The politics of big borders: Data (in)justice and the governance of refugees

Article for *First Monday*, Special Issue on 'Data Governance Across Borders'

By Philippa Metcalfe and Lina Dencik (Data Justice Lab, Cardiff University, UK)

Digital technologies have become instrumental in facilitating coordination, identifying safe travel routes and accessing services for many along migration routes around the world. Yet at the same time, the growing role of data in governance, often generated through these very technologies, is transforming the nature of borders, asylum processes and decision-making. In Europe, this has become particularly pertinent with a so-called refugee 'crisis' in recent years that has placed borders and territory firmly in the spot-light. The turn to digital technologies in this context has made those refugee populations, that balance the line of precarity of Europe's external and internal borders, populations of data experimentation. They are simultaneously the most monitored groups amongst us, just as their struggles and experiences often remain the most invisible. Vast interoperable databases, digital registration processes, biometric data collection, social media identity verification, and various forms of data-driven risk and vulnerability assessments now all form part of the European border regimes for refugees. How should we understand the implications of these developments for displaced people forced to migrate? And what do they mean for the rights of refugees and the pursuit for social justice?

In this article we provide an overview of developments of data collection and use in European border regimes in order to conceptualise their significance. We are particularly interested in doing this within a 'data justice' framework that foregrounds social justice concerns in discussions and practices relating to the wider 'datafication' of society. We understand this to invite reflections on the extent to which data systems enable or undermine the potential of those historically marginalised and mis- or under-represented in society for cultural and political participation, life chances and access to fundamental rights (see also Dencik et al. 2018). We take this approach to analyse the implications of data-driven technologies in border regimes with the view to advance an engagement with data politics that can move beyond techno-legal questions and solutions that have predominantly concerned privacy and data protection issues towards a wider political mobilisation that situates data processes in relation to historical and on-going struggles around borders.

We start by outlining the advent of digital borders and data-driven governance in the context of refugee populations and European border regimes in order to analyse the significance of

these developments for the nature of governance and shifting power dynamics for those who experience the violence of borders. We make the case that within the current policy context of European border control, data functions to systematically stigmatize, exclude and oppress unwanted migrant populations through mechanisms of criminalisation, identification and social sorting. This highlights how developments in data processing need to be understood in relation to on-going social justice struggles. It is only by situating the datafication of borders and asylum-processes in the context of 'Fortress Europe' and the historical policy-driven suppression of the rights of illegalised migrants and refugees that we can understand the politics of data as it relates to the lived realities of European border regimes.

Datafication of borders and refugees

The topic of borders has become particularly salient in public imagination in recent years, not least within Europe where the increasing violence surrounding borders has significantly marked the geopolitics of the European project. At the same time, the mechanisms through which to enact borders are deeply intertwined with technological developments. As Ajana claims "with big data comes 'big borders'" (2015: 13), arguing that increased datafication leads to greater regulation of borders, involving greater collation of personal 'data traces'. These traces note behaviours both relating to physical movement across territories as well as everyday activities including financial transactions, social media use, etc. Data then augments borders significantly; both the management of physical external borders and the dispersal of borders across and within societies. But how exactly are borders datafying? And what does this mean for those who already experience violence and oppression within border regimes, namely refugees and illegalised migrants?

In this article we discuss technological developments of border regimes in relation to European borders, specifically those within 'Schengen Europe', with the inclusion also of European Union (EU) countries that are signatories of the Dublin Convention. This allows for a discussion of EU wide methods of technologically aided border control, including, but not limited to, efforts to create interoperable databases for migration including EURODAC[1] - a centralised EU database originally created to contain biometric information (fingerprints) of anyone attempting to claim asylum in any European country – the Schengen Information

[1] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:EN:PDF

System[2] (SIS II), and Visa Information System[3] (VIS), which collect data on all forms of migration to and within the EU, as well as technologies used within the European Surveillance System[4] (EUROSUR). Such methods in the European context, as Carrera and Hernanz (2015:69) argue, were developed as a means of compensating the freedom of movement within Schengen territory against "the unwanted forms of human mobility and criminality that the free circulation system would allow for". Throughout this article however, we refer mainly to how these developments affect asylum seekers, refugees and illegalised migrants within the EU[5], as efforts to control such individuals have been furthered due to the increased number of arrivals in what is commonly referred as the 'refugee crisis' of 2015-16. Whilst not all of the technologies discussed are aimed specifically at these groups and include data on other forms of migration within Europe, we believe the realities of tightened border control through datafication fall the hardest on those that have been deemed as 'illegal', 'irregular' or 'without papers'.

The term "iBorder", as conceptualised by Pötzsch (2015), refers to a "systematic description" of technologically aided border control, encompassing within it migration databases such as EURODAC or SIS II, and trusted traveller and advanced passenger information schemes such as the Registered Traveller and e-Borders programmes[6]. These databases are used as a means of identification, categorisation, surveillance and monitoring of migration within Europe as well as furthering efforts to develop a 'functioning' Common European Asylum System[7] (CEAS), capable of both policing external borders and determining responsibility of asylum claims among Member States (MS). Such a 'common' framework is a progressively important feature of EU policy following the rise of anti-immigration rhetoric and growing political pressure to control migration to and within Europe after a rise in arrivals since 2015. The usefulness of a term such as "iBorder" depicting the entire socio-technical assemblage is the ability to include the effect of both human and non-human agency in methods of sorting, categorising and filtering individuals on the move. As Pötzsch (2015: 111) argues, the "iBorder" facilitates a "dispersal" of the border into remote, algorithmic decisions capable of

[2] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en
[3] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1418993536491&uri=CELEX:32013R1052
[5] These terms have been chosen to represent politically significant categories of migrants, which are produced as a result of border regimes.
[6] https://www.gov.uk/registered-traveller
https://publications.parliament.uk/pa/cm200910/cmselect/cmhaff/170/17004.htm
[7] https://ec.europa.eu/home-affairs/what-we-do/policies/asylum_en

determining risks, as borders become attached to individuals as they move, no longer bound to physical borders but rather a transcendent entity attached to a physical self, a "technologically afforded aura". Within a datafied, remote control border system, people are followed by their own 'data trace', made up of data points from a wide range of sources - from data scraping social media profiles, to collecting information on meal preferences, financial transactions, previous travels, as well as more traditional data such as place and date of birth (Leese 2014).

