online*, 4 Dec. 2019, available at: https://antipodeonline.org/2019/12/04/legal-technology-law-and-development/ (last visited 19 Jan. 2023); L. Stielike, *The Crisis of European Migration Governance and the Promises of Big Data*, Conference Digital Fortress Europe: Exploring Boundaries Between Media, Migration and Technology, Brussels, Belgium, 30 Oct. 2019.

[5] United Nations General Assembly (UNGA), *Statute of the Office of the United Nations High Commissioner for Refugees*, UN doc A/RES/428(V), 14 Dec. 1950 (UNHCR Statute).

[6] S. Johansen, *The Human Rights Accountability Mechanisms of International Organizations*, Cambridge, Cambridge University Press, 2020, 3.

[7] *Ibid.*, see also M. Janmyr, *Protecting Civilians in Refugee Camps: Unable and Unwilling States, UNHCR and International Responsibility*, Leiden, Martin Nijhoff Publishers, 2014.

[8] K. Sandvik & K. Jacobsen (eds.), *UNHCR and the Struggle for Accountability. Technology, Law and Results Based Management*, Oxon and New York, Routledge, 2016.

[9] M. Jones, "Moving Beyond Protection Space: Developing a Law of Asylum in South-East Asia", in S. Kneebone, D. Stevens, & L. Baldassar (eds.), *Refugee Protection and the Role of Law: Conflicting Identities*, London, Routledge, 2014.

operate to order information, classify populations, and provide benefits closely resembles developments in how State actors are deploying new business models and modes of public administration.[10] UNHCR and other IOs are also at the forefront of the datafication of procedures generally associated with the welfare state and border policing.[11] These practices do not necessarily reduce the power of State actors. As the intrinsically partial "Seeing like a State" practices of IOs are increasingly data-driven,[12] scholars have been asking urgent questions about their long-term consequences and normative implications.[13] Concerns about the digitisation of refugee governance go beyond concerns about risk of failure.

Experimental technologies can also bring about harm if they work as intended.[14] There are some known examples of harms inflicted but the extent of potential consequences of humanitarian digital practices are largely speculative.[15] This is not the same as being unforeseen: speculation can serve as a critical compass that signals the need for being responsive.[16] This article contributes to discussions on the digital transformation of refugee protection by providing additional insights into how complex legal environments allow for treating people seeking refuge as (digital) rights optional. A socio-legal perspective is used to explore how multiple legal positions – often present in refugee protections settings – are established as "exceptional". This provides legitimation for the gathering of vast amounts of data in humanitarian settings and technology use that otherwise – for instance, if it would concern EU citizens – would not be legally permissible and/or would require more thorough legal safeguards. As this study engages with what "exceptions" allow, the violent nature of sovereignty becomes clear.[17] Positioning different yet interacting conditions as "exceptional" allow for legitimation and legalisation of governmental differentiation. It allows, as Ghassan Hage put it, the establishment of "*another* governmentality directed at subjects whose lives are

[10] M. Hildebrandt, *Slaves to Big Data. Or Are We?* IDP 2013, the 9th Annual Conference on Internet, Law & Politics, Barcelona, 25 Jun. 2013.

[11] P. Andreassen, A. Kaun, & K. Nikunen, "Fostering the Data Welfare State: A Nordic Perspective on Datafication", *NORDICOM Review*, 42(2), 2021, 207–223; P. Molnar & L. Gill, *Bots at the Gate. A Human Rights Analysis of Automated Decision-Making in Canadás Immigration and Refugee System*, International Human Rights Program and the Citizen Lab, Toronto, 2018.

[12] J. Scott, *Seeing Like A State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven, Yale University Press, 1998. See also K. Lohne & K. Sandvik, "Bringing Law into Political Sociology of Humanitarianism", *Oslo Law Review*, 4(1), 2017, 4–27.

[13] Some key sources are T. Achiume, *Racial and Xenophobic Discrimination, Emerging Digital Technologies in Border and Immigration Enforcement*, New York, UN General Assembly #75, A/75/590, 2020; B. Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and "Big Data"", *International Review of the Red Cross* 99(904), 2018, 179–209; G. Hosein & C. Nyst, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries*, London, Privacy International, 2013; K. Jacobsen & L. Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care", *Disasters*, 43, 2019, 151–168; K. Weitzberg, M. Cheesman, A. Martin, & E. Schoemaker, "Between Surveillance and Recognition: Rethinking Digital Identity in Aid", *Big Data & Society*, 8(1), 2021; K Sandvik, "Digital Refugee Lawyering: Risk, Legal Knowledge, and Accountability", *Refugee Survey Quarterly*, 40(4), 2021, 414–432.

[14] K. Jacobsen, *The Politics of Humanitarian Technology. Good Intentions, Unintended Consequences and Insecurity*, London, Routledge, 2015.

[15] Agence France-Presse, "Hacking Attack on Red Cross Exposes Data of 515,000 Vulnerable Persons", *Guardian*, 19 Jan. 2022, available at: https://www.theguardian.com/world/2022/jan/20/hacking-attack-on-red-cross-exposes-data-of-515000-vulnerable-people (last visited 9 Jan. 2023); Human Rights Watch, "New Evidence that Biometric Data Systems Imperil Afghans – Taliban Now Control Systems with Sensitive Personal Information", New York, Mar. 2022, available at: https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans (last visited 9 Jan. 2023); Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent – Bangladesh Provided Myanmar Information that Refugee Agency Collected", New York, 15 Jun. 2021, available at: https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent (last visited 9 Jan. 2023).

[16] M. Puig de la Bellacasa, "Matters of Care. Speculative Ethics in a More than Human World", Minneapolis, Minnesota University Press, 2017.

[17] G. Agamben, *State of Exception*, Chicago, University of Chicago Press, 2004. See also: A. Alijla, "Palestine and the Habeas Viscus: An Autoethnography of Travel, Visa Violence and Borders", *Borders in Globalization Review*, 1(2), 8–22, 2020; A. Alijla, "Gazzawi as Bare Life? An Auto-ethnography of Borders, Siege and Statelessness", *Contemporary Levant*, 4(2), 2019, 177–182.

constructed as less valuable in themselves, and against whom more repressive and violent forms of subjugation can be deployed with less difficulty."[18]

Refugees – like any other citizen, non-, and not-yet citizens – do engage in rights-claiming acts.[19] But the article points out how experimental data practices in refugee-hosting are enabled through different legal exceptions and rationalities which further allow for constituting people seeking refuge as rights-optional non-citizens. And it seems that a figure – a sovereign – to direct calls to for more rights is absent. The question therefore remains, following Agamben, if it is only through claiming rights from sovereign power that a qualified life under biopolitical governance can be ascertained? It seems that the real or imagined consequences of data-driven governance serve to further entrench exclusionary, State-centred conceptions of citizenship and can foreclose alternative futures.[20]

This article should not be misread as an argument against technologies. Such a position does not speak to the realities of most people, including refugees. Of course, technological innovations can also benefit refugees, and technology and infrastructure will also allow alternatives and contestations, which explains the importance of data-activism.[21] Louise Amoore's perspective is useful in understanding resistance and rights claim-making, not in opposition to or outside of, but in relation to the iterative learning and attributive power of machines and humans.[22] She urges us – social scientists, scholars of ethics, and humanities – to find ways to engage with the assumptions and arrangement of algorithms.[23]

This brings me to a brief note on my methodology. Ethnographic studies on digital connectivity and refugee protection (Jordan, 2012 – 2020; Kurdish Region of Iraq (KRI), 2020 – 2023) have strongly informed my thinking and further explain the geographical focus of examples given on digital transformations. Earlier, I have shown how digital connections are perhaps even more crucial in the lives of people who have become forcefully displaced than for sedentary populations, not least because they often need to navigate prolonged legal precarity.[24] Here, I draw on few empirical examples from these studies. Rather, I connect studies and reporting on data practices in refugee protection to studies from science and technology studies (STS), sociology of law, migration studies, political geography etc. The datafication of humanitarian systems is very hard to study, given the security barriers, the absence of transparency and other limitations to access. Of course, more work needs to be done to better understand how these systems work (or do not work) in practice and how they interact with the border work of State actors. The settings upon which I draw throughout this article are not exceptional; it is the positioning of people, times and circumstances, places, organisations, and States as "exceptional" that this study seeks to unravel.

