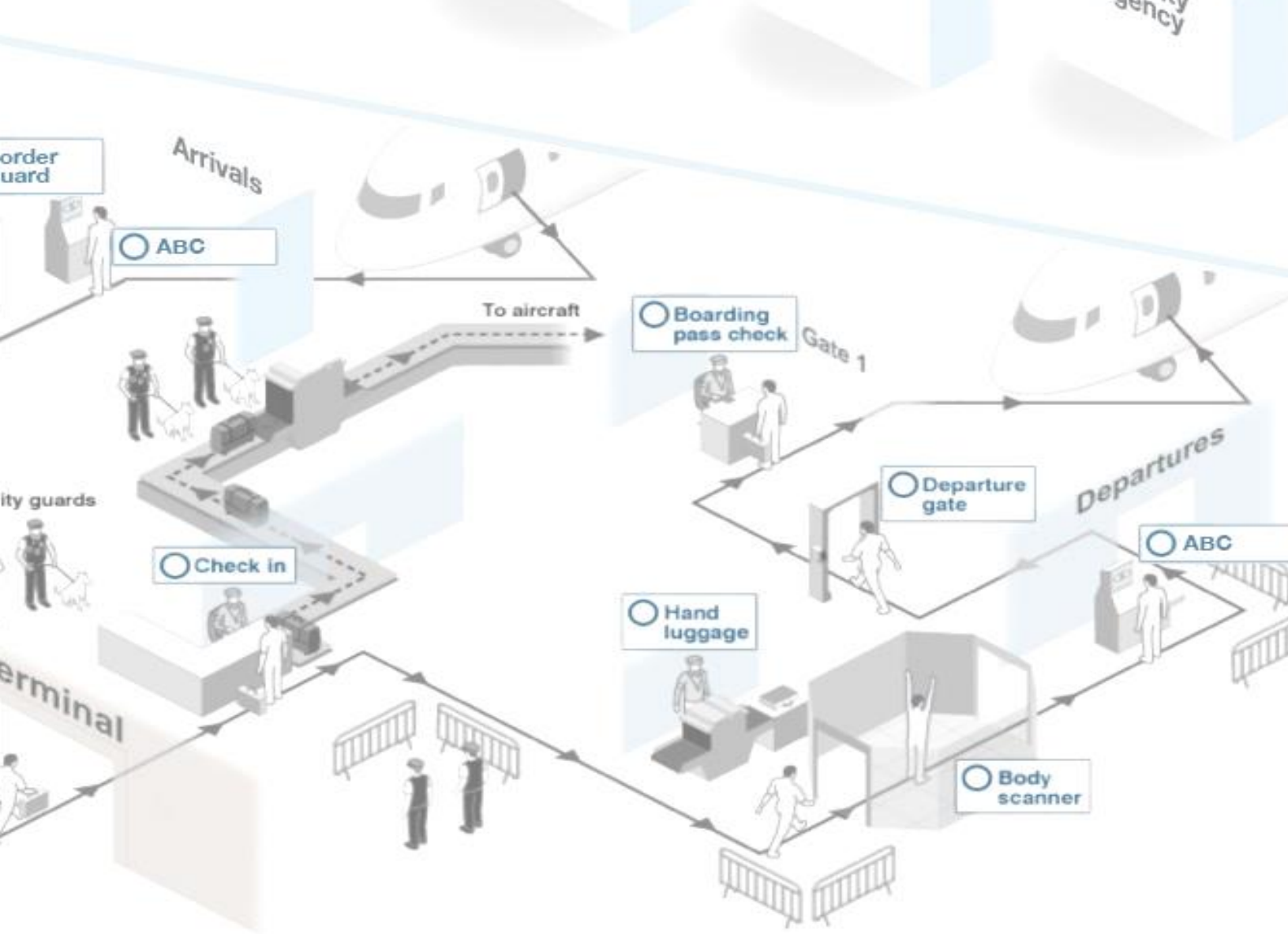

Big Data at the Border

A report by Eticas Research and Consulting for The New Venture Fund 'Quantified Society: Examining the Consequences of Algorithmic Decision Making for Open Societies'

Table of Contents

Table of Figures

Glossary

ABC

Automated Border Control gates rely on biometric identification systems that match travellers' data with the data embedded in their e-Passports in order to automatize travellers' authentication decisions (acceptance or rejection).

SIS I & II

The Schengen Information System (SIS I & II) is a database containing information on criminal activity, immigration violations, and various objects and missing persons. It is aimed at supporting external border control and law enforcement cooperation between the Schengen States and, therefore, it is used by the police, customs, visa and judicial authorities throughout the Schengen Area.

VIS

The Visa Information System (VIS) is a database linking Schengen members' consulates abroad and external borders as a means of avoiding visa fraud by taking and transmitting visa applicants' biometric information.

Biometrics

Biometrics refers to the measurement of human physical characteristics. In this context, the use of the term is related to its application for verifying an individual's identity.

Smart Borders Initiative

The European Commission Smart Borders Initiative is aimed at managing EU external borders more efficiently and consists of two main proposals: the implementation of an Entry/Exit System (EES) as well as a Registered Travellers' Programme (RTP)

EES

The Entry/Exit System (EES), proposed within the framework of the Smart Borders Initiative, would record the time and place of entry and the length of authorized short stays in an electronic database, replacing the current system of stamping passports and making this information available to border control and immigration authorities.

RTP

The Registered Travellers Programme (RTP), proposed within the framework of the Smart Borders Initiative, would allow certain groups of frequent TCN travellers (i.e. people travelling for business purposes, family members etc.) to enter the EU using simplified border checks, after having undergone a pre-screening process.

Watch-list

A list of individuals to be observed or even kept under surveillance, and deserving special attention because of suspicion of wrongdoing, usually based on alerts or relations inferred from their personal data.

BCPs

According to the Schengen Border Code, the term Border Crossing Points (BCPs) refers to any crossing-point authorized by the competent authorities for the crossing of external borders.

EURODAC

The European Dactyloscopy or EURODAC is the European common fingerprint database aimed at identifying asylum applicants and persons who have irregularly crossed the EU's external borders.

EU-LISA

European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice. The Agency is currently managing the EURODAC, the Visa Information System (VIS) and the second generation Schengen Information System (SIS II).

US-VISIT

The United States Visitor and Immigrant Status Indicator Technology program was the U.S. Customs and Border Protection (CBP) management system until 2013.

Introduction

Since 9/11, airports and border-crossing areas have become critical infrastructures and, some may say, states of exception. Enhanced security measures have turned airports into dense data ecosystems. Passenger purchase and travel details are shared, often across borders, among authorities and operators; automated border gates collect and authenticate personal data and biometrics, matching travellers with the information registered in their travel documents (opening the microprocessor chip embedded in the document); and databases with different levels of security protocols determine who is allowed to fly and register who is going where and when. The ongoing implementation of technology and digital data to control peoples' movement is not just a technical matter, but it brings about significant transformations to the features, politics and experience of border crossing.

In the European Union (EU), a 'Smart Borders Initiative' is currently being discussed. The Project intends to expand and harmonize automated border crossings (ABC) at the EU level, develop plans for a Registered Traveller Programme (RTP) to facilitate border crossing for pre-approved third country nationals, create an Entry-Exit System (EES) to identify over-stayers, and propose an amendment to the Schengen Borders Code.

For this initiative, 'facilitation is the main objective to maximize, and security a boundary condition that has to be met… [and] cost-effectiveness is also an important dimension to be observed.'[1] It is expected that ABC systems can both speed up the process, while providing at least equal levels of security, by facilitating a quick validation and identification of each traveller. By making ABC systems interoperable with external databases (e.g. SIS-II and national police watch-lists), it is hoped that red flags will be raised, which will allow for the identification of individuals with suspicious travel patterns, diets, behaviors, or records, for instance. This will advance surveillance practices of automated social sorting and profiling, putting the grounds for algorithmic governance and decision-making at borders.

National laws establish the different levels of screening that citizens and foreigners undergo in a variety of situations. Whilst these requirements used to be executed by means of human decisions, they are increasingly being mediated by technological solutions. This report is guided by the need to map the present procedures, to obtain a comprehensive picture of the potential uses and risks of the gathered data, and to understand how big data could contribute to algorithmic decision-making at the border.

Present-day procedures constitute a hybrid form of human and algorithmic decision-making, as is required by law. However, it is the promise of a border-crossing big data system that underpins the attempts to automate and enhance border control through the use of data-intensive technologies.

While the quest for Smart Borders continues, most efforts seem focused on the technical and financial aspects of new border-crossing technologies and procedures. The human rights and civil liberties implications of securing borders through automatization of data processing, mining, and

[1] Frontex, *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems* (Warsaw: Frontex, 31 August 2012).

matching, however, remain under researched. The development and implementation of ABC systems require a balance between national security concerns, the technological solutions used to that end, and the respect and protection of human rights and civil liberties. After all, citizenship is defined and put to the test at the border. The EC establishes that evidence of identity and document authentication at the border guarantees verification of a traveller's 'claim of EU citizenship',[2] and the rights and freedoms enjoyed accordingly. Our democratic systems, our definition of citizenship and our relationship to the 'other' are captured, and defined, in our border-crossing procedures and technologies.

However, so far most of the research on the relation between big data and algorithmic decision-making has focused on its commercial and market uses. Failures and misclassifications in targeted advertising, and the profiling of audiences, are of utmost importance. This report, however, brings to light the implications of the use of big data and algorithmic decision-making in a sensitive context, such as border checkpoints (BCPs), where acceptance is not optional and where citizens' rights, rather than customers', are at stake.

While the convenience of travellers as they experience border crossings is the primary goal of the e-gates policy, the adoption of the technology and the actual use of it will rely greatly on the interests and attitudes of those designing and operating the system, as well as on their social acceptance. Technology developers and border authorities are thus key stakeholders in the development and implementation of this policy, which will result in a technologically mediated procedure with important ethical, legal and social implications that will be felt by millions of citizens when travelling.

The current situation, with Automated Border Crossing Gates being installed in many airports and Smart Border Pilots being tested at air, land and sea BCPs in the EU, it is of utmost importance to research and identify how new automated practices may impact society and both capture and reproduce social processes (including discrimination and bias); it offers a unique opportunity (and challenge) to think through, and participate in, crucial choices that will shape not only the future of our borders − and the right of mobility − but also the permeability of our societies.

This report is a contribution to the political debate and policy planning. The first section focuses on the changing practice and nature of borders due to the implementation of digital technologies, biometrics and automation, and reflects on the impact of these new borders' morphologies on the mobility of individuals and their rights. It discusses the legal framework of the EU Smart Borders Initiative and provides a description of the role borders play in the configuration of our societies, and how technology and digital data are creating new ways to regulate and control circulation flows. It draws on law, anthropology, sociology and surveillance studies to lay out the relationships between borders, data, citizenship and fundamental rights and values.

The second section maps the data flows at border crossing points, showing how data processing extends identity authentication from the physical space of the border (and specifically airports) to the locations where pre- and post-screening procedures happen (from the embassy to the travel agent, the frequent-flyer program or the immigration authorities).

[2] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Preparing the Next Steps in Border Management in the European Union. Impact Assessment*, SEC(2008) 153 (Brussels, 13 February 2008), p. 55.

Taking as a point of reference the theoretical reflections about borders and technology presented in Section I, and the detailed mapping of data flows in Section II, the last section is devoted to presenting the qualitative empirical data related to how border guards and passengers experience the changing nature of borders due to the automatization of borders and the proliferation of identification and database-matching technologies. In Section III, empirical data on the everyday dynamics of human interaction with algorithmic decision-making processes and big data practices at border crossing points are described through the words of border guards and the observation of traveller flows and interactions at several EU BCPs. The empirical findings and theoretical insights that we present in this report are surely relevant beyond the European context, as these systems are being implemented globally.

The main objective of this report is to identify the risks posed to fundamental rights and values by the use of automated decision-making technologies at border crossings, focusing in three analytical stages: implementation, automation and discrimination. It explores the ways in which the availability of large quantities of data at border checkpoints, combined with the ability to check, match and make decisions with it elsewhere, is shaping and mediating border crossing. Human rights and values that are at stake at such sensitive enclaves are also investigated, especially in relation to biometrics acquisition and database interoperability. It represents the first attempt of this kind, and thus it is exploratory in its nature. At the end of the report, a future research agenda is outlined.

Section I: Borders beyond borders

As physical embodiments of the security apparatus, border technologies function as literal points of contact between individuals and states. The use of big data at the border not only signals new ways of managing borders, but also produces new ways to imagine the relationship between borders, states, citizenship and fundamental rights. This section is dedicated to exploring how the complex intersection of these concepts can be understood in real and specific terms.

Given the increasing turn towards technology as a solution for contemporary border management challenges, it is especially important that decisions regarding the development and deployment of border technologies are made, taking into account fundamental rights, societal values and legal norms. In this section, the legal framework of the technologies and database used at the EU borders is presented. The changing morphologies and socio-political role of borders is also explored, along with the relationship between bodies, biometrics and legal statuses. Finally, the rights and values that can be affected by border technologies and the surveillance capabilities of data-mining processes are addressed.

1. Big data at the border: Legal framework

In 1985 the signing of the Schengen Agreement by five of the then members of the European Economic Community led to the creation of the equivalent of a single state for travel purposes. Internal border controls were slowly abolished and a common visa system was created, together with an external border control for people entering and exiting what became known as the Schengen Area. The Agreement established the abolition of checks at internal borders and the creation of a common external frontier (regulated by the Schengen Border Code, SBC), the creation of a database to verify people and objects accessible and modifiable by Schengen member states (Schengen Information System, SIS) and mechanisms for increased police and judicial cooperation.

The Schengen Border Code also defines border-check standards and procedures and sets the main legal definitions that guide implementation ('persons enjoying the Community right of free movement' versus 'third country nationals'). The Schengen Information System (SIS I & II) is a database containing information on criminal activity, immigration violations, various objects and missing persons and is used by the police, customs, visa and judicial authorities throughout the Schengen Area. The Visa Information System (VIS) is a database linking Schengen members' consulates abroad and external borders as a means of avoiding visa fraud by taking and transmitting visa applicants' biometric information.

SIS I, SIS II and VIS are the backbone of the Big Data Border, and their interoperability and integration with travel documents, Automated Border Control gates and other sources of information linked to the surveillance of border crossing points (CCTV, facial recognition, pattern recognition, identification of abandoned objects, etc.) is the basis of the promise of a 'smart border' able to identify and intercept wrongdoing before it happens while enhancing the experience of *bona fide* travellers (Franko Aas, 2011).

When it comes to data management, the Schengen *acquis* is coupled with current privacy and data protection regulations such as Convention 108, the Council of Europe's Police Data Recommendation and Data Protection Directive 95/46/CE. Convention 108 is the first legally binding international instrument adopted in the field of data protection and regulates transborder flows of personal data. The Police Data Recommendation confirms the lower protection standard to which data held for police purposes can be subject, but also provides data subjects with safeguards through the right to data erasure. The Data Protection Directive establishes the minimum standard of data protection in the EU while also providing a number of exceptions relevant to Automated Border Control deployment (national security, defence and the prevention of crime). As it is only a Directive, it is implemented differently in different member States.

EU regulations on travel documents are another central element of border management. The main piece of regulation is Council Regulation 2252/2004 of 13 December 2004, on 'standards for security features and biometrics in passports and travel documents issued by Member States', on the introduction of biometrics throughout EU travel documents with a focus on harmonization of standard ICAO Document 9303 (especially for biographical data and machine-readable information). The regulation calls for the use of the document bearer's facial image and two fingerprints in interoperable formats (Article 1), but its annex of technical specifications (on questions such as electronic chip layout) remain unpublished for secrecy reasons. It establishes, nonetheless, that biometrics are to be used only to verify document authenticity and the identity of the document holder (Article 4), and nothing more.

Current EU legislation poses a genuine dilemma as, according to the Schengen Borders Code, external databases are only permitted to be checked on a non-systematic basis, and only when there is evidence of a present and sufficiently serious threat. The translation of such complex legal guarantees into algorithmic decision-making is a challenge that has not yet been solved, even though the plans for a Smart Border initiative are moving forward. Ultimately, the social desirability of the Smart Borders Package will depend on the ability of the new technological developments to translate fundamental rights and the current legal framework (and the values and guarantees it embodies) into the technological specifications and overall design of the border data-management system.

1.1. EU Smart Borders proposal

The EU 'Smart Borders' package consists of three elements:

(i) a proposed Entry-Exit System (EES), which would log the place, date, time, identity and fingerprints of all third country nationals (TNCs) crossing the external borders of the Schengen area (including airports);

(ii) a proposed Registered Traveller Programme (RTP), to speed the entry and exit to the EU of pre-vetted, *bona-fide* TNCs;

(iii) Automated Border Control (ABC) gates, linked to the EES and RTP, to check and log the identities of TNCs crossing external borders.

The stated aim of the package is to improve the management of the external borders of the Schengen states, to combat irregular immigration and provide information on 'over stayers', and to facilitate border crossings for frequent travellers. This would work by automatically checking the fingerprints and photographs of TNC's crossing the Schengen external borders against data stored in travel documents and held in the EU Visa Information System, and logging these details in the EES. In cases where a person's exit from the Schengen area is not logged by the EES in the relevant time frame (e.g. 3 months for someone on a Schengen visa), then an 'alert' (a *de facto* arrest warrant) will automatically be issued to the relevant authorities. The RTP would work by providing pre-vetted and registered passengers with an electronic token allowing them to pass more rapidly through ABC gates than other TNCs. The criteria for acceptance into the EU RTP would be similar to the harmonized criteria set out in EU rules on residence permits.

The proposals first appeared in a European Commission (EC) Communication of February 2008,[3] which put the cost of the smart borders package at €113 million. In addition to the proposed EES and RTP, the Communication proposed a European Electronic System of Travel Authorization (ESTA), mirroring the requirements imposed on travellers to the USA from countries on the visa waiver program, who must provide information about themselves and their intentions to obtain a permit to travel before departing for the US. However, the idea of an EU ESTA was dropped from subsequent EU proposals. These proposals built on a second EC Communication on 'Smart Borders' published in in October 2011,[4] in which the expected cost had risen from just over €100 million to 1.3 billion (with a potential saving of 'about 30%' if the EES and RTP were built on the same technical platform). By the time the Commission issued formal legislative proposals establishing the EES and RTP in February 2013,[5] there were substantial concerns about the cost, effectiveness and human rights impact of the entire package.

Firstly, the member states questioned the value of the Entry-Exit System in terms of identifying over stayers (that is persons who have exceeded the duration of their permitted stay or visa), and effectively argued that it would only be worth establishing the system if law enforcement and security agencies had access to the data for intelligence and investigation purposes. This position has now been accepted by the European Commission, meaning that 'Smart Borders' will now serve a security purpose as well as an immigration control one. Secondly, there were concerns that the EU Visa Information System (VIS) and second-generation Schengen Information System (SIS II), to which the EES would be linked, had not yet been implemented (VIS), and beset with technical problems (SIS II). Both systems are now online. Third, significant doubts were raised in

[3] European Commission (2008) *Preparing the next steps in border management in the European Union*. Brussels, COM(2011) 69 final, 13.2.2008.

[4] European Commission (2011). *Smart borders – options and the way ahead*. Brussels, COM(2011) 680 final,25.10.2011.

[5] European Commission (2013) *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*. Brussels, COM(2013) 95 final, 28.2.2013; *Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme*. Brussels, COM(2013) 97 final, 28.2.2013; *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*. Brussels, COM(2013) 96 final, 28.2.2013.

respect to claims in the Feasibility Study, which was produced by a technical sub-contractor, about how much time would actually be saved by automating border crossings. These were set out in a report commissioned by the European Parliament. Fourth, the European Data Protection Supervisor was strongly critical of the proposals, suggesting that 'There is no clear evidence that the Commission Proposals to create a smart border system for the external borders of the EU will fulfil the aims that it has set out… [O]ne of the stated aims of the proposals was to replace the existing 'slow and unreliable' system but the Commission's own assessments do not indicate that the alternative will be sufficiently efficient to justify the expense and intrusions into privacy.'[6]

The legislative proposals were effectively withdrawn in February 2014, following concerns raised by the member states in the Council and the European Parliament. In order to further assess the technical, organizational and financial impact of 'Smart Borders', the Commission then launched a 'proof of concept exercise' consisting of a 'Commission-led Technical Study aimed at identifying and assessing the most suitable and promising options and solutions' and a 'Testing phase entrusted to the Agency for the Operational Management of large-scale IT Systems (EU-LISA), aimed at verifying the feasibility of the options identified in the Technical Study and validating the selected concepts for both automated and manual border controls.'[7] The technical study was delivered in October 2014, while the testing phase was scheduled for completion in September 2015. The Commission also launched a public consultation on smart borders, which runs from July to October 2015. Revised legislative proposals are expected in early 2016.

2. Forming, performing and moving (across) digital borders

'Borders are moving' (Guild, 2001) or 'borders are everywhere' (Lyon, 2005, Perkins and Rumford, 2014) are two of the numerous metaphors alluding to the changing social physiognomy of borders that have thrived in the academic literature in last two decades. These images aim to emphasize the idea that borders are now diffused and increasingly defined beyond a specific physical space. These changes imply transformations of the way mobility is checked and controlled and, thus, in the way borders fulfil their function. Technology is often behind these changes, triggering new morphologies and social functions for borders. As Dijstelbloem et al. (2011) recently argued, technology cannot be understood as a neutral fact and more research on the specific political consequences of the technology regime within the borders is needed. This section explores the relationships that drive the turn towards technological solutions at the border.

Borders are not only physical and visible boundaries but also 'virtual' (Lyon, 2007: 132), supported by a complex architecture of databases, which rely on collecting a large amount of information on individuals and permit real-time data exchanges. With the implementation of technology to monitor and control citizens' mobility, borders are taking the form of 'virtual and portable databases' (Lyon, 2005) that implement 'remote controls' (Guiraudon, 2003) and facilitate 'policing at distance' (Dijstelbloem et al., 2011). Waters also points out how 'the border

[6] EDPS (2013) Smart borders: key proposal is costly, unproven and intrusive, 19 July 2013, Press Release 2013/08.

[7] 'Smart Borders' http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

transforms into a mobile, non-contiguous zone materializing at the very surface of the truck and every place it stops' (2006: 95). In other words, there is a delocalization of the border's functions away from the physical border-crossing point itself. Hence, borders are becoming an extended process that penetrates into the private lives of the individuals who are moving across countries.

