Re:framing
Migrants in the
European Media

DIVERGENCE AND OBFUSCATION

Project title	Re:framing Migrants in the European Media		
Start date	01/02/2022	**Duration**	15 months
Project URL			
Contractual due date	31/02/2023	**Actual submission date**	17/02/2023
Nature	R= Document, report	**Dissemination level**	PU= public
Authors	Mitchel Njoki,Francesca Trevisan, Gemma Galdon Clavell		
Contributors	Evren Yalaz, Patricia Vazquez, Emilia Paesano		
Reviewers	Menno Weijs, Badria Zeino-Mahmalat		

This project has received funding from the *European Commission DG CNECT* under grant agreement No LC01727412.

EXECUTIVE SUMMARY

Obfuscation is the practice of making something difficult to understand or interpret. This can be done for a variety of reasons, such as to protect intellectual property, to hide sensitive information, or to make the inner workings of a system more difficult to reverse engineer. Obfuscation techniques can be applied to various forms of data, including software code, electronic documents, and communication messages. These techniques can include methods such as replacing variable names with random characters, rearranging code to make it more difficult to follow, or encrypting data to make it unreadable without a decryption key. It is often used in the field of computer programming, where it can help to protect the intellectual property rights of software developers. However, it can also be used for malicious purposes, such as to conceal the behavior of malware or to make it more difficult for security researchers to analyze and identify security vulnerabilities. Through semi structured interviews this report analyses different obfuscation techniques and challenges the increased hyper-surveillance of the migrant community

TABLE OF CONTENTS

The issue of justice in migratory movements has been the subject of concerted efforts and debate, more so in the past decade. Whether in the reports of harrowing migrant journeys, drowning refugees, ill-managed camps, uncoordinated asylum granting efforts among others, migrants are at the heart of many policy interventions in Europe and around the world. During this process, an ongoing narrative of migrants as security threat has emerged. The European fortress uses both physical barriers, for instance the border wall on the Belarus border built by Poland or the fence in Melilla, as well as digital barriers, such as the expansion of FRONTEX's surveillance efforts. Framing migrants and refugees as security issues has led to several regulatory actions resulting in increased surveillance and heightened concerns around surveillance measures.

This report seeks to outline the problem with **social media surveillance** as it concerns migrant populations and highlight the **obfuscation mechanisms** that they have been forced to take to preserve their privacy and protect themselves.

Obfuscation (Powles, 2015) is the practice of making something difficult to understand or interpret. As a practice, obfuscation flies in the face of the numerous mini-transactions that we engage in every day that collect data. The various techniques seek to confuse or subvert the original tracking intention or simply add more time to separating bad data from good which frustrates the opposing side of data collection. This can be done for a variety of reasons, such as to protect intellectual property, to hide sensitive information, or to make the inner workings of a system more difficult to reverse engineer. We view obfuscation here as privacy-preserving in the context of migrants for several reasons, mainly to reinforce their data rights, to restrict the unlawful and unethical usage of their data and to return control of both their data and narratives on their lives back to migrants.

Obfuscation techniques (Powles, 2015) can be applied to various forms of data, including software code, electronic documents, and communication messages. This can include methods such as replacing variable names with random characters, rearranging code to make it more difficult to follow, or encrypting data to make it unreadable without a decryption key. It is commonly used in the field of computer programming, where it can aid to protect the intellectual property rights of software developers. However, it can also be used for malicious purposes, such as to conceal the behaviour of malware or to make it more difficult for security researchers to analyse and identify security vulnerabilities.

This report assesses the obfuscation and divergence techniques utilised by migrant communities and challenges the increased **hyper-surveillance of the migrant community**. In parallel, we will explore

existing **ways of subverting social media dynamics** to make them work for migrant and refugee populations. There is scattered evidence that marginalised communities informally adapt social media tools to serve their purposes, for reasons related to activism, convenience and lack of resources. We will look to systematise existing knowledge on these informal practices and to deepen our understanding on why and where they emerge. Therefore, this task will engage in literature review of media sources, but also interviews with key stakeholders, people who either have migrant backgrounds or work in close contact with migrants, who can help us reach the communities that may be engaging in these practices, which may encompass collective accounts or data obfuscation practices.

