 DOI: 10.3986/dd.v0i49.7253

THE EUROPEAN DIGITAL FORTRESS AND LARGE BIOMETRIC EU IT SYSTEMS: BORDER CRIMINOLOGY, TECHNOLOGY, AND HUMAN RIGHTS

Aleš ZAVRŠNIK[1]

COBISS 1.01

ABSTRACT

The European Digital Fortress and Large Biometric EU IT Systems: Border Criminology, Technology, and Human Rights

Today, at a time when we are witnessing the "multiplication of borders", borders are occupying new domains. The article focuses on the erection of digital borders by means of biometric technology, which is creating new knowledge through the compilation of large biometric databases in the EU. By "tattooing" borders onto immigrant bodies, disciplinary power is being superseded by the post-disciplinary power of "instant surveillance". The article continues by analysing re-bordering practices by means of seemingly apolitical information technology, and concludes by delving into the new harms caused by re-bordering, including violations of human rights and the emergence of multi-layered criminal law.

KEY WORDS: biometric data, human rights, information technology, border criminology, large IT database

IZVLEČEK

Evropska digitalna trdnjava in veliki biometrični EU IT sistemi: Kriminologija meje, tehnologija in človekove pravice

Danes, ko smo priča »multiplikaciji meja«, meje zasedajo nova področja. Članek se osredotoča na digitalne meje, ki v EU vznikajo z uporabo biometrične tehnologije, kar z oblikovanjem velikih biometričnih podatkovnih zbirk ustvarja novo vednost. Avtor v članku pokaže, kako s »tetoviranjem meja« na imigrantska telesa disciplinsko oblast nadomešča »hipna oblast«, nato pa odstre dileme, povezane s premikanjem meja, kar omogoča domnevno apolitična informacijska tehnologija. V zadnjem delu predstavi nove oblike škode, vključno s kršitvami človekovih pravic, in nastajajoče večplastno kazensko pravo, ukrojeno glede na »hierarhije državljanstva«.

KLJUČNE BESEDE: biometrični podatki, človekove pravice, informacijska tehnologija, kriminologija meje, velika podatkovna zbirka

[1] PhD in Law, Associate Professor, University of Ljubljana, Faculty of Law; Research Advisor, Institute of Criminology at the Faculty of Law, Poljanski nasip 2, SI-1000 Ljubljana; ales.zavrsnik@pf.uni-lj.si — The research leading to this article received funding from the Slovenian Research Agency (ARRS), research project "Crimmigration between Human Rights and Surveillance", J5-7121, 2016–2018. — The author would like to thanks Primož Gorkič and Mojca M. Plesničar for their insights on the fundamental rights implications of biometric database systems.

INTRODUCTION

European criminologists have been concerned with migration policies since the late 1980s and have described how criminal law measures have merged with the administration of migration. This interest in the convergence of migration and criminal justice has been termed the "criminology of mobility" (Franko Aas, Bosworth 2013) or "border criminologies" (Bosworth, Turnbull 2014) and analysed as the emergence of "crimmigration law", i.e. the convergence of criminal law and procedure and migration law and procedure (Hernández 2017). In this process of convergence of the two fields, cutting-edge information technology plays a significant role. Migration policy does not consist solely of laws, but also of high-tech "solutions", which are changing the borders of Europe into an "e-Border" (Dijstelbloem, Meijer, Besters 2011) and an "electronic fortress" (Unmüßig, Keller 2012). Biometric technology in particular has become "the prime technology for tracing the new globality in both its abject and privileged forms" (Franko Aas 2011). The fascination with such technologies in regulating migration grew exponentially in the aftermath of 9/11, following the USA's power to export its security agenda and impose biometric passports on the rest of the world (Franko Aas, Bosworth 2013: 31). Biometry is now used as a way of "tattooing" borders onto migrant bodies. Despite its inefficiencies, e.g. false positives and separate treatment of migrants by producing 'disqualified bodies' (Adey 2004), biometric technology is spreading and may even employ innovations such as facial expression recognition (Boffey 2018) and language accent detection (Lin 2018) in the near future.

Biometric technologies must be regarded as an immanent part of other political processes. In analysing Frontex, for instance, Wilson showed how the vast technocratic and informational infrastructures reinforce the existing political agendas: "[r]isk analysis endeavours to anticipate and pre-empt border futures through calculation and projection […]. Such imagined futures are then drawn back into the present through the conception of the 'near real-time' border" (Wilson 2018: 46). The employment of these technologies is fostering existing trends such as "securitisation" – the perception that ascertaining the correct identity of an individual, and in particular a foreigner, is accepted as a security issue. At the same time, border technologies are a product of the existing perception that migration must be "managed" and responded to with technology. "Technology, however, is not just the 'means' that allows political and administrative aims to be carried out; technology creates its own possibilities and limitations, which implies that any targets that are thus achieved are always 'mediated'" (Dijstelbloem et al. 2011). The engagement of the vast IT apparatus for migrant purposes in the EU serves to centralise the power of the EU institutions and paves the way towards the Schengen area, which is regarded as "one of the major achievements of integration" (European Commission 2016: 2). EUROSUR, the European external border surveillance system, for instance, has been a catalyst for new social relations among disparate sectors, creating areas for collaboration and competition, compliance and conflict (Andersson 2016). It is not so much a tool for detection

at the borders and beyond, but rather for how border policing is socially organised (ibid.: 35). Moreover, Frontex is also tasked with contributing to technological development (Wilson 2018). It is mandated with purchasing technical equipment on its own behalf (Lemberg Pedersen 2013). By interlinking business entities with the political migration agendas, Frontex thus operates as a chamber of commerce despite its attractive rhetoric of "saving the lives of migrants".