Therefore, the implementation of digital technology at the border does not bring about a mere morphological change, but there is a transformation of the meaning of borders themselves and the role and rights of the different social actors involved in the process. In other words, the increasingly technological nature of borders in Europe − aimed at monitoring and controlling mobility in general − is affecting travellers' rights and the nature of citizenship at the border. As has clearly been outlined, borders exist beyond their geopolitical locations, taking their shape from activities carried out both beyond and within the border. Just as a network of actors constructs the experience of crossing the border, its formation is also determined through a network of actors that make it meaningful.

More than ever, borders are convergence points for a range of actors and stakeholders, each of whom contribute to how the border is constructed and experienced. These different ways to experience the border for the different actors that construct it is illustrated in the empirical findings (see Section III). The rise of public-private partnerships, in particular, has moved the border away from the traditional purview of the state. Understanding the border through a lens of performance brings into relief the extensive work involved in producing and maintaining the border, and doing so can also help reveal the power structures which underpin interactions along the border. This is clearly expressed by the ways in which borders are seen as 'technical landscapes of control and surveillance' (Passi, 2011:62) that are intrinsically related to the politics of life, along with 'the politics of representation and identity' (*Ibid*, 2011: 62).

While the relationship between the public, civil society, end-users, policy makers, technology designers and industry is mutually constituted, it is also heterogeneous and involves complex negotiations as each stakeholder has their own agenda to pursue and bring to completion. While technology is a key factor in the performance and formation of borders, a whole network is required to ensure its constant reproduction and continuation. One particular relationship is instrumental in driving and shaping the use of technologies on the border – the relationship between industry and government. This relationship, which traditionally has been described as a military-industrial complex, is becoming increasingly complex over time. Ben Hayes has offered a new concept, the 'NeoConOpticon', as a means of understanding the relationship between industry and government in relation to the field of security. Hayes (2009) describes NeoCon ideology as being 'centered upon the right to limitless profit-making, which is at the very heart of the EU's desire to create a lucrative Homeland Security industry.' While European Union border control is not technically an apparatus of the military, the collapsing distinction between roles of responsibility for external and internal security, between the military and law enforcement agencies, has reoriented the military-industrial complex towards civil security.

Thus, discourses such as terrorism, migration and efficiency, framed in a language of morality, values and ideals provide powerful means of securing public support for state endorsements of border technologies. In turn, the success of industry depends upon a marketplace which can buy the products it produces, and thus it too has a vested interest in framing the border as a problem which requires a solution only they can provide. Between these two actors, borders have been presented as vulnerable, overwhelmed and under resourced. But states are without the means to

provide more manpower, and even if they could, human error is often perceived as being too risky and unreliable a variable to be entrusted with the responsibility of securing borders. But can technology and algorithms provide more objective, transparent and less biased discrimination methods?

Together with this rich context of stakeholders, it is important to bear in mind how responsibility and cost are distributed among actors. Which populations pay the greatest price for increased security and efficiency? Not only in economic terms, but also in terms of data (increased surveillance and data collection in exchange for quicker passage through border crossing points, for instance). While the trade-off between benefits as an incentive to voluntarily submit personal data is generally considered an unethical proposition, this may not be the position of the public. Depending on the position of power from which one engages with these arrangements, and past experiences with surveillance and border technologies, not all people see increased access to their information as a threat to their privacy. That being said, there is a well-established history involving techniques of population management and control being disproportionately directed at 'risky' populations, such as migrants, offenders, and those of lower socio-economic means.

Thus, the question of who pays, how they pay and what they are willing to pay brings to light the complex social interactions which take place during bordering practices. It forces a consideration of how these costs can be assessed in terms of legitimacy, proportionality, and necessity. Important questions will have to be asked: Who will have oversight of these technologies once they are implemented? How will their efficiency and necessity be measured (security practices being notoriously difficult to assess)? How will cases of abuse and misuse be handled? Will alternatives to technological bordering practices be offered, and will there be any associated cost with refusing to use them? Each of these questions is important for understanding how new and emerging technologies will impact upon the lives of people, whether intentionally or otherwise.

Critical Border Studies emphasizes the social and constructed nature of borders, arguing that the ways in which we imagine, speak about and describe borders, that is, our perceptions of borders, are intrinsically related to how borders are constructed. Thus, the architecture of borders is both malleable and plastic, drawing from a range of discourses, practices, materials, policies, and bodies, which give shape and form to this architecture. The ways in which these different factors come together to form the border have been increasingly understood in terms of performance – a performance where data and technologies play an increasing role.

This idea of performance is key to understanding the constructed nature of borders as it takes into account the societal values and norms (*e.g.* ethics, privacy, and power) that feed into how the border and border technologies are experienced and encountered. A performative approach helps to illustrate that ‘the border is not something that straightforwardly presents itself in an unmediated way. It is never simply ‘present’, nor fully established, nor obviously accessible. Rather, it is manifold and in a constant state of becoming’ (Parker and Vaughan-Williams, 2012: 728). In this blurring of the contours of borders, data management plays a crucial role as citizens are met with a ‘black box’ of data flows where inputs and outputs are known but the internal workings remain a mystery.

The shift towards thinking in terms of performance also helps to make sense of how the border moves beyond its geopolitical location, and is redistributed across time and space, through acts of issuing visas, performing pre-departure clearances and creating interoperable technologies.

This expansion of the border away from its physical location underscores the importance of understanding the broader social, ethical and legal context within which borders and border technologies are situated. Examining the problematizing of the border through a lens of performance brings to light the types of work involved in forming the border through the often invisible data flows that determine how travellers (citizens) are positioned vis-á-vis the state. The following sections provide an exploration of the particular discourses that frame how the border is thought about, with an emphasis on terrorism, migration, efficiency and classification (sorting), and their relation to circulation, anxiety and uncertainty.

2.1. Terrorism

Following the attacks of 9/11, along with the London and Madrid bombings, counterterrorism has become a top priority for border control. A key discourse that has emerged around terrorism is its insidious nature; *(t)errorism is a threat that does not recognize borders and may affect states and peoples irrespective of their geographical location. EU States and citizens are not an exception. Individuals and groups who believe that they can advance their political aims by using terror pose a serious threat to the democratic values of our societies and to the rights and freedoms of our citizens, especially by indiscriminately targeting innocent people* (Directorates-General, Home Affairs, 'Crisis and Terrorism'). Transnational terrorism's disregard for borders has framed them as sites of vulnerability, open to infiltration and attack. Borders have thus become problematic, and immediate actions must be taken to rectify this. This call to fortify and secure state borders is explicitly couched in the language of 'democratic values' and 'rights and freedoms', drawing on a moral imperative to protect 'innocent people'. This association between borders and terrorism has given new life to an old tension, between inside and outside, self and other, where that which lies within the border is classified as safe and knowable (thanks to data), whereas outside the border is dangerous and Other.

And yet, this discourse of terrorism rests on fundamental paradoxes. On the one hand the European Union is founded on principles of movement and increased cross-border cooperation. But, on the other hand, recent years have seen a hardening of Europe's external borders, creating what has been called 'Fortress Europe', and reaffirming the distinction between inside and outside. Furthermore, the balance between producing security and over-securing operates on a slippery slope, which Giorgio Agamben has highlighted in his work on 'states of exception' – the permanent justification for 'a suspension of the juridical order' (Agamben, 2008: 4) in the name of security. Goldstein (2010) goes even further, discussing how a focus on security is not a result of a particular attack that 'changes everything', but is an inextricable part of neoliberalist societies as a security paradigm that frames and organizes contemporary social life.

In his work on data collection, Bruce Schneier highlights the limitations underlying this focus on security, arguing that any strategy which stresses certain threats while minimizing others is doomed to failure. Indeed, the increasing need for securing borders in the face of terrorism entails its own threats to social liberties. 'Ignoring the risk of overaggressive police or government tyranny in an effort to protect ourselves from terrorism makes as little sense as ignoring the risk of terrorism in an effort to protect ourselves from police overreach' (Schneier 2015:11). While the public demands a coherent and effective approach to terrorist threats on the part of the authorities, the

complexity of the problem highlights the limits of data mining and data surveillance as a deterrent for terrorist activities[8]. According to Schneier, these limits can be summed up in three points: firstly, all detection systems have inherent error rates, which might be easily solvable when dealing with minor crimes − e.g. fraudulent credit card usage − but which require a much higher degree of accuracy when tackling terrorism. Designers can 'tune' the detection system in order to minimize false positives or negatives. Since terrorist attacks have such a low frequency but a high impact on society, the system might be tuned to minimize false negatives in order to avoid attacks, but will then be left with an overwhelming number of false positives which could only be handled with great difficulty. Secondly, the very nature of terrorist attacks makes it difficult to establish a pattern which can be useful to identify potential threats. All initiatives that have sought to secure the borders against terrorists have been put forward in the wake of an attack, and each one of them has demonstrated a different modus operandi. Thirdly, individuals engaged in terrorist activities are very wary when providing personal data and are constantly trying to avoid detection.

There is, therefore, a wealth of analysis that questions the use of mass surveillance practices (including big data and algorithmic decision-making) as a solution or response to the terrorist threat. However, it is consistently after terror attacks that a data-based security agenda is pushed in the policy agenda.

2.2. Migration

While the conflation between terrorism and migration has been well documented,[9] this section focuses on how migration, as a general phenomenon, contributes to the production of the image of a problematized border and underpins the need to secure it through data. European borders are increasingly described as being overwhelmed by floods of migrants, refugees and asylum seekers. FRONTEX, the European Union agency that promotes, coordinates and develops European border management in the external Borders of the Member States of the European Union, regularly warns of 'sharp' increases in illegal border-crossing along the EU's external borders (FRONTEX, 2014: 7). This has led countries like Switzerland to place quotas on the number of refugees and economic migrants they will accept. Within these discourses the body of the migrant is presented as something that needs to be regulated and controlled. This regulation has been built around a discourse of needing to know, through processes of identification, authentication and classification made possible by biometrics technologies, large-scale databases and surveillance technologies.

It seems to be taken for granted that migration and security policy are linked (Van der Ploeg and Sprenkels, 2011: 69) and that they are both increasingly leaning on border technologies.

[8] The 9/11 Commission Report described a failure to uncover the plot despite the intelligence community having obtained all the information about it without mass surveillance, and that the failures were the result of inadequate analysis. In another example, mass surveillance didn't catch underwear bomber Umar Farouk Abdulmutallab in 2006, even though his father had repeatedly warned the US government that he was dangerous. And the liquid bombers (they're the reason governments prohibit passengers from bringing large bottles of liquids, creams, and gels on airplanes in their carry-on luggage) were captured in 2006 in their London apartment not due to mass surveillance but through traditional investigative police work.

[9] See for instance the work of Amoore (2009), Graham (2010) and Ackelson (2005).

Technology is not only used at border points to substitute for manual identification of documents, persons and objects. Several authors have pointed out how migration policy is increasingly leaning on technologies and global databases rather than on laws and migration policies. This process has been labelled the 'technologization' of migration policy (Ploed and Sprenkels, 2011: 69) or the 'migration machine' (Dijstelbloem et al., 2011: 9) − concepts depicting the many ways that technological systems are used to register illegal residents and check people crossing borders.

As Huub Dijstelbloem, Albert Meijer and Michiel Besters (2011) have argued, migration policy has become more and more entangled in issues relating to integration and security. In other words, migration and integration policies have both been 'securitized' (Lindahl 2008). As a result, three discussions have become increasingly interrelated in what has been labelled the 'migration machine'. The first relates to migration policy and is mainly concerned with the issues mentioned above, namely, the influx of migrants and the separation of 'desirable' and 'undesirable' aliens. The second discussion is about integration policy and is dominated in the media and politics by questions and problems related to social cohesion and civic integration among newcomers (varying from the obligation to assimilate culturally to the right to participate economically). The third discussion is about security policy, especially on border control in the countries of Europe and the outer limits of the Schengen area, and the screening and refusal of people who are suspected of being a threat to society.

Akin to the discourse of terrorism, there is a paradox in how the discourse of migration is framed within the EU. On the one hand, the removal of internal border checks created the free movement of persons as a fundamental right. Thus, the EU is based upon values and ideals of co-operation and harmony between member states. The mobile body, here, is seen as an important economic resource and source of labour, integrated into European ways of life. On the other hand, migration has been framed as something that is moving beyond the control of states and borders. Illegal migration, in particular, is perceived as being done outside the visibility and regulation of the state. While these mobile bodies may conform to the values and ideals of the EU in every other sense, they are not considered to be *of* the EU. Thus, they represent potentially dangerous and unknown variables, in an already uncertain future. Within this framework regarding the right of mobility and the informatization of EU borders, researchers have criticized how, while the EU has removed its internal borders, it has at the same time fortified its outer boundaries by means of technology (Dijstelbloem et al., 2011), and have pointed out how the implementation of technology in an effort to control the migration flows to the EU makes the contemporary external EU borders resemble the gates of a 'cyber-fortress' (Marin, 2011: 132).

2.3. Efficiency

The questions, 'Who are you?' 'How can you be identified?' and, 'What is your purpose?' bring to the fore the third discourse which has been key in shaping how the border is reformed − efficiency. The importance of identification at the border, along with the increased volume of travellers at border crossing points, has highlighted the challenge of efficiently regulating circulation flows. The desire for efficiency coupled with a climate of economic austerity has driven the turn towards technological solutions, which are presented as cost-efficient solutions to an urgent problem.

While a discourse of efficiency drives technological solutions to regulate circulations across the border on one hand, it also contributes to the mobility of the border itself. An increase in border traffic, along with the growing discourse of an inability to deal with this traffic has produced the border as an object of mobility, through the relocation of traditional border work away from the geopolitical border to foreign visa consulates and processing centres. This movement of the border away from its physical location has often been justified through a discourse of efficiency, as the issuing of visas and background checks appear as time consuming activities which produce delays and long waiting times at border crossing points.

Thus, the border has become untethered, mobile and virtual, only momentarily stabilized and frozen through the accessing of large-scale interoperable border technologies and data, resulting in a process of 'spatial stretching', whereby, the border is 'exported' via 'touchpoints' and 'encounters' between mobile people, objects and data in a system 'designed to operate far beyond state boundaries' (Amoore, 2010 as quoted, 2011: 63). The mobile and virtual nature of the border is closely related to developments in information and communication technologies (ICT) that allow for the capture and circulation of data across large geographic regions in real, or near to real, time, travelling through multiple database networks, shrinking time and space.

3. Solving problems with data: The technological fix

To assess the impact of technology, it is important first to understand the widespread desire for, and trust in, technological solutions. This turn towards technology arises out of the complex interaction of a range of discourses and styles of thinking. For Lesley Regan Shade (2003) and David Lyon (2003) the growing appetite and demand for technological solutions can only be understood in the context of 'technological determinism' or 'technological fixes' that 'approach technology from an uncritical perspective, associating any advance in this field to human progress, and showing a seemingly blind faith in the possibility of technological devices to solve complex social problems and provide certainty and a sense of security' (RESPECT, 2011: 4). This uncritical acceptance of technology is problematic as it fails to take into account the potential societal costs and dangers that may be associated with 'blind faith' in technological solutions. And so it becomes a question of how and why technology has been accepted as the solution.

Contemporary society has become increasingly organized in terms of areas of expertise and specialization, oftentimes placing the knowledge of how society operates out of the reach of the general public and into the hands of experts. This is particularly so in the case of technology, and has resulted in the growth of 'black boxing' - 'the way scientific and technical work is made invisible by its own success. When a machine runs efficiently, when a matter of fact is settled, one need focus only on its inputs and outputs and not on its internal complexity. Thus, paradoxically, the more science and technology succeed, the more opaque and obscure they become' (Latour 1987) so that, today '(t)echnological artefacts are commonly black boxed, in that 'ordinary users' know very little, if anything, about how they really work' (Bell, 2005: 44). In this sense, technology falls within a discourse of expertise that eludes accountability. This discourse of technological expertise draws support from a broader societal value attached to scientific facts as being true. The assumed truth of scientific knowledge has provided it with a privileged position within society, allowing it to be presented and accepted as legitimate and correct, as users are often

without the technical know-how to understand and question how this knowledge is produced. A secondary element of black boxing is that it is 'also about inevitability – it is about saying that phones or iPods or fridges look and work as they do because they offer the only solution to a set of problems.' Thus black boxes are often examined as 'a process which closes down alternatives' (Bell, 2005: 44).

While the ways in which technology are talked about plays an important part in understanding how it impacts upon the formation of the border, the ways in which it is seen to act must also be considered. A growing trend within the EU and abroad is the demand for interoperability and standardization amongst large-scale technology initiatives. The Commission Communication of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (COM (2005) 597) is focused on just this. This communication is specifically designed to improve technical interoperability and synergy between the existing IT systems (SIS II, VIS, EURODAC) in the field of justice and home affairs; to show how these systems could support policies on free movement and combating terrorism and crime, while respecting the need to protect fundamental rights; and to trigger in-depth debate on the shape and architecture of the IT systems. It is interesting to note that while the summary provides a detailed description of the first two matters, there is no mention made of debating the necessity of these databases, illustrating that the black box phenomenon of 'closing down alternative' solutions is not simply restricted to the physical technological artefact but the entire life cycle of the technology. This drive for standardization and interoperability across databases and border technologies promotes the production of technologies that have the same look and feel to them no matter where you are crossing the border. This desire for standardization and homogeneity can be understood in light of the fact that border technologies are designed to reduce uncertain and unknown circulations at the border, through the production of social categories, risk profiles and ever expanding databases of information and knowledge. These technological tools function as a means of stabilizing the shifting and fluid nature of the border, and can be understood as attempts at mapping out an emerging social geography of mobility as the geopolitical nature of the border becomes increasingly murky and hard to pin down.

While technological solutions continue to grow as a key part of bordering practices, and the management of insecurities, they have not been entirely without criticism. The construction of multiple large-scale databases, such as SIS I & II, VIS, the planned Smart Border package composed of an Entry and Exit System (EES) and Registered Traveller Programme (RTP), along with the development of Passenger Name Records (PNR), in combination with the widespread use of biometric identification technologies, increased interoperability between databases and the push towards access for law enforcement agencies have given rise to a number of concerns over the potential misuse of these technologies and the abuse of civil liberties. Several reports have questioned the legitimacy, necessity and proportionality of these large-scale databases.[10] These critiques can serve as important resources for highlighting and understanding the potential risks and challenges of the use of data at the border. They are also a reminder that technology is not passive, but something that actively participates in how contemporary borders are formed. Rocco Bellanova and Gloria González Fuster (2013) have explored how 'heterogeneous elements – both material and immaterial, visible as well as invisible – *actively* contribute to the making of security

[10] See for instance, Hayes and Vermeulen, 2012; Jeandesboz et al. (2013), and Opinion 05/2013 on Smart Borders (Article 29 Data Protection Working Party).

practice and, potentially, to the opening of political landscapes' (Bellanova and González, 2013: 188, emphasis added). To understand technology in terms of performance is to provide a means to understand how it actively shapes the way in which the border is experienced and encountered.

The idea of technology as an actor works against the commonly held notion that technology is neutral and operates outside of human biases and prejudices. If technology is to be understood in terms of the social, ethical, legal and political values which shape its development, deployment and operation, then its air of neutrality must be forgotten, so that it becomes possible to see and understand the ways in which technology is active and holds the potential to produce societal costs.

3.1. Social sorting at the border

To understand the border in terms of circulation is to understand the border as a type of filter, where the idea of circulation as a problem has coalesced around discourses of risk, uncertainty and insecurity. These discourses function to reaffirm divisions between inside and outside, self and other, and the need to establish mechanisms to determine who has and who does not have access. In response to these risks and uncertainties, a variety of tools, technologies and techniques have been produced to stabilize the border. One of the main ways in which control of risk at the border is performed is through the production of risk.

'Social sorting' (Lyon 2003) is a concept that attempts to describe the application of surveillance technology to categorize individuals based on observable, distinguishable features and allow discrimination to take place. This discrimination can be legitimate or illegitimate, or socially desirable, depending on the context, but is clearly 'highly consequential for life chances and choices' (Lyon, 2007: 204). Border checks and the categorization of individuals based on a set of (observable and non-observable) characteristics has profound implications for both travellers and the systems that enact how discrimination takes place.

Today, social sorting is overwhelmingly carried out through the use of data, relying on technologies of identification and authentication to extract and compare personal information and biometric data. In this sense, technology operates as a site of connection between the performance of borders and the performance of security, through the establishment of identity. The anxiety of circulation, and the vulnerability of borders fall within, and complement, a larger discourse of securitization. Louise Amoore has described how the interaction of 'contemporary security assemblages operative in bordering relies upon technologies of identification to stabilize the forces of circulation and the demands of security' (as quoted in Bourne, 2014: 13). And Bourne has argued that technology is increasingly important to identify 'where and how the border is inscribed and distributed' (2014: 5). As we will see below, data is also key in terms of establishing identities and levels of privilege or trustworthiness.

3.2. Bodies and biometrics

When one thinks of data at the border, what first comes to mind are names, addresses and dates of birth. Border data, however, is becoming increasingly complex. IDs and Passports often hold chips

that store not only demographic data but also data related to human characteristics – facial image or fingerprint, usually − known as biometrics. Hence, automated identity checks at borders not only depend on the possibility to have machine-readable documents, but peoples' bodies (fingerprints, facial image, iris, etc.) are increasingly located at the centre of the identification process. Consequently, automated identity checks are transforming the human body into a 'machine readable' identifier (Van der Ploeg and Sprenkels, 2011: 91).

Biometrics has become an integral aspect of the performance and production of border practices, functioning as individual templates against which identification and authentication can be carried out both before and during travel. The body is increasingly treated as information and included in transnational database and digital files. As Van der Ploeg (1999) argued in relation to the implementation of Eurodac, the possibility of using a persons' body itself as a resource of information on his or her identity, independently of the story that the person might recount, is extremely attractive for governments. However, the use of bodies as ID documents is not exempt from controversies. In the case of Eurodac, fingerprints may become 'the mark of illegality written on the body' of asylum seekers or irregular migrants (Van der Ploeg, 1999: 301). Evidence of asylum seekers', refugees' or irregular migrants' self-mutilation of fingers in order to avoid being enrolled in different systems or being recognized as prior Eurodac applicants[11] illustrates the disturbing role of biometrics and the 'informatization' of the body in contemporary migration policy.