Particularly pertinent to the policy developments we are seeing in relation to migration to and within Europe in recent years is the collection of biometric data. Fed into migration databases, the collection of this data is part of creating a fixed individual identity that can be shared across European countries. Though EURODAC, the oldest biometric database in Europe, was established in 2003 as a centralised database facilitating the designation of responsibility for asylum claims among MS, the growing importance of the collection of biometrics can be seen in the recently proposed changes to EURODAC that will allow for biometric information to be taken from a lower age, down from 14 years to 6 years old, and kept for a longer period of time, from 18 months to 5 years[8]. In addition, fingerprinting new arrivals in Greece has significantly increased, rising from 8% of arrivals being fingerprinted in September 2015, to 78% in January 2016 (LOC, 2016). This illustrates the onus placed on the collection and storing of data as a form of governing new arrivals.

At the same time, the use of biometrics is also a key element of providing humanitarian aid to refugees in camps across the world, from the use of IrisGuard in Jordan, through to the deployment of the Population Registration and Identity Management Eco-System (PRIMES) across many parts of Africa (Sánchez-Monedero 2018). Though biometric aid distribution is not yet used in Europe, the development of centralised, interoperable databases for managing aid has been used to cope with rising numbers of arrivals. For example, in Greece where the UNHCR is providing humanitarian aid through the distribution of cash cards in their Greek Cash Alliance (GCA) programme[9], cash assistance for basic needs is 'harmonised' across the mainland and islands through the use of ProGresV4 database, which monitors 'beneficiaries' data through monthly appointments and documentation inspection (Sánchez-Monedero 2018). The database contains not only basic information such as name and age, but also data points

[8] https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en
[9] https://www.unhcr.org/protection/operations/5a14306a7/greece-cash-alliance-meeting-basic-needs-harmonized-partnership-system.html

relating to a person's vulnerability, relationship status, and geographical location, and is shared across the UNHCR ESTIA programme which also provides housing for asylum seekers in Greece[10]. One important aspect of the card is its ability to reinforce geographical restrictions placed on asylum seekers. When a person has entered Greece by the Aegean island route, they have an island restriction placed upon them throughout their asylum claim, unless there are explicit reasons for this to be lifted - a practice in place as a result of the EU-Turkey deal[11]. If a cash card recipient leaves the island of their own accord and attempts to use their card on the mainland it will be automatically suspended. What becomes striking is the reinforcement of geographical restrictions within the same country by a humanitarian organisation. Cash card restrictions then become an extension of the use of hotspots as a method of containment on the islands - a policy that goes against the 1951 Refugee Convention which states in Article 26, that a refugee has "the right to choose their place of residence and to move freely within its territory"[12]. These types of initiatives have led to what Garelli and Tazzioli (2018) refer to as "techno-humanitarianism", which rather than empowering refugees leads to further control, containment and entrapment, whilst doing nothing to aid their legal claims for asylum and long-term prosperity. Without challenging the inherent failures of the Greek state in providing safe accommodation and basic provision for asylum seekers, the practise of geographical restriction, which has proven to be harmful for many due to the detrimental conditions on the islands (Oxfam 2019), becomes further enforced through the UNHCR's cash cards.

These processes associated with the collection of personal and biometric data as a form of geographical containment speak to the "internalisation" of borders in which the increasing focus on the human body as a definitive form of identification means we carry the border with us wherever we go and cannot escape it (Latonero and Kift 2018). Personal data becomes an individual's means of crossing borders and receiving vital aid whilst navigating asylum procedures and surviving in refugee camps and hotspots. Such developments within datafied borders and humanitarian systems highlight a worrying conflation of government and NGO data sharing, including the ability to trace the exact time and place of asylum seekers' financial transactions, facilitating much more invasive surveillance of their movements (Tazzioli 2017). In many respects, therefore, refugees have become populations of experimentation, exercised

[10] http://estia.unhcr.gr/en/home/
[11] http://europa.eu/rapid/press-release_MEMO-16-963_en.htm
[12] https://www.unhcr.org/4ca34be29.pdf

by a growing surveillance apparatus and data collection carried out by a range of actors (Privacy International 2014; Jacobsen 2015).

Whilst these developments have led to the internalisation of border control, data systems have also led to an "externalisation" of borders through the remote control of border security (Latonero and Kift 2018). Developments in digital surveillance technologies such as cameras, drones, integrated surveillance systems and GIS-based risk analysis methods have enabled a change in both how border control efforts are carried out as well as how people experience border crossing attempts (Topak, 2014:819). EUROSUR uses Unmanned Aerial Vehicles (UAVs or drones), amongst other surveillance tools, to better detect people attempting to cross into European territory, creating a "prefrontier" that allows for control of a border beyond traditional physical territories (Suchman et al, 2017:990, also Menjivar 2014). Initiatives within EU's Horizon 2020 programme include plans such as RANGER (RAdars for loNG distance maritime surveillancE and SaR operations) and SafeShore (which aims to create an impenetrable detection line at the border through developing Remotely Piloted Aircraft Systems (RPAS)) to further efforts of surveillance and the datafication of EU borders. The collation of these technologies including unmanned aerial systems, satellites, biometrics, data mining, profiling, and population metrics are part of a system of "persistent surveillance" that operates on the basis of continuous and perpetual intervention (Suchman et al 2017: 985). Carried out by a range of actors from both private and governmental organisations, these practices go beyond a reactive role of developing tools for surveillance and border security and become productive in creating new supranatural structures of surveillance within international border regimes (Aas 2011: 333).