Arendt (2013: 7–8) claims that violence needs tools. The technological revolution has thus always been most notable in the military domain, and the contemporary "militarisation of the border" employs IT on a large scale. Military logic thus underpins the IT tools employed in border control, such as carbon dioxide sensors at border checks, infrared sensors, unmanned aerial vehicles, and the large biometric databases compiling data on retina scans, fingerprints, and DNA. As these tools are of military origin, their deployment in the management of migration reframes migration in security terms. These tools dictate a specific framing of the social challenges, and military tools are in addition attuned to the binary logic of "us" and "them", of exclusion and inclusion, and of the extermination of the "other". From such a perspective, unwanted migration is not a product of "Western" European policies and failures in tackling the roots of the problem, such as the rising tide of global inequalities, but a security management issue which must be addressed with technology. The specific "political and technological framing places migrants as a source of insecurity (and as potential criminals), rather than people who are exposed to considerable dangers on their migratory journeys, and therefore deserving of protection and assistance" (Pickering et al. 2014).

This article focuses on the following two questions: How do the new technologies of mobility control, especially biometric technologies, intensify surveillance by redefining borders? And: What are the dangers and human rights implications of the data-driven IT tools employed for the surveillance of the EU borderlands?

In the second section, the article documents the existing research on the criminalisation of mobility and shows how this is reshaping criminal justice institutions, prisons, and policing, or, more broadly, how mobility is bringing new challenges to understanding criminalisation, crime, and punishment (Franko Aas 2013). In the third section, the article tackles the meaning of what a border actually is. What does the notion of "multiplication of borders" (Balibar 2015; Bendixsen 2017) mean and how do borders move and occupy new terrain and domains, including the digital domain? Here, the article starts from the insight that the EU's borders are in constant flux due to its inability to effectively address the reasons for migration. They are theorised as being neither solid nor liquid, but "gaseous" (Bigo 2014), or, in the context of the 2015 "migrant crisis" in the Balkans, even as "cloudy" (i.e. cloud-based) (Milivojević 2018). Amongst the many technologies of mobility already installed for EU border "security", this article then focuses on biometric technology. It shows how the large EU IT systems in the areas of borders, visas, and asylum, and digitisation megaprojects such as EUROSUR and the Smart Borders Package in the EU, are all

part of the rising transnational governance of the European borderlands. With the electronic upgrading of border controls – externally through EUROSUR and internally through the Smart Borders Package complementing SIS II,[1] EURODAC,[2] and VIS[3] – the EU has been creating one of the world's largest biometric databases. Through the interoperability efforts, i.e. the legislative proposals on interoperability between EU information technology systems presented in December 2017, and the constant monitoring of European borderlands with EUROSUR, i.e. a "system of all systems", Europe is re-defining the concept of border and is designing a post-panoptical type of "instant surveillance".

New technologies provide a constant gaze that obviates the need to discipline crimmigrant bodies. Biometric technology inscribes the border in the body as a form of "political tattoo" that obviates the necessity for disciplinary surveillance. The large biometric EU IT systems play both a reactive and productive role in surveillance – towards a post-panoptical type of "instant surveillance". Because the new IT tools have profound implications for human rights, the fourth section then maps the harms caused by digital borders and discusses several implications of digital borders for human rights. The article then focuses on the functioning of large EU IT systems in the areas of borders, visas and asylum in Slovenia. It points out several human rights concerns and paints a broader picture of harms that the personal data protection law cannot sufficiently address. The article concludes with some views on the relationship between the cutting-edge technologies and the specific social-cultural milieux: these technologies are placed into specific socio-cultural situations and in turn deepen migration control practices in a militarised, securitised and externalised manner.

THE EXISTING RESEARCH ON CRIMMIGRATION

Features of Crimmigration

Current criminological scholarship has identified several features of crimmigration. The increasing interlinking of policy areas such as travel and border management with counter-terrorism, smuggling, and human trafficking has mixed the regulatory boundaries both institutionally and functionally. The blurring of boundaries between the police and border patrol, i.e. the tendency for the police to assume border patrol duties and for the border control to become more police-like, has been observed in several countries (e.g. in Canada in Stumf 2013). Similarly, in the EU the military regularly provides equipment and personnel to patrol the Mediterranean. The hybridisation of prisons and detention centres (Bosworth 2013) has made them

1 SIS II – The second-generation Schengen Information System.
2 EURODAC – European Dactyloscopy System.
3 VIS – The Visa Information System.

indistinct as places depriving individuals of free movement, but with the important difference that migration centres often lack any rehabilitation programmes. The measure of confinement (besides deportation) has become identified as the predominant tool of "bordered" penality. Penal systems with a "double-vision" (one for citizens and one for migrants) or a multi-layered system based on "hierarchies of citizenship" (Franko Aas 2013), in accordance with which resources are distributed, now enables the tailored distribution of welfare benefits. The EU Smart Borders Package, which includes the Entry/Exit System (EES), is a clear example of "double penality". The system will be interconnected with the Visa Information System (VIS) database and will supposedly only allow law enforcement authorities to access the database for criminal identification and intelligence in order to prevent serious crime and terrorism. However, it exclusively targets non-EU nationals with significant data collection (see critique in Roson 2018).

