# Race, Borders, and Digital Technologies

Input by Dr. Dimitri Van Den Meerssche (Asser Institute)

Dear Special Rapporteur,

My aim in this contribution is to share some insights from my academic research on emerging digital technologies in practices of border control. These practices entail clear risks of racial (and other forms of) discrimination and inequality.

**Introduction**

In my academic research, I focus mainly on new technologies of bordering that are being tested and developed within the European Union (Schengen Zone). The pilot projects on which my work focuses are especially important in light of the new EU regulation on the ‘interoperability’ of data systems in the domains of migration, border control and security, as well as the recent EU regulation on the ETIAS system (the European Travel Information and Authorization system – equivalent to ESTA).[[1]](#footnote-1) The latter system should be entering into force into 2021 and orients the decision-making on travel authorization and border control around an algorithmic assessment of ‘security, irregular immigration or high epidemic risk’.[[2]](#footnote-2) The basic challenge, as articulated by a number of decentralized EU agencies (including Frontex, Europol and Eu-Lisa), is to transform vast amounts of big data into ‘actionable’ information. It is in this translation of data into accessible information (appearing on a user interface) that tools of artificial intelligence are promoted. Olivier Onidi, EU Deputy Director-General of DG Migration and Home Affairs, recently claimed that ‘data analytics’ can make ‘data more illustrative for border guards’ and observed that ‘there is tremendous work being done on artificial intelligence in the EU … to use, combine and spread data’. He specifically underlined that ‘machine learning has potential’ for ‘vetting persons’, for ‘screening their application files’ and conducting ‘virtual border checks’. I identify three stages in the operationalization of ‘virtual borders’: the construction and maintenance of large-scale information systems, the infrastructure of interoperability between these systems and the use of algorithmic models that assemble disconnected data as actionable information.

In this brief contribution, I focus on three dimensions of the emerging informational infrastructure of ‘virtual borders’ in the EU: the types of technology, the actors involved and the dominant rationality.

**Types of digital technologies**

Two recently concluded pilot projects – Tresspass and iBorderCtrl – shed light on the types of border control technologies that are being tested and deployed in the EU.[[3]](#footnote-3) These ‘state of the art’ border control systems – funded by the EU Commission, overseen by Frontex and run by a consortium of consultancy firms, computer scientists and private corporations – claim to trade ‘subjective control of human agents’ for ‘objective control with automated means’. They function first and foremost to vastly expand the amount and types of data on the basis of which border controls are conducted. The Tresspass system, for example, provides the capacity for ‘real-time behaviour analytics’ at the border that could detect ‘hidden aspects’ of ‘intent’ and ‘attitude’ through ‘on-site observations’ as well as ‘open source web intelligence and mining’. The project calculates ‘risk’ on the basis of ‘observable’ (‘identity’ and ‘behavior’) as well as ‘hidden’ aspects (‘mental state’, ‘intent’ and ‘capacity’) that are retrieved from ‘biometric technologies’, ‘sensing technologies’ and the ‘links to legacy systems and external databases such as VIS/SIS/PNR’. iBorderCtrl, in a similar vein, trades technologies of facial recognition (which crossmatch images with databases) for new forms of biophysiological reading: in ‘analysing non-verbal micro-expressions’ to ‘quantif[y] the probability of deceit’, the system claims to have moved ‘beyond biometrics and onto biomarkers’ that could read ‘psychological states’ from uncontrollable physical features. In the case of iBorderCtrl, this implies the use of SilentTalker – a patented artificial intelligence tool for lie detection that can be employed for a variety of purposes.

Both experimental pilot projects share a number of features. First, they drastically increase the amount of data that is assembled at the border: they do not only draw on information already present in public information systems or biometric databases but also develop an interface with social media platforms (‘open source web intelligence and mining’), new sensors for real-time behavioral analysis and an infrastructure to read and process ‘biomarkers’. Second, they provide a platform for interoperability between various already existing information systems and databases – a technical interconnection of data that is currently scattered. Third, they aim for an automated reading of subjective, psychological states that presumably signal danger or deceit. These projections are based on deep learning tools for visual recognition and anomaly detection traditionally deployed in the security sector.[[4]](#footnote-4) It has been well [documented](https://iborderctrl.no/blog%3Aiborderctrl_automates_discrimination) how these systems entail clear risks of racial bias and discrimination.