The emerging field of "digital migration studies" (Leurs and Smets 2018) is beginning to advance discussions on these multifaceted developments that often incorporate paradoxical technological uses. Technologies used for governmental border control are part of creating new forms of 'datafied discrimination' and illegalisation of migrants whilst simultaneously providing what Laterno and Kift (2018: 3) call a 'new digital infrastructure for global movement'. The mobile phone, for example, is increasingly being used as a means of identification, risk profiling and monitoring alongside biometric databases. In Germany and Austria legislation has already passed that allows for the temporary containment of mobile phones to extract metadata in cases where a passport or ID is missing (DW 2017), a move that could potentially affect 50%-60% of asylum applicants (Toor 2017). Legislation such as this

illustrates clearly how asylum policy is seeking to incorporate mobile phones as a means of surveillance, identification and categorisation. This is particularly pertinent as such digital infrastructure, like borders themselves, are polysemic and double-edged. They afford agency within migratory routes yet open up further paths of surveillance and exploitation (Latonero and Kift 2018; Gillespie et al, 2018; Leurs and Smets, 2018). We are, therefore, confronted with a complex and comprehensive border regime that encompasses a range of technologies, locations and practices that cannot be reduced to any one actor or directional gaze. It includes both an internationalisation and externalisation of borders, both private and public bodies, and both personal devices and interoperable databases. It is also not ever a 'complete' or 'sublime' project but instead, as Walters (2011) notes, relies on the "technological work" of multiple actors, continuously creating spaces for negation and mediation of bordering practices as they occur.

Data politics in the governance of refugees

Through identifying the ways in which data and technologies are used within datafied border regimes, we can begin to see how the advent of datafication takes on meaning not simply as a technical development, but as a distinctly political one. This requires us to frame data in relation to a particular mode of governance that enacts particular ways of managing populations. We can draw here from insights within Critical Data Studies that have highlighted the performative power in and of data processes. "Dataism" as Van Dijck (2014) terms the ideological component of the datafication paradigm, is premised on a set of assumptions that carry great significance. There is, for example, an assumption that there is "a self-evident relationship between data and people, subsequently interpreting aggregated data to predict individual behaviour" (Van Dijck 2014: 199). The assumption is that algorithmic processing of lots of data can serve to anticipate, conjecture and speculate on future behaviour, activities and threats. As such, onus is placed upon prediction, which finds resonance in wider logics of security in addition to drawing from traditions within data science. The aim is to organise politics according to what Massumi (2015) has described as a wider "operative logic of *pre-emption*". Such logic, in turn, provides an apparent necessity and justification for limitless measures to be taken to ward off possible threats.

In other words, the advent of datafication is rooted in a belief in the capacity of data to interpret social life. As Harcourt (2015) describes it, power comes to circulate by a new form of rationality, one that is based on algorithmically processed data-sets driven by a "digital

doppelgänger logic" in search of our data double. For such assumptions to take effect, and for data systems to be scalable to generate sufficient meaning, there is a necessary trend to reduce social identities, mobilities and practices to data that can be managed and sorted as abstractions without a clear understanding of the embodied power relations and social effects produced by those activities (Monahan 2008; Costanza-Chock 2018). Political reasoning comes to circulate around inferences, what Amoore (2011) calls "data derivatives", that grants authority to knowledge domains based on software engineering and data science. With that, the emphasis within governance is placed on novel ways of calculating risk that provides a framework for generating and collecting infinite amounts of data, whilst at the same time shifting the meaning, boundaries and implications of risk (Yeung 2018).

The turn to data collection and algorithmic decision-making is therefore not simply a question of quantity – being able to process more information at a faster speed. It is also a qualitative shift that shapes reality and political subjects. Of course, the focus on data as a key component of governance is not a new or even recent development per se. If anything, the collection of information on citizens and subjects has always been essential to governance, for everything from land allocation, tax collection and military recruitment (Hintz, Dencik and Wahl-Jorgensen 2018). Classification of information gathered on populations is a familiar practice, starting with censuses in the nineteenth century and gaining further prominence with the development of the centralised state database of personal information in the 1970s (Rule 1973). With regards to borders, the monopolisation of legitimate movement and centralisation of information of people on the move began with the passport and has since developed through electronic databases that collect data traces and biometrics as a means of storing and monitoring information about moving populations (Broeders 2007). Thus, digital transformations, and the onus on the mass collection and analysis of data across social life, have advanced and (re)configured this form of bureaucratisation and, with that, the nature, role and meaning of data in state-corporate-citizen relations.

As a way to illustrate the political significance of the turn to data-driven governance, we now outline how data comes to serve a border security model that aims to control and restrict illegalised migration, targeting politically undesirable refugee populations within Europe. Importantly, we therefore understand data politics as enacting power dynamics at different inter-connected scales that requires us to consider both the politics *in* data and associated infrastructures, as well as the politics *of* data, highlighting the agendas and interests that

advance the implementation of these technologies (Ruppert et al 2017). As Pallister-Wilkins (2016) argues, the use of digital technologies should be considered as part of a wider logic of governance, in which the propagation of datafied borders is a continuation of historical forms of border security "that follow colonial practices of border control" (161). Driving the proliferation of the datafied border is what Green (2012: 24) describes as a fantasy of a "Brave New (fully secure) World", one controlled by rationality, science and "post racial" methods of border control (Vukov 2016: 81). A key aspect of this securitised world is that through biometric identification, interoperable migration databases and high levels of surveillance, borders become omnipresent (Dijestelbloem and Broeders 2015: 25).