Beyond the ethical considerations to be taken into account when assessing a system that uses the body as a document of identification and information, the reduction of identity to unique biological data stored on the body has been heavily criticized for other reasons as well. These critiques follow three lines of development. The first relates to discrimination. Joseph Pugliese (2007) has carried out research demonstrating the 'racialized features of representation' which shaped the design of biometric facial recognition technologies. His research focuses on the failure of biometric technologies to capture a subject's image, 'precisely because of the subject's race, precisely because the subject fails to conform to predetermined white standards that set the operating limits of particular biometric technologies' (Pugliese, 2007: 106). His research demonstrates the social nature of technology, illustrating how the politics of representation and power shapes what is considered to be a 'standard', and anything that falls outside of this is beyond the norm.

[11] For evidence of self-mutilation of migrants reported in newspapers: http://www.praguepost.com/czech-news/49773-chovanec-refugees-prevent-deportation-by-self-harm, http://gulfnews.com/news/migrants-mutilate-fingers-hoping-to-conceal-identity-1.502285

Figure 1 Physical security of a typical eID. Source: Eleconomista.es

The second refers to the fragmentation of a holistic sense of self to the body. Through the creation of an indissoluble connection between the body and processes of authentication and identification, individuals lose control over their bodies, and are no longer in charge of how the state sees them. Often these authentication and identification processes rely on a 'data double' -the result of disassembling and reassembling many bits of data related to a single body. The result is a decorporealized body, a 'data double', of pure virtuality' (Haggerty & Ericson, 2000: 611). It is this 'data double' that travels before the traveller, determining its ability to cross the border or not.

Finally, the third critique relates to the circulation and mobility of biometric data. In the case of biometric identification systems, an image of one part of the body or one body characteristic is captured by a technological gaze; this image is then sent to the computer of the controller who is located away from both the subject and the technology. Already at this stage, the subject has lost control, ownership, and awareness of where their bodily representation has gone, and the image has the potential to become globally mobile. The mobility of biometric information across a range of databases touches on the subject of privacy. The collection and storage of biometric data falls

under data protection legislation, which regulates how much biometric data can be collected and for how long it can be legally retained before deletion. And yet, the impact of collecting biometric data goes beyond the scope of data protection laws and shapes how the border is managed, experienced and encountered.

4. 'Us' versus 'Them'

The relationship between mobile bodies and borders is particularly interesting in the context of the Schengen area, as signatories have entrusted the responsibility of border control to perimeter, or frontier, countries. Thus, it is possible to argue that the growing sense of trust between Schengen countries is accompanied by a growing mistrust of those coming from outside the borders − non-citizens. In other words, whereas the EU has removed its internal borders, it has also fortified its outer boundaries by means of technology (Dijstelbloem et al., 2011).

Technological and data-intensive identification solutions 'have become increasingly central to citizenship' (Lyon 2007: 122) and often rely on biometrics, which are viewed as an 'increasingly reliable means of identifying and verifying individuals' (Lyon, 2007: 124). European directives and regulation governing border management are explicit in identifying biometrics as a reliable way to identify individuals. As noted in EC No 2725/2000, 'Fingerprints constitute an important element in establishing the exact identity of […] persons.'

Rose (1999) has described this growing trend towards using (technological) identification techniques and processes to correctly identify individuals as the 'securitization of identity' (as quoted in Lyon, 2007: 125). The ability to have your identity legitimately classified and confirmed through technological processes has become a key premise in the regulation of mobility (Lyon, 2007). Although freedom of movement is a universal right (Article 13, UN Universal Declaration of Human Rights) it is one that is balanced against other (state) interests, such as 'national security, public order, public health or morality' (Turack, 1972, as quoted in Salter, 2004: 72).

When establishing identities through data and biometrics, different traveller groups emerge − EU and Schengen country citizens, third country nationals (and potential over-stayers), illegal immigrants, asylum seekers and offenders − each having different levels of interaction with the European border management system. The governance of cross-border movements sits within a complex setting of technology and political linkages, which work together towards a purpose of efficiently assessing (the perceived) risk of individuals at border crossings.

The passport, or identity card, which embodies the physical (biometric) data characteristics of the individual, defines the individuals' relationship with the state. 'The passport is the primary document by which mobile individuals are identified, tracked and regulated' (Salter, 2004: 72). Thus, passports should not be seen as static entities: their role is enmeshed in a complex architecture of border management policies, and they contribute to making 'certain things and politics possible, and plays an active role in the global mobility assemblage' (Salter, 2002: 1). The ability to identify an individual using a passport has important implications for the power relationships between the Schengen area and the categories of travellers identified above.

4.1. EU & Schengen country citizens

The relationship between states and individuals has increasingly been understood in terms of the body, and this remains true for citizens. The body functions as a means of distinguishing between citizens and non-citizens through a social sorting of biometric identities. One of the principal ways in which the relationship between states and citizens has been understood is through a discourse of rights and responsibilities.

Traditionally, this discourse has focused on the rights of citizens and the responsibilities of states. Marshall (1965) has distinguished the rights of citizens across three categories; civil rights, political rights, and social rights. The category of civil rights corresponds to the fundamental rights that have been set out in various legal charters, such as the European Charter of Fundamental Rights (2000/C 364/01). Political rights refer to the right to participate in political life through a system of voting and democratic election. And, finally social rights are based on access to a certain quality of life, through education, healthcare, welfare, *etc.* (Kymlicka, 2002: 287).

These categories of rights, civil, political, and social, provide a legitimate language through which citizens can make demands on the state, and ensure that they are fulfilling their responsibilities of public service. A discourse of rights also provides a means to distinguish between public and private spheres of life, and delimits the extent to which states can intervene in the life of citizens. Just as citizens hold rights, they also have responsibilities, and civic duties they must fulfil. This discourse of responsibility centres on the production of the 'good citizen' and is founded on the basis of the citizen as an autonomous rational actor who productively contributes to society.

One of the rights enjoyed by citizens of the Schengen countries is the right to free movement. The capacity to enforce this right, and to segment Schengen country citizens at internal border crossings depends on the Schengen country citizen producing a valid form of identification document. According to the Schengen Border Code, Schengen country citizens enjoying the right to freedom of movement can only be subject to a 'minimum' check at internal crossing points in Schengen − a 'straightforward verification of the validity of the document authorizing the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.' This is supported by a clause that permits border guards to 'consult [on a non-systematic basis] national and European databases in order to ensure such persons do not represent a genuine, present and sufficiently serious threat to the internal security, public policy, international relations of the Member States or a threat to the public health.'[12]

The limitations on the nature of identity verification are crucial in the context of border crossing, and are the clearest instance of how border technologies and data management mechanisms need to embody the legal guarantees that they are supposed to translate into specific sorting procedures. In the case of citizens, border checks should not lay suspicion onto the subject and guarantee its right to enter its space of sovereignty. In technological terms, this means that the procedures put in place to verify the identity of citizens and those formulated for everyone else will need to be fundamentally different.

[12] Schengen Borders Code (SBC) COM (562/2006)

4.2. Third country nationals

Third country nationals in standard border management systems are in a more complex position, in which the state does not have a common policy towards them. Instead, it applies a series of bilateral and multi-lateral visa relationships with countries that set out the entry requirements for the border crossing of travellers. Once a visa has been granted, discrimination at a border crossing point is not applicable unless there is a genuine, present and serious threat.

If a third country national overstays their visa, however, their status changes. While these subjects may have entered a country or area legitimately, once they overstay their visas they become illegal residents and, as such, their personal details can and will be cross-checked against SIS II (COM, 2001), VIS (EC No 767/2008) and EURODAC (EC No 2725/2000) when trying to travel to third countries. The level of protection of their data is thus reduced due to the need to confirm the validity of a visa by checking the data against a database.

4.3. Asylum seekers

Asylum seekers' relationship with Schengen countries begins with a procedural collection of fingerprints and the input of this biometric data is entered into the European Dactyloscopy (EURODAC). EURODAC is a large database of fingerprints of applicants for asylum and irregular border crossers. Since the EURODAC system became operational in 2003, it has captured 2.3 million individuals' identities on asylum applications and irregular movements (Jones, 2014: 1). The database helps the effective application of the Dublin convention on handling claims for asylum, ensuring that the 'principle of first contact' is implemented. Under Dublin (II) Regulation (EC 343/2003), asylum seekers must remain in the (EU) country they land in, and travelling between Schengen countries during the processing of an asylum claim is not permitted. The restrictions of movement in Schengen – and in some countries the right to find work − on asylum seekers as claims are processed, and the greater interaction of their data with European databases represents a level of discrimination that other categories of travellers do not face.

4.4. Irregular immigrants

Borders have become 'privileged places of regulation' (Pellerin, 2005) where the state looks to assert its commitment to a fluid border doxa by combining the requirement for border efficiency with preventing the 'passage of illegitimate entrants' (Lyon 2007: 121). With the increased facility and affordability of travel, population flows increase and borders become 'tightly policed and controlled' (Lyon, 2007: 121), constructing what Klein has called 'fortress continents'.[13].

[13] Klein, Naomi (2003) 'Fortress continents', *Guardian, 16 Jan. p. 23.* First published in the *Nation.* http://www.theguardian.com/world/2003/jan/16/usa.comment

This can be observed in the data practices that follow the apprehension of (suspected) irregular immigrants at border crossing points. Their data is immediately checked against EURODAC to see whether they have applied for a visa or asylum elsewhere. In effect, a comprehensive background check occurs to provide a justification for exclusion from the territory.

4.5. Offenders

Offenders' freedom of movement between Schengen countries is also influenced by data practices, as the Schengen Information System (SIS II) allows for real-time exchange of criminal data about individuals. The first iteration (SIS I) contained information on individuals engaged in serious criminal offences or those that did not have the right to enter or stay in the EU. Under SIS II, an offender who has evaded an arrest warrant in any EU country can be apprehended at internal Schengen border crossings as data is exchanged between police, customs, visa and judicial authorities. SIS II has increased functionalities such as the possibility of using biometrics, new types of alerts, the possibility of linking different alerts (such as an alert on a person and a vehicle) and a facility for direct queries to the system.

5. Fundamental rights

In this section, a set of rights and values that can be affected by the management of data at border points is explored, with the aim of providing a broad picture of externalities to take into account and highlighting both their positive and negative effects (costs and benefits). While the externalities to be considered will depend on the specific characteristics of the project to be developed, the technologies to be deployed and the context in which the action takes place, this section shows how data is not just a resource or identification mechanism, but part of an ecosystem of rights that is enacted at the border, with profound implications for fundamental rights and values. At the end of the day, using data at borders is a form of surveillance. As such, it carries the risks and precautions that come with the generalization and normalization of control and digital tracking of citizens, which extend beyond narrow definitions of privacy and data protection to embrace much broader principles linked to fundamental rights and values.

5.1. Privacy

Without a degree of privacy, individuals cannot easily maintain an individually and socially important distinction between their personal and public lives, or exercise other important social and political rights. However, privacy is a difficult term to define because it means different things to different people in different contexts at different times. There are also many different and overlapping ways in which privacy can be understood and justified, and its erosion criticized.

Some authors have begun to put forward complex understandings of the effect different technologies have on different types of privacy. Finn, Wright and Friedewald (2013), for instance,

look at the seven types of privacy and discuss them in relation to different technologies (whole-body image scanning, RFID-enabled travel documents, unmanned aircraft systems, second-generation DNA sequencing technologies, human enhancement and second-generation biometrics). They conclude that border technologies such as body scanners, for instance, affect the privacy of data and image, and derivatively, of behaviour. RFID-enabled travel documents also affect privacy of behaviour and action, of data, and of location and space. Unmanned aircraft systems also affect these privacy types, as well as association. The privacy of the person is additionally implicated by DNA sequencing technologies. Human enhancement through, for example, neuro-enhancing pharmaceuticals and electroencephalography potentially impact upon all of these plus the privacy of thoughts and feelings. The privacy of communication, in addition to the other types, comes into question through the use of biometrics such as voice and speech recognition technologies (Finn et. al, 2014). While not all of these technologies are routinely deployed at BCPs nor directly experienced by travellers, the sophistication of some of the technological proposals for the future of borders requires that a degree of technological forecasting is taken into account when describing the impact on privacy of big data processes at the border. Evaluating how a system impacts on privacy will thus require an understanding of the privacy types compromised in each case, and a valorization of such impact both now and in the future.

5.2. Autonomy

Privacy 'affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation' (Gutwirth, 2012: 30) There are numerous texts that indicate that privacy is intertwined with other values. After all, an autonomous life is one without external control or influence.

When looking at the impact of border technologies, one of the key aspects to take into account is ensuring data subjects are clearly informed about their rights to refuse participation, about their right to redress and recourse in the case of incorrect information, and about the purpose and scope of the technology so that they may practice informed consent. These issues have an impact not only on expectations, but also on one's ability to make rational decisions that require that all relevant variables are taken into account. Autonomy is also closely related to freedom – one is free when autonomous to decide what kind of life one wants to lead. As we will see in Section III, when the attitudes of passengers towards biometric data and automated systems are described, the autonomy of the citizens is called into question due to the travellers' lack of information and knowledge of the actual significance of crossing an automated border.

Physical autonomy is another aspect of this analysis. Complex technological systems such as full-body scanners or ABC gates, which require that people rid themselves of extra clothes, shoes or other accessories, present significant difficulties for people with disabilities or mobility issues. Those showing physical traits that tend to attract the attention of the surrounding public or technology systems' controllers, such as wheelchair users or people with detectable implants, might also be discouraged from doing certain activities because of the perceived invasive nature of these technologies.

5.3. Dignity

Dignity is closely related to privacy and autonomy. Several authors have highlighted this relationship (Post, 2000-2001; and Whitmore, 2004), and the examples of body scanners and biometric ABCs demonstrate how technology has the potential to cause embarrassment and harm an individual's sense of dignity when its societal impact has not been sufficiently considered. The literature covers this aspect in relation to border technologies, but also welfare applicants, asylum seekers, prisoners, etc. While ABC gates are currently limited to Schengen countries, and can only carry out the minimum check as guaranteed under the fundamental right of freedom of movement, its expansion to third country nationals and the potential for interoperability with other databases such as EES, RTP, EURODAC and SIS I & II makes large amounts of personal data available to border controllers across Europe and beyond. Where alerts in SIS and EURODAC have been entered incorrectly, not updated or deleted, this has the potential to cause embarrassment and discomfort.

Other texts mention also the case of DNA and biometric technologies, which 'may reveal embarrassing information about a person's physical being that she would regard as discrediting, making it difficult to maintain or re-establish her dignity. This information may be sensitive, indicating something about sex, ethnicity, mental and physical health, and other features that the individual would otherwise seek to manage or conceal, partly for reasons of self-image and self-respect, but also because there may be further functional and social consequences of such revelation' (Finn et al., 2014: 264).

The impact of a specific surveillance system on dignity is greater with covert systems where there is no knowledge or consent and if no mechanisms to minimize or neutralize this negative externality have been built into the system or its management.

5.4. Freedom of assembly, association and expression

Freedom of assembly, association and expression are fundamental rights recognized by the EU Charter of Fundamental Rights and the European Convention of Human Rights, designed to protect certain spheres from government interference. In such spaces, interference from the state is not allowed if it infringes on the people's right to establish connections, organize or develop and express ideas. Moreover, the state has the responsibility to ensure that this is the case, and that such spaces exist and such rights are exercised.

These rights rest on the assumption that there is a separation between the state and the public sphere, and that in the public sphere citizens can engage in activities and discussions away from the power of the state. The movement from manual to automated stamping of passports produces a virtual trail of where individuals have travelled. In the case of individuals fleeing from violence and oppression, this poses a significant risk if the data is not securely stored. If information on a person or group's activities and connections is collected and can be used against them, the knowledge of this possibility immediately ups the stakes for social or political organizing and the expression of dissent. This can act as a powerful disincentive for such political participation and civic engagement, but also erodes public trust in institutions.

5.5. Freedom of movement

One of the areas where the effects of September 11, 2001 have been more deeply felt is in the sphere of movement. Terrorists are not only usually seen as foreign elements that need to enter a country (thus the emphasis on airport security) but also have to 'move' to the place they want to attack. Free movement has therefore gone from being seen as a positive element linked, for instance, to regional integration, to being perceived as a potential risk and a threat. Because of this, areas of movement are conceptualized as problems that require intervention and regulation by state and private actors. The idea that guides this process is that if a sufficient volume of data is collected, a total situational awareness will be achieved, providing sufficient information to foresee future attacks through emerging patterns of movement and circulation that will indicate intent.

Thus, mobility emerges as a potential threat to security, but as it cannot be prevented or blocked for most people, processes of identification and authentication emerge as the solution of choice. In this context, border technologies provide the means to identify, monitor, categorize and manage those who move, and create 'soft checkpoints' (Razac, 2009) away from critical areas such as border crossings. It is the existence of these soft checkpoints that is of concern when looking at the social externalities of border technologies, as they limit freedom of movement in areas where it should not exist, but also create vast databases and blacklists which could further impact on people's rights.

When assessing the impact of border technologies on freedom of movement, the key is to identify whether the scheme to be implemented acts or could potentially act as a 'soft checkpoint', collecting data that could later allow for the tracing back of an individual's activities, and also whether the existence of a soft checkpoint can cause a chilling effect, discouraging the mobility of a person who otherwise would have no reason not to 'move'. If this is the case, that technology can be said to have a potential negative impact on the freedom of movement of citizens.

5.6. Non-discrimination

The Critical Border Studies literature has dealt at length with the issue of discrimination, framed as profiling or social sorting by most authors. 'Surveillance today sorts people in categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice,'according to David Lyon (2003: 1). Everyday border crossing is based on the use of databases and classification; in this process of abstraction, discrimination can emerge in the sense of one's being pre-emptively singled out because of one's appearance, behavioural routines, financial transactions, genetic information, consumption habits or many other criteria employed in particular sectors and domains where personal data is systematically mined and matched to derive intelligence.

These data-intensive technologies rely heavily on categorization and automated profiling practices, and are therefore mechanisms of social differentiation (Monahan, 2008: 219). A specific term has been developed to describe the process of classifying people into categories according to varying indicators and markers gathered using data mining processes –social sorting (Lyon, 2001). As mentioned above, the main goal of social sorting is to discover and manufacture differences in order to classify data subjects, targeting them as members of differentiated categories. This has advantages in many different areas, such as marketing or policing, as it introduces an element of 'rational discrimination' that can help to adjust the gaze to specific profiles (high-end consumers, people with a criminal record, etc.).

However, the automated sorting by categories of personal data can (re)produce marginalizing effects and negative discrimination (Monahan, 2010: 92), maintaining historical disparities that negatively affect specific groups (Oscar, 2009: 13). Although this social sorting process is not necessarily unethical in essence, the systematic use of this method tends to reinforce disparities and socio-economic inequalities. Researchers have described how social sorting can be used to exclude and remove undesirable groups from public space, and how this is linked to the broader process of increasing control and regulation in the social and urban sphere (Coleman, 2004: 293). As the research (Armstrong and Norris 1999; Hille 2002; Bannister and Fyfe 1996) shows, exclusionary spatial practices contribute to social exclusion and intolerance, as well as affecting social responsibility.

However, a great deal of contemporary social sorting is not about physical profiling but is based on dataveillance – that is, 'the systematic monitoring of people's actions or communications through the application of information technology' (Clarke, 1988). With the proliferation of databases and automated border technologies, along with increased interoperability and access, the possibilities for dataveillance extend from the computer into everyday activities such as getting on a bus, shopping at the supermarket, going for a walk or withdrawing money from an ATM. One of the fields where people's actions and communications are more intensively assessed for risky behaviors is in financial transactions. Profiling software used in financial institutions often has a double aim –to control, assess risk and target customers better, but also to identify suspicious, potentially terrorist behaviours or flows. 'Tools of [customer] seduction' become 'tools of suspicion', (Oscar, 1993; Lyon, 2007; Marx 1988) and the room for discriminatory practices grows.

In the context of border crossing, discrimination takes a whole new turn. In most cases, border dataveillance is not about gate keeping but about 'gate opening' (Franko Aas 2011: 338) – providing *bona fide* travellers with a seamless border experience, free of queuing and suspicion. Pre-registered traveller programmes, put in place by both border authorities and the private sector − a primary example being the use of fast lanes − create the expectation that wealth can buy the right to avoid suspicion at border crossings.. 'Discrimination through privilege' on the basis of personal data sharing therefore raises concerns about human rights, due process and democratic practice, while also creating new inequalities among citizens when travelling.

5.7. Social integration

According to Emile Durkheim, one of the early sociologists to theorize it, social integration involves society's ability to accommodate the structural forces that lead to differentiation and specialization. In his work, social integration is linked to solidarity, collective consciousness and identity (Durkheim, 1933/1997). In more recent accounts, the United Nations defines social integration as 'an inclusive society' that 'emanates from the well-being of each individual, mutual trust, sense of belonging and inter-connectedness' (UN Social Policy and Development Division).

When referring to social integration, therefore, we are looking at social relations and the structural and informal elements underpinning them. Bordering practices, in their multiple forms, constitute one of those elements with a potential to impact on the way social relations are practiced and organized. As can be observed with diverse externalities, border technologies developed in the name of increasing security can have a negative or a positive impact on social integration. In the formal and physical sphere, for instance, risk profiling can be said to play a positive role in extending rights and thus reinforcing the institutional elements that enable social integration – or, as Monahan et al. put it, contributing to 'individual autonomy and dignity, fairness and due process, community cooperation, social equality, and political and cultural visibility' (Monahan et al., 2010: 106).

This understanding of border technologies emphasizes the relationship between surveillance-enabled identification and citizenship and/or between identification and increased ease in the use of public resources and facilities. The latter can be found in the case of citizenship or ethnic minority status being issued to previously ostracized communities not fully recognized by the state, or when asylum is granted. Studying an instance of identity fraud in Brazil, Murakami Wood and Firmino (2009) compellingly show how in some instances not being part of a national identification database can result in fear of exclusion, or 'to disappear as the victim of arbitrary forces' (Firminio, 2009: 299). In this sense, specific forms of identification and authentication can be seen as enablers of social integration as they can extend citizenship rights, and therefore an expectation of equality, a shared identity and a sense of belonging, to certain groups of people. If any of these effects is identifiable in the dynamics created or promoted by the design and development of a border technology, this should be taken into account as a positive externality, thus reducing the overall social cost of a specific technological initiative.