The structure of this article is as follows: Section 2 clarifies the terminology used and points to some of the nuances required in debates on technology and data practices in refugee protection. In Section 3, I examine elements common to digital transformations associated with refugee governance, particularly when it concerns precarious protection settings. This connects to topics frequently discussed in academic literature on humanitarian interventions, such as the emphasis on crisis and emergency,[25] the

[18] G. Hage, *Is Racism an Environmental Threat*? Cambridge, Polity Press, 2017, 50.
[19] E. Isin, "Doing Rights with Things: The Art of Becoming Citizens", in P. Hildebrandt, K. Evert, S. Peters, M. Schaub, K. Wildner, & G. Ziemer (eds). *Performing Citizenship. Bodies, Agencies, Limitations*, London, Palgrave MacMillan, 2019, 45–56.
[20] L. Amoore, *Cloud Ethics; Algorithms and the Attributes of Ourselves and Others*, Durham, Duke University Press, 2020.
[21] S. Milan, J. Gray, S. Baack, H. Kennedy, L. Dencik, M. Gutiérrez, L. Horgan, P. Dourish, T. Lijster, P. de Vries, N. van Doorn, J. Overwijk, & L. van der Velden, "Data-activism", *Krisis – Journal for Contemporary Philosophy*, 1, 2018.
[22] Amoore, *Cloud Ethics*.
[23] *Ibid*., 158.
[24] M. Twigt, *Mediated Lives. Waiting and Hope among Iraqi Refugees in Jordan*, New York, Berghahn Books, 2022.
[25] G. Calhoun, *A World of Emergencies: Fear, Intervention, and the Limits of Cosmopolitan Order*, 35th Annual Sorokin Lecture, University of Saskatchewan, Saskatoon, Saskatchewan, Canada, 4 Mar. 2004.

marketisation of aid,[26] techno-solutionism, and 'neophilia' – the love of innovations and quick fixes.[27] Less academic attention has been given to the topic discussed in Section 4: the legal positioning of IOs and whether this makes them much desired partners for private bodies to team up with. Even if their data protection policies were legally enforceable, they set mediocre data protection standards compared to those of EU data legislation, for instance. Section 5 explores how persisting citizenship-oriented conceptions of privacy resonate with older othering practices, while newer characteristics of digital technologies can further restrict access to rights. The potential that algorithms in interaction with other technological and sociopolitical developments and human short-sightedness will further restrict space for claim-making for refuge and by people seeking refuge is likely. This demonstrates the need for careful scholarly and practical engagement.

2. SITUATING NEWER TECHNOLOGIES

The capturing of body-centric information and other data for migration governance purposes has a long history which is closely interlinked with colonialism, the institutionalising of racism and policing.[28] Furthermore, trialling techniques and technologies in refugee governance is not new either.[29] What is newer is that technological developments – the increase in computational power coupled with vast quantities of data and algorithmic innovations – have enabled the capture of attributes that were previously imperceptible,[30] and that the extracted data is reconfigured into complex assemblages.[31] These can then be more easily remotely available to other actors who can use it for different purposes. The open-ended shifting lifecycle of data means that it can have multiple and simultaneous meanings, purposes, and effects at different times and places. The following empirical example provides some insights into ways in which data can travel and its influence on people's movement. I will then discuss key concepts and terminology used in this article, such as digitisation, different forms of data, and AI. This enables me to further question the beliefs behind "AI for social good" in subsection 2.3.[32]

2.1. Data travels

I encountered the possible consequences of data practices long before I became more aware of the potential ways in which data can travel. In 2012, my citizenship allowed me the mobility to conduct research for my master's thesis on the experiences of Iraqi refugees in Jordan who had received formal rejection for resettlement in the US. Because of general reluctance to share refugee protection responsibilities, this durable solution to refugees' prolonged legal uncertainty is in short supply. The decision-making is opaque. Most receive little or no

[26] S. Merry, *The Seductions of Quantification: Measuring Human Rights, Gender Violence and Sex Trafficking*, Chicago, Chicago University Press, 2016; M. Krause, *The Good Project: Humanitarian Relief NGOs and the Fragmentation of Reason*, Chicago, University of Chicago Press, 2014.

[27] T. Scott-Smith, "Humanitarian Neophilia: The "Innovation Turn" and Its Implications", *Third World Quarterly*, 37(12), 2016, 2229–2251.

[28] K. Weitzberg, "Unaccountable Census: Colonial Enumeration and its Implications for the Somali People of Kenya", *The Journal of African History*, 56(3), 2015, 409–428; K. Aas,"The body does not lie': Identity, Risk and Trust in Technoculture", *Crime, Media, Culture: An International Journal*, 2(2), 2016, 143–158; P. Arora, "Decolonizing Privacy Studies", *Television & New Media*, 20(4), 2018, 366–378; K. Leurs & P. Seuferling, "Migration and the Deep Time of Media Infrastructures", *Communication, Culture and Critique*, 15(2), 2022, 290–307.

[29] Jacobsen, *The Politics of Humanitarian Technology*.

[30] Amoore, *Cloud Ethics*.

[31] M. Lemberg-Pedersen & E. Haioty, "Re-assembling the Surveillable Refugee Body in the Era of Data-craving", *Citizenship Studies*, 24(5), 2020, 607–624.

[32] M. Madianou, "Nonhuman Humanitarianism: When 'AI for good' can be Harmful", *Information, Communication & Society*, 24(6), 2021, 850–868.

information on it.[33] This was somewhat different for those eligible for the Special Immigration Visa (SIV) which was made available for Iraqi nationals who had been employed by the US government or US forces during the occupation of Iraq.[34] The selection procedures included security screening by the US Department of Homeland Security (DHS), on the premises of the Jordan office of the International Organisation of Migration (IOM). If a person's request was denied, they received a letter stating the reason for their rejection. My research consisted of semi-structured interviews with people who had received such a letter.[35]

One of the persons I spoke to was Sanad, a young Iraqi Assyrian man who had sought refuge in Jordan.[36] As he had worked as a translator for the US Army, he was eligible for an SIV. But Sanad had received a rejection letter citing "security reasons". He was convinced his rejection was due to his fingerprints. In 2006, on the streets of Baghdad, someone in his vicinity shot at US soldiers, who then retaliated. Sanad's friend was killed and Sanad, shot in the leg, was taken to prison. His fingerprints were taken, and he was interrogated for 11 days. It is impossible to say if his rejection of an SIV was directly or indirectly related to data gathered during this incident. But considering the persistence, transferability, and interoperability of personal data and the lack of a regulatory framework, his guess might be correct. I, like him, can only speculate. What this example shows is how the lack of transparency about how life-changing decisions are made and the uncertainty it creates have come to be (perceived as) connected to data practices.

Data gathered at one point in time for a particular purpose, can later resurface elsewhere. Sanad's data, collected and stored by an external State actor (the US Government), might have been used later to identify him as "risky" in a third country (Jordan). It is beyond the scope of this article to discuss what safeguards can be taken against the misuse of refugees' and migrants' data by State actors and regional actors such as the EU and/or under what circumstances such actors would be allowed to infringe on the digital rights of people on the move for security purposes. Instead, I look at the long relationship between security, aid and technology, particularly regarding the capture and circulation of biometric data and other very personal information.[37]

UNHCR's experimental usage of iris scans – not merely for registration but also for wider purposes such as the distribution of aid – is but one example of increasingly automated practices. These include and go beyond the digital capture of other biometric details such as voice and/or facial recognition[38]; the development of large platforms and databases to collect and share information with implementing partners, banks, etc.[39]; the use of information to distribute aid, including experimentation with blockchain for identification and cash distribution purposes[40]; statistics and algorithms geared to assess vulnerabilities and assist in decision-

[33] A. Garnier, L. Jubilut, & K. Sandvik, *Refugee Resettlement: Power, Politics and Humanitarian Governance*, New York, Berghahn Books, 2018.

[34] US Department of State – Bureau of Consular Affairs, *Special Immigrant Visas for Iraqi and Afghan Translators/Interpreters*, available at https://travel.state.gov/content/travel/en/us-visas/immigrate/siv-iraqi-afghan-translators-interpreters.html (last visited 9 Jan. 2023).

[35] This research took place as part of the Master's program International Development Studies, at Wageningen University & Research in The Netherlands. Ethical approval was received. Participants were in-depth informed about the research, its intent and potential outcomes and consented to partaking.

[36] Pseudonyms are used to preserve anonymity.

[37] Jacobsen, *The Politics of Humanitarian Technology*.

[38] International Committee of the Red Cross (ICRC), "Rewards and risks in humanitarian AI: an example", ICRC Blog, 6 Sept. 2019, available at: https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/ (last visited 19 Jan. 2023); J. Mebur, *The Voice ID Project: Verifying Recipients of Mobile Money Supported Humanitarian Cash Transfers in Somaliland*, London, GSMA, 2021.

[39] K. Holloway, R. Al Masri, & A. Abu Yahia, *Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crisis*, London, Humanitarian Policy Group, 2021.

