sicherheits politik-blog

EUROPE'S NEW DIGITAL BORDERS

Aktualisiert am 5. Jul. 2018 Von gast Kommentieren

This article is part of our series Congruence and Competition of Norms and Values in the Context of Global Digitalization.

by Matthias Leese

The European Union's (EU) external border framework is not only increasingly reliant on digital databases, but these databases are now set to become interoperable. By 2020, the European Commission (EC) aims to have a fully interconnected new architecture for identity management at the border in place. Based on biometric enrolment of all third-country citizens, Europe's new digital borders raise a number of concerns, including suspicion, large-scale surveillance, and internal policing that spread well beyond the border site.

Border management today is embedded into a complex network of data collection and data analysis that provides authorities with knowledge about who (or what) attempts to cross the border. While still serving as physical chokepoints for the examination and extraction of dangerous, suspicious, or illegitimate elements from global flows of mobility, border operations therefore increasingly rely on a number of databases.

In the EU, this database infrastructure currently consists of separate systems for visa management (Visa Information System, VIS), for the processing of asylum applications (the EU asylum fingerprint database EURODAC), for the systematic recording of border-crossings of third-country nationals (the recently adopted but not yet implemented Entry-Exit System, EES), and for law enforcement and judicial cooperation (Schengen Information System, SIS). This already impressive list will, if everything goes according to plan, soon be complemented with a European Travel Information and Authorisation System (ETIAS) and a European Criminal Records Information System for third-country nationals (ECRIS-TCN).

All of these systems, while serving distinct domains and purposes (e.g., national/international security, business facilitation, international humanitarian law, migration management, domestic law enforcement), collect data on border crossers, notably with a focus on non-EU citizens. Moreover, most of them collect biometric data (such as for example fingerprints or facial images) that are then turned into so-called templates which enable authorities to identify a person and to match their

claimed identity with unique characteristics of their physical body.

While the current setup of EU border databases already presents an unparalleled effort of data collection, the EC is making an effort to render all of them interoperable, meaning to effectively link the data that they contain. With reference to the identified need for "Stronger and Sma Information Systems for Borders and Security" (COM(2016) 205 final), the EC has since 2016 put forward an impressive number of legislative proposals (including the creation of the EES, the ETIAS, and the ECRIS-TCN, as well as revisions and upgrades to the SIS, the VIS, and EURODAC), which culminate in the plan to draw all of these databases together, using the biometric data that they contain as an anchor.

The "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa)" (COM(2017) 793 final; proposed in December of 2017 and at the time of writing subject to the trilogue negotiation phase between the EC, the European Parliament, and the Council) therefore specifies a layered architecture that is supposed to connect data through multiple tools, and to streamline the digital underpinnings of border work in the EU in an unprecedented fashion. The proposal rests on four interoperability components: (1) a European Search Portal (ESP); (2) a Shared Biometric Matching Service (Shared BMS); (3) a Common Identity Repository (CIR); and (4) a Multiple Identity Detector (MID).

The operational starting point of the proposed architecture would be the Shared BMS that would cross-match biometric data stored in different systems and converge available (but scattered) information on individuals. The identity records created in this way (biometric template plus alphanumeric biographical data) would in turn be stored in the CIR, which would be connected to the distinct databases and provide the biometric baseline anchor that would tie all systems together. Last but not least, the MID would flag identical biometric templates throughout multiple systems, thus helping to identify and eradicate multiple and possibly fraudulent identities. The ESP would, last but not least, provide the front-end interface for this new identity management architecture, eventually enabling authorities to query all available databases through the CIR via a single search and receive matches from all systems that they are authorized to access.

Judging from the hundreds of pages of legislative proposals, accompanying studies, and working group reports that have contributed to the proposed architecture, one might get the impression that interoperability of the digital border infrastructure breaks down to technical rationalities and small-scale engineering and design questions. Keeping in mind this blog series' overarching scope on normative aspects of technology and its development and design, it is however important to stress that the proposed architecture is neither a straightforward technical question nor even a necessity. On the contrary, it is first and foremost a political decision that is underpinned by actor rationalities as well as by the discourse that surrounds it. It is therefore key to closely look at the arguments and choices involved in this process, and to probe the wider normative repercussions of Europe's new

digital borders across society.

