THE POLITICS OF BIOMETRIC TECHNOLOGIES: Borders control and the making of data citizens in Africa

Carolina Polito
LUISS Guido Carli University, cpolito@luiss.it

Cristina Alaimo
LUISS Guido Carli University, calaimo@luiss.it

THE POLITICS OF BIOMETRIC TECHNOLOGIES

Borders control and the making of data citizens in Africa

Research in Progress

Carolina Polito, Ph.D. Candidate LUISS Guido Carli University, Italy, cpolito@luiss.it
Cristina Alaimo Assistant Professor (Research) at LUISS Guido Carli University, Italy, calaimo@luiss.it

Abstract

Biometric technologies are complex hardware and software infrastructures that link biometric data such as fingerprints, iris scans, face scans, or DNA data with personal data. A handful of foreign private actors have implemented biometric solutions in more than half of African countries. This paper investigates the politics of biometric artifacts, it looks at how biometric data furnish the basis for the emergence and institutionalization of certain political discourses and power configurations. To this aim, we link the study of biometric data artifacts to the role of private contractors and the full-scale involvement of public institutions in the establishment of border control markets. The empirical context of the research is the work practices of the actors involved in the export of biometric technologies for border security solutions in Namibia. Preliminary findings suggest that the technological and political rationalities of biometric solutions introduce a set of novel problems in the making and management of data profiles. Border control as a political issue seems to be increasingly intermeshed with a logic of economic profit and technological efficiency raising questions of data justice and political accountability.

Keywords: Biometrics, Data, Control, Borders, Africa, Infrastructures.

1 Introduction

The adoption of biometric technologies, complex hardware and software infrastructures that link biometric data such as fingerprints, iris scans, face scans, or DNA data with personal data, is increasingly widespread across the world and in the Global South. Biometric technologies have been implemented in over half of African countries (Pauwels, 2020). The latest report of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA, 2022) on the State of Internet Freedom in Africa specifically focuses on the rise of biometric surveillance considering it one of the most pressing current issues. Biometric technologies have also been adopted in India in an attempt to streamline and secure the supply chain of the Public Distribution System of basic goods or PDS (Masiero, 2018), as well as in the ASEAN region supporting the implementation of the Bali Process (Indriani, 2020). Biometric technologies represent a rather small constituent of foreign intervention in Africa regarding technology transfer, and their significance should not be overstated (Jacobsen, 2020). Nonetheless, the steady increase in the number of African countries using biometric technologies signals the endurance of the (often misplaced) belief that this technology may be able to resolve complex political challenges.

The embodiment of political rationalities into technological artifacts is not a new phenomenon (Winner, 1986), yet with the development and ubiquitous diffusion of digital technologies it assumes new political dimensions. Today biometric artifacts are used to supposedly ensure “free and fair” elections through Biometric Voter Registration (BVR) (Jacobsen, 2020), more efficient policing through forensic science biometric databases (Pauwels, 2020), or optimize border controls against the ever-greater terrorist fright through facial recognition or body scans (United Nations, 2018). All these solutions run on the making of data artifacts and dispersed data infrastructures that must be aligned and constantly optimized to effectively perform their cognitive and technological function. Data are not just the fuel that empowers the working of machines, they are also the building blocks of meaning-making, and as such, they furnish the basis for the emergence and institutionalization of certain social and political discourses (Alaimo and Kallinikos, 2021, 2022). Recording data, indexing, classifying, and assigning data to broader categories are deeply political acts (Bowker and Star, 1999). What are the specific technological and political problems that emerge from the integration of biometric data into policy making?

These issues assume additional relevance for the data-rich infrastructure-poor African continent which is currently facing an unprecedented inflow of foreign investments in biometric technologies. As mentioned by Kayser-Bril (2019) among the most prominent continent-wide traits of the identity management industry there is "the quasi-absence of local contractors" (p. 24). The increasing foreign support for developing biometric technology in Africa is also intimately linked with the interests of the actors involved in such technology transfer, namely those of international private biometric companies, donor states, international organizations and clients.

We adopt a political approach to the study of biometric technology. Starting from the position that technology is always political (Winner, 1986), we investigate the power configurations biometric solutions uphold. To this aim, we link the study of biometric data artifacts to the role of private contractors and the full-scale involvement of public institutions in the establishment of border control markets. While biometric technologies are often presented as a "solution" to social problems such as border control, their political dimension is often more complex and ambiguous. Their design, implementation and export are seldom the results of an individual designer but come from the entanglement of political interests and business objectives of various powerful actors. Some scholars have pointed out that exporting digital technologies is rapidly becoming another sphere for advancing a new form of colonization to the detriment of African countries. According to such a view, digital technologies are becoming either experimenting grounds for technologies (Madianou, 2019; Jacobsen, 2020), the designated land for expropriating local data (Kwet, 2019; Coleman 2019; Nothias, 2019), or new profitable and exploitable markets. However, few studies have effectively mapped such complex entanglements of interests and how they are embodied in the design and working of technological artifacts.