THE BORDER SYSTEM AND MIGRATION CONTROL

Borders are a combination of the physical, the digital, the human and the legal working in a complex tandem toward the aim of regulating mobility between countries. In the EU, twenty two out of twenty-eight countries follow the Schengen border code which abolished internal border controls and works through the cooperation of member states. A drastic digital transformation has occurred at the borders, particularly regarding the collection of biometric data, the increased use of Closed-circuit television (CCTV) and the consideration of new, largely unregulated technologies such as the deployment of drone technologies in border surveillance. The trend in border management has leaned heavily toward a security related focus with most of the changes and introductions being geared toward immigration control, increased surveillance creep and social sorting measures all which are backed by technological measures targeting policing and mobility control. The increased deployment of technologies is also proving to be a regulatory and technological challenge as the potential for data discrimination is not only high but has been proven to be a barrier to equal access and protection particularly for vulnerable travellers such as asylum seekers.

Automated border control systems rely on self-service devices and systems which take over the role of border control officers. Electronic passports are checked at e-gates and compare biometrics stored on the passport to the person and determine whether they may pass with border guards supervising the process. Migration has become a key concern for EU countries with various digital responses being deployed in an effort to address concerns about migration. The number of forcibly displaced persons has increased and the number of refugees has doubled from 10 million in 2010 to 20.4 million in 2019 (Pandey, 2020). In 2016, several Schengen members began tightening border control measures as a response to perceptions of threats by an increased influx of immigrants. In response, border control

measures have been ramped up with various surveillance technologies, such as the development of databases that use biometric data to control mobility in the EU such as EURODAC and SIS. Regulation (EU) 656/2014 defines the rules for border surveillance as follows: "It establishes greater legal certainty in the context of operations on external sea borders, and the provisions and rules concerning interception, rescue at sea and disembarkation. It emphasises safety at sea, the protection of fundamental rights and the principle of non-refoulement. It distinguishes between the different rules and procedures concerning interception on the high seas, in territorial waters and in contiguous zones". While the regulation seems to provide a rational basis for the expansion of surveillance, there are several stringent control measures which have been perceived as 'violent' in that they enable systematic forms of violence toward migrants and display a disregard for human dignity and equality at borders (Jones, 2016). Vrăbiescu refers to this as 'crimmigration' referring to the prioritisation of deporting criminalised migrants across internal EU borders (Vrăbiescu, 2020). Data extraction in the face of immigration has also become a question of the non-neutrality of data which contributes to 'anti-immigrant' control (de Haas, Castles, and Miller 2020).

The technological securitization of borders has developed preconceived notions that link migration to criminality (Metcalfe and Dencik 2019). The management of borders is not merely an administrative act, aimed at sorting, but in many ways has been framed as a political statement, as a representation of the 'empowerment-control' nexus in border control and management (Nedelcu & Soysüren, 2020).

In September 2020, the EU presented its "New pact on Migration and Asylum" , a migration management strategy intended to provide a greater and more comprehensive strategy on controlling migration. This has various implications on the digital strategy for managing asylum seekers including extending the scope of the Eurodac regulation to allow wider use of the data, including monitoring the secondary movements of irregular migrants who have not sought asylum. The pact seems to be a step towards mass deportation and its effects are already being felt as countries are taking advantage of stricter immigration policies to introduce procedures which are not cognizant of the rights of asylum seekers. Article 31 §1 of the Geneva Convention of 1951 prohibits the punishment of asylum seekers who have crossed borders illegally, provided that they arrived directly from countries where their lives were in danger and/or have valid reasons for violating the rights of entry. Despite the affirmation of the rights of asylum seekers, concerns over digital privacy violations have abounded, leading to legal action in the case of a lawsuit filed by a German NGO, Society for Civil Rights (GFF) against the German Government for a violation of an asylum-seeker's rights as it was stipulated that as part of the process of applying of asylum, the contents of their mobile phone would be required (Kaurin, 2019).