[40] M. Cheesman, "Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity", *Geopolitics* 2020, 1–26; L. Macias, "Digital Humanitarianism in a Refugee Camp", in K. Smets et al. (eds.), *The Sage Handbook of Media and Migration*, London: Sage, 2020, 334–345.

making[41]; the use of chatbots for communication with communities and psychosocial counselling[42]; and predictive modelling.[43] This interacts with the aid sector's difficulties with developing an integrated, transparent and data-driven approach, also since funding for localised cybersecurity systems and policies is severely lacking.[44]

2.2. Digitisation, Datafication, and AI

AI refers to data-focused automated statistics, systems, and decision-making which draw upon advances in machine learning (ML) and natural language processing. Developments in AI have been key for enabling the use of biometrics for verification (one-to-one comparison), identification (one-to-many comparisons) and categorisation (deducing if an individual belongs to a group defined by selected attributes). AI is also used for chatbots, predictive modelling, automated decision-making, etc. The use of AI and Automation Decision-Making (ADM) is closely related to processes of digitisation and datafication. Digitisation is the "conversion and articulation of historically analogue information, processes, and actions through digital tools".[45] Datafication is the turning of numbers relating to our identity, societal positioning, and practices into data and datasets.[46] Often, the belief underlying datafication is that more data will result in more accurate and nuanced information about our behaviour in the present, but also concerning the future. ADM enhances the intensity of modern risk-assessment as it differentiates between information and the possibilities that are available in the present to act upon the future.[47] Prior to this, decision-making and planning was equally predicated on assessments of how the future would and should likely unfold, but arguably in a manner that was more reflexive of the recursive impact.

In the humanitarian sector, there is lack of a consistent definition and shared terminology regarding data.[48] Distinctions need to be made between personal and non-personal data and between sensitive and non-sensitive data. Personal data is information that can be traced back to features specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person. Non-personal data does not relate to any specific person, either because it was never linked to such features or because it was made anonymous. But like personal data, non-personal data can be sensitive. The classification of sensitive data depends on how the likelihood and severity of harms are assessed.

An algorithm has been defined as "a recipe composed in programmable steps . . . organizing and acting on a body of data to quickly achieve a desired outcome".[49] Through techniques like ML, algorithms are "trained" to recognise patterns and to classify them. They operate by learning from data, and this learning changes the process. The common idea that AI operates like a black box is rather misleading,[50] for it gives the impression that the errors

[41] K. Bansak, J. Ferwerda, J. Hainmueller, A. Dillon, D. Hangartner, D. Lawrence, & J. Weinstein, "Improving Refugee Integration through Data-driven Algorithmic Assignment", *Science*, 359(6373), 2018, 325–329.

[42] Madianou, "Nonhuman Humanitarianism: When 'AI for good' can be Harmful".

[43] A. Salah, "Can Big Data Deliver its Promises in Migration eRsearch?", *International Migration Research*, 60(2), 2022, 252–255.

[44] G. Coppi, *A Roadmap Beyond 2022*, Centre for Humanitarian Action, 11 Apr. 2022, available at: https://www.chaberlin.org/blog/humanitarian-digital-panorama-a-roadmap-beyond-2022-2/ (last visited 19 Jan. 2023).

[45] K. Sandvik, K. Jacobsen, & S. McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of the Red Cross* 99(904), 2017, 321.

[46] Andreassen, Kaun & Nikunen, "Fostering the Data Welfare State".

[47] P. Metcalfe & L. Dencik, "The Politics of Big Borders: Data (in)justice and the Governance of Refugees", *First Monday*, 24(4), 2019, available at: http://dx.doi.org/10.5210/fm.v24i4.9934 (last visited 19 Jan. 2023); S. Milan & L. van der Velden, "The Alternative Epistemologies of Data Activism", *Digital Culture & Society*, 2(2), 2016, 57–74.

[48] L. Fast, "Data Sharing between Humanitarian Organisations and Donors. Toward Understanding and Articulating Responsible Practice", *NCHS paper*, Norwegian Centre for Humanitarian Studies, 2022.

[49] T. Gillespie, "Algorithm", in B. Peters (ed.), *Digital Keywords: A Vocabulary of Information Society and Culture*, Princeton, Princeton University Press, 2016, 19.

[50] F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, Harvard University Press, 2015.

of algorithmic decision-making can be traced back to people – most often white men – behind the machine.[51] This would then imply that the solution simply lies in more inclusive design and/or more representative data. Even the designers of the algorithm would struggle to trace a decision back to its source. The complexity of decision-making and how weights are calculated and attribute value in ML systems are, by design, difficult to interpret.

This does not mean that "algorithms are unaccountable as such".[52] They give accounts of themselves all the time. These are partial and incomplete, but as feminist scholars have long argued, accounts of the social world have always been partial.[53] The expression "the human in the loop" seeks to identify the responsible human subject – such as the owner of the company that developed the technology for drone strikes or the surgeon deploying surgical robots – who could be held accountable, for instance in a court of law. It would be too easy to blame automation for mistakes and errors. Returning to Sanad's case, the presence of US army forces in Iraq, their ability to take him in for 11 days and to obtain his personal data, seemingly without clarifying its purpose, are clear examples of bad human decision-making and abuse of power. When it comes to gathering and using data, human decision-making around such procedures is often also a source of risk. This became clear in a more recent example concerning the misuse of data by the Dutch government to predict fraud among social welfare recipients. Although automated systems were used, unlawful forms of analysis, based on racialised attributes, lack of human oversight, and flawed legislation were the main reasons for the prolonged human suffering it caused.[54] The use of AI does not render human beings fully outside the "loop". Rather, there have always been contingent and fragile dynamics to human agency.[55] Human agency in relation to the use of ADM is a complex philosophical and sociological that exceeds the scope of this article. Louise Amoore's *Cloud Ethics* gives important suggestions to which I will return in Section 5.[56]

2.3. AI for (whose) good?

Proponents of AI in humanitarian settings speak of "AI for social good".[57] In themselves, technologies are neither good nor bad. This does not mean they are neutral, for they act upon and within social realities. Their operations, the data they engage with and the outputs they produce are the result of pre-existing human relationships and material conditions. The working of capitalism and the pervasive presence of (post)colonialism are equally present and often already amplified within humanitarian settings.[58] Humanitarian digitisation operates in and reworks these intersecting structures of exclusion, further explaining why, as I stated earlier, many scholars and civil society actors have expressed concern about the extractive nature and unforeseen consequences of digital experimentation in humanitarian settings.

At present, the actual intelligence of AI-driven technologies is still doubtful.[59] But their usage – in combination with the development of large platforms and databases – can have important consequences, particularly because they tend to perpetuate discrimination.

[51] K. Crawford, "Artificial Intelligence's White Guy Problem", *New York Times*, 25 Jun. 2016, available at: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html (last visited 19 Jan. 2023).

[52] Amoore, *Cloud Ethics*, 19.

[53] D. Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective", *Feminist Studies*, 14(3), 1988, 575–599.

[54] European Parliament Research Service, *Governing data and artificial intelligence for all. Models for sustainable and just data governance*, Panel for the Future of Science and Technology, Jul. 2022, 17.

[55] Amoore, *Cloud Ethics*, 65.

[56] *Ibid.*

[57] Madianou, "Nonhuman Humanitarianism".

[58] M. Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society* 5(3), 2019, 1–13; M. Duffield, *Post-Humanitarianism. Governing Precarity in the Digital World*, Cambridge, Polity Press, 2018.

[59] Madianou, "Nonhuman Humanitarianism".

Numerous studies have shown how short-sighted use of AI tends to reproduce racialised, gendered and classed bias.[60] This interacts with the tendency of human beings to ascribe greater credibility and legitimacy to decisions made by computers,[61] further explaining the consensus among computer scientists that extreme caution is needed when using AI in judicial settings.[62] Dangers of exaggerating human bias and discrimination became evident for instance in trials involving risk assessment engines. These were likely to overestimate the risk of black defendants reoffending, also when race is not an input.[63]

The EU is a geographical and symbolic space which actively draws on and develops technologies for migration control purposes.[64] Refugees and migrants often lack adequate data protection, which enables the EU to use migration, asylum and border control management issues as testing grounds for new technologies, under the cloak of security.[65] Discourses around securitisation – that present migration as a threat to national safety, economy, healthcare, culture etc. – are used to bolster this exceptionalism and to institutionalise legal precarity in and beyond the EU.[66] For people who are already legally marginalised, such as those (not yet) recognised as refugees, other migrants in precarious legal situations, and stateless persons, the risks are high. While digital technologies and connectivity enable forced migrants to move, resist and have autonomy they also, often simultaneously, increase the potential for control, exploitation, and surveillance.

The efficacy of biometric and other data-driven systems should not be overstated: often they break down or do not work at all.[67] But whether or not technology works as intended, digital trialling can have serious consequences. For instance, "success stories" about the use of technologies in refugee settings can result in shifts in what is deemed acceptable for citizens elsewhere.[68] Migration control is often presented as the last bastion of State sovereignty,[69] with the figure of the refugee presented as the exception to the rule. This article takes a more complicated view. By taking a closer look at how digitisation efforts in refugee protection settings beyond the EU's borders interact with complex legal frameworks, as will be further explored in Section 4, it is argued that the differential recognition of digital rights interacts with other modes of inclusion or exclusion. This then helps to assert control that takes place beyond borders and sovereignty.

[60] S. Browne, *Dark Matters: On the Surveillance of Blackness*, Durham, Duke University Press, 2015; V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*, New York, Palgrave Macmillan, 2018; S. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York, NYU Press, 2018.

