Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 3, Issue 1 (2023) p.77-122
https:doi.org/10.52907/jipit.v3i1.260

Balancing Human Rights and the Use of Artificial Intelligence in Border Security in Africa

Sherry Bor & Nicole Cheptoo Koech***

ABSTRACT

In a continent marked by its historical pursuit of secure borders, Africa now stands at a pivotal juncture, transitioning from traditional physical barriers to harnessing the transformative potential of Artificial Intelligence (AI) technologies. This transformation signifies the continent's unwavering commitment to efficiency and innovation, yet it unveils a formidable challenge – striking a harmonious balance between the imperative of security and safeguarding of fundamental human rights and freedoms. The integration of AI in border security, with its utilization of biometric data, facial recognition, iris scanning, and more, has given rise to a host of intricate concerns, including ethical considerations such as transparency and accountability. Privacy emerges as a paramount issue as the data reservoirs amassed at border crossings raise questions about storage, accessibility, and potential misuse. The complexities of personal information management take center stage, necessitating scrutiny over data handling, security, and safeguards against abuse. Through an examination of historical trends and a detailed analysis of past and present border security practices in Africa, this paper reviews the evolution of strategies and challenges in Africa's border security. This investigation spotlights the continent's adoption of AI as a cornerstone in safeguarding its borders. However, it underscores that while advancements are evident, a delicate equilibrium must be achieved. This paper argues that achieving a harmonious balance between bolstering security measures and safeguarding individual rights and freedoms, all within the framework of ethical principles is an attainable endeavor.

Keywords: Artificial Intelligence, Border Security, Human Rights, Surveillance, Ethical Principles

* Bachelor of Laws, the Catholic University of Kenya. Advocate of the High Court of Kenya and member of the International Association of Privacy Professionals (IAPP). Associate at TripleOKLaw Advocates, TMT Department.

** The author is an advocate of the High Court of Kenya and holds an LLB from Strathmore University, Kenya.

TABLE OF CONTENTS

I. INTRODUCTION

The rapid adoption of Artificial Intelligence (AI) in African border security presents both opportunities and challenges. On the one hand, AI systems promise to revolutionize security measures, enhancing operational efficiency and accuracy in threat detection and management. On the other hand, integrating AI systems in border security raises pressing ethical questions about individual rights and freedoms.

The justification for this research stems from AI's increasing relevance in border security and the consequential impact on human rights. Therefore, central to this discourse is the fundamental question: how can African nations strike a harmonious balance between advanced AI-driven security measures and the ethical imperative to safeguard individual rights and freedoms? This paper contends that achieving such a balance, firmly rooted in ethical principles, is not just aspirational but realistically achievable.

To support this contention, the paper delves into case studies and scrutinizes relevant ethical and legal frameworks. It aims to offer a comprehensive analysis of both the benefits and the challenges of AI in border security, alongside ethical considerations and legal implications. Ultimately, this study advocates for a balanced approach that simultaneously upholds security needs and ethical standards, contributing to a deeper understanding of AI's impact on border security and human rights.

This paper is divided into five parts, including this introduction as Part I. Part II provides a historical overview of border security practices in Africa, meticulously tracing the evolution from traditional methods to the integration of AI technologies in the modern age. Additionally, it highlights the factors motivating African nations to consider the use of AI in border security. Part III examines two AI technologies adopted for enhancing border security in Africa. It assesses the benefits, the challenges, and the negative impacts associated with the adoption of AI technologies in border security, with a focus on African countries' experiences. Part IV critically analyzes the potential impacts of AI technologies on the right to privacy within the context of border security. Finally, Part V concludes with recommendations and future directions for responsible and ethical adoption of AI technologies in border security while ensuring the protection of privacy rights.

II. FROM TRADITIONAL BORDER SECURITY METHODS TO HIGH-TECH SOLUTIONS IN AFRICA

While recognizing the historical significance of AI implementation in African border security, this part aims to shift the focus towards a distinct aspect: uncovering the driving forces behind the adoption of AI technologies in African borders. This section begins by closely examining the early practices of border security in Africa, illuminating the consequential shortcomings and repercussions that crystallized as African governments endeavored to fortify their borders. Transitioning from this assessment, the discussion delves deeper into the proactive measures undertaken by African governments and the catalytic factors that have spurred the increasing adoption and reliance on AI technologies for the augmentation of border security. A meticulous examination of the decisions and initiatives undertaken by African nations reveals a profound understanding of their transformative journey towards more efficient and secure border management. While there are multifaceted reasons for border security, this paper uniquely centers on the movement of people and migration as a critical dimension, recognizing its profound impact on Africa’s border control landscape.