Asylum seekers have to submit several categories of personal data in order to have their applications processed. Their fingerprints are collected for use in Eurodac which collects and compares fingerprints of asylum seekers and irregular immigrants. The fingerprint data is transferred by national authorities to a central unit which is maintained by the European Commission. The data is compared to determine which EU member state should take responsibility for processing the asylum application. Initially the database was created to prevent 'asylum shopping' and maintain a central registry but it has been expanded since 2015 to include efforts to increase securitization. (Metcalfe & Dencik, 2019)

A combination of digital and regulatory measures has been introduced since 2015 in the area of irregular migration. The efficacy of these measures is in question as it has increased market opportunity for human traffickers and increased irregular migration through more perilous means (FRONTEX 2016). Additionally, it has also increased the number of migrants in detention centres for travelling undocumented and various human rights concerns have been posed about the legality of the stay of irregular migrants in detention centres.

Further to this an increase in funding for border guards and greater surveillance technology has seen irregular migrants being turned around and detained in their country of origin (Habib, 2021). The deployment of surveillance technology like long range cameras and night vision equipment as well as prospective technology like AI powered lie detectors and virtual border guards have been piloted to add onto the existing surveillance measures (Aljazeera, 2021). These measures are concerning and harmful particularly the recently piloted 'sound cannon' which is a long range acoustic device which fires bursts of noise at the border frontier in Greece (Nair, 2021). The largely unchecked use and collection of data has been of concern to data justice advocates as the European Border Surveillance Systems obtains personal data from refugees in the absence of informed consent and without consideration of coercive measures that would lead irregular migrants to acquiesce in having their data collected.

SOCIAL MEDIA DYNAMICS IN THE AGE OF MIGRATION

The exchange of information moves quickly with new technologies emerging that represent different ways to connect, understand and communicate with others. The advent of social media has made this more pertinent still, with users sharing and broadcasting personal information over the expanse of the networks. This presents a double-edged sword effect which will be explained in two ways: first; social media as access (to information, to help, to connection) and social media as surveillance of

migrants. In this way we can point out the myriad benefits and drawbacks and assess the opportunities for obfuscation and divergent practices.

Migrant communication practices through social media channels can, in the first place, foster inclusion, promote communication and allow for greater integration into the destination country. To begin with, nuances of language, behaviour, information on the asylum process as well as information on border patrol, coast guard movements and the safety of making perilous crossings can be sent through various social media channels. Not only does this help migrant communities it can also potentially save lives and allow loved ones to connect more easily with each other.

With the benefits, however, come the drawbacks. Social media can be used by governments and other actors to monitor and control the movements of migrants, and to collect information about their activities and experiences. Golan and Babis (2017) present a quadric-faceted approach to migrant populations on Facebook (now Meta). They relate social media usage with four facets of communication namely utility, care, emotive and legal. These facets help shape, in particular professional networks. Dekker and Engbersen (2013) posit a different fourfold categorization of social media functions in migrant communities: first, that social media maintains relevant networks, secondly that it offers the possibility to revive lost networks, third that it develops new networks and lastly, that the information infrastructure created on social media offers information exchange opportunities. Undergirding these hypotheses is the assumption of factfulness. Social media can also be used to amplify messages and information that may be biassed or misleading, and this can create tension and conflict within communities. Access to migratory information can assist migrants to assimilate. This, of course, depends on digital competencies and existing infrastructure. Obi et al (2020) raise a flag to the use of social media by introducing three hypotheses; that social media information represents informal sources of migration information beneficial to the migratory experience. That the potentialities of that information are constrained and can be hindered by incompleteness or factual incompleteness. Lastly, where the information is incorrect or misleading, the effect could be fatal at worst.

This intersection of migration and surveillance raises a number of concerns about privacy and civil liberties. Migrants, particularly those who are undocumented or who are seeking asylum, may be particularly vulnerable to surveillance. Governments and other actors may use surveillance technologies, such as surveillance cameras, phone and internet monitoring, and other forms of data collection, to monitor the movements and activities of migrants (Golan & Babis, 2017). This can be done for a variety of reasons, often framed as national security or public safety. However, not all of these reasons are done within ethical and legal guidelines. In particular several social media

functionalities exist solely for the purpose of collecting and mining data from users. This data mining is not neutral (Golan & Babis, 2017), its context can involve the personal contacts of a migrant person, resources and agencies they turn toward for assistance and additional measures they plan to take to feed, clothe and shelter themselves. Because they **need** to use these platforms (as often some providers can only be reached through them) a power asymmetry is created. This places migrants at the bottom of a hierarchy and adds to their vulnerability. Their choices are limited in terms of exercising their data rights as often their mere survival consumes a majority of their time and attention and they may not have the resources available to devote to in-depth privacy preservation. Additionally, their data feeds into a funnel of similar results with overarching statistical inferences used to make policy decisions and in several cases, fuel anti-migrant rhetoric.