The operationalisation of data in this omnipresence of borders can be seen clearly in the forms of identification and categorisation that are created on the basis of mass data collection. Data systems produce "measurable types" such as "at risk" that are "actionable analytical constructs of classificatory meaning, based exclusively on what is available to measure" (Cheney-Lippold 2017: 24). We see this, for example, in the way fingerprinting and EURODAC work as a fundamental element of border control and asylum in Europe. The use of compulsory fingerprinting, commonly associated in Europe with criminality, is an integral part of the Dublin Convention and EURODAC, and demonstrates the prevalence of data-driven governance reliant upon what has been described as a general criminalisation and social sorting of displaced peoples - what Aas (2011) refers to as the creation of "crimmigrant bodies". This process relies on the construction of data doubles, which impose upon individuals an identity used within databases and bureaucracies that are premised on practices of mistrust and control. For EURODAC, when a person's fingerprint is taken, they are placed in one of three categories. Category 1 defines a person as an applicant for international protection, category 2 defines a person as having crossed, or attempted to cross, a border illegally, and category 3 defines someone as being a potential illegal immigrant, who has been unsuccessful at gaining asylum status, is without papers, and has been found within a MS. Within these categories, the latter two impose an illegal status upon an individual immediately, though the first category also has the potential to create an illegal body if a person is to move to a second MS through irregular means and apply for asylum there. Such methods are justified on the basis that this will prohibit "asylum shopping", or duplicate asylum claims being made, in line with the Dublin Convention (Broeders and Hampshire 2013; Broeders 2009; van der Ploeg 1999). Regardless of the justifications, the productive nature of such mechanisms creates what Aas has referred to as not only an "immobilised global underclass", but an "*illegalised* global underclass" (2011:332,

emphasis in original), who become the reason for, and target of, intensified surveillance systems.

The practise of fingerprinting is therefore "a major hallmark" of criminalisation in Europe (Ajana 2013: 583), and signals a significant form of function creep in relation to EU migration databases in which data is used for functions beyond its initial scope. Whilst the conflation of refugees with criminality is furthered through the interoperability of SIS II, EURODAC and the Europol Information System[13] (EIS) it is premised on the exploitation of an unintended "added value" of EURODAC and compulsory fingerprinting (Ajana 2013: 581). Furthermore, as legal pathways into Europe are closed through the focus on securing external borders, with EU efforts to fund Turkish and Libyan coastguard operations[14], alongside the expansion of EUROSUR, people are pushed toward irregular means of travel. This creates the illegalised migrant by default, whereby methods of entry classify an individual as illegal despite potential legitimate reasons for acting as such. Thus, the proliferation of methods for tracking and profiling individuals mean border security regimes actively produce the 'illegal migrant' in what Andersson (2014, 2016) refers to as an 'illegality industry'.

Whilst the level of surveillance and data collection may not be categorically different depending on someone's classification – 'asylum seeker', 'economic migrant' or otherwise - the objectives and consequences relating to their data is likely to differ greatly. Importantly, once these data points become attached to an identity they become hard to shake off and difficult to challenge. Through identification processes, surveillance of a person throughout their migration journey and asylum procedure is possible. If someone has been identified as 'illegal', whether this is through a decision within EURODAC, or being intercepted when making an attempt to reach Europe by sea, then this label and identity becomes destructive. "Identification is not reducible to identity" as Amoore (2006: 344) puts it. This not only highlights the paradoxical way in which data analytics within datafied border regimes produce identities that are both independent and permanently attached to a person, but becomes of particular importance when discussing targeted groups such as asylum seekers and refugees

[13] https://www.europol.europa.eu/
[14] http://europa.eu/rapid/press-release_IP-17-2187_en.htm
https://www.avrupa.info.tr/en/project/strengthening-operational-capacities-turkish-coast-guard-managing-migration-flows

whose lives and experiences are continuously shaped by interactions with bureaucratic institutions who enforce such identities upon them.

These datafied identities, in turn, can create a "data-banned" population (Bigo 2014) in which the profiling of individuals based on 'people like them' results in the exclusion of entire categories or groups of people. Or, inversely, in other cases the lack of data to create an acknowledged identification leads to people being kept out. For example, in juxtaposition to databases that intrusively collect information that can damage an individual's ability to access fundamental rights, Latonero and Kift (2018:6) suggest that in the case of EUROSUR the opposite occurs. Here, they argue, a refusal to collect personal data is enacted, and instead any attempts to enter the EU if done so through illegal means is pre-emptively denied, regardless of whether a person may have a right to asylum once they reach European territory. In other words, the category of illegality as determined through surveillance technologies overrides the lived experiences of those subject to such monitoring. This points to the politics that emerges in the constructed 'distance' (Goriunova 2016) between an individual and its data subject, the human and the digital. As Aas argues, this "discursive and political coupling of migration and crime" creates a "specific dynamic of social exclusion" (2011: 337).