A. Early border security measures in Africa: Migration challenges and transformations

Historically, African states have grappled with substantial challenges in managing human migration across their borders.

These challenges have roots in the legacy of colonial-era boundaries that were often drawn arbitrarily, without regard for ethnic, cultural, or linguistic ties (Herbst, 2000). Such borders, which have occasionally ignited inter-state tensions, not only separated communities but also complicated the task of upholding territorial integrity.

Several factors have influenced migration patterns in Africa. These range from socio-economic motives, such as seeking improved employment opportunities or evading poverty, to more urgent circumstances like escaping conflict. The latter is evident in instances like the exodus spurred by the Genocide against the Tutsis in Rwanda, or the displacement seen in the Sahel region (Adepoju, 2004; Okumu, 2011). Complicating the management of these migration patterns have been challenges like the absence of tailored institutional frameworks, inconsistent coordination across governmental levels, and the often-contentious nature of borders (Okumu, 2011).

As globalization took center stage toward the end of the 20th century, these migration dynamics were further magnified. Greater global interconnectivity gave rise to increased cross-border movements, encompassing both voluntary migrations and forced displacements (Gituanja, 2013; Okumu, 2011). In response, the perspective on borders began to shift. Instead of viewing them solely as barriers, there was a growing recognition of their potential as channels for regulated human movement. An embodiment of this shift can be seen in regional initiatives like the East African Community (EAC), which aimed to facilitate movement among member states, echoing a pan-African ambition to recast borders as connectors rather than dividers (EAC, 2010).

However, the reality of managing increasing migration flows, while simultaneously ensuring security and sovereignty, presented a nuanced challenge. While regional initiatives like the EAC symbolized a desire to transform the role of borders, the practical intricacies of managing varied migration patterns, addressing socio-economic disparities, and ensuring security formed significant obstacles. Therefore, it became apparent that striking an optimal balance between fostering human mobility and preserving state security remained a focal point in Africa's border management endeavors.

B. Response measures in the early 21st Century: Consequences and pitfalls

At the onset of the 21st century, driven by the escalating pressures of human migration, African states adopted varying measures tailored to their unique border challenges and migratory patterns. Morocco and Algeria, facing increased pressure from trans-Saharan migration routes, responded by constructing physical barriers, such as fences and walls, aiming to regulate the movement of migrants (Saddiki, 2020; Dahshan & Masbah, 2020). Nigeria, grappling with porous borders and diverse migration routes, leaned towards human patrols to monitor migration flows, especially in areas vulnerable to trafficking (Akinyemi, 2013). On the southern tip, countries like Rwanda and South Africa initiated manual documentation systems, aiming to effectively process travel documents at border checkpoints (Landau & Segatti, 2009; World Economic Forum, 2022).

Nevertheless, these early measures encountered challenges. Over-reliance on physical barriers, while deterring some migrants, often pushed others towards more perilous routes, exacerbating humanitarian concerns (Andersson, 2014). Some regions, particularly those remote and less monitored, became focal points for unauthorized crossings and smuggling networks (Chome, 2021). Manual documentation, while a step forward, faced inefficiencies, often being outpaced by the volume of migrations and being susceptible to fraudulent activities such as forgery (Landau & Segatti, 2009; Akinyemi, 2013).

The implications of these challenges were manifold. A dire consequence was the surge in human trafficking and smuggling networks, which thrived in inadequately monitored zones. Economic and political adversities like unemployment, poverty, and instability compounded migration pressures (Nwadike & Ekeanyanwu, 2012). In such volatile environments, an alarming number of migrants resorted to perilous, often unauthorized, routes. For instance, studies highlight that a substantial fraction of West African migrants, seeking to bypass border controls, became ensnared in informal networks, subjecting them to potential exploitation and abuse (IOM, 2020; Bello & Olutola, 2020).

Furthermore, weak migration management systems inadvertently abetted illegal activities. The Horn of Africa and the Sahel, with their vast and inadequately monitored terrains, became channels for not just irregular migrants but also for malign actors. Instances such as the East Africa bombings between the years 1998 and 2002 underline the intricate relationship between lax border controls, irregular migration, and broader security concerns, with culprits capitalizing on weak documentation systems and porous borders (Okumu, 2011).