[61] L. Skitka, K. Mosier, & M. Burdick, "Does Automation Bias Decision-making?", *International Journal of Human – Computer Studies*, 51(5), 1999, 991–1006.

[62] R. Abede, S. Barocas, J. Kleinberg, K. Levy, M. Raghavan, & D.G. Robinson, "Roles for Computing in Social Change", in Conference on Fairness, Accountability, and Transparency (FAT* '20), Barcelona, Spain, 27–30 Jan. 2020; R. Wang, "Legal Technology in Contemporary USA and China", *Computer Law & Security Review*, 39, 2020. An exception are the few who have adopted the Silicon Valley mantra of disruption and "failing fast".

[63] R. Berk, H. Heidari, & A. Roth, "Fairness in Criminal Justice Risk Assessment: The State of the Art", *Sociological Methods & Research*, 50(1), 2018.

[64] Examples are S. Scheel, *Autonomy of Migration? Appropriating Mobility within Biometric Border Regimes*, Milton Park, Routledge, 2019; B. Ajana, "Asylum, Identity Management and Biometric Control", *Journal of Refugee Studies*, 26(4), 2013, 576–595; M. Tazzioli, "Extract, Datafy and Disrupt: Refugees' Subjectivities between Data Abundance and Data Disregards", *Geopolitics*, 2020; C. Aradau, "Experimentality, Surplus Data and the Politics of Debilitation in Borderzones", *Geopolitics*, 2020.

[65] P. Molnar, "Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective", *Cambridge International Law Journal*, 8(2), 2019, 305–330.

[66] C. Aradau & M. Tazzioli, "Biopolitics Multiple: Migration, Extraction, Subtraction", *Millennium: Journal of International Studies*, 48(2), 2029, 198–220.

[67] K. Weitzberg, *Biometrics, Border Tech and Human Rights*, Just Tech and Migration online event organised in partnership with Queen Mary University of London, Institute for the Humanities and Social Sciences, 25 Jan. 2023.

[68] Jacobsen, *The Politics of Humanitarian Technology*.

[69] C. Dauvergne, "Sovereignty, Migration and the Rule of Law in Global Times", *Modern Law Review*, 2004, 588–615. For how the prevailing doctrine of State sovereignty under international law (re)establishes the European colonial project, see T. Achiume, "Migration as Decolonization", *Stanford Law Review*, 71(6), 2019, 1509–1574.

3. SEEKING REFUGE IN A DIGITALISED "PROTECTION SPACE"

In the next pages, I focus on some common elements in digital transformations of "protection space", a term used by UNHCR in its reporting since the early 2000s. This depiction of refugee protection as a negotiated and operationally focused activity has been critiqued for devaluing legal obligations towards refugees.[70] In combination with the humanitarian imperative and the marketisation of aid, refugee protection activities have become driven by humanitarian neophilia and techno-solutionism as will be explored in subsection 3.2.[71] I subsequently examine an example of how digitisation interacts with UNHCR's legal categorisation procedures. I ask what this pragmatic, rather than normative, approach means for procedures grounded in international refugee law.

3.1. UNHCR's position in "Protection Space"

It was also in the early 2000s, around the same time that UNCHR started to use the term "protection space", that UNHCR began experimenting with biometrics. By taking the fingerprints of people seeking to return from Pakistan to Afghanistan, the UN refugee agency was not just copying the securitisation techniques that State actors had started to deploy after 9/11. It was the US Department of State that earmarked funding for UNHCR to trial this technology.[72] Ten years later, Jordan and Lebanon were among the prime locations for humanitarian digital experimentation. This mainly resulted from the need to respond adequately and urgently to the large-scale displacement caused by the war in Syria. The hopes that humanitarian actors projected onto biometric identification in Jordan can also be seen in response to the difficulties that aid workers had encountered when counting Iraqi urban refugees between 2006 and 2010.[73] Jordan was also particularly suitable for rolling out the use of iris scans for cash-based assistance, as this technology had been part of the country's banking infrastructure since 2008.[74] In contrast, the Lebanese government did not express interest in this system for cash transfers.[75]

The term "protection space" most often occurs in UNHCR's country operation plans for non-signatory States in South East Asia and the Middle East. Many of these States are major refugee-hosting countries and have been reluctant or indifferent about adopting the Refugee Convention and the legal-normative institutionalisation of refugeehood often associated with it.[76] The international refugee regime tends to view States not party to the Refugee Convention as the exception.[77] But not being a signatory does not in itself make a State exceptional. There are 44 States that have not ratified the Convention. They actively engage with international refugee law through, for instance, other international laws, domestic and regional legislation and administrative instructions.[78] Often, Memoranda of Understanding (MoU) between UNHCR and these governments clarify the responsibilities of UNHCR.[79]

In Section 1, I referred to the founder of IrisGuard comparing UNHCR to a country when discussing its activities in Jordan. While this comparison is misguided, scholars have indeed compared UNHCR's position – especially concerning its role in Jordan– to that of a

[70] Jones, "Moving Beyond Protection Space".
[71] Scott-Smith, "Humanitarian Neophilia: The "Innovation Turn" and Its Implications".
[72] Jacobsen, *The Politics of Humanitarian Technology*.
[73] Twigt, *Mediated Lives*, 128; K. Lenner, *Blast from the Past: Policy Legacies and Memories in the Making of the Jordanian Response to the Syrian Refugee Crisis*, European University Institute: Max Weber Programme Working Paper Series, 2016.
[74] J. O'Carrol, "Banking on Iris Biometrics in Jordan", *Card Technology Today*, 20 (4), 2008, 6.
[75] Holloway, Al Masri & Abu Yahia, *Digital Identity*, 18.
[76] G. Cole, "Pluralising Geographies of Refuge", *Progress in Human Geography*, 45(1), 2020, 88–110.
[77] M. Jones, "Expanding the Frontiers of Refugee Law: Developing a Broader Law of Asylum in the Middle East and Europe", *Journal of Human Rights Practice*, 9(2), 2017, 212–215.
[78] M. Janmyr, "The 1951 Refugee Convention and Non-Signatory States: Charting a Research Agenda", *International Journal of Refugee Law*, 33(2), 2021,188–213.
[79] *Ibid.*

"surrogate State".[80] This term refers to the operational obligations UNHCR has taken on and the impossibility of providing full recognition of refugee rights. UNHCR Jordan took on refugee governance functions that are usually associated with the role of a State in response to the urgent needs of Iraqi refugees since 2006. This included registration, access to social services and cash assistance as well as refugee status determination (RSD). RSD is the process by which a government or UNHCR determines if a person seeking international protection is considered as a refugee under international law. Often formal refugee recognition is vital for realising other rights. But the ability of UNHCR Jordan to provide fuller access to rights is limited. It is constrained by its MoU with the Jordanian Government and continues to depend on the willingness of its host and (external) funding.[81]

Notwithstanding important contextual differences, approaches to forced displacement in non-signatory States in the Middle Eastern region are characterized as hospitable yet temporary, with opaque policies and procedures that are often based on the prioritisation of certain national or ethno-religious affiliations.[82] The roles undertaken by UNHCR and third parties and the space provided for establishing refugee protection in these settings are the result of lengthy political negotiations. UNHCR's "protection space" approach has, however, been critiqued for the following reason. By establishing itself as a negotiator through appealing to humanitarian values, the normative obligations of States as of UNHCR, toward refugees, are undermined. By shifting the responsibility for refugee protection to UNCHR and away from rights towards conditional needs, protection is rendered fluid and fragile.[83]

3.2. Addressing scarcity through automation and humanitarian neophilia

Humanitarian approaches to refugee protection are often critiqued for their short-term focus. Their emergency imaginary prioritises immediate solutions over long-term structural concerns and compassion over rights.[84] But since what was supposed to be temporary tends to become prolonged for years, humanitarian settings are often beset by scarcity – of funds, compassion, resettlement slots, rights, authority. Structural shortages make obtaining, ordering, classifying, and assessing information and data foundational for humanitarian programming. The importance of assuring donors, especially those who might be willing to receive resettlement referrals, necessitates careful accounting and reporting.[85]

Automating mechanisms to determine who is eligible to receive aid by ranking of vulnerability would simultaneously make that decision less arbitrary and the process more efficient. One such instrument is the Vulnerability Assessment Framework (VAF). UNHCR, World Food Programme (WFP) and United Nations International Children's Emergency Fund (UNICEF) introduced this proxy means testing instrument in 2014 to assess and standardise the vulnerability of Syrian non-camp refugees in Jordan. The algorithmic processing of quantifiable data by VAF gives a vulnerability score from 1 to 4. A score of 3 (highly vulnerable) or 4 (severely vulnerable) is a requirement but not a guarantee for receiving cash assistance.[86] VAF is based on a predicted expenditure welfare model, together with other factors such as coping strategies, level of

[80] M. Kagan, "'We Live in a Country of UNHCR': The UN Surrogate State and Refugee Policyin the Middle East", *New Issues in Refugee Research*, Research Paper, No. 201, 2011; A. Slaughter & J. Crisp, "A Surrogate State? The Role of UNHCR in Protracted Refugee Situations", *New Issues in Refugee Research*, Research Paper, No. 168, 2009.