It is quite telling in this regard that the EC regularly refers to the fight against terrorism and international crime when seeking to legitimize the need for interoperability. Statements such as "we need to urgently address the remaining gaps, fragmentation and operational limitations of the information exchange tools in place, to make sure that structures for cooperation are as effective as possible, and to make sure that European legislation to tackle terrorist criminals and their activities is up to date and robust" (EC Communication on "Delivering on the European Agenda on Security"; COM(2016) 230 final) can be found in similar wording throughout all relevant documents.

Such statements are a strong testament to how mobility is turned into a security question, as it becomes discursively connected to terrorist/criminal threat, and technical countermeasures are rendered as necessary for effective counterterrorism and transnational policing operations. As a consequence of this presupposed necessity, third-country nationals travelling to the EU are put under general suspicion, regardless of whether they arrive as refugees seeking asylum or as tourists. This suspicion is in turn expressed in the aggravated desire to collect and connect data on travelers from outside the EU, feeding into a logic of surveillance and preemption that rests on knowledge about possible security risks that could be extracted from large amounts of data.

Border work in this sense then becomes turned into a large-scale operation of registering, cross-referencing, and monitoring of travelers. The second implication proposed here derives directly from this transformation, as through the construction of an identity management grid for third-country nationals, border functions can be easily extended from the physical site of the border checkpoint to the outside (for example when individuals enroll for the ETIAS in their home countries, meaning that traveler data will be at disposal long before the actual traveler arrives at the border) and the inside of Schengen zone territory (for example through internal police checks to identify visa overstayers, who account for a large portion of illegal residents, and match their biometric features with entry records from the EES), where they further converge with domestic law enforcement and policing operations.

Last but not least, the CIR raises significant concerns about data protection and IT security. Converging information on millions of individuals in a single repository increases the risk connected to data breaches. Particularly in combination with the stored biometric templates, this opens up vast potentials of abuse, not only in terms of privacy, but for example also in terms of identity theft. If the history of IT security has demonstrated one thing, it is that the question is not if a system can be compromised, but how and when someone will find a way to do so.

Overall, Europe's new digital borders, as proposed by the European Commission, would present a massive and ongoing endeavor to register and identify non-EU citizens as they travel to and from the EU, and to enroll them in an administrative apparatus of identification and population management that would in turn enable new forms of surveillance and policing, both outside and inside the Schengen territory. This would perpetuate a logic of risk and preemption that hinges on

knowledge about the identity of border-crossers. The question of identity, we should keep in mind, is thereby always inextricably tied to the normative evaluation of an individual. As Jane Caplan and John Torpey write in the Introduction to their 2001 edited collection *Documenting Individual Identity*: "The question 'who is this person?' leaches constantly into the question 'what kind of person is this? '" At the border, the answer to this question is more than ever looked for in large-scale, interconnected, and digital databases.

Dr. Matthias Leese is a Senior Researcher at the Center for Security Studies (CSS), ETH Zurich. His research interests are broadly located in the fields of critical security studies, surveillance studies, and science and technology studies. His work has, among others, been published in *International Political Sociology*, *Security Dialogue*, *Critical Studies on Security*, *Criminology & Criminal Justice*, *Global Society, Mobilities, Critical Studies on Terrorism,* and*Science and Engineering Ethics*. With Stef Wittendorp, he is the editor of *Security/Mobility: Politics of Movement* (Manchester University Press). For more information, please refer to https://matthiasleese.com.

Tags: border database European Union surveillance

SCHREIBE EINEN KOMMENTAR

Deine E-Mail-Adresse wird nicht veröffentlicht.

Kommentar

Name

E-Mail

Website

☑

Meinen Namen, E-Mail und Website in diesem Browser speichern, bis ich wieder kommentiere.

☑ By using this form you agree with the storage and handling of your data by this website. *

Kommentar abschicken