C. Initial considerations of AI technology in border security and management

Faced with mounting challenges associated with inadequate border management, the need for transformative, scalable solutions became more pressing. Rather than relying solely on traditional methods, several African countries began to pivot towards leveraging technological advancements as potential game-changers in border security and management. The intersection of burgeoning global technological trends and the pressing requirements of border management was seemingly set to pave the way forward for many African nations.

While individual countries embarked on their technological quests, regional collective bodies, such as the African Union (AU), amplified the call for a shift towards technology-oriented solutions. The AU, through various policy initiatives and frameworks, began to underscore the importance of harnessing technology to address the continent's multifaceted border challenges. A salient manifestation of the AU's emphasis on technology came through the Migration Policy Framework for Africa in the year 2006. This framework advocated for the significant role of technology in border management, particularly emphasizing the improvement of travel document security, refining inspection protocols, and enhancing data-sharing and communication infrastructures (African Union Migration Policy Framework for Africa, 2006).

With the global narrative steering towards technologically enhanced border management, several African nations led by example. South Africa introduced an automated biometric national identification system, not merely for modernity, but as a testament to the capabilities of technology in streamlining data processing (Parliamentary Monitoring Group, 2019). Concurrently, Kenya launched the Integrated Population Registration System (IPRS), an initiative that harnessed advanced technology to integrate biometric techniques, enhancing identity verifications at Kenyan control points (Open Society Justice Initiative, 2020). Nigeria, recognizing the importance of technology in border management, transitioned from conventional passports to e-passports. These digitally enhanced passports were instrumental in facilitating comprehensive data analyses, pinpointing potential illicit cross-border activities (Nigeria Immigration Service, 2023).

Following these foundational steps in embracing technology, the African Union shifted its gaze toward the next frontier, Artificial Intelligence (AI). As delineated by the African Union Panel on Emerging Technologies (APET), the panel strongly advocates for African countries to harness smart technologies tailored to address illegal activities at their borders. The overarching aim was to strengthen border control management systems, enhance data sharing between nations, and ensure the seamless and secure movement of people across the continent (Dugbazah et al 2021).

The promise of AI in this realm is multifold. It can not only deter illicit activities like human trafficking but also improve governance mechanisms in overseeing the movement of people across borders. The integration of smart technologies, as APET suggests, can significantly enhance the detection of illegal activities, such as the smuggling of individuals or illicit trade in human lives. Moreover, leveraging smart border control technologies, especially those powered by artificial intelligence and blockchain, can bolster decision-making support for security officials, enhancing the reliability and efficiency of border control systems (African Union Development Union, 2021).

Such advancements in border technology stand to present numerous benefits not just in terms of security but also the facilitation of legitimate movements. Embracing AI solutions to track migration patterns, verify identities, and predict potential security threats can redefine how borders function, marrying efficiency with humane considerations. These proactive measures, as laid out by the APET, could revolutionize border operations, striking a balance between sovereignty, national security, and individual rights, ensuring that the mobility of people remains both fluid and secure.

These technological strides, fortified by the directives and support from bodies like the AU, signify a broader paradigm shift in Africa's approach to border management. In the forthcoming section, this paper delves into specific AI technologies adopted by African nations at their borders, further exploring their applications and the balance between enhanced security and ethical considerations.

III. AI AT AFRICAN BORDERS: OPPORTUNITIES AND REAL-WORLD CHALLENGES

This part elucidates the transformative impact of AI on Africa’s border control systems, from the implementation of automated passport control systems to advanced biometric technologies.

This part primarily focuses on two key AI applications; Biometric Identification Systems and video surveillance. Furthermore, it explores how these cutting-edge technologies not only enhance operational efficiency but also streamline procedural aspects of border security while addressing challenges associated with the movement of people.

Nonetheless, while the potential benefits of AI in border control are conspicuous, this part rigorously examines the notable challenges faced by African countries in the implementation of these technologies. Lastly, it delves into the negative impacts of AI in its application in border security thus laying the basis of the crux of this paper.

A. Biometric identification systems with AI integration

In the realm of border security and ongoing management of human movement, the integration of AI with Biometric Identification Systems is heralding a new era. As continents, notably Africa, undergo surges in human movement. Be it for trade, tourism, or resettlement, the need to unequivocally verify each individual crossing borders has become paramount.

Biometric Identification Systems stand at the vanguard of this initiative. These advanced systems authenticate individuals based on unique physiological and behavioral markers, ranging from fingerprints and facial contours to nuances like gait recognition (Pato & Millet, 2010). As people traverse borders, these systems serve as vigilant sentinels, deterring identity theft and fraudulent impersonations. What was once seen as mere data, a traveler's biometric profile has now evolved into a critical determinant for their movement. Advanced algorithms diligently oversee this, ensuring seamless and secure transitions for each person.