[81] D. Stevens, "Rights, Needs or Assistance? The Role of the UNHCR in Refugee Protection in the Middle East", *International Journal of Human Rights* 20(2), 2015, 264–283.

[82] C. Lysa, "Governing Refugees in Saudi Arabia (1948-2022)", *Refugee Survey Quarterly*, 42(1), 2023, 1–28.

[83] Jones, "Moving Beyond Protection Space".

[84] Calhoun, *A World of Emergencies*; C. Brun, "There Is No Future in Humanitarianism: Emergency, Temporality and Protracted Displacement", *History and Anthropology*, 27(4), 2016, 393–410; L. Chouliaraki, *The Ironic Spectator: Solidarity in the Age of Post-humanitarianism*, Cambridge, Polity Press, 2013; D. Fassin, *Humanitarian Reason. A Moral History of the Present*, Berkeley, University of California Press, 2012.

[85] Merry, *The Seductions of Quantification*; Krause, *The Good Project.*

[86] H. Brown, N. Giordano, C. Maughan, & A. Wadeson, *Vulnerability Assessment Framework Population Study 2019*. UNHCR, Action against Hunger, International Labour Organization, 2019, available at: https://www.ilo.org/ipec/Informationresources/all-publications/WCMS_734065/lang–en/index.htm. (last visited 8 Aug. 2021).

education, and health. Under different names, similar instruments were rolled out in Egypt, Lebanon, and Iraq. In Jordan, the use of VAF has been extended to Syrian camp refugees, other national cohorts, and Jordanian citizens. Many questions remain, such as: is a system trained on the data of one population suitable to assess other populations?[87]

Humanitarian legibility schemes might be crucial for assessing needs and determining when providing assistance. They are equally a means of control.[88] A logic of audit coincides with a suspicious outlook toward potential recipients of aid.[89] Indeed, the initial use of biometrics in humanitarian settings was driven by the need to reduce so-called 'recyclers': people who would seek to receive individualised support more than once. The motivation of UNHCR for introducing fingerprint capturing in the early 2000s was to ensure that people returning to Afghanistan would only receive support once. By now, evidence that biometric identification reduces this form of low-level fraud continues to be scant. What is clear is that most fraud in humanitarian settings occurs earlier in the aid supply chain.[90] Yet, the reasoning that biometrics and other means of automating aid serves to reduce fraud persists, allowing for such developments to continue.

Threatened donor fatigue incentivizes UNHCR and its implementing partners to provide data that demonstrates their efficiency.[91] VAF is but one of the large-scale vulnerability assessments carried out in Jordan. There is an underlying presumption that more data yields more objective information and therefore allows for more certainty about who to regulate and how. This then reinforces the idea that humanitarian operations are neutral. But aside from the failure to recognise that technologies generally draw on European knowledge systems, it means that unequal power relations already intrinsic to most forms of humanitarianism are likely to be reproduced.[92]

Another response to the lack of substantial funding is that UN agencies and humanitarian organisations have increasingly been developing partnerships with private entities. This alignment of aid with business often goes hand in hand with humanitarian neophilia and techno-solutionism. Humanitarian neophilia refers to the Silicon Valley-inspired drive within the humanitarian sector for novelty, innovation and disruption.[93] It is often supported by big tech companies, including Microsoft, Google, and Facebook. Techno-solutionism refers to reliance on technological tools and the potential of technical expertise and technology to function as anti-politics machines.[94] Sociopolitical issues get turned into technical problems with the promise of a quick fix. Proponents of this shift have been making arguments for innovation labs, which are described as 'safe havens for experimentations' to find solutions.[95] In refugee situations, there is a perennial lack of solutions, which explains the hope projected on technologies and innovations to solve problems that are fundamentally political. This interacts with a thinking often present in emergency settings – "it is better to do anything than nothing" – and serves to justify immediate action involving elements that at another time, or in other circumstances, would be deemed problematic.[96]

[87] L. Turner, *Country report Jordan. D4.2 Interim Country Report*, ASILE – Global Asylum Governance and the European Union's Role, 2022.
[88] F. Cowling, *Seeing Like a Humanitarian: Legibility in Lebanon's Emergency Response*, Oxford, University of Oxford, 2020.
[89] Madianou, "Technocolonialism".
[90] Z. Rahman, *Biometrics in the Humanitarian Sector*, Oxford, The Engine Room and Oxfam, 2020.
[91] *Ibid.*, 13.
[92] P. Pallister-Wilkins, *Humanitarian Borders. Unequal Mobility and Saving Lives*, London, Verso Books, 2022.
[93] Scott-Smith, "Humanitarian Neophilia".
[94] J. Ferguson, *The Anti-politics Machine: Development, Depoliticization and Bureaucratic Power in Lesotho*, Minneapolis, Minnesota University Press, 1994.
[95] L. Bloom & R. Faulkner. *Innovation Spaces. Transforming Humanitarian Practice in the United Nations*, Refugee Studies Centre Working Paper Series 107, 2015, 3.
[96] Holloway, Al Masri & Abu Yahia, *Digital Identity*, 14.

What makes partnerships with private entities particularly troublesome is that many such companies are simultaneously involved in the development of technologies that are commonly understood as harmful. Most public scrutiny has been directed at the partnership between the WFP and Palantir, a data-mining firm known for its involvement in US Immigration and Customs Enforcement's controversial use of AI for border control purposes, and in Cambridge Analytica's election rigging.[97] Many other private partners – including Malhas' IrisGuard and the later discussed company Accenture – have been or are similarly involved in the development of technologies for border control, predictive policing, and the like.

In the next subsection, I come back to VAF as I question how the automation of assessments is interacting with UNHCR's mandated obligations towards refugees. Whereas the example concerns protection in Middle Eastern States, the situation is far from being particular to Middle Eastern non-signatory States, as lessons learned out "there" can easily be used elsewhere or for different purposes. This also becomes clear in section 5, where I discuss how the engagement of some refugee law scholars with the potentials for automation for refugee recognition procedures sound familiar.

3.3. RSD, legal categorisation and automated assessments

The multiplication of legal categories and differing access to rights through them is a well-documented forced migration management technique.[98] In signatory States, prolonging refugee status determination and providing only temporary residence permits to recognised refugees are but two ways to circumvent obligations arguably set out in the Refugee Convention.[99] But also in non-signatory States known to host large numbers of refugees like Lebanon and Jordan, bureaucratic differentiation can have important consequences.[100] This also relates to UNHCR's involvement in ascertaining refugees' protection claims.

UNHCR's involvement in RSD is extensive: by 2011, it held sole responsibility for RSD in 54 countries and shared responsibility with national governments in 23 countries, which shows its involvement does not depend only on whether a State is a signatory.[101] UNHCR's mandate states it can declare *prima facie* status, but it has not declared Syrian nationals as such therefore necessitating RSD to establish a refugee status.[102] Around 2015, in Lebanon, Egypt, Jordan, Turkey, and Iraq, the RSD/Resettlement procedures for Syrian nationals were merged. "RSD proper" was only conducted for those few who are already likely to be considered for resettlement.[103] The merged refugee recognition procedures were then conducted by UNHCR on behalf of States willing to receive people selected for resettlement. It seems that at least in Jordan similar approaches have been used for non-Syrian nationals.[104]

[97] B. Parker, "New UN Deal with Data Mining Firm Palantir Raises Protection Concerns. Critics say it could put 'highly sensitive' Data about Millions of Food Aid Recipients at Risk", *The New Humanitarian*, 5 Feb. 2019, available at: https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp (last visited 18 Oct. 2023).

[98] R. Zetter. "More Labels, Fewer Refugees: Remaking the Refugee Label in an Era of Globalization", *Journal of Refugee Studies*, 20(2) 2007, 172–192.

[99] J. Schultz, "An End to Asylum? Temporary Protection and the Erosion of Refugee Status", in C. Jacobsen, M. Karlsen & S. Khosravi, *Waiting and the Temporarilies of Irregular Migration*, London, Routledge, 2020, 170–185.

[100] M. Janmyr. "UNHCR and the Syrian Refugee Response: Negotiating Status and Registration in Lebanon", *International Journal of Human Rights*, 22(3), 2017, 393–419; D. Stevens, "Legal Status, Labelling, and Protection: The Case of Iraqi "Refugees" in Jordan", *International Journal of Refugee Law*, 25, 2013, 1–38.

[101] L. Abdelaaty, *Discrimination and Delegation: Explaining State Responses to Refugees*, Oxford, Oxford University Press, 2021, 8.

[102] Janmyr & Mourad, "Modes of Ordering: Labelling, Classification and Categorization in Lebanon's Refugee Response", *Journal of Refugee Studies*, 31(4), 2018, 547.

[103] United Nations High Commissioner for Refugees – Lebanon (UNHCR Lebanon), *Accelerated Processing of Claims from Syria in the Context of Large Influxes into Lebanon*, 2015, available at: http://www.refworld.org.ru/pdfid/56c46f8f4.pdf (last visited 8 Aug. 2021).