This paper studies the politics of biometric artifacts in Africa. Focusing on the artifacts' specificities and the role of private actors and public institutions, it investigates (A) what configuration of actors lies behind the export of biometric technologies, (B) what political order the making of biometric technologies helps sustain. The paper is based on an in-depth embedded case study. The empirical context of the research is the network of actors involved in exporting biometric technologies for border security solutions in Namibia and their work practices. A pilot study is also conducted to build a preliminary understanding of the design and markets of biometric technologies. The research draws on interviews, publicly available material such as newspaper articles, policy documents, and white papers. Our work builds on and extends current approaches to data, datafication, and data work which have addressed the political and cultural dimensions of data technologies (Aaltonen et al. 2021; Alaimo and Kallinikos, 2021, 2022; Kallinikos, 2010; Winner, 1986) and contributes to the emerging stream of research in IS and STS which is concerned with data power and injustice and algorithmic bias (Dencik et al. 2019).

In the next section, we present the literature review and analytical framework. The section is followed by a description of the research design and methodology. After briefly describing the case, we illustrate preliminary findings which we discuss in light of our research questions and extend by pointing to directions for future research.

2 Literature Review and Framing

The idea of collecting biometric data to record people and construct their identities as citizens are not entirely new. Already in 1880, Henry Faulds recognized the importance of fingerprints as a means of identification and devised a method for classifying them (Hutchins, 2011). A few years later, Sir Edward Henry, Inspector General of the Bengal Police decided to use fingerprints for criminal identification in India adopting a classification system like the one ideated by Faulds. From the beginning of the 20th century, police officers worldwide started collecting and analyzing biometric data systematically (Polson, 1951).

Political acts are embedded in the recording, classification, and assignment of data to broader categories (Bowker and Star, 1999). Classification affects "spaces of possibilities" as it attaches the realities of being and acting as citizens, clients, or migrants to the technological specificities and political contingencies of how such categories have been constructed (Hacking, 1986). Categories have always operated under the principles of inclusion of some and exclusion of others, yet the principles, values, and modalities of classification change over time as they are unavoidably affected by the technological tools, ideas of the world, and institutional actors who take part in the classifying. Digital data and biometric data are not different in this respect. Despite the allure of trust and infallibility surrounding the use of data derived by scanning body parts, the making of these data and their subsequent operations of aggregation and analysis are still upheld in the politics of categorizing and classifying (Winner, 1986). As with many other classificatory devices, biometric data are a "spatial-temporal segmentation of the world" that is "ineluctably arbitrary" (Bowker and Star, 1999).

Digital data are different kinds of records as they retain their updatability, portability, and re-contextualizability throughout their lifecycle (Aaltonen et al., 2021; Alaimo et al., 2020; Kallinikos et. al, 2010). Profiles constructed out of digital data, in other words, can always be changed, moved into different databases or systems, or re-used in other contexts or for other purposes. Understanding the making of data and the construction of data objects is key to investigating the unique technical, cognitive, and political properties of biometric classification. Data objects are entities made of data structured and aggregated under a specific template (Alaimo, 2022; Alaimo and Kallinikos, 2022). They function as broader categories that give sense and value to data and, in large and disperse data infrastructures, facilitate interoperability and portability (Alaimo and Kallinikos, 2021). Data objects, however, are not just duplicates of existing realities. Data and data objects are artificial models that become the "instruments of social interaction and targets of manipulation and control" (Alaimo, 2022, p. 1092). Furthermore, data objects are always part of larger infrastructures that they help construct and from which they inherit some of their technical properties (Alaimo and Kallinikos, 2022). Extant research has pointed out how these systems "require multiple fragile technologies to work at the same time" (see Masiero, 2018). Analyzing the relation between biometric data, the making of data objects, and the broader infrastructure within which they are embedded appears to be particularly promising as these data make sense and have value only if connected to many other systems.

Biometric technologies are oftentimes supported by institutionalized beliefs and political discourses. A defining aspect of the diffusion of biometric technologies in the Global South has been the instrumental notion of trust that has been pinned to these systems. Under this condition, trust plays a role in the institutionalization and image formation of biometric technologies as an efficient tool (Masiero, 2018). Jasanoff (2004) refers to the concept of trust in terms of "how technologies are factored into the framing and solution of public problems" (p. 34). She relates it to the idea of objectivity and reliability that is often attached to technological developments and that affect their uptake by state or international institutions. The very presence of biometric technologies for identification is, hence, the result of complex and multi-sited processes of negotiation, conflicts, and institutional work (Hacking, 1986).