South Africa offers a compelling testament to this technological shift. The country's progression from the Home Affairs National Identification System (HANIS) – rooted in manual, centralized processes – to the Automated Biometric Information System (ABIS) highlights the transformative potential of AI in border management. ABIS did not just expand the scope of biometric data types, it also embraced AI-driven processes, setting new benchmarks in the domain (Allen & Zyl, 2020). Drawing from expansive datasets, the ABIS model has developed the capability to distinguish individual biometric patterns with growing accuracy, leveraging its innate self-learning abilities (NIST, 2020). The transformation from HANIS to ABIS transcends South Africa's mere transition from manual to automated systems. It epitomized a wider African aspiration, harnessing AI's capabilities to redefine border security, ensuring both fluidity and security in the movement of its diverse populace.

In the evolving paradigm of border security and management, two systems emerge as quintessential exemplars of biometric identification integration: Automated Passport Control, which epitomizes the sophistication in document processing through advanced technological means, and Automated Border Control Gates, representing a pinnacle in entry-point security via the utilization of intricate biometric verification mechanisms.

1. Automated Border Control Gates

Automated Border Control (ABC) Gates, employing contactless facial biometrics, are at the forefront of a new wave in managing human movement and enhancing airport security. This innovative technology allows travelers to undergo identification processes on the move, bypassing traditional document checks at various stages of their journey. The effectiveness of ABC Gates in providing a secure yet seamless experience is evident in both developed regions and countries in Africa, such as Rwanda, Angola, and Tanzania (Vision-Box, 2019).

The core of these systems lies in their advanced facial recognition technology. Utilizing deep learning algorithms, particularly convolutional neural networks, these systems can accurately identify individuals from their facial features (Vision-Box, 2019). These AI-driven algorithms are trained on vast datasets, enabling them to handle a wide range of variations in appearance. By integrating these sophisticated AI models, ABC Gates not only expedites the verification process but also ensures a high level of security by accurately matching individuals against large biometric databases.

In the Global North, the implementation of ABC Gates is marked by extensive investment in state-of-the-art technology and infrastructure. These regions have been able to leverage their resources to integrate these systems extensively at major airports (Kis, 2019). The focus here is on optimizing the flow of large numbers of travelers and migrants through high-speed, automated processing while maintaining rigorous security standards.

In contrast, African countries have embarked on a journey to incorporate ABC Gates within their existing infrastructural and technological frameworks. Rwanda's adoption of the first Automated Border Control system in Africa, developed by Vision-Box, includes an enrollment station and clearance eGates at airports and land borders. This setup demonstrates a holistic approach to border management, addressing both air and land travel (Vision-Box, 2019).

Angola's introduction of the 'Passa Fácil' system at Luanda's international airport is another example (Vision-Box, 2019). This system facilitates the automatic passage of documented passengers, showcasing Angola's commitment to enhancing border efficiency and security. Tanzania, on the other hand, has implemented Facial Matching Systems at major airports like Kilimanjaro International and Julius Nyerere International in Dar es Salaam (Vision-Box, 2019).

The adoption of ABC Gates in these African countries, despite facing challenges such as limited technological infrastructure and funding constraints, illustrates a targeted approach. These nations are progressively overcoming these obstacles through innovative adaptations and international partnerships, showcasing the potential of such technology even in less-resourced environments.

2. Automated Passport Systems

In response to the growing need for efficient and secure border management due to escalating cross-border travel, many African nations have adopted Automated Passport Control (APC) systems. These systems, integrating advanced biometrics and digital security solutions, have become pivotal in modernizing border control mechanisms.

Ghana's Immigration Services (GIS) exemplifies this trend with the implementation of an e-visa and border management solution. As part of the broader eGhana project, supported by the World Bank, this initiative aimed to create a robust IT infrastructure to facilitate the country's sustainable development (Future Travel Experience, 2013).

The e-Immigration solution in Ghana was designed to enhance intelligence sharing among GIS officials and other security agencies. By automating passport inspection and tracking border crossings through a centralized data system, the solution streamlined and secured the border management process. The deployment at Ghana’s major entry points saw a fully computerized system for processing visa and permit applications, leveraging biometric verification. An online portal for visa applications and the implementation of electronic gates at Accra’s Kotoka International Airport were also integral to this project, aiming to facilitate rapid and automated border control (Future Travel Experience, 2013).