The creation of 'crimmigrant bodies' is therefore an integral part of a wider process of what Lyon calls "social sorting" building on Gandy's (1993) notion of the "panoptic sort". This refers to the advancement of data-driven surveillance programmes that are dependent on searchable databases and categorisation of individuals, resulting in differential treatment and discrimination against a person depending on how they have been identified by their "virtual selves" (2004:142, also Lyon 2007). We can illustrate such social stratifications surrounding borders by applying Broeders' and Hampshire's (2013) notion of 'black listing', 'green listing' and 'grey listing'. 'Black listing' is similar to the notion of the 'data banned' population or individual, whereby a security logic dictates that those entering through illegal means or deemed a threat are *automatically* excluded, based on the types of surveillance and data practices we have outlined above. In opposition to this you have the 'green listed' category, a category that refers to efforts to allow 'desirable' travellers easier border crossings based on data analysis prior to travelling. In the UK an example of this is the Registered Traveller programme, which has strict eligibility criteria regarding nationality, visa and frequency of travel, and allows a person to skip the landing card procedure and enter through the UK and EU passport lanes. 'Grey listed' travellers are those who have not yet been either accepted or

banned. Acting as a filter, such categorisation refers to activities of data-driven risk assessments before travel to flag up those requiring further scrutiny. Within this process, a traveller's data will be checked amongst law enforcement and migration databases - EURODAC, SIS II, VIS, EIS - and processed against pre-set criteria, assessing whether or not they pose a security risk. To gain this data, schemes such as Advanced Passenger Information (API), and Passenger Name Records (PNR)[15] are used whereby a passenger submits their personal data, most commonly to the airline they are flying with, before travel. After analysis a person is either 'green listed' or 'black listed', determining their ability to cross borders.

The usefulness of this framework is that it provides a heuristic tool for demonstrating the highly differential experiences of border controls. Whilst Bigo (2014) notes that even for 'green listed' travellers, participation in high levels of dataveillance is premised on mistaking "speed for freedom", the violence of such forms of border control are currently being felt most acutely by those deemed undesirable, or 'at risk', and placed on the 'black list'. The automatic exclusion felt by those 'black listed' compares harshly to those within the 'green listed' category, who freely submit biometric and other data in order to reduce the time spent crossing borders. As Hage (2016: 44) claims: "Some people roam the globe like masters, others like slaves. Some are the subjects of the global order, others are its objects". Increased surveillance and the development of a datafied border significantly entrenches the control of unwanted and undesirable migrant populations. In such cases the border becomes more impenetrable than ever, creating "a world of perennial dataveillance where the border looms large" (Amoore 2006: 343). What is more, this 'productive' and 'persistent' surveillance reflects the priority granted to novel ways of calculating risk that provides a framework for anticipatory and pre-emptive measures as the defining operative logic of politics. Rather than seeking to understand underlying causes, which, in the case of border crossings would signal a focus on the violence, war or environmental disaster a person is fleeing from, pre-emption shifts attention to managing consequences - i.e. controlling and restricting resulting migration to Europe.

As such, practices of categorisation, risk analysis, and identification of individuals that are advanced with datafied borders are an integral part of the production of illegalised migrants as well as being part of a global system that seeks to retain control over movement for a variety of economic and political motives. Harsh disparities exist between experiences of freedom of

[15] https://eur-lex.europa.eu/eli/dir/2016/681/oj

movement, furthering injustice and violence to those identified and categorised as undesirable and placed on the 'black list'. These processes, along with strict criteria for granting asylum, therefore succeed in converting migrants into 'illegal' and 'deportable' individuals, not worthy of protection or rights, but instead viewed as opportunists wishing to exploit the asylum system (De Genova 2013:1181; Crawley and Skleparis 2018:49). Such perceptions are also advanced through the continuation of a 'crisis' rhetoric that is often used in reference to migration within Europe (Kallius et al 2016:127). The acceptance of such forms of datafied categorisation without critical questioning ignores the fact that these categories are constructed within explicitly political systems aimed at limiting migration. The illegalisation of migrants, social sorting, the focus on border security and the overly simplified and often miscalculated categorisation of individuals within these processes do little to curb the migration 'crisis'. Yet they retain a "political usefulness" through the dissipation of blame and accountability (Andersson 2016:1066). Elements of this political usefulness play out in the wider discourse of technological solutionism that has taken hold of European border policies, shifting accountability away from governments and human actors towards digital databases and algorithms. Thus, the advent of the datafied border, which both disperses accountability and claims to increase border security, can be seen as a useful political tool whilst being sold as a natural evolution of border security in a time of 'crisis'. In such context, datafied borders hold, as Broeders and Hampshire (2013) argue, both symbolic and instrumental value within anti-immigration societies.

Situating data in social justice agendas

By focusing on transformative tendencies and logics that accompany data-driven governance and outlining how data is operationalized in the continued suppression of rights for migrants and refugees within border regimes, we can begin to advance a more systemic critique of datafication. The issue here is then not simply how an individual's data is collected, stored or algorithmically processed, but rather how data-driven decision-making is part of a particular economic and political agenda that seeks to systematically stigmatize, marginalise and exclude 'unwanted' migrant populations. Analysing data-driven governance within such a framework is important because it makes an explicit link between data and social justice - a framework of 'data justice' - on terms that demand a response that is necessarily contextual, collective and historically rooted. Whilst a data justice framework is still nascent and varied in interpretation, approaches tend to unite around an emphasis on outlining data in relation to structural

inequality and social (in)justice (Newman 2015; Dencik et al. 2016, 2018; Heeks and Renken 2016; Taylor 2017; Johnson 2018). As such, it challenges the notion that data and data-driven technologies are neutral artefacts, and that what is at stake can be sufficiently captured by simple binaries such as efficiency vs. privacy, or good vs. bad data. It also goes beyond an engagement with the inequalities and discriminatory effects of algorithmic processes that seeks to locate such injustices as 'errors' or as forms of 'bias' within the technologies that can be 'fixed' with more or different data or tweaks to the algorithms. Instead, we see data justice as a framework that understands the trend of datafication in the context of the interests driving such processes, and the social and economic organisation that enables them. This in turn invites an engagement with data politics that is not centered on the data system itself, but rather on how data practices relate to other social practices within particular social and political constellations, a 'decentring' of data in the exploration of the implications of datafication (Dencik 2019). This also suggests that datafication, and datafied borders, are not de facto 'things' but are processes that are continuously shaped by a multitude of - sometimes contradictory - forces, opening up possibilities for intervention and resistance.

