1. Introduction to Digital Identity, Virtual Borders and Social Media

Emre Eren Korkmaz

This book discusses how states deploy frontier and digital technologies to manage and control migratory movements and how they cooperate with tech corporations in this field. Blockchain, artificial intelligence/machine learning (AI/ML), social media, big data analysis and various smart border solutions offer a wide range of opportunities for states to deal with legal and irregular migrants, refugees and asylum-seekers. However, this is an emerging area, these tech-based projects are still experimental and they are understudied topics in the literature. This book aims to contribute to the literature as authors critically examine the consequences of these technologies and evaluate them from the perspective of rights and liberties of migrants.

Despite the obvious power imbalances, technology remains an arena of political struggle. The same technologies can be used to promote peace and spark conflict. For this reason, the political struggle to make corporations and governments accountable can still change the course of technological development. For instance, if workers are concerned about automation or the use of AI by corporate HR departments, trade unions can raise these issues in the public square and political decision-makers can take action to upgrade skills, guide the automation process and grant unions new rights to monitor the decisions of algorithms. For people worried about automated weapons and military AI algorithms, various organisations devote their energy to controlling or even banning these weapons to maintain the peace. Anxiety over fake news and manipulative campaigns undermining democracy and the trustworthiness of elections is spurring many non-governmental organisations (NGOs) and political movements to advocate for democratic principles and make political parties accountable for their social media advertising. Finally, those worried about tech corporations’ ethical missteps and commercial irre-
sponsibility can lobby governments to take the steps necessary to write regulations to ensure accountability and transparency.

However, migrants and refugees do not have the same access to the arena of political contestation to protect and advance their interests. For anyone wishing to observe the likely shape of a dystopian future of a tech-oriented society in which people lose their political autonomy, a close look at the daily experiences of migrants and refugees vis-à-vis the large tech providers will provide sufficient clues. This book aims to challenge such a totalitarian and hegemonic approach to the people on the move and provide cases demonstrating how such technologies are deployed for the interests of states and corporations and deny the basic rights, liberties and agencies of migrants and refugees.

This book consists of six chapters. The first two chapters focus on the blockchain-based digital identity initiatives, two others discuss different forms of smart/virtual borders, comparing the US, Canada and the European Union (EU) which highly invest in AI. The sixth chapter examines the role of social media and mobile applications on smuggling activities and irregular migration and the last chapter evaluates how social media posts against refugees had an impact on the European Parliament elections in 2019.

In the second chapter, Margie Cheesman and Aiden Slavin discuss an important issue on blockchain-based self-sovereign identities (SSI) with the aim of empowering refugees. They analyse the main arguments and approaches of two SSI start-ups and demonstrate how in practice they fall into the trap of their initial critiques towards corporations and states instead of revolutionising the identity management. When I read the chapter, my conclusion was that individualist approaches could not be a genuine alternative to oppose monopoly power of corporations and states. Radical discursive suggestions without any critique of capitalism and ignoring alternative public spheres do not allow these initiatives to keep their promises.

In the third chapter, Aiden Slavin sheds light on the historical background of identification technologies and compares today’s digital identity initiatives with the Nansen Passport invented in 1921 to offer a recognisable form of identification to refugees of the Russian civil war. Aiden’s case study is the Blockchain Pilot Project in Kenya and he points out similar motivations to identify forcibly displaced populations. Aiden
Introduction

 argues that digital identification and the Nansen Passport are similar in so far as both:

• are justified based on the extension of rights and services to the beneficiary
• are the product of entanglement of actors from both the public and private sectors
• make possible control over the individual in order to enable extractive practices on behalf of institutions
• begin as efforts to render communities ‘on the periphery’ of global power ‘legible’.

In the fourth chapter, Roxana Akhmetova and Erin Harris compare the deployment of AI algorithms in the US and Canada for migration governance to control and monitor borders and automate decisions of visa and asylum applications. This chapter demonstrates the risks of automating border security and asylum decisions from the rights of migrants and exposes the role of tech corporations working closely with military, security and intelligence institutions to mine the data of migrants from counter-terrorism and security perspectives.

The US and Canada are at the forefront of incorporating AI and ML technologies into border control and migration governance; however, the extent to which the two governments are incorporating and testing new AI and ML technologies varies and the main argument of the chapter is that the use of AI immigration enforcement technologies infringes upon migrants’ rights of privacy and protection while increasing discrimination to diminish the agency. In attempts to create ‘smart borders’, Roxana and Erin argue that both Canada and the US are using AI technologies to erect ‘invisible border walls’ that are diminishing government responsibility and accountability for their actions and decisions as well as to refuse entrance to undesirable migrants. Another motivation is the multi-layered interests of private technology and security and arms companies.