However, border technologies have also been found to affect social integration in negative ways. If data mining and matching is used as a way of 'sorting' the appropriate from the inappropriate, particularly in public spaces, this control immediately affects the way different groups use these spaces and benefit from their qualities, especially the possibility of social integration and community building. The tendency to stereotype, discriminate and socially select those who end up being scrutinized by the electronic border points to a weakening of mutual trust, sense of belonging, connectedness and, to use Durkheim's words, society's ability to resist differentiation and specialization.

5.8. Equality of treatment

Equality of treatment is a general principle of community that states that similar situations must be treated equitably and prohibits discrimination and discriminatory treatment. Equality of treatment is recognized as a right, for which steps will be taken to prevent or remove differences in treatment. Equality of treatment may therefore be guaranteed by law but also enforced when discriminatory practices and values are identified.

For those who are situated on the watching, listening, locating, detecting and monitoring side of border technologies, those that appear before the lens or the data-gathering mechanism are often just pieces of information that can be used or analyzed both individually and in aggregate form to reach a given objective: be it for market analysis, community safety and security or more efficient management of resources, mobility or sustainability (Lyon, 2003). In this context, categories such as social sorting, digital discrimination, privacy invasion, and racial profiling (Oscar, 1993; Lyon, 2003: Monahan, 2008; Regan, 1995) are useful for understanding how data mining and big data may promote unequal treatment among different categories of people.

The social sorting associated with IDs touches the lives of the weakest, most marginalized members of the population. Many of these IDs increasingly incorporate biometric data, which classifies people according to their bodily and behavioural characteristics, thus abstracting their identities from their everyday ‘struggles and stories’ (Lyon, 2007b: 115). This surveillance-enabled social sorting not only works against marginalized groups, but also in favour of those who are deemed to be trustworthy because of their social or economic status, as mentioned above. In these cases, individuals are subjected to increased surveillance to allow for expedited border crossing, such as participation in RTPs. Inequality of treatment, thus, does not always mean that discrimination is used against the subjects of surveillance, but surveillance can also provide avenues of privilege and freedom from further scrutiny to those who are able to pay for the benefits associated with being watched, or those who comply with the prerequisites of status.

Section II: Mapping border data flows

1. Delocalized and expanded borders

Whereas in the first section of the report we have outlined how, with electronic borders, more and more data on those who cross-travel is collected, in this section what we want to emphasize is that the process of gathering information starts prior to the actual border-crossing and continues after travellers arrive at their destination. This section aims to analytically describe the changing morphologies of borders and the increasing relevance of digital information/data flows at border crossing points, as well as the way these data points interact and how decisions to trigger a digital alarm are taken.

As Van der Ploeg rightly observed, 'governments are not only interested in the fact that people cross a border in a legitimate way but they would also increasingly like to know who precisely has crossed the border and even who will cross the border in the future' (2011: 72). In order to achieve this goal, technological border control – i.e. digital techniques of identification and authentication such as biometrics, and the collection of travellers' data by different means and by different agents – is performed beyond the physical border itself and at three different moments and spaces:

1) Before the journey, in the country of origin.
   - Data to book a ticket (Passenger Name Record)
   - Pre-departure checks to request the right to travel (Advanced Passenger Information and VIS).
2) At border crossing points.
   - Security checks
   - Departures controls (biometrics, EES).
   - Arrival checks (biometrics, SIS, VIS, EURODAC).
3) After the journey. In the country of destination after crossing the border and during the period of stay or residency in the destination country.
   - Surveillance and control activities.

In the following pages, the travel data life-cycle through different spaces and times is reconstructed, so as to provide an overview of the extent to which the border is increasingly being constructed as a data space more than a physical space. Our data travels before us and is retained at the border for extended periods of time, creating data routes that will both precede the moment of border crossing and outlive it.

For the sake of clarity, the following pages recreate the data flows involved in air travel (airports and airlines). We choose airports and air-borders-related practices as an example as they are paradigmatic symbols of contemporary mobility and they offer an interesting case study of how 'mobility may become watched and controlled' (Adey, 2004: 501). While many procedures are shared with land and sea crossing and other means of transport, some of the procedures described below are exclusive to air travel.

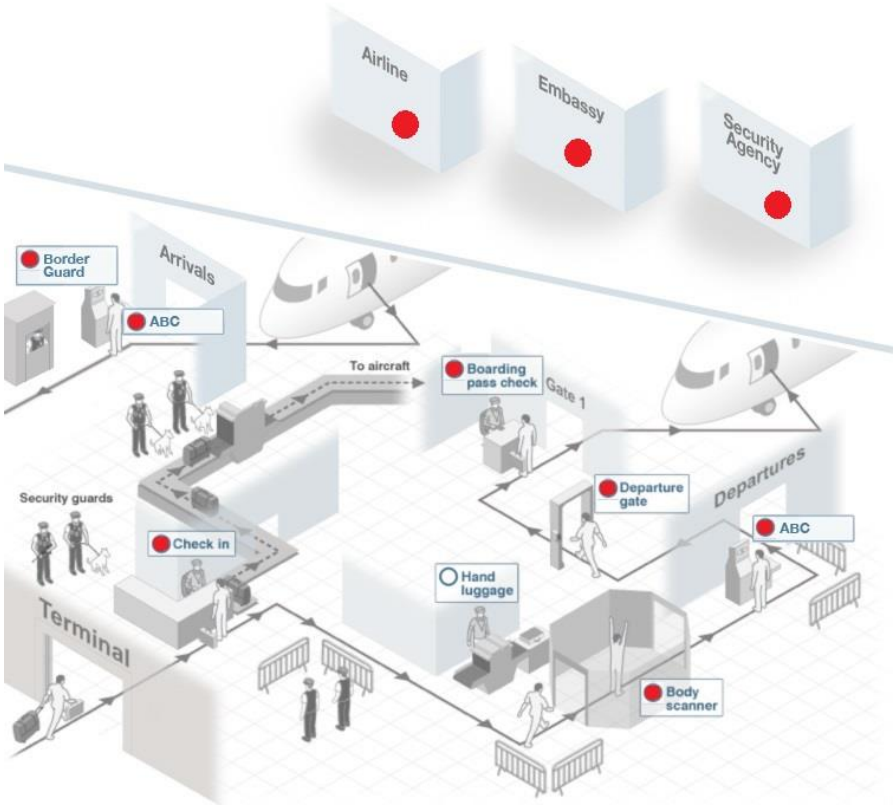

Figure 2: Data mining points in the border-crossing process. Source: authors' elaboration.

2. Mapping data flows

2.1. Before the journey: Booking a ticket

Airlines are increasingly involved in the practices of controlling borders as states delegate document control to them (Marin, 2011:132). When booking a ticket with an airline or through a travel agent, travellers need to provide biographical and contact details, credit card information, frequent flyer number (if any) and passport or ID information (which in some cases can also be collected later). This data is entered by the airline or the travel agent into a linked computer reservation system.

Each passenger produces a Passenger Name Record (PNR). These were first introduced by airlines for the purpose of what is called 'interlining' – using different airlines to cover one single trip, which will require a certain level of collaboration between providers to track delays, luggage, etc. For this purpose, the International Air Transport Association (IATA) published the 'ATA/IATA

Reservations Interline Message Procedures - Passenger' (AIRIMP), defining a series of standards for interline messaging, Passenger Name Records and other data that acts as an informal standard in the industry (while there are many computer reservation and hosting systems, often using proprietary software, the data content and format is similar and therefore interoperable with AIRIMP). When an itinerary is booked, a PNR is generated in the computer reservation system (using a Global Distribution System such as Amadeus or an internal database).

In recent years, and with the growing anxieties around international terrorism, PNRs have developed a secondary police purpose. According to the EU Council:

> *Most organized crime and terrorist activities involve international travel. These include the smuggling of persons or drugs, or the access of terrorists to training camps outside the EU. As a response to this threat, and to the abolition of internal border controls under the Schengen convention, the EU adopted measures for the collection and exchange of personal data between law enforcement authorities. However, these measures focus on data related to persons who are already suspected. The transfer and processing of PNR data would allow law enforcement authorities to identify suspects who were previously unknown.*

Most EU Member States already use PNR data in a non-systematic way or under general powers granted to the police or other authorities. Law enforcement and security agencies have direct access to PNR/CRS databases. These are used for intelligence, criminal investigations and possibly as well for travel pattern analysis, surveillance of movement and automated profiling systems. While the EU already shares PNR data with the USA, Canada and Australia, it has not yet agreed its own PNR Directive. Until recently the debate on the systematic use of PNR for security purposes within the EU had been rejected by the European Parliament over privacy concerns, but is now progressing through the decision-making process in response to concerns about returning foreign fighters. Regulation at EU level would harmonize Member States' legal provisions and, in the words of the European Council 'avoid legal uncertainty and security gaps, whilst at the same time safeguarding data protection.'[14] It is unclear, however, how this balance will be achieved, as the data contained in a simple PNR includes demographic, personal and financial data, as well as information of the IP address and often dietary preferences that can be linked to religious beliefs.

[14] 'Regulating the use of passenger name record data'
http://www.consilium.europa.eu/en/templates/content.aspx?id=26909

Figure 3: Excerpt from a simple Passenger Name Record. Source: The Practical Nomad.[15]

But it is not only the police that can access PNR data. Airlines will check the data against their own internal 'no-fly list', primarily concerned with disruptive or unruly passengers' past behaviour. It may also check it against government, or multiple-government 'watch lists' and 'no-fly lists' (see below). Further checks against national and international sanctions regimes, which include travel bans, may also be undertaken at this point. These regimes include 'terrorist' sanctions lists but are different from government 'watch lists' and 'no-fly lists'.

2.2 Before the journey: 'Pre-frontier' (pre-departure) checks

Before taking off, passengers may need to provide certain information to the airline or travel company (Advance Passenger Information), and to the embassies or consulates representations (VIS).

2.2.1 Advance Passenger Information Systems

Advance passenger information (API) is designed to enhance and reinforce border control and security. The information supplied is processed and received by the government of the country of destination. The information provides Border Control with all the information of 'pre-arrival' and

[15] 'What's in a Passenger Name Record?' http://hasbrouck.org/articles/PNR.html

'pre-departure' passengers and crew members. This information can then be used by Border Control to predetermine any problems that may arise with any passengers wishing to enter the country (using database checks). The API information can also be used to check passengers against warning lists and can also be used for immigration purposes. The main purpose of the API system is to provide advance warning to the Border Control of any passengers or crew members that may be of interest to Security and Border Control. If a passenger refuses to provide the information requested, which will typically include First Name, Family Name, Date of Birth, Gender, Type of Document, Passport or Document Number, Nationality, Issue Date of Passport, Expiry Date of Passport and Country of Residence, the subject will not be allowed to travel. The data that is requested can vary depending on the destination country and can change at any time; in some cases, the passenger may be asked to provide their personal address and/or the address of the place where they will be during their stay at destination.

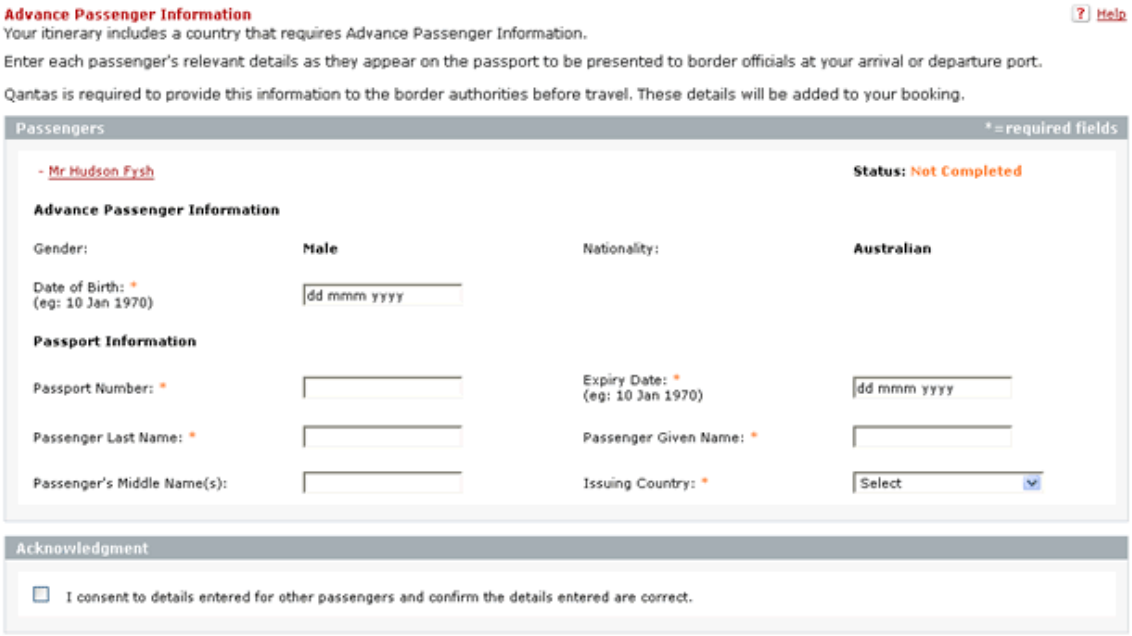

Figure 4: API sample. Source: Quantas.

The information submitted is sent to the Border Control and Immigration Authorities in the country of destination, and they can share it in its turn with other authorities to prevent illegal acts of terrorism or serious crime. The best known API system is the US Department of Homeland Security's Electronic System for Travel Authorization (ESTA). When passenger data is submitted, checks against domestic watch lists and international sanctions lists are routinely performed, and this can result in refusal of entry with no further explanation. Checks against other wanted persons lists, Interpol lists or watch lists of other governments may also be performed.

2.2.2 Visa applications (biometrics) and Schengen Visa Information Systems (VIS)

EU Regulations require all foreign entrants subject to visa requirements to provide fingerprints and biographical details as part of the application process. For visa purposes, the EU relies on a white list of countries whose citizens are exempt from requesting a visa in specific cases (usually for sort-term travel for recreational purposes) and a black list of countries whose citizens need to secure a visa before travelling (see map below). Hence, embassies and consulates function as border-crossing points in advance (Ploeg, 2011).

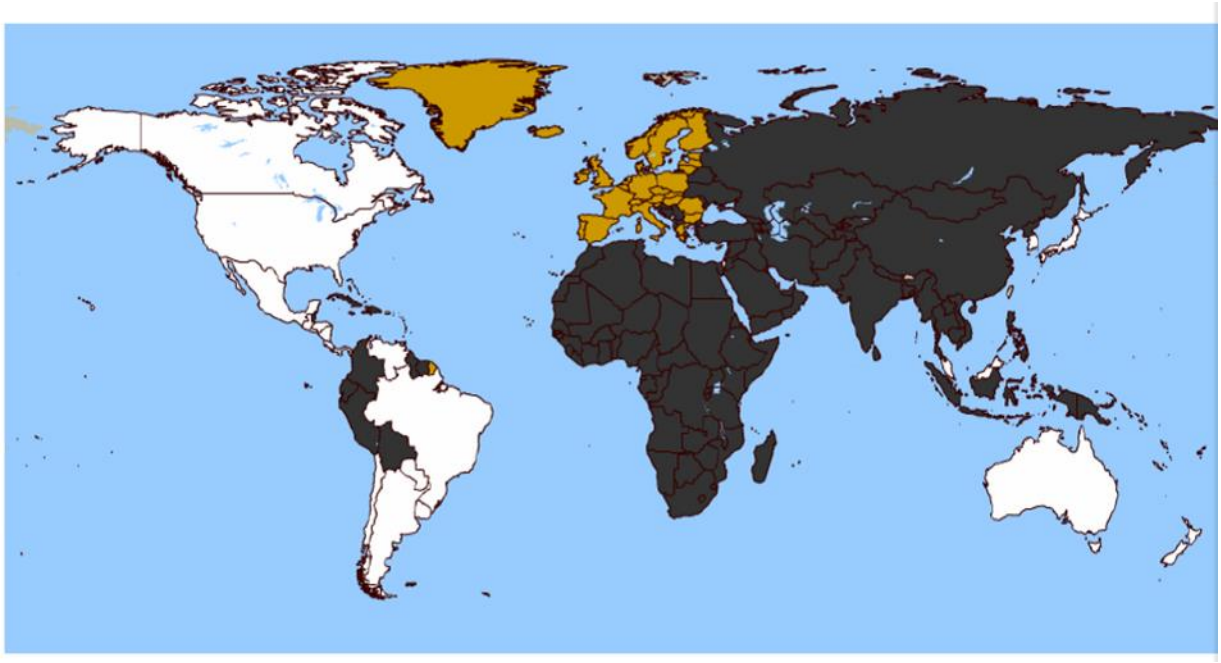

Figure 5: EU Visa requirements, white and black-listed countries. Source: Ben Hayes (2009)

Member state consulates are connected to the VIS database and equipped to register visa applicants and process their fingerprints. Data from all applicants (including fingerprints) are kept in VIS for five years, including data from people whose visa applications are rejected. In its first year (2011-12) of operations, while still limited to pilot countries, approximately one million records were added to VIS (which can hold up to 70 million records).

According to the European Commission's Migration and Home Affairs Directorate-General,

> *10 fingerprints and a digital photograph are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database. 10-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply*

for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.[16]

At the Schengen Area's external borders, the visa holder's finger scans may be compared against a database. In case of a mismatch, further checks will be required until a trusted identity can be established.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories. Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application. In specific cases, national authorities and Europol may request access to data entered into the VIS for the purposes of preventing, detecting and investigating terrorist and criminal offences.[17]

Visa applicants may also be checked against national and international watch lists or analogous databases. In the case of visa applications to Schengen states they will also be checked against the Schengen Information System (SIS) of persons to be refused entry into the Schengen area (e.g. failed asylum applicants, people who have been deported, people who have been banned, etc.).

Between 2007 and 2014, the United Kingdom developed their own e-Borders Programme. Now terminated, the program involved the electronic collection and analysis of data on all travellers entering or leaving the United Kingdom under the responsibility of the UK Border Agency (UKBA), with the aim of identifying and controlling illegal immigration and visa over-stayers. The data to be collected included service information (ferry, flight or train number, name of carrier, departure and arrival point) as well as advanced passenger information (API) and Passenger Name Record data (PNR). The data is checked prior to travel against the Home Office Warnings Index, a watch-list to ascertain whether travellers are 'of interest' to UK authorities. At the actual border, Secure ID would verify the fingerprints of travellers at immigration control against biometric data collected during the visa application procedure.

Despite its ambitious nature (it is closer to the Smart Borders Package than to current border management procedures), in 2014 the Director General of the UK's Border Force announced that the program would be terminated due to delays in the provision of the necessary technology. While the program has not been scrapped, its implementation at land and sea borders has not yet occurred and a contractor has not been appointed.

[16] 'Visa Information System (VIS)' http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

[17] Íbid.

2.3. At the airport: Border crossing points.

Airports are dense data ecosystems where data-mining technologies used for different purposes, public and private, collide and reinforce each other. Those technologies are not only addressed to control passengers, but 'objects' and 'things' (baggage, possessions and aircraft) are also subject to surveillance (Adey, 2014). Airports are critical infrastructures but also often shopping malls, parking lots and transportation hubs, and for each purpose different technologies are laid out.

2.3.1 Airport security

Upon arrival at the airport, plate numbers are often collected using Automatic Number Plate Recognition (ANPR). CCTV covers all airport areas to provide both security and intelligence on how people use the shared areas. More and more, CCTV systems are equipped with smart systems that allow for the automatic detection of faces and gaits, circulation patterns or abandoned objects. Wireless antennas are used to provide limited internet to travellers while at the same time gathering information on their devices' unique identifiers, browsing history and geolocation for commercial and management purposes. At airport stores, boarding passes are requested for tax purposes (to determine how much tax stores should pay to the state depending on the tax status of the travellers, defined by their destination), providing these commercial outlets with detailed information on personal and travel details, linked to their purchases and financial data if they pay using digital means.

While the data-gathering resources deployed before the act of travel are designed to identify potential wrongdoers on the basis of their prior history (being in an existing database) or travel plans (especially relevant if they involve countries subject to suspicion of terrorist activity), at the airport the screening is taken into a new level with the use of behavioural profiling and screening techniques.

Behavioural profiling has been used in interrogation since the 60s, as a way to improve the effectiveness of questioning by picking up on facial traits that may reveal nervousness or unusual body language. In current airport security, however, behavioural profiling has left the interrogation room to be adapted to moving subjects. The version of behavioural profiling currently in fashion at Western airports relies on the ability to identify suspicious behaviour of passengers that are on the move (not being interrogated) with the help of sensors that may identify irregular or unusual circulation patterns or speed, body temperature and other physical traits that may reveal intent from a distance. While these programs have been criticized due to their lack of effectiveness (GAO 2013),[18] airports continue to invest in technologies to assist in the task of identifying potential wrongdoers as they move through the terminals. This requires the creation of a data profile of every single person moving about the airport area, as different sensors need to be able to follow a same subject through a large area.

[18] 'TSA Should Limit Future Funding for Behaviour Detection Activities' http://www.gao.gov/assets/660/658924.pdf

In the end, airports and border crossing areas are increasingly conceived as a continuum of surveillance for multiple purposes, due to their critical infrastructure status and the impact in the social imaginary of past instances of terrorist activity (notably the case of United Airlines Flight 93 on 9/11).

2.3.2 Check-in / no-fly

When checking in, airlines check the validity of travel documents. Typically, this can only be a verification that the names in the booking and on the travel document coincide. However, for specific routes, airlines may carry out full identity checks, as they can be fined for landing people who have inadequate or fraudulent documentation. At this point, travellers may have their data checked against no-fly lists and be refused boarding by the airline.

The most well-known (and controversial) of such lists is the US No Fly List, launched in 2001 and which is thought to include just short of 50 000 names of people who present a specific known or suspected threat to aviation. It is impossible to know whether one is on the list until there is an attempt to board a plane, and little can be done in terms of knowing how one ended up on the short-list. In 2005, plans to use information from commercial databases, including credit records, to establish a risk score had to be scrapped when they were flagged as illegal.