Beyond Ghana, other African countries have embraced similar technologies to improve their border control systems. For instance, South Africa advanced its border management by integrating biometric data with its immigration systems, streamlining the process of verifying traveler identities (Allen & Zyl, 2020).

These initiatives reflect a continent-wide shift toward more secure and efficient border control methods. By leveraging biometric technology and digital solutions, African countries have not only enhanced the security of their borders but also improved the overall experience for travelers. This transition to digital, automated systems is a critical step in addressing the challenges posed by increased regional and international travel.

The adoption of APC systems across some African countries showcases the potential of technology to revolutionize border security and management. As these systems continue to evolve, they are expected to play an increasingly vital role in facilitating safe and efficient movement across borders, aligning with broader goals of regional integration and development.

B. AI-driven video analytics and surveillance

Another AI technology adopted in border security is video analytics. The technical foundation of AI-driven video analytics is layered and intricate. Initially, video data streams from multiple high-definition cameras positioned at strategic points across borders. These cameras, equipped with infrared and night vision capabilities, ensure 24/7 monitoring. The raw footage, laden with vast amounts of data, is then processed through AI-powered video management systems (VMS). Within these systems, deep learning algorithms start by segmenting the video frame into regions of interest, meticulously identifying and classifying objects – humans, vehicles, or potential threats.

Following this initial segmentation, the AI delves into finer recognition tasks. Facial recognition tools cross-reference detected faces against databases of known criminals or individuals flagged for surveillance. Gait analysis might be employed to identify individuals based on their unique manner of walking, a valuable tool when facial features are obscured. These intricate processes are accentuated by behavioral analytics, which examines patterns of movement, loitering, or other suspicious activities that might indicate potential threats or illegal crossings.

The standout feature of these AI-driven systems is their adaptive nature. Continuous learning algorithms refine their detection and prediction capabilities by analyzing countless hours of footage. This ensures that over time, false positives decrease, and the system's efficiency at flagging genuine threats or anomalies skyrockets (Goyal et al., 2020). Moreover, machine learning models embedded within the system can predict potential high-risk events or unauthorized crossing attempts based on analyzed behavioral patterns and historical data.

Morocco's border security paradigm exemplifies the efficacious employment of these systems. Beyond the static vigilance of CCTV installations, Morocco's border surveillance network is now imbued with AI capabilities. It can discern patterns in human movement, distinguishing between regular cross-border traders and potential unauthorized migrants. Immediate alerts are dispatched upon detection of any anomaly, enabling swift on-ground interventions. This AI integration has made Morocco's borders more secure while ensuring fluidity in legitimate human movement (State Watch, 2019).

In juxtaposition, Kenya offers a holistic model, synergizing radar systems with video analytics along its border with Somalia. Here, the video feeds complement radar data. When radar systems detect uncharacteristic movement, video analytics can zoom into the area, offering visual validation and more granular detail. This interplay between different surveillance modes, all underpinned by AI, crafts a formidable border security apparatus that addresses the unique challenges presented by the region (Africa Defense Forum, 2018).

C. Inhibiting factors to the use of AI technology in border security

The prospect of harnessing AI for border security across African nations is compelling. Yet, despite its potential, there are pronounced barriers that hinder its full-scale implementation, especially when viewed through the lens of individual country experiences.

At the heart of the debate surrounding the integration of AI in border control is the critical issue of data deficiency. The prowess of AI in this domain relies heavily on its ability to rapidly process and analyze vast amounts of data. However, the effectiveness of these AI systems is significantly hampered in many African countries due to the absence of a robust data ecosystem (Adi-Ibijola & Okonkwo, 2023).

A 'data ecosystem' refers to a dynamic, interconnected network that encompasses the collection, storage, sharing, and analysis of data. It involves not only the technological infrastructure for data processing but also the policies, practices, and collaborations that govern and facilitate the effective use of data. In the context of border control, this ecosystem would typically include databases of personal and biometric information, travel records, surveillance systems, and AI algorithms that work in tandem to ensure accurate and efficient processing of information (Stobierski, 2021).

In the Global North, the integration of AI in border control has seen significant strides, largely due to the availability of extensive data. These regions leverage advanced technologies to enhance border security effectively. Automated systems here, despite criticisms of racial bias or profiling, generally function efficiently, thanks to the rich data pools that inform and refine their algorithms.