Scholars have long explored the use of biometric technologies for border security. Frowd (2014) focuses on the internalization of political discourses imported by external actors, the absence of indigenous development, and the problems deriving from it. Foreign actors such as international organizations or security professionals play a critical role in introducing knowledge and norms about how borders should be controlled, most of the time (over)promoting the possibilities offered by these technologies (Frowd, 2014). He stresses the importance of looking at the actors' role in building the field of border security and border governance in West Africa. Along similar lines, Madianou (2019) stresses the emergence of a 'biometric assemblage' (p. 582) which is adopted during humanitarian operations by humanitarian organizations, donors, host states, and the private sector. According to this view, technology should be "situated in the wider assemblage of which it forms a part" (Andrejevic and Selwyn, 2022, p.53). In the case of biometrics, the assemblage would include sensors, networks, and storing systems, among others.

The literature on biometric technologies, however, often treats the technology as a black box and the politics or the specificities of the technology are rarely addressed.

This paper takes stock and expands current approaches across IS and STS literature on biometric systems for security purposes. The paper adopts Winner's (1986), politics of technological artifacts analytical framework. Under this approach is key to look at the specificities of the artifacts and acknowledge how technological developments and large infrastructures implementations are interwoven with broader political discourses, dominant market mechanisms, and the work of powerful private corporations, states and international organizations. Despite private companies having a powerful function as designers and managers of biometric artifacts, their role has often been overlooked, or not adequately problematized. Their increasing involvement in the 'datafication' of border management is linked to the growth in border securitization and techno-solutionism (Valdivia et. al., 2022), and is key for the implementation of large-scale migration control markets. Such markets have been defined by Lòpez-Sala and Godenau (2020) as "markets for services aimed at controlling cross-border mobility in which states, in alliance with supranational entities, monopolize the demand, and in which private corporations sit on the supply side" (p. 7). While biometric technologies are presented as a "solution" to social problems, the modalities by which they are designed, implemented and exported are seldom the result of an individual designer but come from the entanglement of the political interests and business objectives of various powerful actors.

3 Research Design

This paper studies the politics of biometric artifacts in Africa. Focusing on the artifacts' specificities and the role of private actors and public institutions, it investigates (A) what configuration of actors lies behind the export of biometric technologies, and (B) what political order the making of biometric technologies helps sustain. To address the research questions, a qualitative research design has been chosen. Qualitative research consists of a set of interpretive practices that make the world visible by turning it into a series of representations (Norman et. al., 2018). The research is based on an in-depth embedded case study of the market of biometric technologies. The empirical context of the research is the network of the actors involved in the export of biometric technologies for border security solutions (the case) in Namibia (the embedded unit of analysis). The Namibian border control biometric market, in particular, is characterized by the presence of the French company Thales which provided for the country's border control system at the Hosea Kutako International Airport. The company Thales and its biometric business are investigated by combining a reconstruction of the company's acquisitions and supply chain with a reconstruction of the relationship between the company and other relevant actors, such as the European Commission and the French State. The Namibian case has been selected based on its representativeness - i.e., capturing the circumstances and conditions of a typical situation (Yin, 2009). The analysis of the subunit Namibia serves as a device for focusing the case study inquiry when the broadness of the case could lead to an "unduly abstract research design" (Yin, 2009, p. 182). In order to set the framework for the in-depth embedded case study, a pilot study is conducted to build a preliminary understanding of the design and markets of biometric technologies. The pilot case is currently undergoing and has already enrolled an Italian start-up company that has developed a multi-factor authentication Facial Recognition System and a Dutch company active with multiple technologies in the biometric market. The pilot case study will also help refine the data collection plans (Yin, 2009).

Phase 1. Pilot Case	**Phase 2. In-depth Case Study**	**Phase 3. Embedded Unit**
Scope: Building a preliminary understanding of the design of biometric technologies and their market dynamics. *Empirical context:* Experts, practicioners such as private firms	*Scope:* Investigating the network of the actors involved in the export of biometric technologies for border security solutions	*Scope*: Investigating the border control working practices with the implementation of biometric technologies *Empirical context:* The Namibian border control.

and developers involved in the making and commercialization of biometric solution. *Data gathering techniques*: Interviews, publicly available data, companies' documents.	*Empirical context:* Thales' network of suppliers and clients, working practices and products. *Data gathering technique*: Publicly available data, currently mapping the network of Thales' suppliers and clients, gathering all the available public material.	*Data gathering technique*: Publicly available data, currently negotiating access for interviews.