The complexity of the data ecosystem at the border was well-captured by Bruce Schneier in an article in 2008, when he used an example to show how the different border controls could be fooled by understanding the data flows:

> *Use a stolen credit card to buy a ticket under a fake name. Print a fake boarding pass with your real name on it and go to the airport. You give your real ID, and the fake boarding pass with your real name on it, to security. They're checking the documents against each other. They're not checking your name against the no-fly list—that was done on the airline's computers. Once you're through security, you rip up the fake boarding pass, and use the real boarding pass that has the name from the stolen credit card. Then you board the plane, because they're not checking your name against your ID at boarding.*[19]

Cases of false positives have been so common that in 2007 a Traveller Redress Inquiry Program had to be set up for travellers who had been affected by No Fly or other watch lists. Besides NFL, there are other databases and watch lists related to criminal or terrorist activity that can be used to check a traveller's identity and rights at the border. These lists can be shared across borders – the FBI, for instance, shares information on banned passengers with 22 foreign governments using its Terrorist Screening Centre and Database (TSDB), where data on known or suspected international terrorists is held, including data on their families.

[19] 'The Things He Carried' http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/

2.3.3 Passenger screening

After check-in, passengers need to head towards passenger screening, where a conveyor belt carries each item of luggage (including jewellery, shoes, coins, jackets and any other item requested by airport security) past an X-ray machine that detects and differentiates between organic, inorganic and metal objects.

Commonly, passengers are asked to go through some sort of detector. In some instances, Whole Body Imaging (WBI) will be used. WBI was introduced at EU airports after a failed terrorist attempt. On Christmas Eve, 2009, a 23-year-old Nigerian attempted to set off plastic explosives concealed in his underwear as the Amsterdam to Detroit Northwest Airlines Flight on which he was travelling was on its final descent. The plane made an emergency landing in Detroit without any fatalities, as the explosives failed to function properly. Upon investigation it was found that at the Amsterdam airport, the offender was subjected to the same screening as other passengers − he passed through a metal detector, which didn't detect the explosives that were sewn into his underwear.

The policy response to this incident was to resuscitate a debate on the need for Whole Body Imaging techniques to be used as a way to enhance airport security and prevent similar attacks from occurring. Full-body scanners were discarded by the European Parliament and the European Commission in 2008 until more information was available about their privacy and health effects.

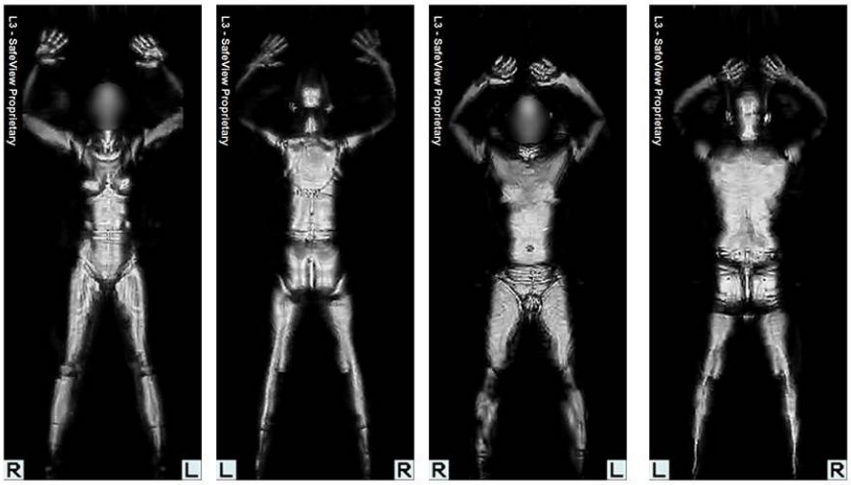

Figure 6: Image from an active millimetre wave body scanner. Source: Wikipedia.

After the failed terrorist attempt, however, WBI systems made it into the political agenda once again. Although it is arguable that full-body scanners may have headed off the attack, the fact that explosives were hidden in the subject's underwear pointed to the need for better imaging technologies. In the US, the Transportation Security Administration (TSA) ordered over 300 scanners; the Netherlands announced they would immediately begin to use this technology for

screening passengers on flights headed towards the US; British Prime Minister Gordon Brown announced that this technology would be introduced in the UK, and France and Italy made similar announcements. While other countries showed less enthusiasm, many acquired several devices.

There are two types of these scanners currently in use: 'millimetre wave' machines that use non-ionizing radio waves to produce a three-dimensional image, and backscatter scanners that use X-rays. Ironically, these scanners initially dramatically increased queuing time because every time a scanner detected something suspicious, it would trigger an alarm and a full pat down would ensue.

In terms of data sharing, however, the regulation states that images cannot be saved or recorded. While some full-body images have sometimes ended up on YouTube or social media, there is no indication at the moment that the detector/scanner data is kept or linked to a specific person or their luggage on a systematic basis.

2.3.4. 'Random' selection

People who are flagged on watch lists, including those on the SIS database, or those who trigger suspicion at the airport due to a database search, suspicious behaviour or association with a suspicious piece of luggage may be interviewed by the security services.

The reasons for the interview are routinely not provided – people are likely to be told that they have been randomly selected. As identified elsewhere,[20] however, random checks based on police profiling tend to rely on cues linked to ethnic traits or indicators of status such as clothing and overall image (see focus group analysis below).

One of the arguments in favour of the automation of border control is based precisely on the argument that data-based or algorithmic decision-making will be both more effective and less biased than human selection. Several authors have, however, alerted to the uncontrolled development of suspicion of people based on their noncriminal data patterns, called 'high-tech profiling.'

The intersection between rights, technology and discrimination is a case in point here, specifically relevant to border-crossing procedures. So far the introduction of technological solutions in the border-crossing process has resulted in a shift from selected surveillance and control to mass surveillance and control, on the basis that surveilling everyone is less discriminatory than surveilling only some based on subjective cues. Generally speaking, we could say that there is a surveillance of mobility, which is not only directed at passengers but also to "objects" and 'things', such as baggage, possessions and aircraft (Adey, 2014). This is controversial both from a legal and an ethical perspective – first, because citizens enjoy the right to the presumption of innocence and, as several EU and US courts have ruled, mass surveillance is illegal; secondly, because technology also has biases (built in precisely by those designing the technology and the decision-making algorithms).

[20] 'Addressing Ethnic Profiling by Police'
https://www.opensocietyfoundations.org/sites/default/files/profiling_20090511.pdf

2.3.5. Registered Traveller Programs

In the last few years, several airports have developed individual schemes to provide frequent travellers with a speedy check-in, border control and boarding procedure.[21] Those desiring to access this special treatment need to be pre-vetted by providing personal information, including data on the nature of their residence permit, details about their past and, often, biometric information.

Sometimes accessing a RTP requires some sort of payment, thus establishing a second layer of discrimination based on income, and creating a two-tier system where 'trusted' and affluent travellers have access to a different airport experience. In this case, voluntary provision of biometric data that would not otherwise be needed when crossing the border acts as a symbol of trustworthiness.

These schemes usually work in conjunction with automated border control gates, which are responsible for verifying the identity of those wishing to travel, either by matching their facial or iris image with that contained in the travel document or by accessing other databases.

The EU has proposed a harmonized RTP scheme open to third country national business travellers as part of Smart Borders package. The criteria for acceptance to the EU RTP would be similar to that required for a residence permit, and according to COM (2013) 97 Final 'Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme' it would work by issuing a token in the form of a machine-readable card to each registered (i.e. pre-screened and pre-vetted) traveller. The token would contain a unique identifier (i.e. application number), which would be swiped on arrival and departure at the border using an automated gate. The gate would read the token and the travel document (and visa sticker number, if applicable) and the fingerprints of the travellers, which would be compared to the ones stored in the Central Repository and other databases, including the Visa Information system (VIS) for visa holders. If all checks are successful, the traveller is able to pass through the automated gate. In case of any issue, the traveller would be assisted by a border guard.

The need for harmonization highlighted in the EU documents on RTP reflect the current limitations of moving towards a unique automated border mechanism. This is due to the fact that the personal and biometric data stored in EU IDs is usually only accessible to the authorities of the country of issuance.

[21] See, for instance, https://www.gov.uk/registered-traveller.

2.4 Departure controls

2.4.1. Document checks / biometrics

Upon leaving a country, documents are usually checked by immigration officers, and holders of biometric visas are fingerprinted and their identities verified (making sure that the traveller's biometrics match those stored in their visa document).

These exit controls are increasingly being performed by Automated Border Control (ABC) gates. In the last few years, many ABC gates have been deployed at main European airports, most of them as pilot projects intended to test their ability to improve the border-crossing process in terms of speed, automation, security, efficiency, false rejection rates, etc. While most ABC gates look similar, the ways in which they check the traveller's identity, their ability to access the data of the e-Passport chips and to match the information against different databases can vary, and will depend on the software and hardware developed for each specific machine. These differences are often invisible to the traveller, who is unaware of what kind of data is being retrieved and how it is used. As an example of this complexity, the graph below maps the data flows of what an automated border gate for Third Country National Visa-Holders (TCNVH) could look like.

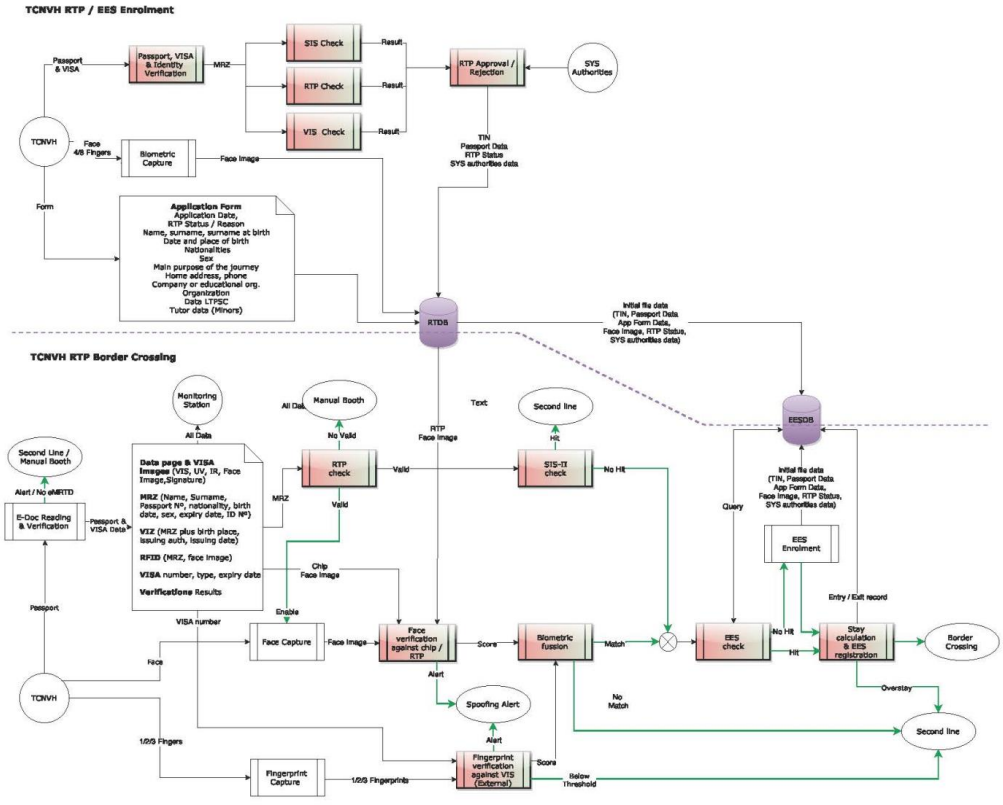

Figure 7: Data flows for TCNVH. Source: authors' elaboration.

ABC gates are biometric systems that are used for authentication decisions: they must decide on acceptance or rejection. This is precisely why such technologies are useful in the determination of identity at the border, where accurate accept/reject decisions are crucial. However, because biometrics relies on *recognition*, this process may fail in two key ways: by falsely rejecting someone who should be allowed entry, or by falsely accepting someone who should not.

False rejection (or 'false negative') in biometrics occurs when 'mistaking two biometric measurements from the same person to be from two different persons' (Jain, Ross and Prabhakar 2004). In this case, a failure of *identification* (1: many verification) is more likely to be the case, but FR can also result from an *authentication* (1:1 search) mismatch between a stored biometric template and the live biometric presented at the terminal/system. Most ABC programs reviewed in this program rely on 1:1 biometric matching using facial recognition or fingerprints, and occasionally of the iris, meaning that false rejection is often most likely due to a mismatch between stored and live biometrics, or due to factors such as lighting, temperature, or traveller error (wearing headgear, glasses, or making too many failed attempts).

False acceptance (or 'false positive') is 'mistaking biometric measurements from two different persons to be from the same person' (Jain, Ross and Prabhakar 2004). This can be the result of intentional spoofing of biometric systems, whereby the fingerprints of others (whether dead or alive) are used to trick a biometric system into authenticating an impostor. This can be overcome by features such as liveness/vitality detection in biometric readers. False acceptance rates are generally lower than false rejection rates in biometric systems with security implications.

False rejection or acceptance is a multi-layered process and it is not always caused by the biometric process itself. It can result from events such as travellers' being rejected at the document verification stage. For instance, travellers at an airport may be rejected by the ABC gates simply because they do not have e-Passports. In some cases, human interface is the cause of false rejection, as was the case with the failed UK IRIS program, whereby travellers' difficulties often lay more with lining up their eyes for iris scanning than with the iris legibility itself.

FAR and FRR are interrelated: reducing the strictness of a system, by definition, increases the FAR, demonstrating that the two are correlated. This loosening can be done for a range of reasons such as to increase throughput and improve traveller convenience. Increasing the strictness of a system, usually done as part of a security-maximizing rationale, will increase the FRR but the existence of alternatives (such as manual processing) may mitigate the negative impacts of this. One of the major problems of false acceptance and false rejection lies with authenticity verification. Many ABC systems proceed in two steps: first the passport is verified, and then the holder is verified against the passport. However, a false acceptance of a fraudulently-held but genuine document can potentially be repeated infinitely as the verification system will not detect a mismatch between the passport and the holder. This suggests that breeder documents and identify verifications in countries of issuance are as crucial as the biometric authentication itself.

FAR and FRR are therefore strongly reliant on enrolment factors as well as environmental and human interface factors at the point of real-world use. Current biometric control schemes have varying rates of FA and FR as well as different acceptable rates of failure. It is notable that in most systems, the FRR is calculated by counting how many otherwise *bona fide* travellers are rejected, thus making it a relatively straightforward empirical calculation. The FAR, however, is much

harder to calculate and is often derived from estimations (using the FRR) or from controlled tests involving document swaps. The FAR is a key metric for the determination of the security element of ABC systems, as it is the measure of how many impostors or *mala fide* travellers are allowed in. Knowing the FAR, and comparing it to other metrics such as FRR, overall throughput and cost, allows authorities to determine the security, convenience and cost-effectiveness of an ABC deployment. Not having clear figures on FRR makes it very difficult, by extension, to make conclusive statements about the efficiency, effectiveness, and value of ABC.

Different biometric identifiers display different failure rates, and these are also modulated by factors such as environmental context (lighting, humidity, temperature) and human factors (quality of fingerprint, age of holder, ethnicity). Something as seemingly obvious as lighting has drastic effects on the FRR with all else held constant, with inadequate lighting resulting in rates of up to 50%.[22] Adequate calculations of these rates are often difficult to come by, as most tests tend to be carried out by biometric suppliers in tightly controlled conditions. In some cases, FRR rates are given for real-world usage, but tend to be higher than the generally-accepted 2% threshold.

This threshold is set manually by the operator, who establishes performance thresholds. This is an automated mechanism to decide whether to prioritize identification matches over processing times and queue latency, thereby causing the decisions of border guards to be directly affected by the inner workings of the technology designed by engineers. Against the backdrop of operator security and efficiency concerns, false positives may cause distress to passengers, or induce some to feel that the technology infringes upon their dignity and reputation. Furthermore, those impacts can be uneven depending on certain personal attributes (gender, age, origin, socio-cultural background). It may be possible to run both non-systematic checks and the FRR/FAR ratio by a rules engine or other fully automated, algorithmic mechanisms. While full database integration is not yet taking place at border crossings, current legislation is such that it can occur in the future, and many security assumptions of the policy agenda rely on the technology's capacity to amass and analyze substantial amounts of data, thereby identifying information overlooked by humans.

2.4.2. Entry-exit systems (EES)

Many countries are looking for ways to identify visa over-stayers and control the entry and exit of every single person crossing their territory. In 2009, twelve EU Member States had EES schemes. In the UK, the EES system is part of the broader e-borders scheme. Entry-exit systems (EES) record the biographical details (from the alphanumeric details in the passport), biometrics (photos and fingerprints), time, place, date and visa details of people entering and exiting a country.

While the 'entry' part of EES is relatively easy to implement, especially at controlled border crossings such as airports, controlling 'exits', especially when they happen using land borders (by car, for instance) is much more difficult, as the infrastructure at those points does not typically exist and in many places it would be costly if not impossible to implement.[23]

[22] FRONTEX, *BIOPASS*, 25.

[23] 'U.S. Visit adds system to track departing travellers' http://gcn.com/articles/2004/08/13/us-visit-adds-system-to-track-departing-travellers.aspx

The possibility of tracking all entries and exits, however, constitutes one of the aims of the Smart Borders Package. Specifically, COM (2013) 95 Final 'Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union' contains the rationale for introducing such a system and the legal framework that might be required to support it. In the proposal, the electronic registry of the dates and places of entry and exit of each third country national admitted for a short stay in a specific country or region if foreseen. Currently, the Schengen Border Code does not include the possibility or need to record all cross-border movements, and stamping the travel document is the sole method used to indicate the dates of entry and exit which can be used by border guards and immigration authorities to calculate the duration of the stay of a third country national in the Schengen area (which shall not exceed 90 days within a period of 180 days). Other tools available at border crossing points, such as SIS and VIS databases, which need to be checked at entry but not at exit, were not designed for the purpose of recording border crossings and do not provide for this functionality.

The purpose of the proposed EU EES system is to improve the management of the external border and the fight against irregular migration by providing a system that can calculate upon entry the authorized stay of each traveller and how many days are left of the maximum of 90 days within 180 days. At exit, the aim is to verify that the traveller has not over-stayed their visa or authorized stay. In the case of third country nationals, EES can determine the legality of their stay. EES can also assist in the identification of any person who may not or no longer fulfil the conditions for entry (this mainly concerns those whose identity is checked once they are inside the territory using their travel documents or any other means of identification). Finally, EES is expected to support in the analysis of the entry and exit of third country nationals in order to get a precise picture of travel flows at the external borders and the number of over-stayers by nationality, age, etc.

With the implementation of an EES system at the EU level, travellers with visas or not requiring a visa would need to submit their personal and biometric data, which would be stored and checked against VIS and SIS. In the case where someone who has entered does not produce evidence of 'exit' within the agreed time, an alert (a kind of de facto arrest warrant) will be issued, and law enforcement and security agencies will also be given access to EU EES for surveillance purposes.

While an EES at the EU level was formally proposed in 2013, the technical feasibility and cost of such a system has been questioned by a report commissioned by the European Parliament.[24] Since then, the European Commission has published a new technical study,[25] and the EU-LISA pilots and a public consultation are currently underway. New legislative proposals are expected in 2016.

In the US, the Customs and Border Protection (CBP) management system, US-VISIT, incorporates an Entry-Exit Initiative. However, the failure of the US-VISIT biometric border information system to adequately account for those leaving the United States by means other than by air has led the US and Canada to design a Canada-US *Beyond the Border* Declaration (and action plan) by which both countries have implemented a joint Entry-Exit Initiative along their land border. This gap in the 'exit' portion of the US-VISIT system, which could only be filled by a huge

[24] The Commission's legislative proposals on Smart Borders: their feasibility and costs http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493026/IPOL-LIBE_ET(2013)493026_EN.pdf

[25] Technical Study on Smart Borders http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf

investment in human resources at land and sea borders, has been solved in a more economical way with the US relying on Canadian entry data to furnish it with land exit data for the northern border. This joint EEI has been achieved in a number of 'phases' of biographical (not biometric) information exchange. In this system, the biographical information collected is reconciled along a number of key variables: first name, middle name, last name, DOB, nationality, gender, document type, document number, document country of issue, border point code, date of entry, and time of entry. Canada has a matching success rate of 94.5% (across 343,363 records) and the US of 97.4% (413,222 records). The failure rate has been reduced by 'exact and probabilistic matching' and the system is able to identify overstays and outstanding warrants for immigration offences.[26] The purpose of the EEI is therefore to supplement these data variables with dates and times of *exit*, with each country sharing entry information with the other to fulfil this information requirement. The remainder of the information is already collected as part of entry processes for each country.

2.5 Arrival checks

Upon arrival in a country, the national authorities may choose to perform document and biometric checks, depending on the point of origin of the passenger. Visa entrants to the EU will be checked against VIS (including fingerprints). In the US and other countries, everyone is checked and fingerprinted on arrival. As mentioned above, EU citizens or citizens entering their own country will typically only have their identity verified against an ID document. On a non-systematic basis, however, border control agents may choose to proceed to check a document against a database or engage in further questioning.

Arrival checks are increasingly performed by biometric ABC gates (see above) that check the data (physical and document-based) of the traveller and, depending on their status, perform database checks.

[26] Canada Border Services Agency and Department of Homeland Security, Entry/Exit Information System: Phase I Joint Canada-United States Report (2013), 6.