We advance such a framework as a way to 'situate' data (Haraway 1988), an important practice for overturning the normalisation of data collection for knowledge and decision-making, particularly in relation to border regimes. This means that when approaching any kind of knowledge, it is essential to ask about the social, cultural, historical and material conditions in which that knowledge was produced, as well as the identities of the humans who are making that knowledge (D'Ignazio and Klein 2019). This has particular pertinence for the nature of political mobilisation that has so far surrounded developments in data-driven governance. Issues of data systems and digital surveillance have tended to primarily engage groups who have a particular concern with digital rights or technical infrastructures. We have seen this in the numerous efforts to advance data protection legislation, mainstream encryption, and lobby on upholding individual privacy. These efforts have sought to raise public awareness and push back on extensive and intrusive forms of data collection (Dencik and Hintz 2017). However, we have seen much less engagement with these developments from groups outside digital rights and technology oriented spaces, groups that we might consider as being concerned with social justice issues, such as inequality, discrimination and oppression, or who come from historically marginalised communities. That is, there has been a degree of 'disconnection' between those concerned with technology on the one hand and those concerned with social justice on the other (Dencik et al. 2016).

By highlighting how data is situated, and outlining how data processes come to serve particular policy agendas, we see the potential for also 'decentering' data in political mobilisation that encompasses an engagement with data-driven governance whilst drawing on expertise and on-going struggles for social justice (Gangadharan and Niklas 2019). Moreover, such an approach positions the lived experiences of the turn to data-driven technologies at the centre of any analysis of its implications, forcing us to consider how such technologies enact forms of 'violence' against particular communities and social groups (Hoffmann 2018). A data justice framework therefore invites a broader range of stakeholders and entry-points than the relatively narrow parameters of digital rights and technology activism, and advances a debate on how to integrate datafication within social justice agendas, including those concerned with borders and the rights of refugees. This is particularly pressing as the rapid introduction of data-driven decision-making in the governance of borders, asylum-processes, and social services more broadly, significantly circumvents and dislocates established frameworks that are in place for the protection of social and economic rights, not least for vulnerable populations. These are frameworks that are not necessarily addressed by a focus on data protection issues. As we have outlined, dataveillance has advanced the omnipresence of borders, establishing stratifications through identification, registration, categorisation and interoperability, determining access to basic needs and human rights. There is an urgent need to (re)articulate these rights and related freedoms as they intersect with processes pertaining to datafication (see also Taylor and Mukiri-Smith 2019). By highlighting the criminalisation and sorting processes that accompany the datafied border, we can start to pinpoint the nature of injustices that people experience and relate them to the interests that are being served and whose interests are being ignored or undermined.

As such, from this data justice perspective the question of what is at stake with data, and a datafied society, requires a political engagement from the outset rather than one that privileges technological or technocratic processes. Moreover, it asks of us to consider the current datafication paradigm as a continuation of certain power dynamics that have historically advanced the oppression of certain groups and populations, with the view to identify possibilities for intervention and resistance from multiple directions, many of which will not be about data. Instead, challenges can be aimed at the logics and functions that are being advanced, determining control over data collection, allowing for a space of refusal, in addition to thinking through alternative infrastructures that privilege the experiences and interests of

those people who are being impacted – in this case asylum-seekers, refugees and illegalised migrants. In this way we can then also politicise some of the paradoxes we have touched upon above in which humanitarian causes come to intersect with oppressive forms of governance; or when personal digital devices are weaponised for the purposes of suppressing targeted groups. Coming to grips with the way data enacts border security regimes therefore requires the active participation from those who experience and understand the on-going struggles that surround the politics of borders as well as those who engage with questions of technology.

Conclusion

The topic of borders has in many ways become the definitive feature of contemporary international relations, not least with regards to the 'Fortress Europe' approach that has shaped migration policy within and beyond Europe in recent years. The so-called refugee 'crisis' of 2015-16 provided the impetus for a rapid deployment of technologies and a turn to data as a central component of enacting border control. The advent of 'big borders' consolidates an overt enthusiasm for funding, creating and contracting digital infrastructures that explicitly seek to take advantage of the possibility to collect and analyse large amounts of data from a range of sources. In Europe this has manifested itself as a border regime increasingly organised around a set of interoperable databases, digital registration technologies, identity verifications, and various algorithmically processed risk assessments that involve a range of different actors, locations and devices.

The role of digital technologies in border control and asylum-processes puts a stark light on the meaning of a turn to data-driven governance. The effort to 'know' and 'see' populations through data systems designed and optimised to enforce notions of security at scale shifts our engagement with data towards an explicit concern with power and control. With that, there is an explicit need to (re)socialise and (re)politicise data processes as situated forms of knowledge. In our analysis of changes in border regimes we have shown how developments propagate datafication whilst retaining historical methods of governance over unwanted migrant populations, advancing an ongoing political project aimed at limiting freedom of movement for displaced people. Within this, the disparities between lived experiences of datafied borders become glaring, emphasising how data processes productively further discrimination and marginalisation, negatively impacting upon the life chances of resource-poor and targeted populations.