Table 1. Research Design

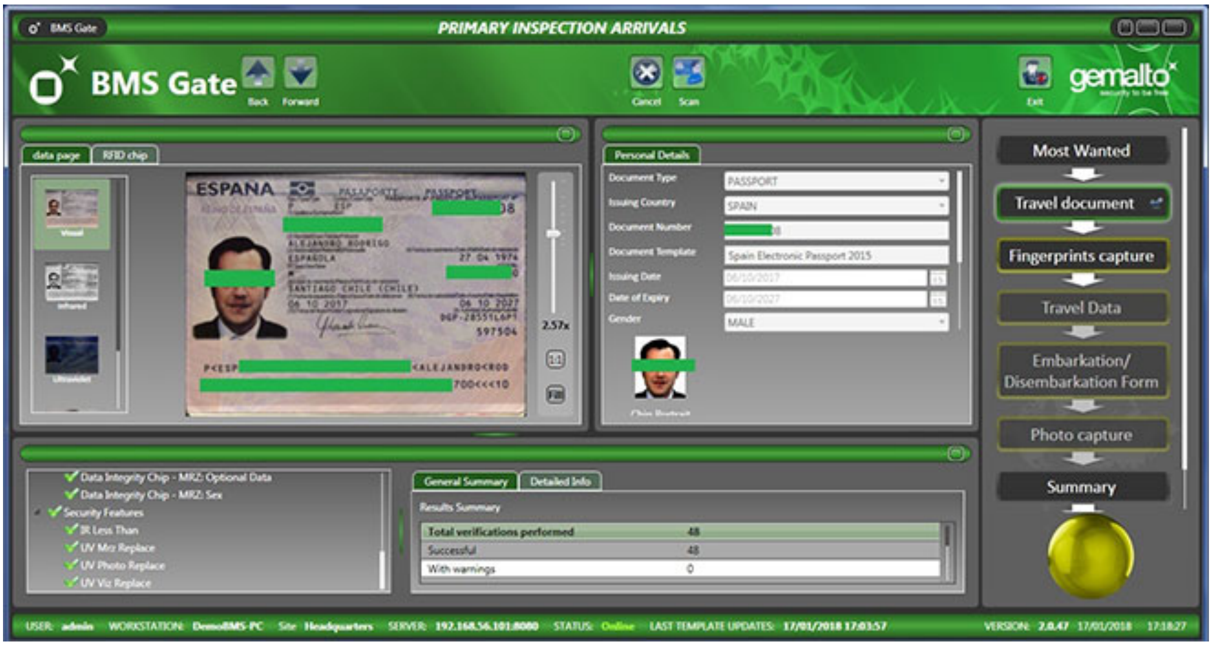
4 Exporting biometric technologies: The case of Thales and Namibia

Thales is one of the leading European companies in the field of biometric technologies. Formerly known as Thomson-CSF, Thales is a multinational corporation providing advanced electronic systems and equipment for civil and military use. Identity solutions are a very important segment, albeit not the largest, of the company's sales, accounting for about 19% of its transactions (Thales, 2020). The company's "Identity and Access Management" segment is forecasted to double in terms of market growth by 2025 and tip 15 billion euros worth (Thales, 2020). To date, Thales participates in more than 200 identity programs around the world and its Border Management Systems are used in several African countries. The conglomerate offers hardware solutions – biometric scanners – and biometric software solutions. A key lever for accelerating Thales's identity solution strategy was the 2019 acquisition of the Dutch Gemalto, a leading corporation in biometric technologies and digital identity. Gemalto's technologies are now systematically included in Thales's security offers for sensitive sites such as airports and ports. With the acquisition of Gemalto, the conglomerate also acquired the company 3M which in 2017 completed the sale of its identity management business to Gemalto. 3M's identity management business provides biometric hardware and software enabling identity verification and authentication, as well as document readers. The business includes 3M Cogent, Inc., a wholly-owned subsidiary of 3M. Out of 133 suppliers of Thales, 16 companies produce biometric solutions. Among others, there are Idemia another French leader in digital technologies, Sopra Steria, Innolux, and Idex Biometrics. This shows the interdependence and integration among biometric companies' supply chains.

The complexity and interdependence of Thales supply chain are mirrored by the complex infrastructure supporting biometric applications. Biometric technologies require multiple data-based technologies to work together at the same time. There are five major components in a biometric authentication system: sensors, feature extractors, template databases, matcher, and decision modules (Jain et. al., 2008). Sensors scan the biometric traits. The feature extractors module processes the scanned biometric data to extract a feature set which is stored in a database as a biometric template and indexed by the user's identity information. Biometric templates are the mathematical representations of the feature set. Templates databases can be geographically distributed and contain millions of records, such as in the case of international databases of 'most wanted' individuals. In the case of 1:N identification, hence, the feature sets have value only when connected with the broader templates database. The matcher module accepts the two biometric feature sets as inputs and outputs a match score indicating the similarity between the two sets. Finally, the decision module makes the decision about the identification or verification (Jain et. al., 2008). In the making of these technologies, different vendors can supply different components.