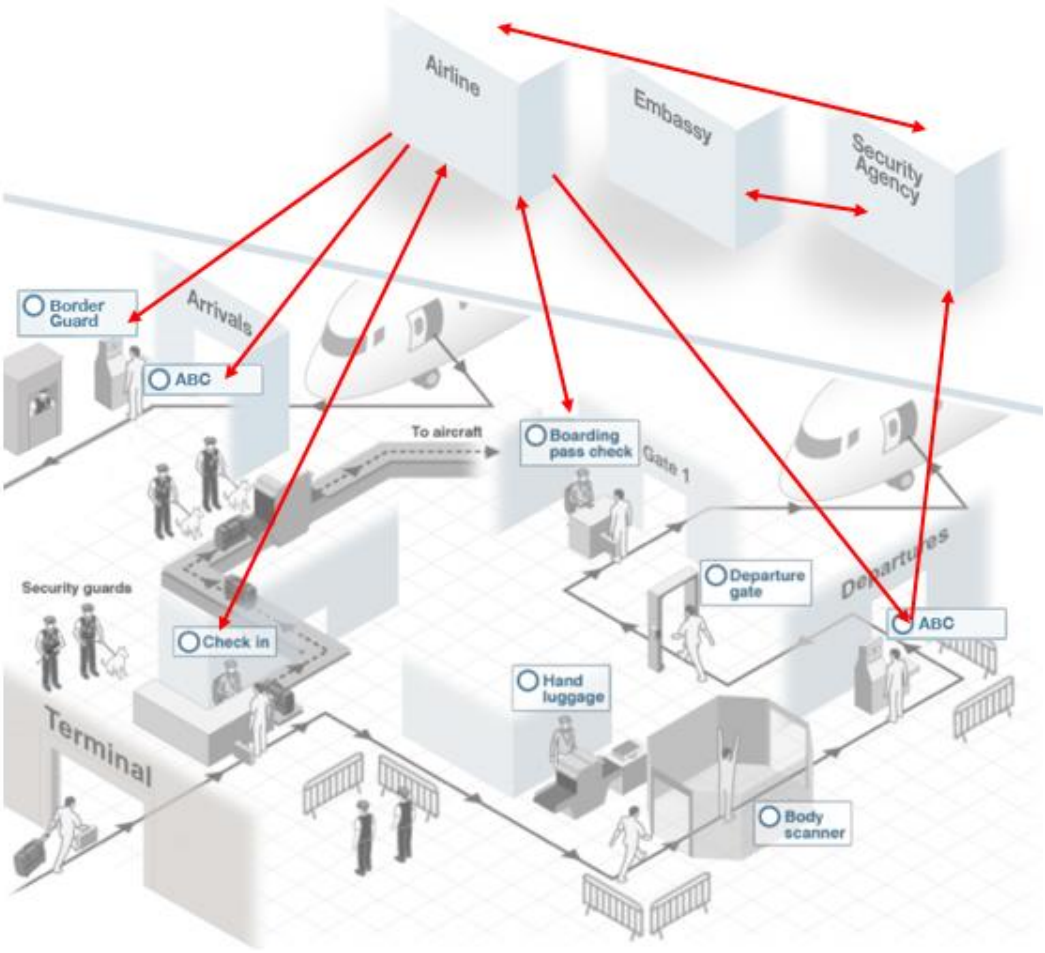

Figure 8: Data flows throughout border-crossing process. Source: authors' elaboration.

2.5.1. Schengen Information System (SIS I & II)

All entrants to the Schengen area from non-Schengen countries should be checked against the Schengen Information System (SIS). The Schengen Information System was established as an intergovernmental initiative under the Schengen Convention, now integrated into the EU framework. It is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. It holds information on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. It also keeps alerts on missing persons, particularly children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents that may have been stolen, misappropriated or lost. Information is entered into the SIS by national authorities and sent via a Central System to all Schengen States. On 9 April 2013, the second generation Schengen Information System (SIS II) entered into operation. SIS II has enhanced functionalities, such as the possibility of using

biometrics, new types of alerts, the possibility of linking different alerts (such as an alert on a person and a vehicle) and can accept direct queries. It also ensures stronger data protection.

SIS is one of the world's largest IT database systems, and it is composed of a central system (Central SIS II), which includes a technical support function ('CS-SIS') containing a database, the 'SIS II database' and a uniform national interface ('NI-SIS'). The second part is a national system (the 'N.SIS II') in each of the Member States. N.SIS II consists of national data systems which communicate with Central SIS II. An N.SIS II may contain a data file (a 'national copy'), containing a complete or partial copy of the SIS II database. Each Member State is responsible for setting up, operating and maintaining its own N.SIS II and connecting it to NI-SIS. The third part is a communication infrastructure between CS-SIS and NI-SIS (the 'Communication Infrastructure') that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux. The 'SIRENE Bureau' is an authority designated by each Member State which shall ensure the exchange of all supplementary information provided by SIS II.

SIS II is regulated by (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Regardless of these separate instruments, SIS II constitutes one single information system that should operate as such.

According to its own regulation, SIS II alerts can only be used for third country nationals (any individual who is neither a EU citizen or national of a third country who, under agreements between the Community and its Member States on the one hand, and these countries, on the other, enjoys rights of free movement equivalent to those of citizens of the European Union) who are not entitled to enter into or stay in the Schengen Area (on 1 January 2013 there were 659,347 'unwanted aliens' listed in the system); persons wanted for arrest (Article 26 of Council Decision 2007/533/JHA) for whom a European Arrest Warrant or Extradition Request has been issued; missing persons (Article 32 of Council Decision 2007/533/JHA), including children, to place them under protection if lawful and necessary; persons sought to assist with a judicial procedure (Article 34 of Council Decision 2007/533/JHA) to find out the place of residence of persons sought to assist with criminal judicial procedures (for example witnesses); persons and objects for discreet or specific checks (Article 36 of Council Decision 2007/533/JHA) (The number of people listed in the Schengen Information System (SIS) for 'discreet surveillance or specific checks' by European law enforcement authorities reached 41,097 at the end of December 2013); and objects for seizure or use as evidence in criminal procedures (Article 38 of Council Decision 2007/533/JHA), including vehicles, travel documents, credit cards, number plates and industrial equipment. Therefore, SIS II should only be checked for EU citizens on a non-systematic basis

A SIS alert always consists of three parts: firstly a set of data for identifying the person or object concerned in the alert, secondly a statement why the person or object is sought and thirdly an instruction on the action to be taken when the person or object has been found.

2.5.2. Schengen Visa Information System (VIS)

The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

The VIS was established in June 2004 by the Council decision 2004/512/EC. The main Acts concerning the Visa Information System are regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the VIS and the exchange of data between Member States on short-stay visas (henceforth referred to as VIS Regulation) and Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the VIS by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. From these documents, it emerges that VIS is only applicable to 'third country nationals', as defined in SBC. In other words, VIS should not be used for border checks on persons enjoying the Community right of free movement, since third country nationals enjoying this right must have either a residence permit or a long-stay visa.

The purposes of VIS include facilitating checks and the issuance of visas (VIS enables border guards to verify that a person presenting a visa is its rightful holder, and thus facilitates the visa issuance process, particularly for frequent travellers), fighting abuses such as 'visa shopping' (making further visa applications to other EU States when a first application has been rejected), protecting travellers from identity theft and making it easier for states to determine who is responsible for examining an asylum application

For VIS purposes, 10 fingerprints and a digital photograph are collected from persons applying for a visa. This biometric data, along with data provided in the visa application form, is recorded in a secure central database. 10-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

2.6 After your journey

Upon arrival, travellers may be subject to further checks, including an entry interview, 'random selection' etc. under similar circumstances as those described above for other moments of the travel process. However, in some cases the surveillance and control do not end there, and the data provided (PNR, VIS, SIS or EES data) continues to travel and may end up being part of a police investigation if one finds oneself or one's routines intersecting with suspicious or criminal activity.

Moreover, for those who entered a country for a fixed or limited amount of time (visa holders), the data processing continues until their entry file can be closed with an exit record. In the

meantime, the system can trigger alerts for over-stayers. Likewise, hand-held fingerprint scanners can extend the border to every corner of a territory, and perform the same level of control, verification and database checking that one may expect at a critical infrastructure in any other location. As Van der Ploeg has noticed, borders are also performed 'within a country's territory by surveillance activities that enact and maintain the demarcation between those who are entitled to be there and those who are not' (2011: 82).

As we will see below, technology extends the border outside the realm of the border crossing point and both inwards, into the body, and outwards, into every corner of a territory. In the context of the big data border, a border check ceases to be an event and becomes instead a never-ending process of database checking, matching and automated decision-making.

Section III: Implementation and social acceptability

Borders and mobility policies are increasingly taking on the character of a 'machine' that combines social and technical processes. There are many factors and actors involved in these processes, including high-tech, politicians, policy-makers, customs officers, border guards and the travellers themselves. In order to ascertain the nuanced ways in which technology mediates human interaction, and the often subjective quality of discrimination and human dignity, the third section of this report draws on the research conducted on mapping border data flows and establishing the socio-political context in order to explore matters of implementation and social acceptability. We aim to provide cues to determine what are the current challenges posed by the proliferation of data mining and matching processes at border crossings.

In order to do that, two methods have been designed to approach two key stakeholders in the process – border guards and travellers. In the case of border guards, the report focuses on those with a direct experience of working with automated border crossing gates, one of the most innovative and data-rich points of control at border crossings, where machines are expected to substitute for human personnel in the medium term. In the case of travellers, the report focuses on third country nationals travelling to the EU.

1. Stakeholders at the big data border: Target groups and research sites

1.1 Border guards

Two focus groups were conducted to explore the attitudes of border guards towards the implementation and uses of technology at the border. They were conducted in the Madrid and Lisbon international airports, with the aim of establishing a comparative framework to observe and identify latent variability and diversity among automated BCPs in different EU Member States. Spain and Portugal were among the first EU countries to introduce automated border control gates, and thus have had a longer experience with the transition to a fully automated border crossing experience (Smart Borders).

The focus groups gathered first-line border guards as well as high-ranking police officers responsible for managing automated borders. This proved to be the optimum method to capture the daily routine of border guards working with automated border technology, as it provided them with a free space to debate and discuss their ideas and points of view. The main topics of the discussion were listed in the focus group topic guide and included the following factors: the process of implementation of technology at the border, issues linked to social acceptability and decision-making at the automated borders (human versus automated/algorithmic), and the challenges and risks of automated borders.

Each focus group lasted an average of one hour and the audio was recorded after gathering explicit written consent from all participants. In order to guarantee the total anonymity of the participants a coding system was designed to identify each participant. The code was used during the focus

group and so none of the names of the participants were recorded. The signed consent forms have been detached from other research products and stored separately and securely at a physical facility. The recorded focus group were transcribed verbatim for the analysis of the content and manually coded to address the following research questions:

- How does current technology for automated identification affect human decision-making at the border, and vice versa?
- What aspects of the border-crossing process are appropriate to be delegated to algorithmic decision making? What are the limitations, challenges and risks of this?
- What is the societal impact of these technologies, especially in terms of the right to non-discrimination, dignity, autonomy and freedom of movement of travellers?
- How do they facilitate or hinder the social sorting and profiling of travellers?

The Lisbon focus group was made up of eight border guards (five male and three female) working at the first line of the automated border at Lisbon international airport. Regarding the longitudinal perspective of their experience as border guards, participants can be classified into two groups − one group of four male participants who started working at the airport border in the mid-1990s, and one group of four border guards (three female and one male) that took the position at the airport border after 2007, when the automated systems began to be implemented. Portugal introduced automated border crossing (ABC) gates in 2007, together with the electronic passport.

The heterogeneous composition of the focus group with regard to their previous experience at the border was crucial for the longitudinal and diachronic analysis and provides useful insight into the outcomes of the implementation of technology at the border. The relative inexperience of some of the participants, who were not familiar with the functioning prior to 2007, did not hinder the analysis, as their current routines involve working at different positions (traditional non-automated checking points, automated gates of ABC4EU, as well as second-line tasks) and they could all therefore add elements to the comparative and diachronic discussion.

The focus group in Madrid comprised five people (two female and two male). Unlike the Lisbon focus group, in Madrid the FG was integrated by high-ranking police officers working in management and organizational duties rather than by border guards working at the borders' first line on a daily basis. Four of the five participants belonged to the same working team within the Borders' Central Unit (three male and one female), and their main duty was to deal with and manage the automated border at the Madrid international airport. They coordinate, manage, solve problems and transmit instructions to the first-line border guards. Although they are working in the police headquarters and have an office-based working routine, they do also make scheduled visits at the Madrid airport BCP to support, monitor and supervise the implementation of the technology on site. One of the Madrid participants was not working in the aforementioned team, but oversaw the implementation of ABC technologies at different Spanish BCPs, organized border guard training and dealt with the communication between the different BCPs and the Borders' Central Unit in Madrid. Regarding their previous working experience, two of the male participants had been working at the Borders' Central Unit for the last six years, one male participant for two years, and the two female participants had recently taken up their positions (for less than a year).

Therefore, all the participants started to work in their positions at the Borders' Central Unit at the time of the introduction of the ABC technology.

1.2 Travellers: Third country nationals at the EU external borders.

Whereas the Focus groups in Lisbon and Madrid provided exploratory data about the outcomes of automated borders from the point of view of key stakeholders (border guards and police officers), during the Summer of 2015 a series of fieldwork observations were carried out at seven Border Crossing Points in six EU Member States to gather relevant empirical data from the perspective of the passengers.

The observation was conducted while carrying out a small-scale survey with 1146 randomly selected third country nationals on the impact of automated processes on fundamental rights. This was done in parallel with the deployment of the EU-LISA pilots. Besides conducting the survey, qualitative data was also obtained through informal conversations with passengers and border guards, as well as by means of observing the patterns, fluxes and border-crossing practices at each BCP. The survey was conducted in three airports (Charles de Gaulle in France, Frankfurt in Germany, and Madrid airport in Spain), three land borders (Sculeni and Iași in Romania, and Narva in Estonia), and one port (Helsinki in Finland). The target group were third country nationals (non-EU citizens) aged 18 years or older crossing an external border of the European Union (EU). Citizens from approximately 80 different countries participated in the survey but most of the respondents were Russian citizens (24.6%) and Moldovans (19.5%) that were interviewed at the BCPs in Romania and Estonia. In the other BCPs the population was more heterogeneous in terms of the citizenship, and included passengers form Asia (21%), Latin America or the Caribbean (12.3%), North America (9.5%), Africa (9.4 %) and Oceania (1 %). Besides that, 1.6 % of respondents where 'stateless' persons in Estonia. The interviews were carried out in airport check-in and boarding areas, in trains and train platforms and with travellers crossing land borders by bus, car or on foot.

The attitudes of the passengers towards the survey varied a lot depending on their experience concerning the two main topics or dimensions of the questionnaire: (1) automatized systems of identification and (2) border crossing. Although the survey addresses the intersection between these two dimensions, passengers generally stressed one of the two topics according to their previous experience. It was observed that the travellers' previous experience with the topics of the survey (technology and/or border crossing) determined their willingness to participate. In some cases, participation was incentivized due to previous experiences with automated systems of identification (because they had encountered it before and, thus, it made sense for them). In other cases, it was the border experience itself that propelled participation. These choices and preferences are socially and cultural grounded and based on travellers' past experience. Therefore, different socio-cultural variables that shape individuals' experience (mainly place of residency, citizenship and degree of mobility) were found to be relevant to the passengers' approach to the survey and the interaction with the research team and topics.

It is also worth mentioning that the physical spaces where the survey took place created an obvious bias in the kind of travellers that were approached. Specifically, VIP areas or fast lanes could not be accessed for the purpose of this study, and due to their use of privileged 'fast lanes', it can be

assumed that affluent frequent travellers or wealthy citizens are under-represented. During the fieldwork and observation, the proliferation of reserved areas for specific profiles of travellers who can 'opt-out' of common areas was very obvious and confirms a growing trend establishing a two-tier border policy, especially at airports. The premium seating classes seem to be extending from the aircraft to the whole border-crossing process, mirroring stratification processes elsewhere and reproducing social inequalities.

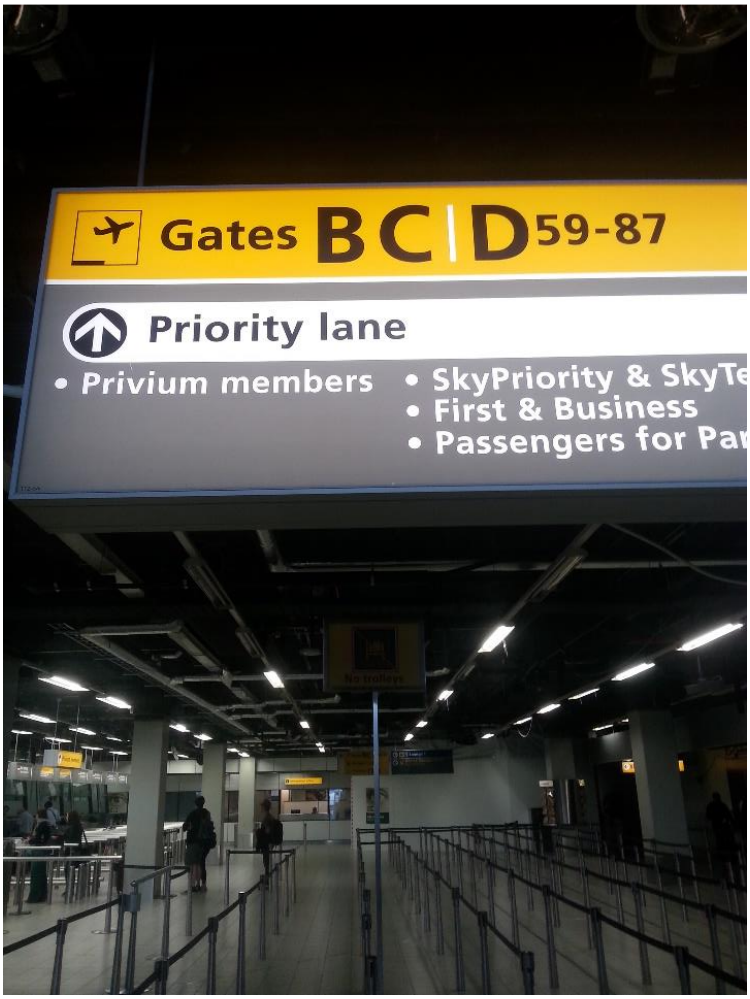

Figure 9: Sorting by privilege at Schiphol Airport. Source: authors' elaboration.

In the following pages, some of the survey results are presented. Emphasis will be places on the observation ofand informal interaction with survey respondents and travellers in general.

2. Big data border: Implementation, automation and profiling

In the following pages an analysis of the focus group with border guards and the fieldwork (observations and survey) conducted with travellers is presented and discussed in keeping with the four main topics that arose from the empirical data: implementation, automation, profiling and discrimination. These emerge as crucial elements of a future research agenda on the impact of technology on borders and border-crossing processes, with the aim of establishing practical solutions to the concerns that are raised from a social, policy and technological perspective; the goal is to study, address and improve the feasibility and desirability of the technical changes being introduced at the big data border.

Firstly, the implementation of digital borders at the Lisbon and Madrid airports is discussed from the perspective of borders guards, with a focus on how they see their role changing with the introduction of automation technologies in their workplaces. Secondly, we reflect on the realities concomitant to the automation of borders as they are perceived by both border guards and travellers. In this context, two main elements emerge: the social and ethical constraints derived from technical problems, and the structural and technological privileges (discrimination of *bona fide* travellers) generated by the way automated borders are designed and operate in practice. Finally, data related to the present and future impact of technology on the process of sorting and profiling is addressed from both the perspective of border guards and the point of view of third country nationals crossing EU external borders.

2.1 Implementation

The first implementation of an automated border system at Lisbon airport took place in 2007. With the perspective of almost a decade since then, border guards who had been on duty since the mid-1990s described the gradual transformation of their job with respect to the development of technology and border-crossing policies:

> *The distinction between the non-electronic and the electronic border, and between Schengen and non-Schengen, marked an obvious stage here at the airport − especially in our work. In the electronic part, things were implemented progressively. I mean, if we compare the current system with the one which was implemented in 2007… It was archaic… But at that time, it was extremely innovative. Passengers were amazed about the way it worked.* ***It was almost like magic***. [Emphasis added] (A5 - Lisbon, Male in his 50s).

Considering the above quotation, we can see how a diachronic perspective is crucial when researching the implementation of new technologies to understand the extent, meaning and nuances of the notion of 'novelty' for non-experts. Participants explained that there have been changes and improvements since 2007, and how today both travellers and border guards are beginning to get used to the technology employed. Regarding the process of implementation of technology, border guards continually brought up the issue of lack of training and emphasized problems of communication with the travellers that create difficulties in their daily activity at the border and may infringe on the rights of the passengers.

2.1.1 Lack of training

> *I think that the first system implemented wasn't too clear. I mean, even on our side, as border guards with little training, we also had problems using it. Of course that with experience, and through experience, we can reach it. It took a long time at the beginning. It was a long process.* (A4-Lisbon, Male in his 50s).

None of the eight participants in the Lisbon Focus group had ever received specific training on automated borders (technical, ethical or of any other kind) − neither at the beginning of the implementation nor later on when problems and limitations became evident. All of the participants agreed that during their daily work routines they had learned by experience, by making mistakes, and by trying to understand and improve the way passengers use the system. However, it's important to note that while automated border-crossing technologies have become a day-to-day reality for border guards, that is not the case for infrequent travellers[27].

Higher-ranking border police officers in Madrid spoke of a different situation regarding their training and the implementation of automated solutions in Spain. According to these officers, specific short-term training seminars are being held on-site at each border point where the system is being implemented. The training seminars are conceived as demonstrations to show how to use the system and to encourage border guards and high-ranking officers to promote their use. During these sessions, an officer from the Central Borders Unit explains the operational dimension of the new system from the perspective of border guards while an engineer from the developing company presents the technical side. According to police officers, training is much more effective when border guards are already familiar with the system, as they feel more confident about raising questions and problems.

All the border guards from the Lisbon focus group agreed that training would have been very welcome and would have made their job a lot easier. However, from their point of view, the lack of training is intimately related to the lack of personnel to assist and help passengers crossing the border using ABC gates, which was identified as a constant problem during the focus groups. For instance, there are twelve automated gates at Lisbon Airport but only one border guard to supervise the flow of passengers from a booth located at one of the ends of the gates. Participants clearly expressed how, in order to improve passenger flow, more human agency (more border guards) are needed to monitor the flow from the booth and also provide instructions and assist passengers to cross the border. This is the set-up in Madrid, where participants confirmed that two border guards are enough to control ABC gates when machines are working properly and travellers are using the automated gates correctly. However, even in Madrid, when technical problems arise and/or passengers make mistakes when crossing the border, the lack of personnel becomes a problem:

[27] As we will see in the next sub-section, there are crucial inherent technical privileges for those travellers for whom crossing borders is part of their daily job.

It's sometimes a bit overwhelming because there's too many doors and a minimal and scarce amount of personnel. So, when a door is blocked and a passenger does not know how it works, and another one gets an alert, a big fuss can happen there. (A4-Madrid, Male in his 30s).

Therefore, from an organizational and structural point of view, the discussions of border guards seem to challenge one of the main justifications offered by the supporters of automated borders, which is the rapidity and ease of passenger flow.