However, the situation is markedly different in many African countries. The absence or inadequacy of comprehensive data systems presents several challenges. Firstly, it limits the capacity to train AI systems effectively, leading to potential inaccuracies and inefficiencies in border control processes (The Cable, 2023). This problem is compounded when implementing technologies like facial recognition, which require diverse demographic data to function accurately. Moreover, the lack of standardized data systems across different nations in Africa hampers interoperability and cross-border cooperation, crucial for effective border management.

The lack of a structured data ecosystem presents a significant impediment to the deployment of AI in border security across Africa. AI initiatives in border control require extensive and accurate datasets to provide reliable responses and decisions (The Cable, 2023). In cases where AI systems are trained on data that does not reflect the demographic diversity of the population, these systems are prone to errors and biased ecosystems (Adi-Ibijola & Okonkwo, 2023). This is particularly problematic in border security, where incorrect identification or misjudgment can have serious implications.

Moreover, the scarcity of African AI experts on the global stage is a glaring concern that cannot be underestimated. One of the primary impediments to the adoption of modern technology, specifically AI, is the shortage of expertise (Bianco, 2021). Any successful project demands the right skill set, and AI is no exception. AI skills are notably intricate to master, and there exists a palpable disparity between supply and demand in Africa. In the development and implementation of AI systems, the incorporation of expert knowledge is imperative (Adi-Ibijola & Okonkwo, 2023). Even though IT professionals such as software developers and engineers design and develop AI applications, they are not the primary end-users of AI (Bianco, 2021). Within developing countries, the dearth of individuals prepared to work with AI is a significant predicament. Closing this skills gap through educational and training programs is essential to ensure that AI caters to the specific requirements of African border security.

Nonetheless, legislative lag appears to pose the most overarching challenge. The absence of government support stands as a substantial hindrance to the integration of AI into the African context (Adi-Ibijola & Okonkwo, 2023). African governments have lagged in formulating comprehensive legislation to govern AI's use. This delay can be attributed to various factors, including the swift pace of AI technological advancement, limited available resources, and competing national priorities.

While some African countries, including Mauritius, Egypt, Zambia, Tunisia, and Botswana, have recognized AI's potential and have devised national AI strategies, and South Africa, Nigeria, and Kenya have enacted data protection laws, these efforts are still in their infancy (Pedro et al., 2019). The African Union (AU) proposed the enactment of AI laws and regulations, designed to manage the benefits of this technology for Africans (Effoduh, 2020). Nonetheless, most of the African population adopts innovation at a more gradual pace, embracing a 'wait-and-observe' approach to technology.

Even so, in the absence of proper legislation and regulatory frameworks, grave concerns regarding the safeguarding of fundamental rights come to light (Adi-Ibijola & Okonkwo, 2023). This leads to a pivotal consideration of how AI possesses the potential to infringe upon these core rights, thereby diminishing public enthusiasm for its widespread implementation.

The subsequent part delves more profoundly into these concerns, exploring how AI may impact individual rights and privacy within the realm of border security in Africa, underscoring the critical necessity for comprehensive regulatory measures.

D. Negative impacts of AI technologies on border security and management

The adoption of AI in African border security has marked a significant shift, merging automation with human decision-making. While AI has brought enhancements, it has also surfaced critical challenges, especially in migration management. The integration of AI has raised human rights concerns, with issues like bias and privacy violations becoming evident. These challenges, far from theoretical, have real and significant consequences, particularly affecting vulnerable groups such as refugees and asylum seekers navigating these AI-enhanced border environments.

1. Bias and discrimination

AI-based border security systems in Africa represent a significant technological leap in surveillance and monitoring capabilities. However, these advancements are not without their challenges, particularly concerning bias and profiling, which disproportionately affect marginalized groups. Central to these challenges are issues rooted in flawed algorithm design, biased training data, and discriminatory programming. When these systems are trained on datasets that fail to represent the diversity of racial and ethnic groups adequately, they are prone to produce biased outcomes (Amoako-Gyampah & Salam, 2020). This can result in erroneous decision-making processes, where individuals are unfairly targeted or subjected to differential treatment based on characteristics such as race, ethnicity, nationality, or religion (Gwagwa et al. 2022).

In South Africa, the application of AI technologies in border security has brought to light the critical issues of unethical stereotyping and discrimination, accentuated by the nation's existing xenophobic tendencies (Darch et.al, 2020). AI-driven tools like facial recognition and data analytics, adopted ostensibly to streamline migration management, often embody biases that reflect deep-seated societal prejudices. This has led to discriminatory practices at borders, where AI systems have been reported to erroneously profile individuals based on their ethnicity or nationality (Darch et.al, 2020). Such incidents are particularly troubling in a region wrestling with xenophobia, as documented in a Human Rights Watch report on AI and Discrimination in South Africa (Darch et.al, 2020).