Going back to Thales, it is relevant to highlight that it is not just a private company, but it embeds and reflects key political and strategic interests of the French government. The French state owns 25.67% of Thales' shares, corresponding to 34.75% of voting shares. The French state is hence by far the company's major shareholder. Besides, Thales is one of the most important shareholders of Civipol, a consulting and technical cooperation operator of the French Ministry of Interior, which "helped shape the EU border externalization policies" (Akkerman, 2018, p. 72). The organization operates between a state operator and a private company. The French state owns 40% of Civipol, while a few companies, including Thales, own respectively over 10% of the shares (Akkerman, 2018). Like many other nations, the French government also openly supports the development and adoption of biometric technologies. For example, it is “establishing an agency and legislative framework to conduct an experimental test of facial recognition technologies in public places” (Andrejevic and Selwyn, 2022, p. 59). As such, the segment of the biometric market we analyze is characterized by the presence of different public and private sector players whose interests seem to converge.

Additionally, the European Union plays a pivotal role in the biometric market. The EU not only issues the tender contracts for implementing and maintaining data infrastructures at the EU's external borders but also establishes the rules for designing and exporting these systems. It should be noted, in this respect, that the EU's export control regime is considered at times less stringent than the US one. Incongruous and/or incomplete export control regulation, the proliferation of tender contracts and more generally the interest of the EU in controlling the migrant flux are all aspects shaping the current political discourse around biometric technologies. It should be noted that specific choices related to the design and implementation of the biometric system are always the result of political and economic considerations across multiple existing trade-offs and along all the supply chain of the application. Biometric technologies, in fact, are a family of technological solutions which are classifiable according to different parameters such as the type of feature sets that are stored in the databases. More advanced privacy-preserving biometric techniques include irreversible encryption by multi-party computation protocols, cloud-based biometrics, and cancellable biometrics – in which the feature set is distorted and encrypted before storage. Multiple trade-offs, therefore, exist between accuracy, security, the number of sensors the systems use and the cost of the technology. At least theoretically, the greater the number of sensors, the greater the accuracy (i.e., lower false acceptance rate and lower false rejection rate) and security of the technology. The accuracy of the technology is also closely linked to the risks of identity records remaining unreliable due to improper identification and registration procedures, undocumented border crossing (Leese, 2020), and data duplication. It is not unusual that when the automated enrollment of the data is not successful, it is transferred to a human performing the matching in a non-automated manner.



ESPANA PASAPORTE PASSPORT
P ESP [redacted]
[redacted]
ALEJANDRO RODRIGO
ESPAÑOLA 27 04 1974
[redacted]
SANTIAGO CHILE (CHILE)
06 10 2017 06 10 2027
DGP-28551L6P1
597504
P<ESP[redacted]<ALEJANDRO<ROD
[redacted]700<<<10

Document Type	PASSPORT
Issuing Country	SPAIN
Document Number	[redacted]
Document Template	Spain Electronic Passport 2015
Issuing Date	06/10/2017
Date of Expiry	06/10/2027
Gender	MALE

- ✓ Data Integrity Chip - MRZ: Optional Data
- ✓ Data Integrity Chip - MRZ: Sex
- ✓ Security Features
  - ✓ IR Less Than
  - ✓ UV Mrz Replace
  - ✓ UV Photo Replace
  - ✓ UV Viz Replace

Results Summary

Total verifications performed	48
Successful	48
With warnings	0

USER: admin WORKSTATION: DemoBMS-PC Site: Headquarters SERVER: 192.168.56.101:8080 STATUS: Online LAST TEMPLATE UPDATES: 17/01/2018 17:03:57 VERSION: 2.0.47 17/01/2018 17:18:27

Figure 1. *Namibia interface on primary inspection arrivals*
Source: Thales, Namibia invests in world-class border management. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/border-management-namibia

In Namibia, Thales exported the biometric solution for the Hosea Kutako International Airport. Foreign companies such as Thales are usually also entrusted with consultancy and training, and management of border security solutions (Akkerman, 2018). Whenever someone crosses that smart border, information is captured by immigration officers. Faces and fingerprints are scanned via "purpose-designed gateways" (Thales, n.d.). The scanned data are then associated with travellers' identification documents, specifically passport numbers. This real-time captured information is compared with travellers' historical data and with a list of the "Most Wanted People and stolen/lost documents" (Thales, n.d.). The data are also sent and synchronized with a central database hosted by the Namibian Minister of Home Affairs and Immigration (MHAI). The database is then linked with INTERPOL's database of Stolen and Lost Travel Documents (SLTD) and INTERPOL's database of Nominal Data containing records about international criminals or missing persons (Thales, n.d.). Namibian elites are among the most important proponents of the adoption of these technologies. The MHAI states that "complete, reliable, and trusted" identity management solutions are being rolled out and that their "societal impact cannot be underestimated" (World Bank Group, 2016, p. 37). Namibia, among others, has also adopted ICTs technologies capturing and using biometric data during voters' registration and at polling stations (IDEA, n.d.). The national political discourse used to motivate the implementation of biometric solutions for border control has been centred around the rhetoric of the need to fight against terrorist attacks and maintain and strengthen the integrity of national borders. The narrative however is in stark contrast with the figures of the Institute for Economics and Peace on Global Terrorism Index (2020) according to which Namibia faces no impact of terrorism (p. 9). This shows how the construction of biometric technologies is not only the result of technological affordances, capabilities and economic means but also powerful political discourses.