In some cases, surveillance may be used to target specific groups of migrants, such as refugees or asylum seekers, and to discriminate against them based on their ethnicity, religion, or national origin. This can lead to human rights abuses and breaches of international law. Furthermore, the use of surveillance to monitor migrants can also have negative effects on the communities in which they live. At times, surveillance can create a climate of fear and mistrust, leading to social isolation and discrimination. This can make it difficult for migrants to integrate into their new communities, and can hinder their ability to access essential services, such as healthcare and education.

The electronic databases that are being constructed are set to transform into influential tools of surveillance on a European scale and develop into the new digital borders of Europe. Irregular migration comes in many shapes and sizes. Many of those individuals we call irregular migrants began their journey legally, for example travelling on a tourist visa, and became 'illegal' or 'irregular' when they overstayed it. Most classifications of 'irregular' migration are therefore set up around three main criteria: legal and illegal entry, legal and illegal residence and legal and illegal employment. These criteria can combine in many ways and produce different forms and 'degrees' of irregularity (see, for example, Tapinos, 2000: 18; van der Leun, 2003: 19). As legal entry does not preclude the possibility of later 'irregularization', border policy alone cannot be the sole policy response to 'irregular migration'. In recent years, policies to counter irregular immigration have increasingly turned inwards. Border controls remain important but in light of their 'structural flaws' have to be supplemented with policies of discouragement of those unwanted aliens that have passed the border. This shift towards internal migration control comprises a wide array of policy measures such as employer sanctions, exclusion from public services and surveillance by the police (Cornelius et al., 2004; van der Leun, 2003). The focus on internal migration control draws attention to two interrelated challenges for the state (Torpey, 2000: 33). The first dimension, territorial access, chiefly raises questions about the

capacity of states to identify citizens, distinguish them from non-citizens and regulate their movement in keeping with policy objectives. The second dimension, establishment, concerns the extent to which states may be able to exclude non-citizens from opportunities for work, social services or simply unperturbed existence once they have already entered the territory.

OBFUSCATION AND DIVERGENT PRACTICES

As a form of privacy control, obfuscation acts to mislead or interfere with surveillance and data collection. As a practice, obfuscation presents several challenges as more cunning and innocuous data collection methods are constantly evolving. From metadata to sites that 'guarantee' encryption, obfuscation presents an opportunity to maintain and sustain one's privacy. A shopping decision can lead to the later denial of health insurance or intrusive targeted advertising which directly contradicts, if not the legal protections of privacy, the spirit of privacy protection and enforcement. Divergent practices, on the other hand, intend to deviate from data collection exercises entirely. This is essentially avoidance, rerouting or otherwise escaping detection. Obfuscation is typically used on the back-end of websites and applications. WikiLeaks, for example, obfuscates its users' movements by developing a script that produces false signals to confuse any tracking efforts. To this end, several tools are developed for instance:

1. TrackMe Not: a browser extension that acts to shield web searchers from surveillance and data profiling by search engines

2. AdNauseum: a browser extension that automatically clicks on web ads to interfere with behavioural tracking and profiling. This obfuscates a users' profile as it is impossible to narrow down any specific wants, needs or personal preferences since every advertisement is viewed as part of the profile. The extension works as a community security blanket as it also prevents profiling others based on association with different profiles.

3. Swapping cards: card programs, particularly loyalty card programs are intended to track user profiles. Stores offer them for discounts

4. Bogus individuals refers to creating false personas to generate false leads in the case of investigation, or tracking. The goal with creating these individuals is protective but can be a double edged sword as lying about one's identity or creating fictitious personas may lead to legal action.