2.1.2 Machine-based societal interaction: Communication and interaction with between border guards and travellers.

Border guards working at Lisbon Airport agreed that one of the main changes that big data borders have brought about is the loss of contact and communication with passengers, which generates a crucial transformation of the borders themselves and the border guards' function. In the last part of this section we will deepen the analysis of border guards' changing role and responsibilities in relation to sorting and profiling practices. Here we merely want to illustrate how they perceive their role at the border in the context of machine-based societal interaction.

The communication factor arose repeatedly throughout the discussion in Lisbon and was raised by each of the participants without exception. Although Madrid participants did not emphasize this problem to the same degree, it is important to bear in mind that they did not work on the first line of the automated gates. The analysis of the focus group revealed that border guards are still occupied with the stage of technology implementation and react ambivalently to the new situation. On the one hand, they retain a nostalgic point of view (missing their previous role and authority in interaction with the passengers); on the other hand they try to enhance the relevance of their role in spite of the machine-based border-crossing reality.

When discussing these issues, border guards suggested alternative strategies to make the most of automated processes. Border guards at Lisbon Airport mentioned that they would like to have a closer interaction with passengers to act as liaisons between the citizens and the machines. In order to mitigate the physical distance between border guards and travellers, a new monitoring system is being implemented in some automated BCPs in Spain: instead of being inside the booth, border guards monitor the system using tablets that allow them to move around ABC gates and, thus, to interact more with the passengers, assisting them and resolving communication problems explained above. If anything, the analysis points to the need for increased user-operator-machine interaction, and not for the elimination of human operators.

When discussing ways to better communicate the boarding crossing procedure to travellers, FG participants stressed the need to add a verbal 'human-like' communication within the automated border context. They reported that the lack of an 'interpersonal' relationship between travellers and border guards, as well as between machine and passengers, leads to substantial problems when crossing borders. According to the FG participants, verbal communication is one of the main things missing in automated border control. As illustrated by the quotation below, border guards envisage two alternatives to improve verbal communication. On the one hand, they suggest adding a verbal

interaction between the machine and the passenger (voice instructions leading to a 'humanization of the machines') and, on the other hand, they strongly recommend reverting to a more traditional procedure of communication between passengers and border guards.

> *In terms of the electronic border being user-friendly, I think that tfor us border guards, the one implemented here in Portugal is easy to use. For the passengers, not so much. It could be more intuitive; we might have been given the possibility of talking with the passengers from inside the booth, which we can't do. The machine itself could provide voice instructions to the passengers, which it doesn't. And all that would surely make it easier for the passengers to use the electronic borders.* (A3 – Lisbon, female in her 30s).

This highly relevant communicative dimension emphasized in the quotation above offers insight into the relationship between machines and individuals (and border guards and travellers), and underscores decisive factors that will determine the direction of border crossing and the features it will possess at present and in the near future. What is in question here is the relationship between the three types of social actors taking part in the border-crossing process: travellers, border guards and the machines. Whereas nowadays we are facing a hybrid border system involving human and machine-based interaction, we will want to consider the next step in this process and how the automated border will evolve in relation to this communicative and societal dimension. And from this perspective, what is the role of humans (in this case, border guards) within the sphere of the machine-based borders? Who has the authority and the power to control mobility across digital borders?

2.2 Automation

During the fieldwork conducting surveys addressed to third-country nationals in seven border control points, passengers were often eager to comment on their experiences with automated systems of identification both before and after answering the survey. Given that automated border checks and their societal impact is a relatively new and unfamiliar phenomenon to most, it is not surprising that those travellers that had some knowledge or experience with biometrics in their daily life were more willing to participate in the survey and share their views. In some cases, however, respondents' previous experience with biometrics had not occurred at a border crossing point but in other spheres of their life.

Whereas some people had experienced the use of biometrics when crossing borders, other passengers had never encountered an automated border control and, thus, they evoke other aspects of life related to biometrics and automated systems of identification. Hence, besides the experience of having their biometrical data registered when crossing borders, or when applying for a passport or an ID card, other passengers recounted their experiences of biometrics and technology in other spheres.

We had that [fingerprint enrolment] in my workplace for some months. The director thought it would be a good tool for monitoring the workers and securing the area, but after the trial we didn't use it anymore. There were too many errors and problems with the system so I think that it is very important to have a good backup plan when some problems arise. If it was like this at my job I guess the same problems might happen at borders (Passenger at Charles De Gaulle airport. Chinese citizen, male, 40s).

2.2.1. Technical problems and fundamental rights of the travellers

The quantitative analysis of the survey confirms the ethnographic observation quoted above. Like the Chinese citizen who recounted his experience with the technical problems of using biometrics in the workplace, a relevant percentage of survey respondents expressed their anxiety at the possibility of a false positive while crossing the border. Thus, one of the main concerns of passengers related to smart borders is the infringement of their right of mobility when machines and technology do not work properly (see Figure 10). Similarly highlighting the lack of trust in a possibly flawed machine-based decision, travellers also believed a mistake in their data would not be easy to correct (see Figure 11). For that reason, even those respondents who believe machines should be implemented for the sake of neutrality also feel more confident when somebody (i.e. a border guard) is present and able to solve problems that might arise.

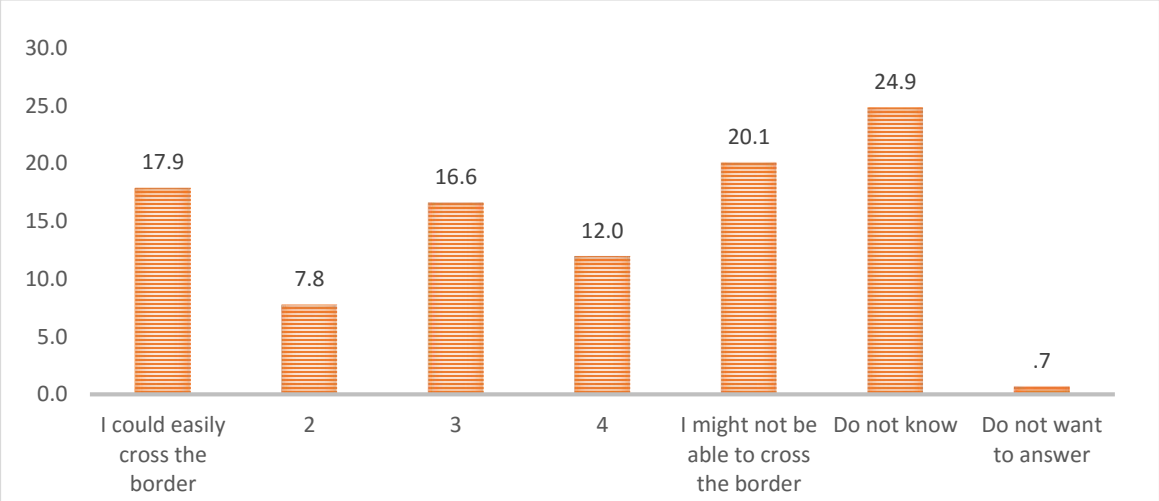

Figure 10: Ability to cross the border in the event that the technology does not work properly, average of the seven BCPs surveyed (%).Question: *In the event that the technology does not work properly, to what extent do you believe you would be able to cross the border?* N = 1,118

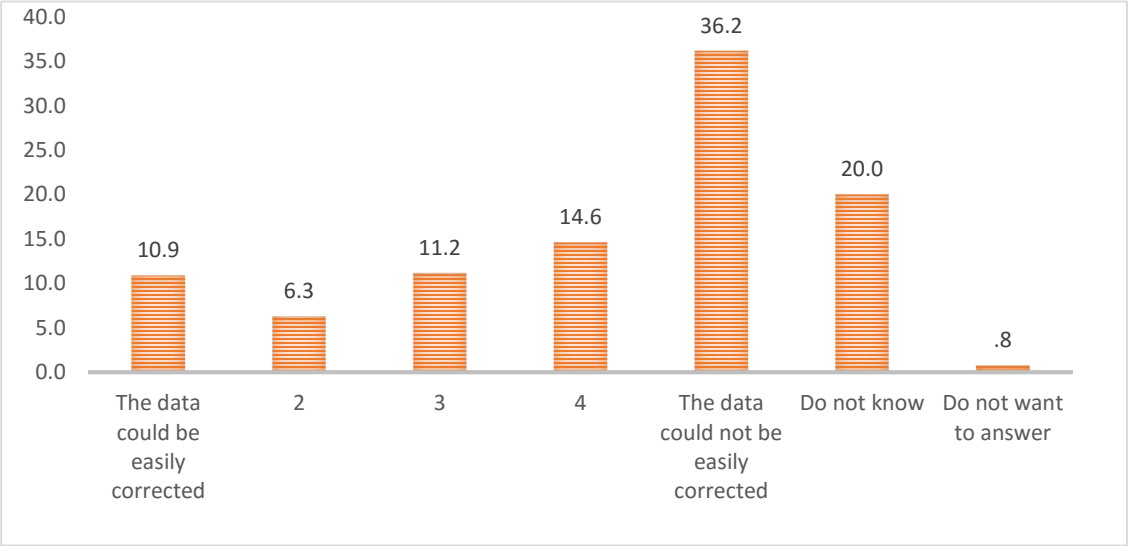

Figure 11. Opinions on the possibility of correcting the data in the event of an error in the personal data, average of the seven BCPs surveyed (%).Question: *In the event that there is an error in your personal data when crossing the border, for example if your biometrics do not match with your name, do you think that your personal data could be easily corrected?* N = 1,109

Our empirical findings confirm what several authors have noted regarding the vulnerability of travellers – and especially migrants − towards digital identification and authentication by means of electronic databases (Dijstelbloem 2009, Dijstelbloem et al. 2011, Van der Ploeg 1999, Van der Ploeg and Sprenkels, 2011, Marin 2011). Dijstelbloem (2009: 14) mentions that personal data is not always removed from the SIS (Schengen Information System) according to the conditions of use, which can lead to a wrongful refusal of entry. He also states that aliens have less chance of obtaining rectification of the mistaken data than native citizens of a country. Therefore, it is common for 'migrants to have a weak position in the everyday practice of migration policies with little means to check or to correct data that are gathered from them' (Dijstelbloem at al 2011: 15).

This is consistent with opinions expressed by border guards in informal settings about the credibility of automated decisions versus human decisions. Generally, concern about the difficulties of contradicting the technology were raised in different settings and point to an important problem: while social processes are in place for people to explain why they may have been wrongfully accused by a physical person, and thus to seek redress or clarification, such processes do not yet exist for false positives rendered by technology, thus creating uncertainty and a feeling of powerlessness.

In the course of the focus groups, border guards also reported several technical problems related to the automated border gates, including issues related to the interface and mechanism of the machines (doors blocked, failure of technology systems to read documents) as well as mistakes by technology in identity authentication through biometrics.

I think when it works well it's better than a manual point, but ***when there's a problem, it gets complicated****, since in [Madrid Airport] there are 6, 7 or 12 gates in each terminal, and only 2 colleagues working (…) When two or three doors are blocked, there is a passenger who is not supposed to enter - because they are not from the European Union - and another one with an alert…. Then it's a mess and very stressful. And it's true that it has its good side, but it also has its other side. You can get very stressed out working there.* [Emphasis added] (A2- Madrid, Male in his late 30s).

The novelty of data processes and the black-box effect mentioned earlier on in the report, however, point to the need to improve the methods of enquiry in the relationship between technology and society. Using biometrics at BCPs, for instance, has consequences very different from those resulting from their use in a workplace setting. Lack of awareness of the data processes that are hidden behind a fingerprint scanner or a PNR form means that peoples' opinions can change considerably depending on the associations they make or their past experiences, thus affecting the robustness of any survey results.

2.2.2 Structural and technological privileges: Automated borders addressed to 'technology-ready passengers'

The analysis of the focus groups, as well as of the observations and the survey of travellers, pointed out how automated borders are not designed to treat everyone equally but involve privileges and discrimination according to travellers' age, mobility experience, as well as ethnic and cultural background. Hence, the empirical findings challenge the notion that automated borders might offer equal and non-discriminatory treatment to all citizens. Rather, as we will see below, automated borders are creating new spaces of discrimination that facilitate the mobility of a privileged elite – at a price.

FG participants agreed that not everyone has reacted in the same way to automated systems, and emphasized two main factors influencing this relationship – frequency of use and age. According to the participants, whereas frequent travellers tend to prefer automated systems and do not have any problem using them, other passengers who cross the border less frequently feel much more vulnerable.

A7: Frequent flyers use the electronic border very easily. Because they have used it many times, they know how to use it, they know they can't wear glasses, that they can't wear hats, that they must stand still on the mark and look at the camera, that the passport can't have any cover because the chip won't be in the right place to be read… They know all that and they use the machine correctly and quickly. And it usually works the first time. There is another type of passenger… … It's much harder. (A7-Lisbon, female in her 30s).

It can be argued that current automated systems for border control benefit − in terms of time and flexibility − those frequent travellers who are already used to, understand, and know how to deal

with the whole security processes. However, when occasional or less frequent travellers go through the automated process, different problems arise, related to the way information is given and the lack of a communication at the sensitive moment of passport control. 'Why do I have to leave my fingerprints here?' 'What are they going to be used for?' are, according to border guards, some of the most common questions passengers ask when facing electronic borders for the first time.

These problems are strongly associated with the way automated borders are designed and implemented, as well as for whom they are intended. During the FG, participants were asked to assess the signs and warnings that currently inform travellers on how to use the automated systems, and Lisbon participants agreed that current systems do not fulfil their goal − travellers are confused and do not receive proper and clear information when using biometric, automated border gates.

We might suggest that automated gates are designed with frequent travellers in mind and that this introduces a fundamental bias in the technology, which therefore enacts a process of 'natural selection' by which those who are young, tech-savvy and affluent (able to travel extensively) have more options than the rest. As Franko Aas, Oppen Gundhus and Mork Lomell state, 'airport surveillance is far more than simply a task of screening and checking people, but is also about educating passengers about their security responsibilities, changing their consciousness and eventually turning them from 'security-unready' passengers to 'security-ready' passengers' (2009: 5). Applying this perspective to the analysis of the Focus group we could say that the adoption of technology at the borders adds a further step to the specialization of mobility, as it is mainly addressed to those young and 'technology-ready' passengers who cross borders often.

Age is another major factor influencing the use and function of automated processes. FG participants discussed how older people are the most vulnerable group, the one that needs most assistance going through automated processes. In their opinion, current information and practical difficulties mean that, effectively, the elderly are excluded from the system, and when they attempt to cross electronic borders their rights to information are not respected. The form (design, function and arrangement) of automated border crossing points does not resemble traditional passport control procedures, and so the level of confusion is more evident in this age group.

> *A7: I get the feeling that older people don't realize what they just did in the machine.* (A7-Lisbon, female in her 30s).
>
> *A6: Otherwise, they wouldn't do it.* (A6-Lisbon, male in his 50s).
>
> *A7: They get in there, they walk around, they turn their faces because they are told to… And when they get out, they don't even realize that they passed a border control.* (A7-Lisbon, female in her 30s).

The statements of the border guards were confirmed by the passengers themselves. Older people travelling alone had significant problems in understanding the conditions, meaning and state of digital borders and, when crossing automated border points, needed to rely on younger relatives or acquaintances travelling with them. Even when elderly passengers were asked to answer the survey, they would refuse by saying that they 'don't understand technology' and, if travelling with younger people, they generally passed the questionnaire to them.

Border guards consider that the current warnings and signs are not functional and that this situation is prejudicial to elderly passengers and also to those travellers who are not habituated (i.e. not frequent travellers) and makes the work of the border guards more complicated in comparison with the traditional system.

Lisbon participants also agreed that visual information outside and inside the gate/machine is not well presented, and passengers do not have a precise and unequivocal idea of the procedures to follow when crossing the border. Hence, border guards in Lisbon and police officers in Madrid both reported how some passengers attempt to cross the border through ABC gates when they are not eligible (i.e. adults with children, third country nationals, passengers wanting to exit the airport or to enter international flight zones, etc.), or do not proceed correctly when they are already inside the gate/machine (making confusing movements, not removing glasses or hats, not looking at the camera, moving, etc.).

> *It has failures […] like the issue of the communication with the passenger, the issue of the feedback that the passenger has regarding the process, or what is happening. Many of them aren't even aware that an image of them is being collected, and therefore they aren't concerned to hold still and look at the machine. They keep moving, asking why it doesn't open… The matter of the EU or not… Many people from other countries try to go through it. In other words, identifying more clearly who can and can't use the system [is important].* (A4-Madrid, Male in his 30s).

Communication failures have a particular impact on minors. According to border guards, one of the main problems triggered by the unclear information about automated controls is experienced by those travelling with minors. Although automated border crossings should neither be used by minors nor by the adults accompanying them, the border guards say that this is a common situation. Given that the information about this limitation is not clear, adults only become aware of it once they enter the gate/machine.

> *And I would like to add that the matter of the minors must be clearly explained, because the electronic border often ends up separating parents and children. Despite the fact that it's written that people who are less than 18 years old can't use it, it happens frequently. Parents use it and they think their children will be able to pass, and they can't. Then, there is a great confusion generated in the line behind them and they can't see where their parents are.* (A8 – Lisbon, Female in her 30s).

Finally, there is also a need to focus and attend to different attitudes depending on specific socio-cultural contexts. African women carrying babies on their backs were a concrete example indicating how the system's design does not take socio-cultural diversity within the EU into consideration.

And people with minors on their backs. Minors on the back are very complicated. African people, African ladies who have those things… I can't remember the name… Small babies who are only months old, come on their mothers' backs. And the mother enters the border, and the machine doesn't detect the presence of the baby. It isn't easy at all. (A6-Lisbon, male in his 40s).

2.3 Profiling and discrimination

Profiling is the main discrimination activity at border-crossing points. As we have discussed in the theoretical considerations (Section II), the function of borders consists in establishing a categorization of citizens by means of different kinds of socio-technical apparatus. Given the link, commonly accepted nowadays, between security and migration polices, profiling relates directly to the role of border guards in their working sphere, and to the rights of migrants in their mobile trajectories. First we will present the border guards' perceptions of the changing nature and methods of profiling at the border, and then we will give a voice to third country nationals by presenting the ethnographic data gathered from those who felt unfairly treated by border politics – profiling – when entering the EU.

2.3.1 From analogue to digital profiling

We have described above how border guards perceive that the major transformation of their role is due to the lack of interaction with passengers, who increasingly face the machine alone. However, interacting with a human operator when that human operator is a border guard or police officer has its own complexities, which were acknowledged by the FG participants. Machines, they mentioned, could offer increased feelings of objectivity or neutrality.

Sometimes it's faster for them and less… how to say? Maybe because they interact less with police and, I don't know, they get less nervous or... Because at the end it's just a machine; it's like an automatic teller machine. We could say it's less aggressive than having a police officer looking at you to see if you have a passport or not, as if he's evaluating you (A2 – Madrid, male in his late 30s).

With the proliferation of automation and data-induced decision-making, the role of border guards is obviously changing. Identification and control tasks that previously were only performed by border guards are nowadays a process shared between machines and humans. FG participants acknowledged a positive transformation in their role, from an authoritarian and controlling function to a more supportive one. But they also mentioned less positive outcomes and the limitations on procedures that machines 'cannot do as well as humans', namely, sorting and profiling.

Border guards are aware that their job description, duties and responsibilities are transitioning to an unknown future role. The leader of the police officers' team at the Madrid Borders Central Unit

mentioned that, with new technologies at the border, police responsibilities have been transferred from actually executing the border crossing to merely overseeing or monitoring it. First-line border guards in Lisbon went even further, saying that:

> *With the machine, we don't do our job anymore. We just help people to do something. 'Put the passport here.', 'Look at the camera.', 'Okay, you have to go back.' So, you are not doing your border guard work, okay? But you are helping someone to pass through a system. Okay? It is a self-service* (A6 – Lisbon, male in his 50s).

With this new supportive role, police officers have detected a change in the way travellers perceive them − from 'somebody inspecting and controlling you' to 'somebody able to help you'. Statements like this point to a shared vision of the inevitability of the technological transition. Machines and data are here to stay. FG participants seem to acknowledge that border controls are becoming increasingly liquid and diluted in their spatial and material form. Consequently, electronic borders and the use of big data is leading to an increasingly imperceptible and diluted, yet constant, border control. For FG participants, an important difference between human and machine interaction is the less (overtly) invasive nature of automated control and biometric data mining technologies, which they deem to be a positive thing.

Border guards' comparing their routines and ways of working to the automated processes was a fixed feature in the focus group discussions. Participants also demonstrated suspicion towards biometric and facial recognition, reporting different anecdotes of fraud that were not detected by the machine (passengers using other people's passports, recognition of the picture on a passenger's T-shirt, etc.). All participants agreed that sorting and profiling were duties that were better performed by humans, and that should be a cornerstone of the further development of automated borders from a fundamental rights perspective. One of the border guards' main complaints (being located in a booth away from the traveller flow) was related precisely to their inability to profile passengers. They 'cannot do their job' because they cannot see the passengers. In this new setting, they have lost control and it is unclear who is replacing their traditional profiling duties:

> *Because we don't have a clear idea about people's profiles. Because we are far away, we don't talk to them, we don't see if they are nervous or not… We don't get to see their profile* (A7-Lisbon, female in her 30s).

In Lisbon and Madrid, participants referred to the sort of cues they looked for when profiling passengers − nationality, appearance, clothing, attitudes (way of walking and approach, etc.). These are the main visual elements that border guards rely on to sort passengers and determine whether they constitute a threat and what kind of security controls (identity and database check) need to be performed.

> *From my point of view, I continue emphasizing that… there is the issue of profiles. For example, a Japanese person and a Senegalese are not the same. A Japanese person, you*

know, won't be a threat for illegal immigration. He fulfils all the requirements for staying a certain amount of time here, and once he is done and finished he will go back. Whereas the Senegalese, potentially, I don't want to generalize at all, but seeing the situation of the country [Senegal] you know he will probably remain here, so you will do an interview to see the real aim of his trip, etc. (A5 - Madrid, male in his late 30s).

I really think we do a better job than the e-gate. The human component is really important. Because we can see the profile, we can see if the person is nervous… The clothes that the person is wearing, the way the person acts… And the machine cannot do that. (A6 – Lisbon, male in his 50s).