Moreover, the global trend of generating virtual personal profiles using advanced data-processing technologies, while modernizing border control, simultaneously raises significant privacy concerns. The collection, analysis, and storage of personal data, especially biometric data, pose risks of misuse and unauthorized access. In South Africa, these practices have spurred apprehensions regarding the use of this data in crucial decision-making processes for visas and asylum applications, potentially infringing on individual privacy rights (Darch et.al, 2020).

The reliance on AI technologies and training data primarily sourced from the global north further compounds the problem of bias and profiling in African border security systems. These technologies, often tailored to specific ethnicities and races, overlook the rich diversity and complexities of African populations. The consequent lack of representation and cultural understanding in training data perpetuates biases and reinforces discriminatory practices (Benjamin, 2019). These shortcomings challenge the validity and fairness of AI applications in African border security contexts.

The role of algorithms in decision-making necessitates critical scrutiny. The reliance on fully automated decisions, where machine learning algorithms function without significant human intervention, particularly in ethically sensitive situations, poses a substantial threat to the legitimacy of these systems. This form of decision-making often lacks in recognizing individuals as unique moral agents. Thus, can endanger individual rights and lead to objectionable generalizations. Incorporating human agents in the decision-making process to provide meaningful justifications and address concerns raised by affected individuals, is essential. This human involvement is not merely advisable but imperative for mitigating issues of discrimination and ensuring fair outcomes in AI implementations in border security.

2. Freedom of movement

In the intricate world of border security, the emergence of Artificial Intelligence (AI) technologies has ushered in a new era, marked by both advancement and controversy. These technologies, notably facial recognition and automated decision-making systems have been seamlessly integrated into the fabric of border control processes. However, their application has unveiled a complex array of challenges, particularly for those in dire need of refuge – the refugees and asylum seekers.

Take South Africa, for instance, a poignant example where the adoption of AI-based systems for visa processing and identity verification at border crossings has inadvertently erected barriers rather than bridges for those seeking asylum. These individuals, already caught in the throes of vulnerability, find themselves ensnared in a web of bureaucratic exigencies. They are required to furnish extensive documentation and submit to biometric data collection, a process that often leads to protracted delays. Such impediments do not just represent administrative hiccups; they pose a grave risk of refoulement or prolonged detention, starkly contradicting the sanctity of their rights and the essence of human compassion.

The specter of bias in these AI systems looms large, casting a long shadow over the objectivity and fairness of the asylum process. Algorithms, though designed to be neutral, are not impervious to the prejudices that may seep into their programming. When trained on datasets that do not represent the diversity of the human tapestry, these systems are prone to error, leading to incorrect risk assessments or, worse, the wrongful denial of asylum claims.

This intersection of technology and human rights is not merely a theoretical concern but a practical dilemma, bringing into question the alignment of AI implementations with international law. African countries, many of which are signatories to treaties and principles that champion the rights of refugees and asylum seekers, find themselves at a crossroads. These legal commitments, as underscored by the Report of the Special Rapporteur (2020) and the UN Special Rapporteur (2021), mandate a careful, individualized consideration at borders – a stipulation that seems at odds with the automated, impersonal nature of AI-driven decisions.

The solution to this conundrum lies not in the abandonment of AI technologies but in their reformation. The call is for a recalibration of AI practices in border security, where transparency in algorithm design and human oversight in decision-making are not just idealistic aspirations but essential requisites. The challenge is to strike a delicate balance between the imperatives of national security and the inalienable rights of refugees and asylum seekers. This necessitates a concerted effort to craft a framework where the use of AI in border security is not only technologically sound but also ethically grounded and legally compliant.

In the context of AI reshaping border security, a pivotal concern that emerges alongside the impact on refugees and asylum seekers is the right to privacy. The implementation of AI in border control, while enhancing security measures, introduces significant ethical challenges concerning privacy invasions, a fundamental human right enshrined in global legal standards. The inherent data collection and surveillance capabilities of AI systems necessitate a critical balance between national security interests and the preservation of individual privacy rights. This aspect of the discussion is not merely a subsidiary of the broader human rights dialogue but a central theme in the discourse on digital border management. The next chapter aims to examine this issue, exploring the complexities surrounding privacy rights in the era of AI-augmented border security.