Border control is increasingly associated with the language and hardware of warfare. For instance, Frontex's pre-packaged rhetoric is full of military jargon and adjectives that emphasise the illegitimate, threatening and thus 'criminal' character of irregular migration (Campesi 2014). Similarly, EUROSUR can utilise unmanned air vehicles, which resonates "uncomfortably with the US government's use of unmanned 'drones' in the Afghanistan conflict" (Singh Bhui 2013). The so-called "situational awareness" of EUROSUR has its origins in aerial combat dating back to the First World War (Wilson 2018). The language of business enterprises coexists with the deployment of military jargon, with the external border described as the "operational theatre" (Andersson 2014: 76).

Strengthening Criminalisation and Changing Penality

Criminologists have so far tackled the following two broad questions related to migration: What are the novel types of crime/perceived dangers? And: How do agencies, e.g. the police, public prosecutors, courts, etc. change their response when crimes are committed by individuals without formal membership?

The first question concerns the strengthening of states' ability to deport, apprehend and detain migrants and to extend the state's punitive practices to the realm of border control. This in itself is a disruption of the traditional distinction between criminal and migration law. Another aspect of this question relates to extending power in the border domain in a different, often harsher, manner (e.g. for the evolution of a two-sided penal culture see Barker 2013; Lacey 2008; Ugelvik 2013). Some even suggest that this is in fact a multi-layered penal culture (Franko Aas 2013).

Strengthening criminalisation includes changes in both substantive and procedural criminal law. In terms of the substantive part, scholars' concerns have focused on the establishment of offences for human smuggling, as well as for irregular entry, transit, and stays (Mitsilegas 2017). As regards procedural law, several innovations

are undermining the due process of law, denying migrants the effective assistance of counsel, privacy rights, and the rights to asylum and protection (Greene, Carson, Black 2016; Kogovšek Šalamon 2017).

The second question relates to changes in penality. Scholars have shown how the goals of penal intervention have changed from the reintegration of offenders into society towards deportation; called also "bordered penality" (Franko Aas 2014). However, the role of technologies in redefining the border has not attracted much-needed attention in criminological studies.

WHAT AND WHERE IS THE BORDER?

There are now more physical barriers at European borders than at any time during the Cold War (Bremmer 2018). Since the fall of the Berlin Wall, more than forty countries around the world have built fences against more than sixty of their neighbours (*The Economist* 2016). These physical borders are leaving countries such as Turkey and Greece to house large numbers of migrants. As these bottleneck countries cannot absorb them all, wealthier countries are investing heavily in new technologies.

What is the Digital Border?

The conventional thinking according to which borders are understood as territorial demarcations that separate (and thus constitute) sovereign nation states has been broadly criticised (Bigo 2014; Balibar 2015). Borders should be understood as physical devices as well as structures of the imagination – giving a sense of belonging. In the latter sense, the notion of an "inner border" (*innere Grenze* as per Fichte, in Pajnik 2017: 236) encapsulates the insight that we all perpetuate borders between "us" and "them" as we live in "imagined communities" (Anderson 1998). For criminologists, the differential treatment in prisons between citizens and foreigners ultimately serves as a constant re-enactment of the border and a reminder that they do not belong (Franko Aas, Bosworth 2013). But what about the digital border? What is a digital border and how does it function?

At a meeting coordinated by Frontex, along with eu-LISA[4] and the European Asylum Support Office (EASO) on the island of Lesbos in 2016, EU officials asked tech companies to pitch ways to track and control people trying to reach the continent before they get here, and several tech companies showcased their latest ideas (Taylor, Graham Harrison 2016). Unisys, for instance, had devised a "refugee management suite" for enabling the pre-registration of asylum seekers. Its proposals included

4 eu-LISA – The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

controlling refugees before they reach Europe using phone apps and biometric data gathering; tracking people once they are inside Europe using new identity cards; a system of red flags; and data analytics to highlight those with backgrounds that merit investigation. This "refugee management suite" merely offers a new form of surveillance. "The use of behaviour analytics which treat past conduct as currency for food and shelter marks a new descent into the moral abyss," claimed civil liberty groups (ibid.). The vignette shows that with digital surveillance, borders can be "everywhere". They have changed as a concept as they are digitised and inscribed in the body.

The multiplication of borders in digital realms shows how the notion of the border is in constant flux. The new borders are not "liquid" or "solid" but "gaseous", claims Bigo (2014). Milivojević (2018) suggests that we should speak of "cloud-based" borders: borders are "deployed and defended in the digital sphere". But what and where is the border when large EU IT systems, such as SIS II, VIS, and EURODAC, are employed in border control? Large biometric IT systems clearly draw new borders following from novel demarcations. Here it is necessary to turn to Balibar's (2015) insight into the multiplication of borders in Europe. He observes how the perception of being "truly" a European country changes over time and space. Some European countries are tentatively perceived by others as not being fully European, or as merely belonging to "buffer zones", and this ascription is relative rather than absolute. Such labelling follows a north-south "gradient" in the sense that the controller of a state's border is its southernmost (or rather south-easternmost) neighbour (Balibar 2015). The "external borders" of Europe, he concludes, actually cut right through it and fragment Europe into several superimposed slices.

His argument has to be extended in order to encapsulate digital borders, due to the fact that another type of multiplication is taking place. By relying on the new knowledge created by the large databases, the EU countries are inscribing borders in the body – the "body becomes a password or passport" (Franko Aas 2011). By employing biometric technology and stockpiling biometric data for "real-time" (or "near real-time") background checks, borders are directly inscribed, or "tattooed", in the body. The border is inscribed into individuals' retinas, voices, or DNA. The new border is mobile and migrates with the unwanted body. "Border checks are changing their location" (Dijstelbloem et al. 2011) as the border has become portable (ID cards) and virtual (databases) (Lyon 2005).