In the fifth chapter, Johanna Bankston discusses the virtual-smart borders in the EU and focuses on the use of frontier technologies to counter smuggling activities. Johanna focuses on internet governance at the micro and macro levels and compares competing strategies of migrants, the EU and social media corporations. She argues that EU member states engage in internet governance to deter irregular migration through ‘virtual border enforcement’ and concludes by emphasising the dangers of creating digital policies and partnerships aimed at subverting
human smuggling which would eclipse migrants’ digital rights and identities.

In the sixth chapter, Ruta Nimkar, Emily Savage and Abdullah Mohammadi analyse the relationship between smuggling activities and new technologies from the perspectives of smugglers in Afghanistan. Based on their fieldwork results, Ruta, Emily and Abdullah contend that smuggling networks are building an alternative mobility regime and that mobile technology is augmenting the network capital required to build this regime. They use network capital to analyse the demand, supply and organisational aspects of smuggling networks and argue that mobile technology improves the logistics and organisation of smuggling networks, but has not, to date, significantly affected trust between various networks and actors.

In the last chapter, Deniz Yetkin Aker evaluates the role of social media posts that shape the attitude of the European Parliament election voters towards migration. By using Eurobarometer data (91.5) and by focusing on the European Parliament (EP) 2019 Post-Electoral survey, this study compares three EU member states – Finland, Hungary and Bulgaria – where the Facebook posting themes and sentiments of refugees are generally negative. Deniz discusses whether voting for different parties is related to individuals’ attitudes towards migration.

The following issues are expanded upon below:

- digital identity initiatives
- a question on the future of voluntary consent when United Nations (UN) agencies and humanitarian NGOs employ frontier technologies in their projects
- how social media and smartphone applications could be converted to resistance tools by migrants and refugees to oppose policies of states and corporations.

**DIGITAL IDENTITY INITIATIVES**

Blockchain has often been in the news lately thanks to the speculative cryptocurrency market. It is increasingly being touted as something of a magic bullet in a whole range of disciplines, and has been put forward as an answer to ongoing challenges in the field of international development, humanitarian aid and refugee studies.

I suggest that while blockchain may be used to support people in need, we have to bear in mind that these are not just technical issues – they are
Introduction

political questions. Focusing solely on the technical side is unlikely to bring the promised progress – and might even have the opposite impact.

In recent years, new partnership models bringing together technology companies and humanitarian NGOs have been promoted as a way of supporting refugees and displaced people – for example to facilitate payments and data protection and to support local businesses. A particular focus of such initiatives is the role of distributed ledger technology (DLT) to provide services rapidly and cheaply through cryptographic security without intermediaries, while also offering transparency and accountability.

According to these initiatives, over one billion people have no form of identity, but with the help of technology, multi-stakeholder collaboration might provide these people with digital identities that would allow them to access essential services, open a bank account and receive aid and social benefits. And as it is digital, the technology offers the necessary conditions for accountability and governance to improve the efficiency of the delivery of development aid.

Jim Yong, the World Bank Group President, has described digital identity as ‘the greatest poverty killer app we’ve ever seen’. If such initiatives are successful, according to Mastercard Vice Chairman Walt Maenee, an additional 500 million new ‘consumers’ and 40 million ‘new merchants’ can be brought into the global economy from among the world’s 2 billion ‘unbanked’ people. ‘The firm believes that greater financial inclusion around the world is a path to long-term sustainable economic growth.’

The World Bank Group released a paper on the role of financial services in humanitarian crises in April 2017. The report argues that in order to integrate humanitarian programmes with a developmental approach, refugees and low-income households in host societies should have access to quality financial services, so they can save, invest and receive loans. Donors may also inject liquidity into local financial markets to support market players.

Other voices have been less positive, however. Mercy Corps contributed to the report as follows: ‘delivering aid through e-transfers does not automatically lead to the uptake of new financial services by program participants. Instead, participants typically withdraw their full transfer when it becomes available and rarely use their new accounts after programs end. This holds true in both large government social safety net programs and humanitarian cash transfer programs.’ This suggests that such proposals to support refugees do not necessarily have approval from the refugees themselves.
Such initiatives are not limited to digital identity. The UN World Food Programme (WFP) has introduced a pilot project called ‘Blockchain Against Hunger’ deploying technology in Jordan’s Azraq camp to make cash-based transfers to 10,000 refugees. WFP relies on biometric registration data provided by the UN High Commissioner for Refugees (UNHCR) and refugees can shop from local supermarkets using iris scans; the system confirms the identity of the refugee in this way, checks their account balance and confirms the purchase.

However, we need to ask some more questions. Technological progress may help us to reach and track any person in need. It may offer them digital identities, mobile numbers and bank accounts. But do all these mean that people are empowered? Does all this progress provide a solution to poverty? And what are the risks?

Firstly, we should not overstate the value of such technologies as emancipatory tools.