[104] D. Baslan, R. Johnston & A. Kvittingen, "Realizing the Rights of Asylum Seekers and Refugees in Jordan from Countries Other Than Syria with a Focus on Yemenis and Sudanese", 2019, available at: https://www.academia.edu/

As a result, the majority of those who are referred to as "refugees" by UNHCR and humanitarian organisations in their reporting on the Middle East are not legally categorised as such. Most likely they are registered for refugee protection with the UNHCR country office yet have not undergone RSD. Instead, there is a wide array of bureaucratic labels in use – registered refugee, asylum-seeker, Person of Concern, displaced person, foreigner, labourer etc.[105] – which result from negotiations with State actors and efforts to appease them. UNHCR has in its own selection criteria for who is deemed eligible for third country resettlement.[106] In addition, they need to follow criteria set by receiving States. But in Jordan, VAF scores are also increasingly taken into consideration when deciding who ends up being interviewed.[107]The sorting work undertaken by digital technology has either come to coexist with and/or has come to replace work that was previously carried out by bureaucratic means. Before automation started to impact them, UNHCR's RSD procedures or the selection process for consideration for resettlement were also known to lack in accountability and were bedevilled by politics, human bias, and other exclusionary mechanisms. Most likely, people were already excluded from procedures set up to ascertain whether a person is a recognised refugee, a procedure grounded in international refugee law.[108] How then does this automation of selection for RSD compare to the prior state of affairs?

The VAF measures poverty rather than whether people are "at risk", as this was the purpose for which the VAF was designed. The use of this automated assessment of relative vulnerability is an example of function creep: the collection of data or use of technologies intended for one purpose (assessing one's need for cash assistance) for another purpose (assessing who qualifies as a "real" refugee). Automated decision-making might further solidify decisions made, not least because human beings tend to ascribe more credibility and legitimacy to decisions made by computers.[109] One of the critiques on the limits of UNHCR's "protection space"– that who is deemed a legible refugee is determined on conditional needs rather than on rights – might have become stickier.[110]

Quantified measurements can appear more "neutral", "objective", or "fair". But classification is the result of and conceals politicisation.[111] Classification mechanisms operate along with racialised, gendered, and other reductive logics. For instance, Jordan's and Lebanon's protection spaces tend to overlook the gendered harms and vulnerabilities of Syrian refugee men.[112] They are also state-centric, as becomes evident in UNHCR Iraq's vulnerability assessments. Statelessness is not taken into account despite widespread recognition that it contributes to vulnerability.[113] Analytical frameworks and experience derived from commercial platforms and epistemologies from the Global North can easily help strengthen the "power of the identifier, UNHCR, at the expense of the identified – the refugee".[114] Who

42948715/realizing_the_rights_of_asylum_seekers_and_refugees_in_jordan_from_countries_other_than_syria_with_a_focus_on_yemenis_and_sudanese (last visited 18 Oct. 2023).

[105] Janmyr & Mourad, "Modes of Ordering".

[106] UNHCR, *UNHCR Resettlement Handbook*. Geneva, 2011.

[107] Turner, "Country report Jordan. D4.2 Interim Country Report", 13.

[108] K. Sandvik, "Blurring Boundaries: Refugee Resettlement in Kampala – Between the Formal, the Informal and the Illegal"' *PoLAR Political and Legal Anthropology Review*, 34 (1), 11–32.

[109] Skitka, Mosier & Burdick, "Does Automation Bias Decision-making?".

[110] Stevens, "Rights, Needs or Assistance? The Role of the UNHCR in Refugee Protection in the Middle East", Jones, "Moving Beyond Protection Space".

[111] C. Clark, "Understanding Vulnerability: From Categories to Experiences of Young Congolese People in Uganda", *Children and Society*, 21(4), 2007, 284–296.

[112] L. Turner, "The Politics of Labeling Refugee Men as Vulnerable", *Social Politics*, 28(1), 2021, 1–23; Cowling, *Seeing Like a Humanitarian: Legibility in Lebanon's Emergency Response*.

[113] T. McGee, "Recognizing Stateless Refugees", *Forced Migration Review*, 65, 2020, 45–47.

[114] S. Madon & E. Schoemaker, "Digital Identity as a Platform for Improving Refugee Management", *Information Systems Journal*, 31(6), 2021, 20.

and what is being optimised here, and who gets to decide? In Section 4 I look more closely at how differential power is manifested in legislation regarding data protection.

4. LEGISLATING REFUGEE DATA GOVERNANCE?

All over the world, data governance is guided by models that involve large amounts of data being appropriated – often without meaningful consent – and used to generate value for different purposes and by different actors. For instance, States and large technology companies often have competing interests, power, and capacities. This then influences how data governance operates and the extent to which data is linked to privacy and identity rights, treated as a surveillance tool under the cloak of national security, or exchanged as a commodity.[115] In order to reduce the potential for abuse and excessive power, legislation has been developed to formalise requirements around the collection, storage and processing of data; these regulate when various data practices are legally allowed.

IOs are subject to international law and have responsibilities for international human rights. UNHCR is also legally bound to its mandate, which is set out in the UNHCR statute. The Refugee Convention includes no provision on privacy, unlike other international human rights instruments. Article 12 of the Universal Declaration of Human Rights (UDHR) defines it as individual autonomy and identifies the right to seek the protection of the law against arbitrary interference.[116] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) formulates obligations to protect privacy against interference by governments or other actors, without any clause of limitation.[117] In October 2018, the UN High-Level Committee on Management agreed to 10 Personal Data Protection and Privacy Principles, to set a common framework for data collection, processing and storage, and the transfer of personal data in mandated activities by, or on behalf of, UN System Organisations.[118] UNHCR also has its own data protection policy as do other IOs such as WFP and IOM. It should be borne in mind that accountability mechanisms in instances of UNHCR human rights violations are limited and restrict internal oversight, despite much "accountability talk".[119]

IOs have immunity from national legislation, the idea being that this helps to ensure they can fulfil their mandate independently and to comply with principles such as neutrality and humanity. Regional legislation, such as the EU's General Data Protection Regulations (GDPR) also does not formally apply, notwithstanding its potential normative impact.[120] Below I refer to EU legislation for this allows a comparison between what the EU deems necessary safeguards for EU citizens and what is available for refugees beyond the EU. But EU legal regimes contribute to 'exceptionalising' migration contexts, within and beyond the EU, as they systematically carve out exceptions for data protection of refugees and other people on the move. This occurs through straightforward discriminatory legislation, as is the case in the currently proposed AI Act.[121] GDPR formally applies to non-EU citizens, but its

[115] R. Dowd, *The Birth of Digital Human Rights*, London, Palgrave Macmillan, 2022.
[116] UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III), 10 Dec. 1948.
[117] UN General Assembly, *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, 16 Dec. 1966.
[118] UN High-Level Committee on Management (HLCM), *Personal Data Protection and Privacy Principles*, 36th Meeting, 11 Oct. 2018, available at https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf (last visited 19 Jan. 2023).
[119] Johansen, *The Human Rights Accountability Mechanisms of International Organizations*, 191
[120] For data transfers from the EU to IOs the rules of GDPR on international data transfer do apply. C. Kuner, "The GDPR and International Organizations", *AJIL Unbound*, 114, 2020, 15–19.
[121] EDRi, "Civil Society calls for the EU AI Act to better protect people on the move.", 6 Dec. 2022. Available at: https://edri.org/our-work/civil-society-calls-for-the-eu-ai-act-to-better-protect-people-on-the-move/ (last visited 10 Jan. 2023).

restrictions – like "national security" or "public security" – or means to establish a legal basis such as vital interests, including "humanitarian grounds" allow sovereign space for interpretation, especially in migration contexts. Indeed, the reasoning that migration control equals security and crime control – crimmigration – serves to systematically exclude people on the move through, for instance, the various EU-Schengen information systems.[122] Plans to make these systems interoperable are being rolled out, despite awareness that this will probably brand almost all so-called third-country nationals as "risky by default".[123]

In the rest of this section, I take a closer look at UNHCR's data protection policy. I compare the *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* to the EU's GDPR.[124] Comparing UNHCR's policies to what the EU deems essential data protection for some allows additional insights into how UNHCR's policies would have fallen short, had they been legally enforceable. UNHCR published its data protection policy in 2015 – two years after it first started to obtain biometric information on people registering for protection in Jordan. The policy starts with recognition for the importance of people's consent, their right to be informed about its purpose and the ability to refuse and to request corrections and deletions.[125] It is then stated that if data is transferred to implementing partners or other third parties, the "data subject is informed of this fact".[126] Further on, it is formulated that all cases are "permanently retained", raising questions about the earlier mentioned potentials for deletion.[127] Throughout the policy, no mention is made of personal data that ought to be considered sensitive – as in GDPR. Rather, along with biometric details, information about religion, ethnicity, and opinions are put under the header of personal data.[128] And unlike GDPR, there is no mention of the importance of data minimisation: only obtaining essential data.