This new feature of connecting identity and citizenship with the body offers the allure of objectivity and infallibility. The body becomes an unambiguous token of truth (Franko Aas 2006). As Franko Aas (2011) puts it, "the body does not lie" – documents can be counterfeited and lost, while fingerprints, DNA, iris scans, etc., cannot be forged by the extensive illicit migration industry. It can no longer be avoided or escaped. By means of large biometric databases, the EU is imposing its own regimes of truth. The need for trust vanishes in the materiality of the body – and biometric technology fills the void. By establishing biometric databases regarding third country

nationals, the EU does not have to rely on documents issued by third countries to their own populations, thus enabling it to decide who deserves and who does not deserve to cross its borders and remain on its soil.

This new type of surveillance is in essence post-disciplinary. One way of theorising this shift was offered by Bigo, who claims the new surveillance is "ban-optic". Its goal is "banning" and expelling people instead of integrating them into the EU (Bigo 2006). While this explains one part of the change, it is not clear how the compliance of docile bodies is achieved. It is not achieved through the "training of the soul" or self-discipline, but instead by power directed into the body through sensors, based on biometric data. The new type of post-panopticon does not need a presumed watcher in the tower (cf. Andrejevic 2016; Bučar Ručman 2016) as the gaze becomes ever-present. Docile bodies may literally be constantly tracked. The migrant subjectivity no longer needs to be disciplined and is no longer at the centre stage of surveillance – in the exercise of power, the body replaces the soul and becomes the focal point of the post-disciplinary "constant surveillance".

Migrant bodies with the right "tattooing" may move freely, while others cannot. Technology ascribes risk based on big data analytics directly in the body. Some bodies are perceived as being riskier than others simply due to algorithmically inferred high-risk scores. In practice this means that IT tools are changing the regime governing the flow of people. Bodies with the right "political tattoo" can enter the EU and be granted fundamental rights according to refugee and asylum law, while others are left in the borderlands. At one extreme, as Balibar (2015) graphically demonstrates, are those who "practically 'live' in planes, airports, shopping centres, conference halls," while at the other end of the mobility spectrum are groups "who travel by foot or on trucks on the roads of exile, carrying a child in their arms and a backpack on their shoulders – the only things that they still own." When the algorithms recognise someone as a security risk, in-depth security checks are triggered; the calculations are made based on a variety of techniques using big data and algorithmic inference of risk, based e.g. on voice analysis (Boffey 2018) or travel patterns (Kahn 2014). While resistance to earlier types of biometric technologies such as fingerprints led migrants to burning or disfiguring their fingertips (Franko Aas 2011) in order to disable the "tattooing" of borders, more advanced technologies such as voice analysis ("voiceprint") attach legal regimes directly to the bodies, rendering resistance futile. These are the new "violent borders" (Jones 2017), which span and multiply not only over geographical areas. They are compressed into digital language and thus also span over the digital space.

Instruments of Digital Bordering

Reliance on the "political tattooing" of unwanted bodies evolved in the aftermath of the Arab Spring in late 2010 in Tunisia, when the heads of the EU Member States

adopted the conclusions of the EU Council resulting in new border policies "protecting" the Union against immigration (Unmüßig, Keller 2012). Basically, the decision was made to reinforce the external borders using state-of-the-art surveillance technology, "thus turning the EU into an electronic fortress" (ibid.).

In their critical review of the earlier proposal of the European Commission's Smart Borders Package, i.e. the Entry/Exit System (EES) and Registered Traveller Programme (RTP), Guild et al. (2008) claimed that the enhanced use of new technologies in European security policies is merely a "step closer to a 'cyber-fortress Europe'". The travelling public will find itself increasingly the object of state suspicion, with no concrete reason or grounds (ibid.). Disproportionate measures will very likely be ineffective e.g. in facilitating the entry of bona fide travellers, and the large databases will breach data protection laws. Back than several layers of security were already in place for checking third-country nationals, and additional databases were not a necessary means to combat illegal stays. A decade later all of the proposed systems are operational, i.e. the SIS II, VIS, and EURODAC databases are fully operative and have even been expanded to include more types of data (SIS II). The Smart Borders Package was signed on 30 November 2017, and the EES is scheduled to become fully operative by 2020. Moreover, new agencies have been established, such as eu-LISA, the EU Agency for the operational management of large-scale IT systems, which is mandated to manage and further develop large IT systems. Multi-layered technical development, such as the EUROSUR multi-layered surveillance, is being reinforced (Hayes, Vermeulen 2012: 23). The further digitisation of border surveillance is expected with the proposed European Travel Information and Authorisation System, i.e. ETIAS, a visa waiver system planned to be operative in 2021. Automatic application processing envisages checks against SIS II, VIS, EUROPOL, Interpol (SLTD[5] & TDAWN[6]), and EURODAC data. All of the data will be cross-checked against these databases to determine if a person is a security risk. Moreover, the formerly separate VIS, SIS II, and EURODAC databases will be integrated and interlinked. Reliance on the knowledge created by large biometric databases puts digital borderlands at the centre stage of human rights concerns.