5. A cloning service observes an individual's activities and assembles a plausible picture of his or her rhythms and interests. At the user's request, it will spin off a cloned identity that can use the identifiers provided to authenticate (to social networks, if not to more demanding observers) that represents a real person. These identifiers might include small amounts of actual confidential data (a few details of a life, such as hair color or marital status) mixed in with a considerable amount of deliberately inaccurate information.

6. Geofencing and obfuscation. Geofencing refers to tracking one's location data through various devices such as mobile phones. If a mobile phone is being used In a particular location, the phone connects to a cell tower and its location is logged. This can be used to conduct profiling exercises, tracking individuals and can lead to surveillance creep. Avoiding geofencing can include swapping mobile phones with persons in different areas which would then provide 'false data' to the telecommunications provider.

Divergent practices can be classed as anonymity techniques. Anonymity techniques are differentiated from privacy preserving techniques as they seek to avoid total detection by avoidance whereas privacy preservation necessarily includes engagement. These practices would include denying all location tracking requests for applications or turning them all off entirely for instance. While powerful they can be viewed as impractical considering migrants often **must** engage with different surveillance systems for the purpose of gaining access.

The obfuscation techniques and rationales laid out in this report, while helpful and useful, cannot form a substitute for concrete legal protection and enforcement for the privacy rights of migrants, with the spillover effect of privacy rights for all.

SURVEILLANCE COUNTERMEASURES (OBFUSCATION PRACTICES)

Surveillance countermeasures can broadly refer to tactics for disrupting digital platforms. Largely, these practices leave information out in public but make it difficult to parse through and make use of, particularly for identification.

PHYSICAL SURVEILLANCE COUNTERMEASURES·

Physical countermeasures are things that people can do to protect their privacy in the physical world. For example, they may use curtains or blinds to prevent surveillance cameras from seeing inside their home, or they may use physical barriers, such as walls or fences, to prevent unwanted surveillance.

- Using curtains or blinds to prevent surveillance cameras from seeing inside a home or office
- Installing physical barriers, such as walls or fences, to prevent unwanted surveillance
- Wearing clothing or accessories, such as hats or scarves, that can obscure a person's face from surveillance cameras

The CV Dazzle website earlier this decade offered patterns it said avoided detection from FR algorithms.
(Website: CV Dazzle)

TECHNICAL SURVEILLANCE COUNTERMEASURES

Technical countermeasures are technologies that can be used to protect against surveillance. These can include tools such as encryption software, which can protect the confidentiality of communications, or anti-surveillance software, which can detect and block attempts to monitor a person's activities.

- Using encryption software to protect the confidentiality of communications

- Installing anti-surveillance software that can detect and block attempts to monitor a person's activities
- Using a virtual private network (VPN) to encrypt internet traffic and hide a person's online activities

Behavioural surveillance countermeasures

Behavioural countermeasures are actions that people can take to reduce their likelihood of being surveilled. For example, they may avoid discussing sensitive topics in public or on the phone, or they may use pseudonyms or other methods to obscure their identity online.

- Avoiding discussing sensitive topics in public or on the phone
- Using pseudonyms or other methods to obscure a person's identity online
- Being cautious about the information that is shared on social media or other online platforms

Interview analysis

Methodology

A qualitative approach was used in this study to contextualise migrant identities in light of increasing surveillance and the need for obfuscation. Interviews as a qualitative method were selected to give further insight into migrant surveillance. Interviews were semi-structured and in-depth allowing participants to discuss (or decline to discuss) their experiences. Participants were guided with open ended questions and, where necessary, specificity was provided to maintain relevance. Interviews were conducted using digital applications, primarily Zoom and Google Meets.

Sampling

In order to find participants, networks within and outside the project working with and consisting of refugees were contacted. Preference was given to migrants with a more recent migrant background and a total of 13 participants were selected for the interviews.