5 Preliminary Discussion

We set out to investigate the politics of biometric artifacts focusing on the artifacts' specificities and their links to the role of private actors and public institutions, specifically, (A) what configuration of actors lies behind the export of biometric technologies, (B) what political order the making of biometric technologies helps sustain. Our preliminary findings raise a few critical aspects concerning how biometric technologies work and which kind of society or political configuration they require (Winner, 1986).

To begin with, biometric technologies seem to differ from other types of data-based systems. For the biometric solution to work, different components must coexist simultaneously in a dispersed and fragile network where data of disparate formats belong to different cultural, political and regulatory contexts. This is not solely a technical problem that can be solved with better technology or better data, but it requires the alignment of socioeconomic and political interests and a compatible normative landscape. Consider how multiple complex databases such as the central database hosted by the Namibian Minister of MHAI and the INTERPOL databases have to coexist and work simultaneously. It is not only a matter of data circulation or database interoperability. The coexistence requires the coordination and integration of two different conceptions of the world that see citizens as different entities and assembles data objects accordingly (Alaimo and Kallinikos, 2021, 2022; Bowker and Star, 1999). Profiles are put together by aggregating data that respond to certain political objectives or views of the world (i.e., INTERPOL records on international criminals and missing persons obey specific cognitive criteria). In the paper, we underline how these profiles result from technological affordances and capabilities, economic means, and political discourses which coexist within a complex interaction of actors. Based on our reading of the central database hosted by the Namibian Minister of Home Affairs and Immigration (MHAI), the design has disregarded risks of data loss and the risks to the confidentiality of data by implementing inappropriate cross-linking of data across systems (Waugh, 2015). As we progress in our research, we intend to further investigate Thales' specific choices related to the design of the biometric systems and connect them to the multiple existing trade-offs, intrinsic to the work of biometric solutions, that emerged from preliminary findings. In particular, the relation between feature sets and data ingested in the system seems particularly promising for understanding how certain decisions and political rationalities become embedded in data and data objects. The concept of interoperability of the data collected among the list of databases that should be able to communicate with one another is another aspect worth investigating. The databases for border management, migration, and security which are based on different legal grounds can, indeed, hardly be integrated, leaving public authorities with blind spots and incomplete pictures (Leese, 2020). Finally, an aspect that requires further investigation is the maintenance and repair of these fragile technologies (Passi and Jackson, 2018). As of today, biometric solutions are managed by a vast network of operators which includes Thales experts, local contractors and international organizations. Sharing data, deciding their format, and maintaining these databases are not just technical issues but embed and sustain specific structures of established power (Winner, 1986), understanding how these conflicts and negotiations occur in the working practices of actors is the focus of the next step of our research.

If we follow Winner (1986), we can certainly claim that the specificity of biometric technologies is associated with certain views of the world or political rationalities and configurations of power. To the fragile and politically loaded work of biometric technology corresponds a central power authority whose contours are clearly shifting. The MHAI host a central database yet depends on Thales Gemalto for maintenance. Authority today is shared with those who are entitled to guarantee the correct functioning of the system, for instance by rendering multiple databases interoperable or by establishing the correct version of identity solutions to verify and cross-validate identity records. As such, the ways in which biometric technologies are designed, implemented, and managed may help consolidate novel power configurations among the ecosystem of actors involved. Mapping such ecosystem's actors and the role they play in the making of biometric solutions seems a promising avenue for our research and one we intend to pursue looking at the case of Namibia.

Finally, the almost unavoidable trend toward the digitalization and privatization of border control has consequences for the nature of the market, of the state, and of the citizen subject to this privatized and datafied control. The complexity of current configurations makes the old project of understanding the export of consumer goods by looking at market forces of demand and supply a chimera (Gammeltoft-Hansen, 2015). Data-based products such as biometric technologies warrant a much more composite and polymorphous market that results from the complex interaction of multiple public and private actors, such as international private biometric companies, donor states, international organizations and clients. The dynamic interplay between the interests of these multiple actors form a contested political and economic terrain where biometric technology projects develop, embodying commercial objectives, political rationalities, and strategic goals that call for additional research.