In the most positive scenario, this support would help some refugees to set up their own businesses or become waged employees (in countries where they are permitted to work). Thus a Syrian refugee living in one of the neighbourhoods of Istanbul or Amman, for example, would have similar financial and economic opportunities to his or her local neighbours. So they would compete in the same job market, earn similar wages – or have an equal probability of being unemployed.

And in fact the majority of refugees live in the global South and these host countries face serious socio-economic structural problems. Thus refugees would face the same obstacles as locals: high unemployment rates, instances of modern slavery, harsh working conditions, an abundance of cheap labour and constraints on the right to organise and bargain collectively. And even in the countries of the global North, working conditions are increasingly precarious. So even if blockchain technology allows refugees to obtain a digital ID and receive aid or loans from agencies securely, this would not automatically mean that they are empowered or able to overcome poverty.

Secondly, there is a risk of abuse.

Digital identities, bank accounts and mobile phones allow corporations, donors, international agencies and local-national authorities to track people’s choices and desires. Such control might allow authorities and corporations to increase surveillance over refugees. An authoritarian state could use such data collected from refugees against refugees – or nations of the global North, which have no sympathy for the movements
of refugees and immigrants towards their countries, could use such information to keep refugees in neighbouring countries.

Even in institutionally democratic countries, there are debates about mass manipulation through fake news, interference in democratic elections, the use of search engine algorithms to offer people tailored search results or expose them to different advertisements based on their preferences and choices. Thus millions of people who are not classified as vulnerable can be manipulated and/or mobilised based on the power of corporations and their technological superiority. Therefore, it is also possible that this power could be used to mobilise refugees in a particular direction or discourage them from making certain decisions. Thus they could end up in a more vulnerable and dependent position.

Thirdly, we need to be aware of the motivations of the corporations involved.

As we have seen from the language used – ‘underserved customers’, ‘merchants’ – corporations do not define their efforts as philanthropy and we can assume that they expect some profit from their investments. The debate on addressing the problems of 60 million refugees and displaced people may shift to discussions on those 2 billion people without bank accounts who are therefore potential customers. As refugees and displaced people live in other countries for decades, any project towards refugees requires investment in their host countries, and an important portion of the population who are outside formal financial services live in those refugee-hosting countries. Therefore, any investment to formalise refugees will help corporations to reach locals as well. Refugees may be seen as a good starting point for further business goals.

Proposals for using blockchain technology could address some of the basic challenges faced by refugees, displaced and stateless people. However, it seems rash to present such technological progress as a genuinely emancipatory tool.

All such issues – conflicts, climate change and the refugee question – are political questions and they cannot be resolved without political, social and economic solutions; technological answers alone are unlikely to be sufficient.

In addition, it is worth noting that these initiatives seem to offer a top-down solution: a group of people representing giant technology corporations, the UN agencies, humanitarian NGOs and governments, meeting in Munich, Davos or California to empower ‘poor immigrants’. But as the Mercy Corps’ comment shows, the proposed solutions might not necessarily be accepted by refugees. So, there is a need to listen to
and understand the real expectations and desires of people in need and on the move.

**Voluntary Informed Consent (?)**

The second concern on deploying these technologies in the humanitarian setting is about the informed consent. In the humanitarian literature, the informed consent of refugees is a widely discussed concern. Informed consent means that signing up to a particular project is voluntary and refugees should have the chance to opt-out. Concrete problems arise when technological solutions are introduced in these projects. Because both refugees and the staff delivering services in the field lack the expertise to assess the ethical and practical implications of these technologies.

The UN agencies are increasingly preferring to employ tech-based solutions in their projects. The main reasons are to be more efficient and obey the ‘know your customer’ requirements of financial institutions for cash transfers. But, what would happen to people who are not willing to share their data, for any reason, be it political, religious or individual? Such a decision would have a huge impact on the future of voluntary informed consent.

**Technology as a Resistance Tool for Migrants**

Nevertheless, despite the vast power imbalance, refugees do benefit from information and communication technologies (ICTs). The flow of information from networks is vital en route and in making choices after arriving in the country of destination. Mobile applications and social media help refugees to connect with the UN agencies and humanitarian organisations and are used to stay in touch with families back home.

Therefore, comparing and contrasting the ways that new technologies are used to surveil migratory movements with how they are used by refugees to resolve the challenges they encounter will provide insights about the impact of technologies. Neglecting this power imbalance leads to an inevitable romanticisation of the relationship between refugees and their smartphones.

It is also necessary to analyse the digital divide within migrant and refugee communities themselves. It is highly skilled, male and literate refugees and migrants that appear to have disproportionate access to smartphones and mobile applications. Thus, gender and socio-economic
conditions have an impact on who can benefit from the advantages offered by smartphones.

The tech-based power to track people, and the use of algorithms and drones provide immense opportunities for states to manage migratory movements and for corporations to expand their customer base. In stark contrast to such displays against citizens, this power play against refugees can proceed openly, undermining the political agency of these vulnerable people.

NOTES