5 SLTD – Stolen and Lost Travel Documents.

6 TDAWN – Travel Documents Associated with Notices.

THE HARMS CAUSED BY DIGITAL BORDERS

The Human Rights Implications of Digital Borders

The new digital borders, erected alongside the physical fences, may have the same devastating effects as razor-wire fences – their immateriality hides their effect. Fences are purportedly intended to scare off migrants, rather than to actually prevent them from crossing. In terms of physical strength, fences are weak and cannot be placed along the entire border between states. An army would be needed to guard them, as migrants can destroy, fly over, or dig under such fences. In contrast, migrant management tools, e.g. databases, algorithmic decision-making tools, risk assessment instruments, and predictive analytics to screen migrants, are building impenetrable mobile digital walls. These borders are indiscriminately forced upon migrants. Like all "weapons of math-destruction" (O'Neil 2016), i.e. automated-decision making tools based on algorithms and databases, their features are opacity, scale and harm. In terms of opacity, their inner operations and capacities are mostly unknown, and their impacts are hardly analysed, but are rather black-boxed. They are rarely challenged in practice (see the Slovenian example below). In terms of scale, they subject entire populations to their control. And in terms of harm, they often do not work properly and deliver false results, e.g. by refusing entrance to those that should be allowed to enter.

The EU migration regime contains several dichotomies that undermine the right to freedom of movement and the rights to asylum and protection, and put migrants at risk of increased surveillance. First, human rights concerns with regard to people who have entered the EU are relatively high compared to those left at the outskirts of the EU. The social inclusion of migrants and their descendants is closely monitored (see the European Union Agency for Fundamental Rights – FRA 2017). In response to the 2015 asylum emergency, the FRA has been assessing the long-term impact on fundamental rights and examining what has happened to those people who sought asylum in the EU. The FRA is especially concerned with "vulnerable populations", but these are defined very narrowly, encompassing mainly children, which is short-sighted given the stressful situation of all migrants – are not migrants as a whole a vulnerable population?

However, there is no real regard for the human rights of those left at the outskirts of the EU. The technological solutions are complementary to the EU's long-standing collaboration with countries of origin and transit in the form of migration compacts, readmission agreements, and Memoranda of Understanding. These two factors – technology and agreements – are both pushing the border into third countries. Among the recent agreements is the EU-Turkey Statement of 2016 (European Commission 2016), which exemplifies the "external governance" of the EU in an attempt to extend its policies into non-member states (Wunderlich 2012), according to which an EU Member State (most often Greece) can reject the asylum applications

of people who pass through Turkey as being inadmissible and shift the responsibility to assess their merits to Turkey. However, it is highly doubtful whether Turkey can offer effective protection and be considered a "safe third country". As the EU has not put into place any effective mechanism for monitoring the situation of individuals readmitted to Turkey, the EU is, through the provisions of the Statement, preventing refugees from accessing asylum procedures and denying them their right to protection against *refoulement* (Alpes et al. 2017).

Second, the FRA has extensively analysed the human rights implications of the new electronically fortified border regime in the EU (European Union Agency for Fundamental Rights 2018a). However, its reports do not question whether the technologically enhanced border controls by means of EUROSUR and the employment of biometric technologies in the Smart Borders Package are creating a "Digital Fortress Europe". There is an unquestioned reliance on technological fixes with regard to immigration. The human rights concerns identified by the FRA (2018a) relate solely to the quality of the data in SIS II, VIS and EURODAC informing data subjects about data processing, and the lack of adequate safeguards with regard to controlling data access. The FRA warns that the data may be hacked and abused, e.g. by oppressive regimes, or used unfairly, e.g. infractions committed as juveniles may carry over into adulthood. But from a critical perspective, it is doubtful whether these personal data protection rights are sufficient. The right to information (e.g. about collected or accessed data, or the means to correct or delete inaccurate data, etc.) alone cannot prevent the "net-widening" effect of one of the largest biometric databases in the world. The total surveillance of the Mediterranean and the electronic upgrading of border controls bring all ordinary travellers into the focus of border guards. "The EU is building a data juggernaut" (Unmüßig, Keller 2012). The plan to make all biometric databases interoperable may lead to inconceivable consequences, e.g. concerning the security and abuse of data (see critique in European Union Agency for Fundamental Rights 2018b).

Moreover, EUROSUR is being promoted as a tool to provide the right to life, i.e. to rescue refugees. But the system cannot deliver such a promise. As Hayes & Vermeulen (2012) show, maritime rescue services are not even part of EUROSUR, and border guards do not share information with them. Moreover, there are no procedures in place for the treatment or settlement of the "rescued" (Hayes, Vermeulen 2012). Technology – in this case EUROSUR – is employed to whitewash the political process of the externalisation of the border. Human rights discourse is merely a façade for securitisation (Campesi 2014).

Another forthcoming technological solution, the EES, which will collect biometric data such as fingerprints and face scans from all third-country nationals entering the Schengen area, is similarly vague in its objectives. The European Commission's impact assessments do not demonstrate compelling reasons or a pressing need for such a large database, and the alleged goal of the EES to increase the detection and return of "illegal immigrants" is unfounded (Hayes, Vermeulen 2012).

Moreover, there is significant reason for scepticism regarding the need for the large EU biometric databases arising from the vaguely defined and high costs. Andersson argues that the "fight against irregular migration", rather than curtailing movement, has led to more distress and drama at the borders, which in turn has fuelled a self-reinforcing industry of controls (Andersson 2014). It appears that the only real beneficiaries of these systems are defence contractors. While the European Commission estimates the cost of the Smart Borders Package to be on the order of €400 million, plus annual operating costs of €190 million, researchers have shown that the price may well be on the order of €2 billion (Hayes, Vermeulen 2012). For comparison, the cost of upgrading SIS to SIS II was also five times higher than the initial estimates.