Alongside concerns regarding the adequacy of UNCHR's data protection policies, there are many questions regarding feasibility and actual implementation. For instance, concerning informed consent and being informed about data-sharing, studies reaching from Jordan and Bangladesh to Uganda and Ethiopia have shown that usually very little information is provided before, during, or after registration. Reporting suggests that even false information is provided, such as assurances that biometric registration is carried out for health purposes. Other people were told that biometric registration is required to receive aid.[129] Perhaps this has become true by default: the system might no longer give the option to not obtain biometric information or staff might have forgotten how to do these procedures manually. The question also remains if there are real possibilities for meaningful consent in refugee protection settings, considering the difficult circumstances in which people find themselves. And UNCHR's Policy states that subjects can raise any additional concerns, for instance regarding data sharing, with a person who is established as a so-called data focal point. This function is usually held by the most senior UNHCR protection staff member of a country office.[130] In reality, people holding such a position are rarely accessible to refugees.

[122] See for instance Ajana, "Asylum, Identity Management and Biometric Control"; D. Broeders, "The New Digital Borders of Europe EU Databases and the Surveillance of Irregular Migrants", *International Sociology* 22(1), 2007, 71–92; H. Dijstelbloem, H. Meijer, & F. Brom, "Reclaiming Control Over Europe's Technological Borders", in H. Dijstelbloem & A. Meijer (eds.), *Migration and the New Technological Borders of Europe*, London, Palgrave Macmillan , 2011, 170–185.

[123] N. Vavoula, "Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism", *European Journal of Migration and Law*, 2021, 1–23.

[124] UNHCR. *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, 2015, available at: https://www.refworld.org/docid/55643c1d4.html (last visited 18 Oct. 2023).

[125] *Ibid.*, 3.1, 19.

[126] *Ibid.*, 3.1.ii, 19.

[127] *Ibid.*, 4.6.2, 29.

[128] *Ibid.*, 1.4, 11.

[129] E. Schoemaker, D. Baslan, B. Ponn, & N. Dell, "Identity at the Margins: Data Justice and Refugee Experiences with Digital Identity Systems in Lebanon, Jordan, and Uganda", *Information Technology for Development*, 27(1), 2020; Z. Rahman, *Biometrics in the Humanitarian Sector*.

[130] UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, 7.2.1, 41.

Worries about registering excessive biometric information on refugees and other data-driven humanitarian actions relate to concerns about possible data breaches, leaks, and the sharing of data with third parties with different and potentially harmful agendas.[131] In 2016, the UN's internal oversight body Office of Internal Oversight Services (OIOS) brought serious data breaches to light.[132] Three of the five UNHCR missions investigated, had shared refugees' personal data with host governments, without assessing the data protection offered by these governments or establishing a transfer agreement.[133] IOs' data policies are devoid of legal implications when they are breached.[134] Third parties do not enjoy the same privileges and immunities as the IOs they work together with, meaning they can be subjected to the jurisdiction of State parties who might be interested in gaining access.[135]

As mentioned in Section 3, there are many dubious public–private partnerships within the humanitarian realm. Private companies might be involved in refugee settings for altruistic motives or for "ethics bluewashing" – trying to come across as more ethical by being involved in aid. But the economic models of big tech companies suggest otherwise. Humanitarian settings can provide additional opportunities for extractive data mining, which explains technology companies' interest in them. More data allows for further fine-tuning prediction models, which might inadvertently be used to predict the behaviour also of European citizens. Another less altruistic motive is so-called "ethics dumping": the exportation of unethical digital processes and products to countries with weaker frameworks or enforcement mechanisms, after which the outcomes are re-imported.[136]

Even when ample precautions are taken, private partnerships can be problematic. When WFP established its partnership with Palantir, a statement was issued saying that the company would not get access to WFP's personal data. But non-personal data can also be sensitive. And no mention was made of whether the company has access to WFP's metadata.[137] Metadata (data about data) can be used to re-identify persons or groups, which explains why ICRC and Privacy International have called for humanitarian metadata protection.[138]

Finally, knowledge that companies obtain by trialling technologies in humanitarian settings can be used elsewhere for instance for border control purposes. One example is the company Accenture and how it oscillates between technological support in humanitarian settings and for border control purposes. In 2013 the company became involved in creating UNHCR's Biometric Identity Management System (BIMS) in Malawi. Around the same time, Accenture and its partners were awarded a contract for maintenance of the EUs Visa Information System (VIS). By 2016 the company was invited to a workshop by EU-Lisa the agency established to manage EÚs large scale IT-systems, known for operating as surveillance technologies for border control purposes. Accenture was asked to consider how UNHCR's biometric registration could be useful for EU-Lisa's technological

[131] Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent – Bangladesh Provided Myanmar Information that Refugee Agency Collected".

[132] Office of Internal Oversight Services, "Audit of the Biometric Identity Management System at the Office of the United Nations High Commissioner for Refugees", Report 2016/181, Geneva: United Nations, 2016.

[133] S. Ladek, N. Abdelkhaliq, Z. Scott Cameron, S. Green, & C. Procter, *Evaluation of UNHCR's Data Use and Information Management Approaches*, UN doc ES/2019/07, UNHCR, 2019, available at https://www.unhcr.org/5dd4f7d24.pdf (last visited 29 Nov. 2022).

[134] K. Sandvik, "The Digital Transformation of Refugee Governance", in C. Costello, M. Foster, & J. McAdam (eds.), *Oxford Handbook of International Refugee Law*, Oxford, Oxford University Press, 2021.

[135] International Committee of the Red Cross, and Privacy International, *The Humanitarian Metadata Problem "Doing No Harm" in the Digital Era*, ICRC, Geneva and Privacy International, London, 2018, 27.

[136] L. Floridi, "Translating Principles into Practices of Digital Ethics: Five Risks of being Unethical", *Philosophy and Technology*, 32, 2019, 185–193; A. Tsamados, N. Aggarwal, J. Cowls, J. Morley, H. Roberts, M. Taddeo, & L. Floridi, "The Ethics of Algorithms: Key Problems and Solutions", *AI & Society*, 2021, 215–230.

[137] Parker, "New UN deal with data mining firm Palantir raises protection concerns. Critics say it could put 'highly sensitive' data about millions of food aid recipients at risk".

[138] International Committee of the Red Cross, and Privacy International, *The Humanitarian Metadata Problem "Doing No Harm" in the Digital Era*.

infrastructure.[139] By now, the company is major recipient of contracts from EU-Lisa, whereas it also continues to work in humanitarian settings. For instance, it works closely together with earlier mentioned IrisGuard and WFP to record consumption behaviour in Jordan's refugee camps though blockchain technology.[140]

5. ENGAGING WITH NEW TECHNOLOGIES AND OLDER OTHERING TECHNIQUES

I have just shown how data protection falls short in refugee protection situations, even if it were legally enforceable. A too narrow focus on regulations, laws, and corporate policies alone, however, would obscure what is really at stake, which is human dignity and autonomy.[141] A legalistic approach weakens consensus on what privacy is – that is, the ability to control the boundaries between one's sense and knowledge of self and others, and those between private and public.[142] Understanding of privacy evolved over time, in response to technological changes and in interaction with organisational and social settings. It is implicated in struggles over secrecy and power between people and their communities, governmental (and non-governmental) actors, scientists, civil society, and corporations. Trust is another factor – there are shifting boundaries between those who should and should not be trusted, what is and is not suspicious and what should or should not be controlled.

Privacy continues to be regarded as a bourgeois, western or individual concept. For instance, in her otherwise pivotal study on data extraction and the surveillance economy, Shoshana Zuboff makes the bold claim that privacy is simply less of a concern for people in China.[143] For many people all over the world, privacy is not always a possibility. But technology-mediated negotiations and struggles over information, private lives and trust are certainly taking place. This is also the case when it comes to people navigating humanitarian emergencies or living in precarious protection settings. Approaches to privacy urgently need to become decolonized not least because short-sighted views on privacy allow it to be seen as something that can be (more easily) bypassed, especially when it comes to non-western "others" and even more so when they are considered "at risk" (vulnerable) or "a risk" (dangerous).[144] In short, it allows for exceptions.

Newer technological developments often further interact with other, often older, othering techniques. When I discussed Sanad's experience with the capturing of his fingerprints and how he associated this with the decision that he was rejected for US resettlement, I also explained that his experience was unusual. Most often, refugees living in prolonged legal uncertainty do not receive any information regarding such decision-making. Especially when it concerns UNHCR's resettlement programmes, chances to seek redress or hold an actor accountable are notoriously difficult. Different tasks are spread out over different implementing organisations and private actors and further obfuscate responsibility and conceal where accountability might be sought. "Agency laundering", a term coined to describe how moral responsibility can be obfuscated by deploying technology,[145] is therefore not just a recent phenomenon.