6 Conclusion and future work

This paper investigates the politics of biometric artifacts in Africa. We presented preliminary findings of an embedded case study on the export of biometric technologies for border security solutions in Namibia. Our investigation has begun to unpack the specificities of biometric technology and its links with certain power configurations. We investigated issues of interoperability and data storage not just as technical problems but as data work practices that inherit and reproduce certain views of the world embedding political rationalities into data solutions (Bowker and Star, 1999). Data and data objects are never just technological inputs but as sociocultural artifacts (Alaimo, 2022; Alaimo and Kallinikos, 2021, 2022), in the case of biometric technologies it becomes evident by observing the choice and design of features sets and the relations they ented with ingested data. By observing decisions involved in the design of the artifacts and their implications we may be better positioned in assessing the politics of biometric technologies and their impact on the global south. Our research seeks to contribute to IS literature and cognate fields such as STS by integrating a politics of artifacts perspective with attention to market dynamics and the emergence of novel power configurations. Our work builds on and extends current approaches to data, datafication, and data work which have addressed the political and cultural dimension of data technologies (Aaltonen et al. 2021; Alaimo and Kallinikos, 2021, 2022; Kallinikos, 2010; Winner, 1986) and contributes to the emerging stream of research in IS and STS which is concerned with data power and injustice and algorithmic bias (Dencik et al. 2019).

References

Aaltonen, A., Alaimo, C., & Kallinikos, J. (2021). The making of data commodities: Data analytics as an embedded process. *Journal of Management Information Systems*, 38(2), 401-429.

Akkerman, M. (2018). Expanding the fortress: The policies, the profiteers and the people shaped by EU's border externalization programme, Transnational Institute

Alaimo, C. (2022). From people to objects: the digital transformation of fields. *Organization Studies*, 43(7), 1091-1114.

Alaimo, C., & Kallinikos, J. (2021). Managing by data: Algorithmic categories and organizing. *Organization Studies*, 42(9), 1385-1407.

Alaimo, C., & Kallinikos, J. (2022). Organizations decentered: data objects, technology and knowledge. *Organization Science*, 33(1), 19-37.

Alaimo, C.; Kallinikos, J.; and Aaltonen, A. (2020) Data and value. In, S. Nambisan, K. Lyytinen, and Y. Yoo (eds.), *Handbook of Digital Innovation.* Cheltenham: Edward Elgar, pp. 162–178.

Andrejevic, M., & Selwyn, N. (2022). Facial recognition. John Wiley & Sons.

Bernot, A. (2022). Transnational State-Corporate Symbiosis of Public Security: China’s Exports of Surveillance Technologies. *International Journal for Crime, Justice and Social Democracy*, 11(2), 159-173.

Breckenridge, K. (2005). The biometric state: The promise and peril of digital government in the new South Africa. *Journal of Southern African Studies*, 31(2), 267-282.

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. Cambridge MA: The MIT Press.

CIPESA (2022), State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance, September

Coleman, D. (2018). Digital colonialism: The 21st-century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. Mich. J. Race & L., 24, 417.

International Institute for Democracy and Electoral Assistance (2018), ICTs in Election Database. Available at: https://www.idea.int/data-tools/data/icts-elections

Debos, M. (2018). La biométrie électorale au Tchad: controverses technopolitiques et imaginaires de la modernité. *Politique africaine*, 152(4), 101-120.

Debos, M. (2021). Biometrics and the disciplining of democracy: technology, electoral politics, and liberal interventionism in Chad. *Democratization,* 28(8), 1406-1422.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society*, *22*(7), 873-881.

Epstein, C. (2007). Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders. *International Political Sociology*, 1(2), 149-164.

Erastus, L. R., Jere, N., & Shava, F. B. (2015). Exploring challenges of biometric technology adoption: A Namibian review. *In 2015 International Conference on Emerging Trends in Networks and Computer Communications* (ETNCC) (pp. 91-94). IEEE.

Frowd, P. M. (2014). The field of border control in Mauritania. Security Dialogue, 45(3), 226-241.

Hitchcock, P. (2020). Exceptional biometrics. In *Liberal Disorder, States of Exception, and Populist Politics* (pp. 112-126). Routledge.

Gammeltoft-Hansen, T. (2015). Private Security and the Migration Control Industry. In R. Abrahamsen y A. Leander (eds.), *Routledge Handbook of Private Security Studies*, London, Routledge, 207–213.

Gelb, A., & Clark, J. (2013). Performance Lessons from India's Universal Identification Program. Working paper 253. Washington, DC: Center for Global Development.

Gelb, A., & Decker, C. (2012). Cash at your fingertips: Biometric technology for transfers in developing countries. *Review of Policy Research*, 29(1), 91-117.

Glouftsios, G. (2021). *Engineering Digitised Borders: Designing and Managing the Visa Information System*. Springer Nature.