The Massive EU Biometric Databases in Slovenia

Analysis of the fundamental rights implications of the large EU IT systems in the areas of borders, visas, and asylum in Slovenia shows another dichotomy: the systems operate well; in fact, in 2015, the Slovenian EURODAC controller received an award from the Information Commissioner for best practices in personal data protection. There is no imminent danger as regards human rights, but these remain hidden. The persons affected by EURODAC are vulnerable, with little or no understanding of foreign legal system, with no knowledge of the foreign language, and with little interest in antagonising the system they seek to become a part of.

Another database, SIS II, is highly targeted, focusing on just those individuals involved in criminal law proceedings, police surveillance, or banned from entry into EU territory. A study of the legislative, institutional, and practical aspects of SIS II shows that it poses no specific human rights issues. However, the targeted populace is very unlikely to challenge this IT system. As mentioned above concerning EURODAC, these are either vulnerable populations (e.g. foreigners, missing persons) or individuals escaping justice systems (e.g. persons wanted for arrest, extradition, or for discreet or specific checks). A study of the fundamental rights implications of biometric data stored in large-scale IT systems in the above areas in Slovenia furthermore shows that data subjects have low awareness of the power of these large EU IT systems, even though the police and the Information Commissioner offer detailed instructions to individuals regarding the exercise of their rights. Nevertheless, there have been no complaints and very little case law regarding the matter. The low awareness is even more important if connected to another fact – that the authorities rely on the SIS database to a considerable degree. A hit in a database offers powerful semiotics as to what the "truth" is in a particular case.

CONCLUSION

The turn to "the surface", from narrative to new regimes of truth in the form of biometric databases (Franko Aas 2004) and algorithmic decision-making systems is not specific to the "criminology of mobility." It is rather a part of the increasing reliance on the capacity of IT to tackle social problems. Digital technologies, ranging from big data analytics and real-time intelligence to algorithmic predictions and pre-emptive action, are supposed to solve social problems ranging from crime to migration. This is the mythology of technology (Boyd, Crawford 2011) – IT is supposedly more objective, unbiased, and precise. From such perspective, Frontex, EUROSUR and the large EU biometric IT systems in the areas of borders and asylum are part of a global trend towards the allure of the technological fixes to all kinds of social problems. Technology is conceived as the "ultra-solution" (Bigo, Carrera 2004). Technologies employed for tracking migrants, mobile phone applications for migrants, large biometric IT databases, "lie detectors" at borders (Boffey 2018) etc. are technological fixes that do not address the deeply-rooted causes of migration.

This article shows how mobility control technologies intensify surveillance by redefining the border. Increasing reliance on the capacity of supposedly objective, value-free and apolitical technology is producing a "Digital Fortress Europe". Digital walls are being created to complement the physical walls. In terms of the scale, opacity and harm of these systems, digital walls re-conceptualise the border in a new and often harsher way. Escape from the EU digital wall embodied in the large IT databases – EURODAC, SIS II, VIS, and, in addition, the four new IT systems planned, i.e. EES, RTF, ETIAS, and ECRIS-TCN,[7] and the new framework for their interoperability with a Common Identity Repository, is made impossible through the use of biometric technologies that inscribe a political identity in the body. The currently used and planned biometric data comprise fingerprints, palm prints, face scans and DNA profiles, with fingerprints predominating in all the above-mentioned databases (except ETIAS). However, new "lie-detectors" scrutinising "crimmigrant" bodies are on the brink of being employed (Boffey 2018).

Moreover, by "tattooing" borders onto migrant bodies, disciplinary power gives way to the post-disciplinary power of "instant surveillance". The crimmigrant body can be checked at anytime and anywhere within the EU. Borders are "tattooed" in the body. The border is inscribed into individuals' retinas, voices, or DNA. The new border is mobile and migrates with the unwanted body. The border thus becomes portable and digital.

The article shows how digital borders are expensive and mostly ineffective, and produce substantial collateral social harm: they reproduce inequality, increase incarceration, violate human rights, cause unnecessary deaths, and break up families (Jones 2017; Vitale 2017). Due to the numerous extreme forms of harm, borders should

7 ECRIS-TCN – the European Criminal Records Information System for Third-Country Nationals.

be de-policed, de-militarised, and, as this article shows, not augmented by means of technologies. The decision to employ technology to solve fundamentally non-technological issues eliminates the possibility of thinking of other solutions. Digital bordering is thus part of a larger managerial mentality and approach to tackling social problems. The current framing of migration follows the logic of "solutionism" – the view that for every social problem there must be a corresponding technological solution (Morozov 2013). IT is viewed as an infrastructure that will ensure unity in the EU Schengen border regime. However, IT fosters the colossal power of both the digital technology industry and military contractors, which are the only real beneficiaries of the digital borderlands. The construction of "Digital Fortress Europe" thus further perpetuates the cycle of global inequalities and triggers even more "irregular" migration.

REFERENCES

Adey, Peter (2004). Surveillance at the Airport: Surveilling Mobility/Mobilising Surveillance. *Environment and Planning A* 36/8, 1365–1380.

Alpes, Maybritt Jill, Tunaboylu, Sevda, Ulusoy, Orcun, Hassan, Saima (2017). *Post-Deportation Risks under the EU-Turkey Statement*. Policy Brief. Florence: European University Institute.

Anderson, Benedict (1998). *Zamišljene skupnosti*. Ljubljana: Studia humanitatis.

Andersson, Ruben (2014). *Illegality, Inc.: Clandestine Migration and the Business of Bordering Europe*. Oakland, CA: University of California Press.