[139] Lemberg-Pedersen & Haioty, "Re-assembling the Surveillable Refugee Body in the Era of Data-cravings".
[140] *Ibid.*
[141] E. Renieris, *Beyond Data. Reclaiming Human Rights at the Dawn of the Metaverse*, Cambridge, MIT Press, 2023.
[142] I. Van der Ploeg, *The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body*, Maastricht, Shaker Publishing, 2005.
[143] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile Books, 2019, 392.
[144] Arora, "Decolonizing Privacy Studies".
[145] A. Rubel, C. Castro, & A. Pham, "Agency Laundering and Information Technologies", *Ethical Theory and Moral Practice*, 22, 2019, 1017–1041.

But whereas the ways in which newer technologies work and operate does resonate with older othering techniques there are also additional complicating factors. For instance, regarding the deployment of automated vulnerability assessment, a study in Lebanon shows how technological developments can move decision power and expert knowledge elsewhere – to headquarters, consultancies, algorithms who attribute weight and establish relations etc. – away from people who are familiar with the local contexts.[146] Meanwhile, as technologies tend to obfuscate how decisions are made and therefore complicate seeking accountability of institutions and human actors that have adopted a tool, the results are often given greater credibility.[147] The human operating the machine tends to ascribe more legitimacy to decisions made by a computer than to themselves or those impacted by them.[148] Proving that a computer made a mistake is often difficult. When this is combined with the "trickster" stereotype that is almost always associated with the figure of the refugee, it is highly probable that the scope for refugees and other precarious migrants to address errors and bias has been reduced.[149]

The development and deployment of highly controversial and invasive technologies can therefore have profound consequences for legal and bureaucratic procedures around being and becoming a refugee. Data and statistical inferencing result in predictions, through anticipating the future and closing off actions.[150] This may interact with the requirement for protection as formulated in the Refugee Convention: "a well-founded fear of being persecuted", which focuses on the likelihood of future persecution. It is a forward-looking test that provides room for uncertainty and doubt, even if uncertainty and lack of knowledge are unequally distributed.[151] Datafication, however, focuses on reducing uncertainty. As seen with racialised policing and security algorithms, the futures they condense contain "within it the residue of all violence of past colonial histories, migrations, journeys and border crossings, a fulsome sediment of all the actions and transactions of past movements in the name of justice".[152] The likelihood that AI will make it more difficult to make claims, not least claims for asylum or claims when one is in a precarious legal position, is very real.

This means there is an urgent need for scholars and practitioners working on law, migration, and technology to carefully engage with how data flows and algorithms are transforming contemporary ethics and politics. This includes actively participating in discussions on the consequences of experimenting with algorithmic and data-driven forms of refugee and migration governance. How to go about this is not straightforward. For instance, there is general agreement that extreme caution is needed with deploying AI in judicial settings, not least because of the considerable risk that people who are already marginalised are disproportionately affected. Yet some of the pioneering scholarship on technology and refugee law has started to discuss the potentials in migration court settings.

One explanation for this is that AI development for government decision-making is unlikely to slow down just because of ethical quandaries.[153] Others argue that AI can be useful to provide valuable and visible insights into fairer RSD procedures. It could, for instance, expose disparity in outcomes in RSD between different States and divergences in national legal

[146] Cowling, *Seeing Like a Humanitarian. Legibility in Lebanon's Emergency Response.*

[147] K. Sandvik & K. Jacobsen, "UNHCR and the Pursuit of International Protection: Accountability through Technology?", *Third World Quarterly,* 39(8), 2018: 1508–24.

[148] Skitka, Mosier, Burdick, "Does Automation Bias Decision-making?".

[149] F. Johns, "Data, Detection, and the Redistribution of the Sensible in International Law", *American Journal of International Law*, 111(1), 2017, 57–103.

[150] Hildebrandt, *Slaves to Big Data. Or Are We?*

[151] H. Storey, "What Constitutes Persecution? Towards a Working Definition", *International Journal of Refugee Law*, 26, 2014.

[152] Amoore, *Cloud Ethics. Algorithm and the Attributes of Ourselves and Others*, 64.

[153] N. Kinchin, "Technology, Displaced? The Risks and Potential of Artificial Intelligence for Fair, Effective and Efficient Refugee Status Determination", *Law in Context*, 37(2), 2021.

interpretations.[154] AI can make uncertainty in RSD visible, as Evans Cameron, Goldfarb and Morris contend. Their study is positioned in "theoretically ideal" circumstances, as the authors recognise it most likely would hurt people seeking refuge, unless an additional obligation under the Refugee Convention was made to resolve doubts in decision-making in favour of the claimant.[155] Indeed, the above-mentioned scholars are deeply aware of the many risks and pitfalls that come with ADM in refugee governance.[156] But they seem to disregard how knowledge production on migration governance can contribute to or be misused for political purposes.

The establishment of social research centres as "labs" is yet another example of how the engagement of refugee law scholarship with technologies can show similarities to the exceptionalising tendencies of humanitarian neophilia. Such centres are designed to bring social scientists, activists, and tech developers together to do bottom-up innovation. Some do great work on, for instance, countering the racist deployment of technology or AI in border governance. But the word "lab" does not only have painful associations with colonial histories and the misuse of people as test objects.[157] It also points to the present risks that people and their data will be harmed by being treated as exceptional and therefore rights-optional test objects.

Ensuring that training data is more representative regarding, for example, gender, race, and class, having a more diverse team of techno scientists, or establishing user-centred design, can indeed help achieve more data justice. But how (inter)governmental and private actors are able to deploy data and how technologies operate depends on power, access, and privilege. And as it is impossible to "optimise" around the political, economic, and social power dynamics that are intrinsic to borders, forms of data justice need to be sought that move beyond techno-legal solutions.[158] There might be possibilities for more effective just data governance, but this would require more attention to the temporal and spatial dimensions of data flows, regular controls and ensuring that people or settings are not systematically singled out from legal safeguards.[159] Several questions remain: how to establish and ascertain the above-mentioned conditions if and when a sovereign figure to direct calls for more rights is absent and/or complicit? Furthermore, where is the critical or redemptive aspect of agency located here?

Louise Amoore's *Cloud Ethics*[160] argues for a move beyond political demands for privacy or transparency. Amoore underscores that potentials that algorithms have for profound violence goes beyond already manifest harms (to steer or determine outcomes around immigration decisions, policing, elections). ADMs operate by reducing the multiplicity of potentials into condensed single outputs, meaning that alternative futures can easily become foreclosed. The bounded outcomes that ADM produce are therefore potentially more harrowing, for they can render the space needed for political claim-making, including and perhaps especially by people seeking refuge. Amoore's approach, however, is neither a definitive method for resistance or for critique, nor does it stand outside of, or in opposition to, the attributive power of algorithms. Rather, she points to foregrounding relationality, opacity, and partiality, which

[154] T. Gammeltoft-Hansen & W. Hamilton Byrne, *Data Driven Futures of International Refugee Law*, at Refugee Law Initiative 5th Annual Conference – Ageing Gracefully? The 1951 Refugee Convention at 70, London, University of London, 9–11 Jun. 2021.

[155] H. Evans Cameron, A. Goldfarb & L. Morris, "Artificial Intelligence for a Reduction of False Denials in Refugee Claims", *Journal of Refugee Studies*, 35(1), 2021, 493–510.

[156] *Ibid.*; Gammeltoft-Hansen & Hamilton Byrne, *Data Driven Futures of International Refugee Law.*

[157] Jacobsen, *The Politics of Humanitarian Technology.*

[158] R. Benjamin, *Race after Technology*, Cambridge, Polity Press, 2019.

[159] European Parliament Research Service, *Governing Data and Artificial Intelligence for all; Models for Sustainable and just Data Governance.*

[160] Amoore, *Cloud Ethics.*

are also intrinsic to algorithmic decision-making. The ways in which weights are calculated and predictions are derived – based on attributes – always carry with them degrees of uncertainty. Paying closer attention to this and to the social and technical conditions under which algorithms can emerge and operate, could allow ways for accountability, also for people on the move.

6. CONCLUSION

The ability to seek and enjoy protection under the Refugee Convention is closely interrelated to the recognition of other fundamental human rights, including the right to movement and digital rights. Across the globe, refugees and other migrants existing in a state of enduring legal uncertainty are perhaps the most monitored persons there are.[161] This article has looked closer at Middle Eastern protection contexts. In these settings, different forms of legal "exceptions" interact, which allow people seeking refuge and the settings in which they live are treated as rights optional.

The distinction between citizens and non-citizens is increasingly enacted through digital techniques and data flows which are far from contained by the model of the juridical sovereign State. A more complex assemblage of people, organisations, and technologies interact with a sovereign security discourse, humanitarian reason, and other reasons for exceptions that are further influencing the enactment or deprivation of rights. And as algorithms are generative of the politics of contemporary societies, technologies deployed for refugee and migration governance purposes are likely to reinforce exclusionary, State-centred citizenship. This, combined with the structural undermining of the digital rights of people seeking refuge in the present, can easily further restrict the right to seek refuge in the future.

[161] Metcalfe & Dencik, "The Politics of Big Borders".