Analysis

A thematic analysis was used to analyse the interview data. Key themes that emerged included:

- A reliance on technology as a means of survival
- Coercion as a tool to gain more information
- Persistent feelings of dehumanisation and denial of opportunities to assimilate in the destination country

At the outset, the participants were asked to give their perspectives on migrant representation in the media. Participants stated that there was a separation between them and citizens, that they felt there was a persistent narrative of criminal activity, rowdiness and 'stealing' the jobs of citizens. These feelings could be fuelled by something as simple as a whatsapp message, circulated among thousands, or a facebook post that would go viral. One participant pointed out the case of the Rohingya and how their displacement since 2017 still has not been addressed in a way that is judicious. Media representation has been negatively skewed against migrant communities furthering their 'othering' and preventing them from making vital connections with citizens of their home countries. They are framed not as victims and survivors of war-like or dangerous conditions in their country but rather as 'free-loaders' wanting to crowd developed cities and negatively impact the social, economic and political sphere. Often, crime in countries with high migrant populations blame the rates of crime on the migrant community. Where a crime is indeed committed by a migrant, the emphasis is placed on the crime in a manner that suggests that this is indicative of the entire migrant population. With this ostracism, it becomes natural for migrant communities to turn inward and seek solutions from amongst their own communities and, using social media, foster a sense of communal understanding with others from similar backgrounds around the world.

On surveillance, participants felt inhumane treatment and had little choice in issues like having their photos taken without their consent. Concerns were also raised around having their fingerprints scanned and having no information provided to them in a language they could understand. They often had to use coded language and misnomers to communicate with each other as they did not trust border officials. They used platforms like twitter and facebook to keep in touch with family members but stayed away from posting personal photos and giving away their location. Participants also emphasised that they 'felt watched' on their accounts even when they were trying to protect themselves and would, at times, keep from posting to prevent further surveillance. The use of surveillance to monitor migrants can also raise concerns about privacy and civil liberties. In some cases, surveillance may be used to target specific groups of migrants, such as refugees or asylum seekers, and to discriminate against them based on their ethnicity, religion, or national origin. This can

lead to human rights abuses and violations of international law. Furthermore, the use of surveillance to monitor migrants can also have negative effects on the communities in which they live. In some cases, surveillance can create a climate of fear and mistrust, leading to social isolation and discrimination. This can make it difficult for migrants to integrate into their new communities, and can hinder their ability to access essential services, such as healthcare and education. Politically, immigration control has reached the top of the agenda and the public unease in Western Europe fuels the resolve of politicians to dedicate more resources to the agencies involved. As a result, much has been invested in the various manifestations of the borders of the EU and its member states. The image of a Fortress Europe emerged to describe the development of policies aimed at keeping out (bogus) asylum seekers, irregular migrants and 'unwanted' immigrants in general. The external borders of the EU (including sea- and airports) have been transformed into formidable boundaries. Borders have been strengthened with guards, watchtowers, concrete and fences. They have also been equipped with state-of-the-art technology, such as infrared scanning devices, motion detectors and video surveillance. Moreover, visa requirements have been stepped up, and the visas themselves have been modernised and are increasingly difficult to forge. And yet, despite funding and political backing for the 'fight against illegal immigration' and the strengthening of borders and border control, the presence of irregular migrants remains a fact of life for most EU countries. The gradual realisation that borders alone cannot halt irregular migration has led to a widening of the scope of immigration policy. Border control is 'moving away from the border and outside the state' (Lahav and Guiraudon, 2000), or is becoming 'remote control' (Zolberg, 2002) or is moving 'upwards, downwards and outwards' (Guiraudon, 2001).

Lastly participants were asked if they felt that the risks of migration had worsened due to social media surveillance. A majority of participants indicated that physical risks remained the key focus of their anti-surveillance methods and were more worried about CCTV cameras and border patrol guards than they were about being monitored on social media. In the midst of the border control process transformation, with an increasing securitization, integration, automatization and digitalization, particular attention must be given to the inclusion and assurance of fundamental rights. The issue of fundamental rights in border control processes, in particular the right of non-discrimination is a notably sensitive topic, which must be addressed in a responsible and adequate manner. Potential legal inadequacies or violations may affect the lives of thousands of people who cross the EU external borders annually. Thus, when discussing the issue of discrimination in border control it is critical to avoid simplifications and naturalizations that may lead to a reduction of the space for reflection and critical considerations.