Andersson, Ruben (2016). Hardwiring the Frontier? The Politics of Security Technology in Europe's 'Fight Against Illegal Migration'. *Security Dialogue* 47/1, 22–39.

Arendt, Hannah (2013). *O nasilju*. Ljubljana: Krtina.

Balibar, Étienne (2015). Borderland Europe and the Challenge of Migration. *Open Democracy*, www.opendemocracy.net/can-europe-make-it/etienne-balibar/borderland-europe-and-challenge-of-migration (14. 9. 2018).

Lin, Belle (2018). Amazon's Accent Recognition Technology Could Tell the Government Where You're From. *The Intercept*.

Bendixsen, Synnøve (2017). The Production of Irregular Migrants: The Case of Norway. *Dve Domovini / Two Homelands* 45, 29–43.

Bigo, Didier, Carrera, Sergio (2004). *From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU*. CEPS Commentary. Brussels: CEPS.

Bigo, Didier (2006). Security, Exception, Ban and Surveillance. *Theorizing Surveillance* (ed. David Lyon). Cullompton: Willan, 46–68.

Bigo, Didier (2014). The (In)Securitization Practices of the Three Universes of EU Border Control. *Security Dialogue* 45/3, 209–225.

Boffey, Daniel (2018). EU Border 'Lie Detector' System Criticised as Pseudoscience. *The Guardian*.

Bosworth, Mary (2013). Can Immigration Detention Centres be Legitimate? *The Borders of Punishment* (eds. Katja Franko Aas, Mary Bosworth). Oxford: Oxford University Press, 149–165.

Bosworth, Mary, Turnbull, Sarah (2014). *Immigration Detention, Punishment, and the Criminalization of Migration* (SSRN Scholarly Paper No. ID 2451088). Rochester, NY: Social Science Research Network.

Boyd, Danah, Crawford, Kate (2011). *Six Provocations for Big Data*. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, https://ssrn.com/abstract=1926431 (20. 11. 2018).

Bremmer, Ian (2018). *Us vs. Them: The Failure of Globalism*. New York: Portfolio.

Bučar Ručman, Aleš (2016). Družbeno nadzorstvo in mednarodne migracije. *Dve domovini / Two Homelands* 43, 11–22.

Campesi, Giuseppe (2014). *Frontex, the Euro-Mediterranean Border and the Paradoxes of Humanitarian Rhetoric* (SSRN Scholarly Paper No. ID 2519410). Rochester, NY: Social Science Research Network.

Dijstelbloem, Huub, Meijer, Albert, Besters, Michael (2011). The Migration Machine. *Migration and the New Technological Borders of Europe* (eds. Huub Dijstelbloem, Albert Meijer). London: Palgrave Macmillan, 1–21.

Franko Aas, Katja (2004). From Narrative to Database: Technological Change and Penal Culture. *Punishment & Society* 6/4, 379–393.

Franko Aas, Katja (2006). 'The Body does not Lie': Identity, Risk and Trust in Technoculture. *Crime, Media, Culture* 2/2, 143–158.

Franko Aas, Katja (2011). 'Crimmigrant' Bodies and Bona Fide Travelers. *Theoretical Criminology* 15/3, 331–346.

Franko Aas, Katja (2013). The Ordered and the Bordered Society. *The Borders of Punishment* (eds. Katja Franko Aas, Mary Bosworth. Oxford: Oxford University Press, 21–39.

Franko Aas, Katja (2014). Bordered Penality: Precarious Membership and Abnormal Justice. *Punishment & Society* 16/5, 520–541.

Franko Aas, Katja, Gundhus, Helene O. I. (2015). Policing Humanitarian Borderlands: Frontex, Human Rights and the Precariousness of Life. *The British Journal of Criminology* 55/1, 1–18.

Greene, Judith A., Carson, Bethany, Black, Andrea (2016). *Indefensible: A Decade of Mass Incarceration of Migrants Prosecuted for Crossing the Border*. Create Space Independent Publishing Platform.

Guild, Elspeth, Carrera, Sergio, Geyer, Florian (2008). *The Commission's New Border Package: Does It Take Us One Step Closer to a 'Cyber-Fortress Europe?* (SSRN Scholarly Paper No. ID 1334058). Rochester, NY: Social Science Research Network.

Hayes, Ben, Vermeulen, Mathias (2012). *Borderline – The EU's New Border Surveillance Initiatives*. Berlin: Heinrich Böll Foundation.

Hernández, César Cuauhtémoc García (2017). *Crimmigration Law*. Chicago, Illinois: American Bar Association.

Jones, Reece (2017). *Nasilne meje*. Ljubljana: Založba *cf.

Kogovšek Šalamon, Neža (2017). Mass Migration, Crimmigration and Defiance. *Southeastern Europe* 41/3, 251–275.

Lemberg Pedersen, Martin (2013). Private Security Companies and European Borderscapes. *The Migration Industry and the Commercialization of International Migration* (eds. Thomas Gammeltoft Hansen, Ninna Nyberg Sørensen). London: Routledge, 152–172.

Milivojević, Sanja (2013). Borders, Technology and (Im)Mobility: 'Cyber-Fortress Europe' and its Emerging Southeast Frontier. *Australian Journal of Human Rights* 19/3, 101–123.

Milivojević, Sanja (2018). *Border Policing and Security Technologies in the Western Balkans*. Lecture at the Faculty of Law, University of Oxford.

Morozov, Evgeny (2013). *To Save Everything, Click Here*. London: Allen Lane.

O'Neil, Cathy (2016). *Weapons of Math Destruction*. New York: Crown.