In outlining these changes, it therefore becomes pertinent to discuss these developments happening with the implementation of data systems in relation to on-going experiences of injustice. As we have argued in this article, the functionality of securitised and datafied border systems relies upon practices of criminalisation, identification and social sorting, and relates to certain assumptions of data-driven governance that hold substantial political significance. This therefore means privileging justice concerns that are not just about the distribution of resources, but that can also address the structural violence that emerge from how these data systems are attributed meaning within the current political climate of Europe. By engaging with data politics in this wider sense, we can begin to assert social justice implications on terms that are simultaneously more inclusive of groups who have so far viewed issues pertaining to data and technology as primarily technical or digital rights focused, and can position the experiences of those who are disparately impacted by the deployment of data-driven technologies at the forefront of discussions.

References

Aas, K. F. (2011) 'Crimmigrant' bodies and bona fide travellers: Surveillance, citizenship and global governance, *Theoretical Criminology*, 15(3), pp.331–346

Ajana, B. (2013) Asylum, Identity Management and Biometric Control *Journal of Refugee Studies* 26(4), pp.576-595

Ajana, B. (2015) Augmented borders: Big Data and the ethics of immigration control, *Journal of Information, Communication and Ethics in Society*, 13(1), pp.58 – 78

Amoore, L. (2006) Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25, pp.36-351

Amoore, L. (2011). Data Derivates: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society*, 28(6), pp. 24-43.

Andersson, R. (2014) Hunter and Prey: Patrolling Clandestine Migration in Euro-African Borderlands, *Anthropological Quarterly*, 87(1), pp.119-149

Andersson, R. (2016) Europe's failed 'fight' against irregular migration: ethnographic notes on a counterproductive industry, *Journal of Ethnic and Migration Studies*, 42(7), pp.1055-1075

Andrejevic, M. (2017). To pre-empt a thief. *International Journal of Communication*, 11(2017), pp. 879-896.

Bigo, D. (2014) The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts. *Security Dialogue*, 44(3), pp. 209-225

Broeders, D. (2007) The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants, *International Sociology*, 22 (1): 71–92.

Broeders, D. (2009) *Breaking Down Anonymity: Digital Surveillance of Irregular Migrants in Germany and the Netherlands.* Amsterdam: Amsterdam University Press.

Broeders, D. and Hampshire, J. (2013) Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe, *Journal of Ethnic and Migration Studies*, 39(8), pp.1201-1218

Carrera, S. & Hernanz, N. (2015) Re-Framing Mobility and Identity Controls: The Next Generation of the EU Migration Management Toolkit, *Journal of Borderlands Studies*, 30:1, 69-84

Cheney-Lippold, J. (2017). *We Are Data*. New York: New York University Press.

Costanza-Chock, S. (2018). Design Justice, AI, and Escape from the Matrix of Domination. *JoDS*. Available at: https://jods.mitpress.mit.edu/pub/costanza-chock

Crawley, H. and Skleparis, D. (2018) Refugees, migrants, neither, both: categorical fetishism and the politics of bounding in Europe's 'migration crisis', *Journal of Ethnic and Migration Studies,* 44(1), pp.48-64

De Genova, N. (2013) Spectacles of migrant 'illegality': the scene of exclusion, the obscene of inclusion, *Ethnic and Racial Studies*, 36(7), pp.1180-1198

Dencik, L. (2019) Situating practices in datafication – from above and below. In: Stephansen, H. and Treré, E. (eds.) *Citizen Media and Practice*. London and New York: Routledge.

Dencik,L. and Cable, J. (2017). The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication*, 11(2017), pp. 763-781.

Dencik, L. and Hintz, A. (2017) Civil society in an age of surveillance: beyond techno-legal solutionism? *Civil Society Futures.* Available at: https://civilsocietyfutures.org/civil-society-in-an-age-of-surveillance-beyond-techno-legal-solutionism/

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambivalence of anti-surveillance resistance in political activism. *Big Data & Society, 3*(2), 1–12. doi:10.1177/2053951716679678

Dencik, L., Jansen, F. and Metcalfe, P. (2018). A conceptual framework for approaching social justice in an age of datafication. *Datajusticeproject blog*. Available at: https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/

D'Ignazio, C. and Klein, L. (forthcoming) *Data Feminism*, MIT Press

Dijstelbloem, H. and Broeders, D. (2015) Border surveillance, mobility management and the shaping of non-publics in Europe. *European Journal of Social Theory*, 18(1) pp.21–38

DW, (2017) German parliament passes tighter asylum laws. *DW,* available at http://www.dw.com/en/german-parliament-passes-tighter-asylum-laws/a-38897488

Gandy, O. H. (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO:Westview.

Gangadharan, S. P. and Niklas, J. (forthcoming) Decentering Technology in Discourse on Discrimination. *Information, Communication & Society.* Special Issue on 'Data Justice'.

Garelli, G and Tazzioli, M. (2018) Migrant Digitalities and the Politics of Dispersal: An Introduction. *Border Criminologies* Available at: https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2018/05/migrant

Gillespie, M., Osseiran, S. and Cheesman, M. (2018) Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances. *Social Media + Society* 2018(1), pp.1– 12

Goriunova, O. (2016). Data Subjects. Paper presented at *Social Media and Politics Symposium*, Ulster University, 3 June 2016.