**Actors involved**

The focus on pilot projects not only reveals the types of technology that are being tested and deployed but also sheds light on which actors are involved in the construction of ‘virtual borders’. It is clear that this construction and the associated need for new digital technologies and data mining models entails a strong reliance on private technology corporations and risk consultancy consortia. While Europol is ‘scouting the market for available [AI] technologies’,[[5]](#footnote-5) Frontex has institutionalized this scouting process in the ‘tool’ of ‘technology foresight’ through which ‘industry representatives’ are invited to pitch the ‘technologies that may, in a medium or long-term perspective, impact the EU borders and the Border and Coast Guard community the most’.[[6]](#footnote-6) EU border control authorities are not developing technologies on their own, they buy from the market (usually in public procurement). One way to conceptualize the pilot projects discussed above is as formations of public-private networks where available tools on the market are tested and traded. In the iBorderCtrl consortium, for example, we find border control agencies (from Hungary, Latvia and Greece) and academic institutions side by side with consultancy firms (such as Everis or European Dynamics) as well as private technology and security actors specialized in biometrics and artificial intelligence (such as BioSec and JAS). In the same vein, the Tresspass consortium employs the services of Vicarious Perception Technologies for its ‘people tracking, person re-identification and stress detection solutions’ – a corporation priding itself on having designed the ‘world’s first tool capable of automatically analysing facial expressions’. The ‘security and intelligence’ firm Zanasi & Partners ‘will leverage its expertise in risk assessment methodologies and human factors in border control to drive the identification of risk indicators and support the definition of methods for threat and risk assessment’. When looking at the emergence of ‘virtual borders’ through the prism of these pilot projects, in other words, what we see is the alignment of security logics with the private sector interest of selling ‘state of the art’ artificial intelligence tools and risk modelling systems. This has obvious repercussions on the level of political decision-making, transparency (most of the new sensors and models deployed by iBorderCtrl and Tresspass are patent-protected and not open to scrutiny) and democratic control.

**Logics and rationalities**

Associated with the previous point is the prevalence of a sociotechnical imaginary in which political dilemmas are displaced by the invocation of technological objectivity and progress. This is what we clearly observe in the assertion by iBorderCtrl that ‘subjective’, ‘human’ decision-making is traded for ‘objective control with automated means’. It is also prevalent in other EU policies and legislations, such as the ECRIS-TCN regulation (installing a criminal records information system for third-country nationals), which grants the EU Commission the delegated power to adopt facial recognition policies employing automated biometric verification whenever these technologies ‘become available’. This is an explicit deference of legislative power to a speculative futurity of technological enhancement.

Yet, while narratives of techno-optimism or neutrality are omnipresent, I conclude by pointing to the central logic at play in both Tresspass and iBorderCtrl: the rationality of risk. This entails an extension of post-9/11 security discourses, infused with the promise of enhanced algorithmic pattern detection. Aiming to translate disaggregated data in formats amenable to automation, Tresspass designs a ‘single cohesive risk-based border management concept’ that provides ‘risk indicators’ on the basis of data associations. In an explicit expression of governmental change, the project claims to move away from the ‘old and outdated rule based to the new risk-based strategy’. Similarly, iBorderCtrl sets out that ‘risks are key to the performance of the system as they declutter the information by compressing all data into meaningful actionable risk scores’. In its shift from a ‘rule based’ to a ‘risk based’ order, the ‘advanced risk modelling’ tools used by iBorderCtrl and Tresspass become authorized in public decision-making as techniques of association that displace thicker forms of identification and social affiliation to which (international) legal thinking is more directly attuned (those linked to territory, population or legal status). The promises of algorithmic pattern detection have significantly altered and expanded the logic of ‘risk’, leading to new forms of subjectivity, discrimination and inequality.

1. See Regulation (EU) 2018/1240, Regulation (EU) 2019/816, Regulation (EU) 2019/817, Regulation (EU) 2019/1896. [↑](#footnote-ref-1)
2. See article 33, Regulation (EU) 2018/1240. [↑](#footnote-ref-2)
3. For more info: <https://www.iborderctrl.eu/Technical-Framework> and <https://www.tresspass.eu/Technical-Framework>. [↑](#footnote-ref-3)
4. My work draws on the great insights of C. Aradau, T. Blanke, “Governing Others: Anomaly and the Algorithmic Subject of Security”, *EJIS*, Vol. 3:1, 2017. One of the architects of Tresspass noted: ‘through advancements in Artificial intelligence and mainly through the application of machine learning, security professionals have greatly augmented their capability of analyzing data concerning the behavior and profile patterns of attackers, both in terms of volume of data and in terms of availability of sources’. In D. M. Kyriazanos et al, “Automated Decision Making in Airport Checkpoints: Bias Detection Toward Smarter Security and Fairness”, *IEEE Security and Privacy Magazine*, 2019. [↑](#footnote-ref-4)
5. See eu-LISA, *Conference Report: Going Digital for a Safe and Secure Europe*, 17-18 October 2017, Tallinn, 17. [↑](#footnote-ref-5)
6. Indicatively, Frontex has recently also contracted RAND corporation to conduct a comprehensive study on the possible future uses of AI technology in border control. See <https://www.rand.org/randeurope/research/projects/european-border-coast-guard-artificial-intelligence.html>. [↑](#footnote-ref-6)