Hacking, I. (1986). *Making up people.*

Hitchcock, P. (2020). Exceptional biometrics. In *Liberal Disorder, States of Exception, and Populist Politics* (pp. 112-126). Routledge.

Hutchins, L. A. (2011). Systems of friction ridge classification. *The Fingerprint Sourcebook*, 1.

IDEA (Institute for Democracy and Electoral Assistance) (n.d.), If the EMB uses technology to collect voter registration data, is biometric data captured and used during registration? – Namibia. Available: https://www.idea.int/answer/ans73868815992

Indriani, M., & Paripurna, A. (2020). Biometric Data Sharing in Addressing Irregular Migration and Security Issues within the Bali Process Framework for Indonesia and ASEAN Member States. *JSEAHR*, 4, 449.

Institute for Economics and Peace (2020), Global Terrorism Index 2020 Measuring the Impact of Terrorism

Jacobsen, K. L. (2020). Biometric voter registration: A new modality of democracy assistance?. Cooperation and Conflict, 55(1), 127-148.

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on advances in signal processing, 2008, 1-17.

Jasanoff, S. (2004). Ordering knowledge, ordering society. In Jasanoff S. (ed.) *States of knowledge: The co-production of science and social orde*r. London: Rutlege, 13-45.

Kallinikos, J. (2010). *Governing through technology: Information artifacts and social practice*. Springer.

Kallinikos, J., Aaltonen, A., & Marton, A. (2010). A theory of digital objects. *First monday*, 15(6), 1-22.

Kayser-Bril, N. (2019), Identity-Management and Citizen Scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe, and China. *Algorithm Watch*, October 22.

Koskinen, K., Bonina, C., & Eaton, B. (2019, May). Digital platforms in the global south: foundations and research agenda. In *International conference on social implications of computers in developing countries*. Springer, Cham, 319-330.

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3-26.

Leese, M. (2022). Fixing state vision: Interoperability, biometrics, and identity management in the EU. *Geopolitics*, 27(1), 113-133.

López-Sala, A., & Godenau, D. (2022). In private hands? the markets of migration control and the politics of outsourcing. *Journal of Ethnic and Migration Studies*, 48(7), 1610-1628.

Lusch, R. F., & Nambisan, S. (2015). Service innovation. *MIS Quarterly*, 39(1), 155-176.

Madianou, M. (2019). The biometric assemblage: Surveillance, experimentation, profit, and the measuring of refugee bodies. *Television & New Media*, 20(6), 581-599.

Masiero, S. (2018). Explaining trust in large biometric infrastructures: A critical realist case study of India's Aadhaar project. *The Electronic Journal of Information Systems in Developing Countries*, 84(6), e12053.

McGrath, K. (2016). Identity verification and societal challenges: explaining the gap between service provision and development outcomes. *MIS Quarterly*, 40(2), 485–500.

Mayhew, S. (2018), Namibia makes the switch to biometric passports, *Biometric Update*

Norman K. Denzin and Yvonna S. Lincoln (2018). Introduction: The Discipline and Practice of Qualitative Research, in: Norman K. Denzin and Yvonna S. Lincoln (eds), The SAGE Handbook of Qualitative Research, 5th edition, SAGE Publications, Inc, Los Angeles, CA, pp.29-71.

Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, 42(3), 329-348.

Omike, C. (2021). Evaluation of a Technology Public Private Partnership Project Between the Swedish Government and Thales Group. Available at SSRN 4025554.

Owusu-Oware, E., & Effah, J. (2022). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organization. Information Development, 02666669221085709.

Passi, S., & Jackson, S. J. (2018). Trust in data science: Collaboration, translation, and accountability in corporate data science projects. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-28.

Pauwels, E. (2020), The anatomy of information disorders in Africa: Geostrategic Positioning & Multipolar Competition Over Converging Technologies, *Konrad Adenauer Stiftung*, September

Polson, C. J. (1950). Fingerprints and finger printing: an historical study. *J. Crim. L. & Criminology*, 41, 495.

O'Reilly, C. (2010). The transnational security consultancy industry: A case of state-corporate symbiosis. *Theoretical criminology*, 14(2), 183-210

Salter, M. B. (Ed.). (2008). *Politics at the Airport*. University of Minnesota Press.

Thales (2020), Integrated Report Corporate Responsibility 2020-2021

Thales (n. d.), Namibia invests in world-class border management. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/border-management-namibia

Waugh D. (2015), The risk of centralized storage for biometric data, *Biometric Update*

United Nations (2018), UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism

Valdivia, A., Aradau, C., Blanke, T., & Perret, S. (2022). Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders. *Big Data & Society*, 9(2), 20539517221124586.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 109(1), 121-36.

Winner, L. (1986), *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University Chicago Press

World Bank Group. (2016). Namibia Identity Management: System Analysis. World Bank.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.