Pajnik, Mojca (2017). Spremna beseda. *Nasilne meje* (ur. Reece Jones). Ljubljana: Založba *cf.

Pickering, Sharon, Bosworth, Mary, Franko Aas, Katja (2014). *The Criminology of Mobility* (SSRN Scholarly Paper No. ID 2451108). Rochester, NY: Social Science Research Network.

Roson, Maria (2018). *Smart Borders*. European Digital Rights, https://edri.org/smart-borders-the-challenges-remain-a-year-after-its-adoption/ (14. 9. 2018).

Singh Bhui, Hindpal (2013). Introduction: Humanizing Migration Control and Detention. *The Borders of Punishment* (eds. Katja Franko Aas, Mary Bosworth). Oxford: Oxford University Press, 1–17.

Taylor, Diane, Graham Harrison, Emma (2016). EU Asks Tech Firms to Pitch Refugee-Tracking Systems. *The Guardian*, 18. 2. 1016.

The Economist (2016). More neighbours make more fences. *The Economist*, 7. 1. 2016.

The European Commission (2016). *EU-Turkey Statement*. Brussels, http://europa.eu/rapid/press-release_MEMO-16-963_en.htm (14. 9. 2018).

The European Union Agency for Fundamental Rights (2017). *Country Studies for the Project on Social Inclusion and Migrant Participation in Society*. Vienna: FRA.

The European Union Agency for Fundamental Rights (2018a). *Under Watchful Eyes – biometrics, EU IT-Systems and Fundamental Rights*. Vienna: FRA.

The European Union Agency for Fundamental Rights (2018b). *Interoperability and Fundamental Rights Implications*. Vienna: FRA.

Unmüßig, Barbara, Keller, Ska (2012). Preface. *Borderline* (eds. Ben Hayes, Mathias, Vermeulen). Berlin: Heinrich Böll Foundation.

Vitale, Alex S. (2017). *The End of Policing*. London, NY: Verso.

Wilson, Dean (2018). Constructing the Real-Time Border: Frontex, Risk and Dark Imagination. *Justice, Power and Resistance* 2/1, 45–65.

Wunderlich, Daniel (2012). The Limits of External Governance: Implementing EU External Migration Policy. *Journal of European Public Policy* 19/9, 1414–1433.

POVZETEK

EVROPSKA DIGITALNA TRDNJAVA IN VELIKI BIOMETRIČNI EU IT SISTEMI: KRIMINOLOGIJA MEJE, TEHNOLOGIJA IN ČLOVEKOVE PRAVICE

Aleš ZAVRŠNIK

Evropski kriminologi migracijske politike proučujejo od poznih osemdesetih let, ko so začeli prepoznavati trend zbliževanje kazenskopravnih ukrepov z upravljanjem migracij. Ta raziskovalni interes so imenovali »kriminologija mobilnosti« (Franko Aas, Bosworth 2013), »kriminologija meje« (Bosworth, Turnbull 2014), zbliževanje pravnih panog pa kot »krimigracijsko pravo« (Hernández 2017). Avtor v prvem delu članka prikaže obstoječe raziskave o kriminalizaciji mobilnosti in preoblikovanju kazenskopravnih institucij, zaporov in policijskega dela. Nato se osredotoči na digitalno področje, kjer z gradnjo velikih zbirk biometričnih podatkov vznikajo novi digitalni zidovi. To so SIS II (Šengenski informacijski sistem), VIS (Vizumski informacijski sistem) in EURADAC (Evropski sistem za primerjavo prstnih odtisov prosilcev za azil) ter predvideni štirje novi sistemi, paket Pametne meje (Sistem vstopa/izstopa in Program za registrirane potnike), ETIAS (Evropski sistem za potovalne informacije in odobritve) in ECRIS-TCN (Evropski informacijski sistem kazenskih evidenc), hkrati s pripravo interoperabilnosti med omenjenimi podatkovnimi zbirkami. Osrednja teza članka je, da s temi zbirkami EU »vpisuje« meje na telo migrantov in ustvarja novo vednost, ki disciplinsko oblast spreminja v »hipno oblast«.

Biometrične tehnologije so v uporabi po terorističnih napadih 11. septembra 2001 v ZDA. Te so uspele izvoziti idejo, da je migracija prvenstveno varnostni problem, ki ga je mogoče rešiti z vrhunskimi informacijskimi tehnologijami (IT). Evropska unija se je temu pridružila in gradi »digitalni zid«. Članek pokaže, kako ta odločitev opušča druge načine reševanja težav, kako je IT »politika z drugimi sredstvi«, in to kljub vtisu, da gre za apolitično in objektivno sredstvo, namenjeno »reševanju življenj«. V nadaljevanju avtor analizira pojem meje. V nasprotju s konvencionalnim prepričanjem prikaže, da se meje »multiplicirajo« in vznikajo na digitalnem področju. Pri tem se opre na obstoječe razmisleke Bigoja (2014) in Balibarja (2015). Digitalni zidovi so komplementarni fizičnim mejam, nove meje so »vpisane« neposredno v telo, so bolj učinkovite, premikajo se skupaj z »neželenimi« telesi. Takšno »tetoviranje« meja na imigrantska telesa kaže na vznik nove postdisciplinske »hipne oblasti«, ki se ne opira več na discipliniranje duše. V zadnjem delu članek prikaže škodljivost novih digitalnih zidov, kršitve človekovih pravic in večplastnost kaznovanja, ukrojenega glede na mesto človeka v »hierarhiji pripadnosti«.