CONCLUSION

Enforcing privacy rights as they apply to migrants is fast becoming a controversial subject, the delicate balance between protecting data rights seems to be overlooked in the face of mass data collection and use exercises. There is an overarching need for Data protection impact assessments to determine the dangers that vulnerable groups are in and whether the ambit of data collection practices falls within the purpose limitation principle, which requires that personal data be collected only for specific, explicitly defined purposes (European Union Agency for Fundamental Rights and Council of Europe, 2020). The application of this principle in border management has been contested with human rights organisations raising concerns about excessive data collection and surveillance creep. Digital technologies transform what we understand as the border through both intensifying its power of identification and enabling it to diffuse inside the states. However, technology cannot be separated from the social context. The responsibility that states owe to migrants has not been clearly elucidated in various documents with the dominant narrative being that of control of migrant mobility, limiting their freedoms but there has been little on the actual responsibility that states owe to migrants. The legal acknowledgement of these responsibilities has been scarce with legislation largely noting that respect and dignity applies in a general context but with no specific provision and its applications to migrants and the dignity that is owed to them by nation states. For instance, the EU charter on Fundamental rights includes several provisions on human dignity but fails to mention a connection between human dignity and migrants. In 2018, two global compacts were adopted by the United Nations to address growing interest in and concern about the migratory crisis emphasising that states have shared responsibilities over the treatment of migrants and should endeavour to protect and fulfil the human rights of migrants. Without an adequate rights framework, data collection and misuse will run unchecked and infringements on privacy rights will continue.

REFERENCES

Achiume, E. T. (2021). Digital Racial Borders. *American Journal of International Law*, *115*, 333–338. https://doi.org/10.1017/aju.2021.52

Aljazeera. (2021, May 31). *Migrants, refugees will face digital fortress in post-pandemic EU*. Www.aljazeera.com. https://www.aljazeera.com/news/2021/5/31/migrants-refugees-will-face-digital-fortress-in-post-pandemic-eu

Bellanova, R., & Glouftsios, G. (2020). Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance. *Geopolitics*, *27*(1), 160–184. https://doi.org/10.1080/14650045.2020.1830765

Bloj, R., & Buzmaniuk, S. (2020, November 16). *Understanding the new pact on migration and asylum*. Www.robert-Schuman.eu. https://www.robert-schuman.eu/en/european-issues/0577-understanding-the-new-pact-on-migration-and-asylum

Brownsword, R. (2021). Migrants, State Responsibilities, and Human Dignity. *Ratio Juris*, *34*(1), 6–28. https://doi.org/10.1111/raju.12303

Casagran, C. B. (2021). Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU. *Human Rights Law Review*, *21*(2). https://doi.org/10.1093/hrlr/ngaa057

Christou, G. (2010). The European Union, borders and conflict transformation: The Case of Cyprus. *Cooperation and Conflict*, *45*(1), 55–79. https://doi.org/10.1177/0010836709347213

Csernatoni, R. (2018). Constructing the EU's high-tech borders: FRONTEX and dual-use drones for border management. *European Security*, *27*(2), 175–200. https://doi.org/10.1080/09662839.2018.1481396

Cymbranowicz, K. (2020). The development of the European Union in the areas of migration, visa and asylum after 2015. Priorities, effects, perspectives. *Studia Migracyjne - Przegląd Polonijny*, *46*(1 (175)). http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-bf3b898e-789a-4cae-9e1c-d6553d0aa497

Digital Freedom Fund. (2021, June 18). *The Ongoing Digitisation of Europe's Borders*. Digital Freedom Fund. https://digitalfreedomfund.org/the-ongoing-digitisation-of-europes-borders/

eu-LISA. (2020). *European Entry-Exit System*. https://pages.nist.gov/ifpc/2020/presentations/12_European%20Entry%20Exit%20system%20-%20IFPC%202020%20v1.0.pdf

European Commission. (n.d.). *Press corner*. European Commission - European Commission. Retrieved February 24, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/ip_21_503

European Union Agency for Fundamental Rights and Council of Europe. (2020). *Handbook on European law relating to asylum, borders and immigration Edition 2020*. https://www.echr.coe.int/documents/handbook_asylum_eng.pdf

Glouftsios, G., & Scheel, S. (2020). An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering. *Third World Quarterly*, *42*(1), 123–140. https://doi.org/10.1080/01436597.2020.1807929

Gülzau, F., Mau, S., & Korte, K. (2021). Borders as Places of Control. Fixing, Shifting and Reinventing State Borders. An Introduction. *Historical Social Research / Historische Sozialforschung*, *46*(3), 7–22. https://www.jstor.org/stable/27075115