Green S. (2012) Absent details: the transnational lives of undocumented dead bodies in the Aegean. *(Published in Greek in: ΤΟ ΠΡΟΣΦΥΓΙΚΟ ΚΑΙ ΜΕΤΑΝΑΣΤΕΥΤΙΚΟ ΖΗΤΗΜΑ ΔΙΑΒΑΣΕΙΣ ΚΑΙ ΜΕΛΕΤΕΣ ΣΥΝΟΡΩΝ. Εκδόσεις Παπαζήση. Editor: Σεβαστή Τρουμπέτα)*

Hage, G. (2016) ´ Etat de si`ege: A dying domesticating colonialism? *American Ethnologist*, 43(1), pp. 38–49

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

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

Hintz, A., Dencik, L. and Wahl-Jorgensen, K. (2018) *Digtial Citizenship in a Datafied Society*. Cambridge: Polity Press.

Hoffmann, A. L. (2018) Data Violence and How Bad Engineering Can Damage Society. *Medium.* Available at: https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4

Jacobsen, K. L. (2015) Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees. *Security Dialogue*, 46(2): 144-164.

Johnson, J. (2018) *Toward Information Justice: Technology, Politics, and Policy for Data in Higher Education*. Springer.

Kallius, A., Monterescu, D. and Rajaram, P. K. (2016) Immobilizing mobility: Border ethnography, illiberal democracy, and the politics of the "refugee crisis" in Hungary. *American Ethnologist*, 43(1), pp. 25–37

Latonero, M. and Kift, P. (2018) On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control, *Social Media and Society* pp1-11

Leese, M. (2014) The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), pp.494–511

Leurs, K. and Smets, K. (2018), Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe. *Social Media + Society*, 2018(1), pp.1-16

Library of Congress (LOC) (2016), Refugee Law and Policy: Greece. *Library of Congress*. Available at: https://www.loc.gov/law/help/refugee-law/greece.php

Lyon, D. (2004) Globalizing Surveillance, Comparative and Sociological Perspectives. *International Sociology,* 19(2), pp.135–149

Lyon, D. (2007) Surveillance, Security and Social Sorting Emerging Research Priorities. *International Criminal Justice Review*, 17(3) pp 161-170

Massumi, B. (2015). *Ontopower: War, Powers, and the State of Perception*. Durham and London: Duke University Press.

Menjıvar, C. (2014) Immigration Law Beyond Borders: Externalizing and Internalizing Border Controls in an Era of Securitization. *Annual Review of Law and Social Science*, 10, pp. 353-369

Monahan, T. (2008). Editorial: Surveillance and Inequality. *Surveillance and Society*, 5(3), pp. 217-226.

Newman, N. (2015) Data Justice: Taking on Big Data as an Economic Justice Issue. Report. Available at: http://www.datajustice.org/blog/data-justice-report-taking-big-data-economic-justice-issue

Oxfam (2019) *Vulnerable and Abandoned*, Oxfam Media Briefing. Available at: https://www.oxfamnovib.nl/Files/rapporten/2019/2019-01%20Greece%20media%20briefing_FINAL-embargo%20notice%20(1).pdf

Pallister-Wilkins, P. (2016) How walls do work: Security barriers as devices of interruption and data capture. *Security Dialogue* 47(2) 151–164

Pötzsch, H. (2015). The emergence of iBorder: bordering bodies, networks, and machines. *Environment and Planning D: Society and Space*, 33(1), 101-118.

Privacy International (2014). Wherever you go, they can follow: Modern surveillance technologies and refugees. Available at: https://arxiv.org/pdf/1806.02711.pdf

Rule, J.B. (1973). *Private lives and public surveillance*. London: Allen Lane.

Ruppert, E., Isin, E. and Bigo, D. (2017). Data politics. *Big Data & Society*. July-December, pp. 1-7. Available at: http://journals.sagepub.com/doi/abs/10.1177/2053951717717749

Sánchez-Monedero, J. (2018) The datafication of borders and management of refugees in the context of Europe. *Working Paper*, DATAJUSTICE project. Available at: https://datajusticeproject.net/wp-content/uploads/sites/30/2018/11/wp-refugees-borders.pdf

Suchman, L., Follis, K. and Weber, J. Tracking and Targeting: Sociotechnologies of (In)security. *Science, Technology, & Human Values*, 42(6), pp.983-1002

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms. *Big Data & Society*, 4(2).

Taylor, L. and Mukiri-Smith, H. (2019) Global Data Justice: framing the (mis)fit between statelessness and technology. *European Network on Statelessness.* Available at: https://www.statelessness.eu/blog/global-data-justice-framing-misfit-between-statelessness-and-technology

Tazzioli, M. (2017) The Circuits of Financial-Humanitarianism in the Greek Migration Laboratory. *Border Criminologies* Available at: https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/09/circuits

Toor, A. (2017) Germany moves to seize phone and laptop data from people seeking asylum, *The Verge,* Available at: https://www.theverge.com/2017/3/3/14803852/germany-refugee-phone-data-law-privacy

Topak, O. (2014) The biopolitical border in practice: surveillance and death at the Greece–Turkey borderzones *Environment and Planning D: Society and Space*, 32, pp.815 – 833

Van der Ploeg, I. (1999) The Illegal Body: ‘‘Eurodac’’ and the Politics of Biometric Identification. *Ethics and Information Technology* 1, pp.295–302

Van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society*, 12(2), pp. 197-208.

Vukov, T. (2016) Target Practice The Algorithmics and Biopolitics of Race in Emerging Smart Border Practices and Technologies. *Transfers* 6(1), pp. 80–97

Walters, W. (2011) Rezoning the Global: Technological Zones, Technological Work and the (Un-)making of Biometric Borders. In: Squire, V. (ed.) *The Contested Politics of Mobility: Borderzones and Irregularity*, Abingdon: Routledge, 51-73.

Yeung, K. (2018) Algorithmic government: Towards a New Public Analytics? Paper presented at *ThinkBig*, Windsor, 25 June.