The transference of profiling tasks from the decision of border guards to data-intensive technologies based on database checking and simple algorithmic decisions has implications that do not seem to have been properly addressed. While border guards defend the added value of their 'human touch', an over-reliance on ethnic profiling and cues related to status would point to the need to develop more objective solutions for border profiling. On the other hand, the technological solution to this problem tends to rely on mass surveillance, which is also detrimental to fundamental rights and values. Border guards showed a certain degree of frustration at their algorithmic substitutes:

The relationship between people is important, because I am on this side [of the border] and on the other side, I feel certain problems, that will determine if the person can pass or not. The machine doesn't define that. (…) The machine just looks to see if it is the right person or not, but doesn't go further. (A6 – Lisbon, male in his 50s).

High-ranking officers in Madrid, however, seemed to accept that the future lies in improved automated systems, not improved human processes:

In the future it is also expected that systems will be more developed for monitoring passengers once they have crossed the border. To know how long he stays. So… so… more effort will be devoted to control the entrance and exit of the territory. So the profiles that we mentioned before will be more deeply analyzed to issue risk profiles. And then according to the reports more or fewer people from a specific country will be allowed to cross the border or not to cross it (A4- Madrid, male in his late 30s).

Overall, the FG discussions provide a glimpse of a situation that is transitioning from manual to automated processes, with data playing an increasing role. It is worth noting, however, that for all the data flows involved, communication, information and clarity remain a challenge for automated systems. Moreover, while the biases in current manual procedures are known, most of the technological biases related to sorting and profiling are either unknown or remain unaddressed.

Policy-makers, border officers and engineers have thus a crucial responsibility in the future development of border technologies.

2.3.2 Discrimination beyond the technological debate: EU border-crossing experiences of third country nationals.

During the fieldwork with third country nationals, we realized that people who lead a highly mobile life had different attitudes towards the survey than those who travel occasionally and do not have a highly mobile existence. Passengers from countries that have a long-standing history of border crossing from and to Europe were less interested in the dimension of technology but were eager to express their opinion on discrimination and profiling at borders.

The following ethnographic vignette is illustrative of the passengers' willingness to participate in the study due to historical and present-day inequalities when crossing the external EU borders. In this case, a Latin American woman felt compelled to take part in the survey as a way to voice her negative experiences.

> *I was approaching the passengers who were waiting in the sitting area next to the gate before the flight was ready to board. The third passenger in the row was a woman in her 50s who was staring into space and looked tired. When I approached her and started to speak to her she immediately told me she wanted to rest and didn't allow me to continue with the introduction of the study. I continued the sampling process and approached the next third passenger who was sitting at the other edge of the bench. I was luckier here and I could proceed with the interview. However, when I finished the interview with the second passenger, the first woman called to me and told me that after hearing my conversation with the other passenger she had decided to take part in the study. She emphasized that she was not interested in 'this technology thing' but that she wanted to take part of the study to express her feelings towards the unfair situations she and her family have had to face when travelling and crossing borders (Fieldwork notes, 8 August 2015, Paris).*

As seen above, border guards frankly admit that the cues for suspicion are often related to ethnic and status traits. It is thus easy to infer that certain groups and people feel the impact of profiling more than others, and for reasons that are not related to any objective risk analysis. BCPs, therefore, tend to reproduce the inequalities and the fragmented structure of society through both their physical space (which distinguishes between privileged and non-privileged) and profiling practices. These inequalities may relate to economic status (i.e. fast lanes accessible upon payment of a fee), citizen status (requirements for visas and border crossing documents are very different depending on the nationality of the passenger), as well as other variables such as ethnic or social class-related assumptions.

During the fieldwork, Latin American citizens were the most vocal in their interest in taking part in the survey as a way of expressing their complaints about the treatment they received, followed by African citizens and people from Arab countries.

Whereas in airports inequalities based on citizenship involved a myriad of particular cases that were mixed with global and commonly-shared assumptions and clichés, we were able to observe particular and localized discrimination processes related to citizenship when doing fieldwork at land border-crossings. In the same way that air travellers who had experienced ethnic profiling were more willing to participate in the study and express their views, Moldovan citizens who live in Spain or Italy and were queuing at the Sculeni BCP in order to enter the EU also used the survey as an opportunity to voice their complaints. At the land border between Russia and Estonia, it was 'stateless' citizens holding an 'alien passport' issued by the Estonian government who showed interest in participating, eager to report the situation of the 160,000 Russian-speaking non-citizens who were put in limbo when Estonia joined the EU.[28]

Finally, regarding the interest and willingness to participate in the survey on the topic of border crossing itself (rather than the element of technology and biometrics), it's also important to take into consideration that the fieldwork was conducted during the Syrian refugee crisis. It was noticeable that when introducing the survey to potential respondents, references to 'borders' and 'EU' were immediately linked with a situation that was making headlines at that time. In one instance, a person who had managed to arrive at an EU airport irregularly used the survey to ask for help and information on how to request asylum.

The diversity of situations encountered during the fieldwork points to an additional matter of concern – how can technological solutions take account of the diversity of situations that people find themselves in at the border? If carrying a baby in a non-Western way renders the system useless, as seen above, how will the complexity and diversity of national affiliations and situations be managed technologically?

In the previous section, border guards were asked to assess the benefits and costs of transitioning from human control to automated control. As we saw, FG respondents tended to argue in favour of the need for the 'human touch', while at the same time admitting to the application of cultural and ethnic biases when profiling travellers. During the survey, respondents were asked what their preference was (human or automated) with regard specifically to discrimination. The quantitative analysis of the survey shows that more than half of the sample (60.9%) believes that automated systems of identification at the border could cause less discrimination than border guard checks (see Figure 12). Since most people's experience with biometric checks and their own built-in bias and error margins is still small, the results point to complaints about current practices rather than predict a smooth proliferation of automated systems and their social acceptability, especially among the groups that may be more affected by those biases and error margins. The results are, nonetheless, highly relevant.

[28] These individuals are being forced to choose between: learning a new language and passing an exam to acquire Estonian citizenship; applying for Russian citizenship and thus surrendering the benefits of EU membership; or remaining stateless with limited political access and foreign travel restrictions.

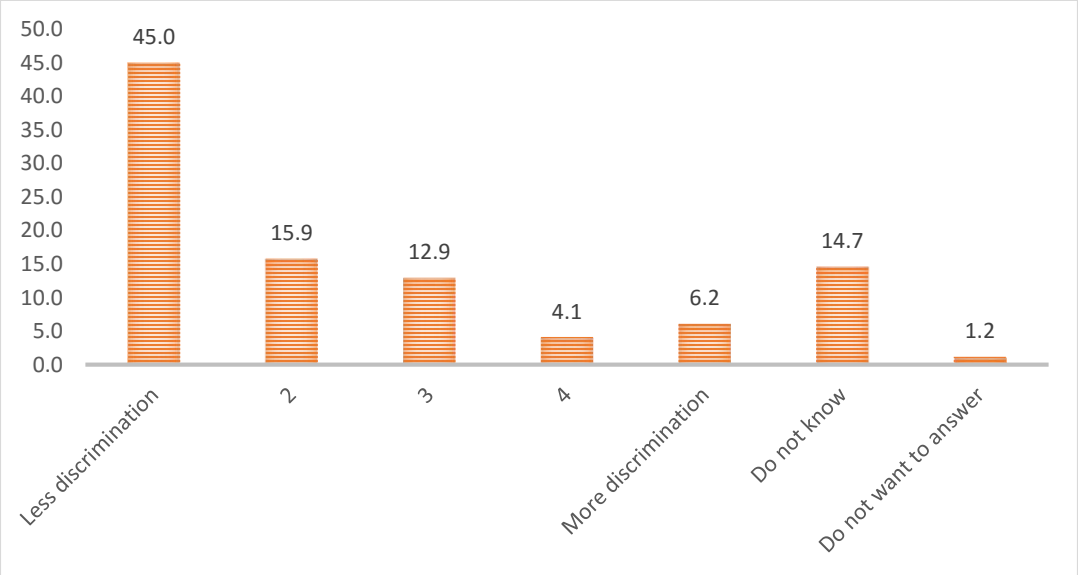

Figure 12. Travellers' opinions on the extent to which automated systems cause more or less discrimination, average of the seven BCPs surveyed (%).Question: *Do you think that automated systems could cause more or less discrimination compared to checks done by border guards? By discrimination we mean when somebody is treated unfavourably compared to others because of their skin colour, age, sex, sexual orientation, disability, ethnic origin, religion or religious beliefs*. N = 1,089

Conclusions and recommendations

The aim of this report has been to explore the intersection between rights, technology and discrimination at borders, with a specific emphasis on data processes and flows. Its main conclusion is the need to look at the new dynamics that emerge in data-rich ecosystems and account for how they interact with existing processes and expectations. In doing so, the report has mapped border-crossing data-flows and situated them in relation to broader developments in how borders, bodies and the notion of citizenship are being redefined by and through the impact of technology. A taxonomy of rights and values to take into account when looking at the societal impact of data-driven processes has been suggested, and the results of two empirical exercises with different stakeholders presented.

As mentioned at the beginning, the goal of this report is not to provide answers, but to point to the right questions. These can be classified and summarised as follows.

1. Methodological challenges

Exploring the relationship between technology and society and rights and values is no easy task. The long-term effects of technology and data-driven processes are difficult to grasp and, in the absence of a proper public debate or knowledge about how technologies work, people's opinions and responses to surveys or other traditional methods of enquiry are highly volatile. Often, researchers cannot escape the feeling that they are imposing the subject onto those being interviewed, who usually do not have formed opinions on technological issues. This was certainly the case while conducting the fieldwork for this report, and has been the case in the many related research projects the authors have been involved in. The resulting picture of traditional attempts is often contradictory, characterized by respondents' lack of trust in the protection of, and control over, their personal information, combined with a general perception of usefulness of the technologies involved in data mining.

There continue to be, however, very valuable insights to be gained from such exercises, and hints as to what future direction to take in order to disentangle the relationships and effects among technological decisions, social processes and rights. Asking citizens about technology can reveal cultural or age differences, for instance, as was the case in this research. The challenge that emerges is the need to improve the design of the tools used to explore the relationship between technology and society, in order to be able to get into the black box of the relationship. If the long term effects of the routine collection of personal information are to be explored, and new policies and regulations drawn up, scenarios will need to be designed to grasp how people may feel once they become familiar with the specifics of technological development, privacy and the fundamental rights and values that are at stake. More efforts are needed in this direction.

2. Fundamental rights

The research shows that automating border-crossing process is not just a matter of convenience. Data changes the nature of border-crossing by expanding the border and turning border control into a continuum. This can affect people's mobility and perception of others, as well as have an impact on a myriad of fundamental rights and values. Being able to assess these impacts and foster awareness of how their data flows will affect citizens is crucial to the development of responsible technologies. Improved methods of societal impact assessment should be designed and implemented at critical infrastructures such as BCPs to better account for the possibilities, limits and challenges of automating border crossing. Privacy Enhancing Technologies, as well as policy assessments and acceptability studies can contribute to better integrating fundamental rights and values into the design process and data flows of new technologies.

3. Policy recommendations

Throughout the report, matters related to information, profiling and implementation have frequently taken centre-stage, and they emerge as the main points of concern.

The empirical research has shown how information and knowledge is one of the weaknesses in the implementation of automated borders. As we have seen in the analysis of the border guard focus groups, the ethnographic observations at the BCPs, as well as in the quantitative analysis of the survey with passengers, automated borders are surrounded by a sphere of distrust due to the lack of clear and accurate information about the data life-cycle, as well as the ways in which mistakes might be resolved. Information and communication channels related to different projects aimed at introducing technology and biometrics at borders are, at present, insufficient and may create feelings of vulnerability. Hence the transparency of the process related to the data collected needs to be improved.

Profiling and discrimination are also a major concern in the context of the big data border. While surveyed travellers seemed to prefer automated controls over human checks, the research reveals that technology and the data it produces can also be biased. As shown in the report, 'smart' border processes have often been aimed at middle-aged, affluent and frequent travellers. Older people or people with less travelling experience can be perceived as a problem by those responsible for the technology the by the technology itself. Taking account of the new forms of discrimination that emerge and are made possible by data-rich environments is a clear and urgent challenge.

Finally, implementation continues to be a pending task. Being able to properly roll out new technological initiatives requires thorough planning − not only in terms of the development of the technology, but also in terms of its implementation needs. When technology is involved, matters related to the training and staffing of first-line responders become crucial, as new data processes may not be easily understood by all those involved, or may significantly alter working routines and processes. Incorporating a specific emphasis on implementation in any new technological initiative is as important as having the right technology.

As the EU and other non-EU countries continue to move towards ‘smart borders’, centred on the automation of border checks, the identification and pre-vetting of low-risk and high-frequency TCN travellers, and improved identification of and action regarding TCN movements, it becomes essential to assess technological developments and the implications of big data and algorithmic decision-making in their context, taking into account its limits and possibilities. If matters related to technology, privacy and fundamental rights are important in all areas of society, their implications in critical spaces such as border crossing points would be difficult to underestimate. With the appropriate methods of enquiry, impact assessment methodologies and privacy-preserving mechanisms, new systems can be designed and implemented that reflect a commitment to promoting responsible research and innovation and a rights-based technological future.

Acknowledgements

This report is the result of a collective effort, and would not have been possible without much input from different people in different projects. The research team would like to thank colleagues in the ABC4EU project who not only facilitated part of the empirical work, but have also been crucial to the development of many of the ideas the report explores. Without the EC funding and the work of the last two years, the expertise of the research team in border control technologies would be nowhere near where it is now. Participating in the EU Fundamental Rights Agency's survey on biometrics and fundamental rights at EU-LISA piloted border crossings has also been indispensable to extending the analysis beyond air borders. We are thankful for the interest that the societal impact of Smart Border initiatives is garnering and for the opportunity that several funding agencies have given us to explore the many aspects of such critical junctures from the point of view of technology, society and fundamental rights.

Finally, we would like to thank the New Venture Fund and its partners for launching a research initiative on algorithmic decision-making and algorithmic discrimination. Our previous work at the intersection of society and technology has taught us that matters related to the societal impact, desirability, social acceptability and management of data-intensive technologies and processes are still underexplored, and that a collective effort is required to develop the methods of enquiry that will allow us to grasp what are the short, medium and long-term consequences of the information society, big data and algorithmic decision-making. We hope that this report, which is still tentative and exploratory, contributes not so much to providing answers, but to posing the right questions.

Barcelona, December 4, 2015

References

Ackelson, J. (2005). Constructing security on the U.S. - Mexico border. *Political Geography*, 24 (2): 164-184.

Adey, P. (2004). Secured and sorted mobilities: Examples from the airport. *Surveillance & Society*, *1*(4): 500–519.

Amoore, L. (2009). Algorithmic War: Everyday Geographies of the War on Terror. *Antipode*, 41: 49–69.

Armstrong, G and Norris, C. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Bannister, J. and Fyfe, N. R. (1996). City watching: Closed circuit television surveillance in public spaces. *Area*, 28 (1): 37-46.

Bellanova, R. and Gloria González F. (2013). Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices. *International Political Sociology*, 7: 188-209.

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM*, 31 (5): 498-512.

Coleman, R. (2004). *Reclaiming the Streets: Surveillance, Social Control and the City*, Cullompton, Devon: Willan Publishing.

Dijstelbloem, H., Meijer, A. and Besters, M. (2011). The Migration Machine. In Dijstelbloem, H. and Meijer, A. (Eds.) *Migration and the New Technological Borders of Europe*, Palgrave: Macmillan: 1-21.

Dijstelbloem, H. (2009). 'Europe's new technological gatekeepers. Debating the deployment of technology in migration policy', *Amsterdam Law Forum*, 1 (4): 11-18.

Durkheim, E. (1997/1933). *The Division of Labour in Society*. New York: The Free Press.

Finn. R and McCahill, M. (2010). The Social impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums'. *Surveillance & Society*, 7 (3-4): 273-289.

Finn, R, Wright, D. and Friedewald, M. (2013). Seven Types of Privacy. In Gutwirth, S., Ronald L., Paul De Hert, *European data protection: coming of age?* Dordrecht: Springer.

Finn et al. (2014) IRISS, Deliverable 1.1. Surveillance, fighting crime and violence. Available at www.irissproject.eu.

Firmino, R. and Murakami, W. D (2009). 'Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud''', *Identity in the Information Society (IDIS),* Vol. 2, Issue 3: 297-317.

Franko Aas, K. (2011). ''Crimmigrant' bodies and bona fide travellers: Surveillance, citizenship and global governance', *Theoretical criminology* 15(3): 331- 346

Franko Aas, K., Oppen Gundhus and Mork Lomell (2009), 'Introduction: Technologies of (in)security' In: Franko Aas, K., Oppen Gundhus and Mork Lomell (Eds), *Technologies of InSecurity: The surveillance of everyday life*. New York: Routledge.

Goldstein, D. M. (2010). Toward a Critical Anthropology of Security. *Current Anthropology*, *51*(4): 487-517.

Graham S. (2010). *Cities under siege: the new military urbanism*. London: Verso.

Guild, E. (2001). Moving the Borders of Europe. Inaugural lecture, University of Nijmegen.

Guiraudon, V. (2003). 'Before the EU Border: Remote Control of the 'Huddled Masses'. In Groenendijk, K., Guild, E. and Minderhoud, P. (Eds) *In Search of Europe's Borders*. The Hague: Kluwer.

Gutwirth, S. (2012). *Privacy and the information age*. Rowman & Littlefield, Lanham.

Haggerty, K. D. and Ericson, R. V. (2000). The Surveillant Assemblage. *The British Journal of Sociology*. 51 (4): 605-622.

Hayes, B and Vermeulen M. (2012). *Borderline. The EU's New Border Surveillance Initiatives. Assessing the Costs and Fundamental Rights Implications of EUROSUR and the 'smart borders' Proposals*, Heinrich Böll Foundation, Germany.

Hille, K. (2002) 'Video surveillance, gender, and the safety of public urban space: 'Peeping Tom' goes high tech?' *Urban Geography,* 23: 257-278.

Jain, A. K., Ross, A., and Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14 (1): 4-20.

Jeandesboz, J., Bigo, D., Hayes, B. and Simon, S. (2013) The Commission's legislative proposals on Smart Borders: their feasibility and costs. Directorate-General for Internal Policies. Policy Department C, Citizen's Rights and Constitutional Affairs.

Kymlicka, W. (2002). *Contemporary Political Philosophy. An Introduction*. Oxford University Press.

Lindahl, H. (2008). Border Crossings by Immigrants: Legality, Illegality, and Alegality. *Res Publica*, 14: 117–35.

Lyon, D. (Eds.) (2001). *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London.

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London: Routledge.

Lyon, D. (2007). Surveillance studies: An overview. Cambridge: Polity.

Lyon, D. (2007b). National ID Cards: Crime Control, Citizenship and Social Sorting. *Policing. A Journal of Policy and Practice*, 1 (1): 111-118.

Marin, L. (2011). Is Europe Turning into a "Technological Fortress"? Innovation and Technology for the Management of EU's External Borders: Reflections on FRONTEX and EUROSUR. In Heldeweg M. A. and Kica E. (Eds.), *Regulating Technological Innovation: Legal and Economic Regulation of Technological Innovation*, Palgrave: Macmillan, pp. 131–151.

Marshall, T. H. (1965). *Class, Citizenship and Social Development*. New York: Anchor Books.

Monahan, T. (2008). Editorial: Surveillance and inequality. *Surveillance & Society*, 5 (3): 217-226.

Monahan, T. (2010). Surveillance as governance: social inequality and the pursuit of democratic surveillance. In: Kevin Haggerty and Minas Samatas (Eds.*), Surveillance and Democracy*, Routledge, New York.

Monahan *et al.* (2010). Editorial. Surveillance and Empowerment. *Surveillance & Society*, 8 (2): 106-112.

Oscar, G. (1993). *The Panoptic sort: a political economy of personal information*, Westview, Boulder.

Oscar, G. (2009). *Coming to terms with chance. Engaging rational discrimination and cumulative disadvantage*. Farnham: Ashgate.

Parker, N. & Vaughan-Williams, N. (2012). Critical Border Studies: Broadening and Deeping the 'Lines in the Sand' Agenda. *Geopolitics*, 17 (4): 727-733.

Pellerini, H. (2005). Migration and border controls in the EU: economic and security factors. In: DeBardeleben J. (Ed.) *Soft or hard borders? Managing the divide in an enlarged Europe.* Adershot: Ashtage.

Perkins, C. A. and Rumford, P. C. (2014). The Vernacularization of Borders. In: Jones, R. and Johnson, C. (Eds), *Placing the Border in Everyday Life*. Ashgate Publishing: 15 - 32.Post, R. (2000-2001). Three concepts of privacy. in *Georgetown Law Review*, 89: 2087-2098.

Pugliese, J. (2007). Biometrics, Infrastructural Whiteness, and the Racialized Zero Degree of Nonrepresentation. *Boundry 2*, 32 (2): 105-133.

Razac, O. (2009). *Histoire politique du barbelé*. Paris: Editions Flammarion.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: University of North Carolina Press.

Rose, N. (1999). *Powers of Freedom, Reframing Political Thought*, Cambridge: Cambridge University Press.Salter, M. (2002). *Thing-Power-Politics: The Passport as an Object of Global Circulation.* Available on-line: https://millenniumjournal.files.wordpress.com/2012/10/salter-passport-things-power-politics-lse.pdf

Salter, M. (2004). Passports, mobility and security: how smart can the border be? *International Studies Perspectives*, 5: 71-91.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company.

Turack, D. (1972). *The Passport in International Law*. London: Lexington Books.

van der Ploeg, I. (1999). "Eurodac" and the Illegal Body: The Politics of Biometric Identity. *Ethics and Information Technology*, 1(4): 296-302.

van der Ploeg, I. and Sprenkels. I. (2011). "Migration and the Machine-Readable Body: Identification and Biometrics" in Dijstelbloem, H., Meijer, A., and Besters, M. *Migration and the New Technological Borders of Europe*, Palgrave: Macmillan: 1–21Walters, W. (2006). Border/Control. *European Journal of Social Theory*, 9 (2), 187–203.

Whitmore, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*, 113: 1151-1221.

Woolger, S. (2002). *Virtual Society? Technology, Cyberbole, Society*. Oxford: Oxford University Press.