Hanke, P., & Vitiello, D. (2019). High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability." *Use and Misuse of New Technologies*, 3–35. https://doi.org/10.1007/978-3-030-05648-3_1

Jeandesboz, J. (2016). Smartening border security in the European Union: An associational inquiry. *Security Dialogue*, *47*(4), 292–309. https://doi.org/10.1177/0967010616650226

Kaurin, D. (2019, May 15). *Data Protection and Digital Agency for Refugees*. Centre for International Governance Innovation. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/

Leese, M., Noori, S., & Scheel, S. (2021). Data Matters: The Politics and Practices of Digital Border and Migration Management. *Geopolitics*, *27*(1), 1–21. https://doi.org/10.1080/14650045.2021.1940538

Lehtonen, P. (2020). *The Technologization of European Union Border Control Political Agency Steering Societally Significant Practices*. https://trepo.tuni.fi/bitstream/handle/10024/122458/978-952-03-1591-7.pdf?sequence=2&isAllowed=y

Lehtonen, P., & Aalto, P. (2017). Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States. *European Security*, *26*(2), 207–225. https://doi.org/10.1080/09662839.2016.1276057

Metcalfe, P. (2021). Autonomy of Migration and the Radical Imagination: Exploring Alternative Imaginaries within a Biometric Border. *Geopolitics*, *27*(1), 47–69. https://doi.org/10.1080/14650045.2021.1917550

Metcalfe, P., & Dencik, L. (2019). The politics of big borders: Data (in)justice and the governance of refugees. *First Monday*. https://doi.org/10.5210/fm.v24i4.9934

Moffette, D., & Walters, W. (2018). Flickering Presence: Theorizing Race and Racism in the Governmentality of Borders and Migration. *Studies in Social Justice*, *12*(1), 92–110. https://doi.org/10.26522/ssj.v12i1.1630

Nair, N. (2021, June 21). *E.U. Spends Billions On Digital Fortress To Keep Out Migrants*. The Organization for World Peace. https://theowp.org/e-u-spends-billions-on-digital-fortress-to-keep-out-migrants/

Nedelcu, M., & Soysüren, I. (2020). Precarious migrants, migration regimes and digital technologies: the empowerment-control nexus. *Journal of Ethnic and Migration Studies*, 1–17. https://doi.org/10.1080/1369183x.2020.1796263

Noori, S. (2021). Suspicious Infrastructures: Automating Border Control and the Multiplication of Mistrust through Biometric E-Gates. *Geopolitics*, 1–23. https://doi.org/10.1080/14650045.2021.1952183

Schimmelfennig, F. (2021). Rebordering Europe: external boundaries and integration in the European Union. *Journal of European Public Policy*, *28*(3), 311–330. https://doi.org/10.1080/13501763.2021.1881589

The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change. (2021, October 15). Privacy International. https://privacyinternational.org/long-read/4651/eu-externalisation-migration-control-and-id-systems-heres-whats-happening-and-what

The New Pact on Migration and Asylum: One year on, a fair and humane asylum system is needed more than ever | The IRC in the EU. (2021, September 23). Eu.rescue.org. https://eu.rescue.org/article/new-pact-migration-and-asylum-one-year-fair-and-humane-asylum-system-needed-more-ever

The role of security and defence companies in EU migration and border control and the impact on the protection of the rights of refugees, migrants and asylum seekers 1. (n.d.). https://www.ohchr.org/Documents/Issues/Mercenaries/WG/ImmigrationAndBorder/kumar-submission.pdf

Trauttmansdorff, P., & Felt, U. (2021). Between Infrastructural Experimentation and Collective Imagination: The Digital Transformation of the EU Border Regime. *Science, Technology, & Human Values*, 016224392110575. https://doi.org/10.1177/01622439211057523

Witteborn, S. (2021). Digital placemaking and the datafication of forced migrants. *Convergence: The International Journal of Research into New Media Technologies*, *27*(3), 637–648. https://doi.org/10.1177/13548565211003876

Zolberg, A. R. (2006). Managing a World on the Move. *Population and Development Review*, *32*, 222–253. https://www.jstor.org/stable/20058950