IV. SECURITY, HUMAN RIGHTS, AND ETHICAL CONSIDERATIONS

The integration of AI into border security demands a delicate balance of reinforcing security while upholding individual privacy rights. This equilibrium becomes even more complex when navigating ethical concerns around transparency and accountability. This section aims to address the pivotal research question 'How can countries effectively harness AI in border security without infringing upon individual rights to privacy?' By examining the Kenyan context, this paper delves into the theoretical apprehensions, potential misuse scenarios, and the broader ethical quandaries associated with the role of AI in border security.

A. Right to privacy in the African context

The right to privacy stands as a foundational pillar of human rights globally. Notably, in the African landscape, this right takes on a unique dimension. Deep cultural, societal, and historical ties inform the African perception of personal liberties, making the preservation of privacy not just a legal but also a profound socio-cultural necessity.

While regional instruments like the African Charter on Human and Peoples' Rights may not overtly delineate the right to privacy, it is worth noting that a substantial number of African nations have been proactive in echoing the global sentiment towards this right. Indeed, at least thirty-five jurisdictions across the African continent have, with foresight, acknowledged and enshrined this right within their national constitutions and legal frameworks (Mavedzege, 2020). This proactive legislative move suggests that, even amidst rapid technological advancements and the challenges they pose, several African countries have recognized the importance of individual privacy rights and are committed to preserving them.

For instance, South Africa's Protection of Personal Information Act (POPIA) of 2013, Nigeria's Data Protection Act of 2023, and Ghana's Data Protection Act of 2012 are further indicators of the continent's earnest efforts to safeguard its citizens' privacy in an increasingly digital world.

Beyond national efforts, the African Union's Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, outlines a comprehensive framework to uphold the right to privacy (African Union's Convention on Cyber Security and Personal Data Protection, 2014). Adopted in 2014, it aims to bolster cybersecurity and data protection measures across the continent. The convention champions principles such as lawful data processing, data minimization, and the rights of the data subject. These principles underline the commitment to protecting individual rights and ensuring personal data is processed transparently, fairly, and with utmost security.

However, despite these legislative strides, the true crucible for the right to privacy in Africa is its intersection with security interests, especially in the age of Artificial Intelligence (AI). As AI technologies seamlessly integrate into various spheres, including border security, the very essence of privacy is put to a rigorous test. While the nuances of privacy rights might vary across African jurisdictions, the fundamental essence is a universal chorus – the inviolable nature of individual privacy.

Thus, as African nations grapple with the mounting pressures of modern border security mechanisms, the challenge is twofold: to leverage technological advancements effectively and to ensure these tools do not become instruments of disproportionate encroachments on cherished privacy rights. Yet, even with such comprehensive safeguards in place, privacy in Africa faces its biggest adversary, the looming shadow of security imperatives. This tug-of-war between the right to privacy and security interests sets the stage for the following section's discourse, an exploration of the delicate balancing act between these two powerful forces.

B. Privacy vs security interests: The AI conundrum

The intricate tension between individual privacy rights and collective security imperatives, particularly in the context of integrating AI technologies in border security, is a reflection of a profound discourse that has been echoed for generations and is resonating deeply within the African context in the digital age. This debate is deeply entrenched in philosophical traditions.

On one side stands utilitarianism embodied by the 'All or Nothing Argument', positing that the attainment of collective security enhancement may, and arguably should, supersede individual privacy rights (Solove, 2011). The underlying belief here is that maximizing overall happiness and security is paramount, even if it necessitates potential compromises on individual autonomy. In stark juxtaposition stands a view reminiscent of naive contractarianism, encapsulated by the 'Nothing to

Hide Argument'. It suggests that if state surveillance operations are transparent and entered consensually, then the ordinary law-abiding individual should not be concerned or feel threatened. This perspective emphasizes transparency over the intrinsic value of privacy, implying that surveillance, when done openly, does not breach any social or moral contract (Solove, 2011).

The pull and tug of these philosophical standpoints find more concrete manifestation in scholarly works. Allan F. Westin (1967) presents a compelling case for the inherent worth of personal autonomy. He views privacy not merely as an individual's luxury but as the cornerstone upon which democratic societies stand (pp. 167). It is a right, a privilege, and a necessity. On the flip side, Amitai Etzioni (1999) presents a contrasting narrative in his analysis of privacy and its relation to societal welfare. He argues that many theories of privacy treat it as sacrosanct, even when it conflicts with the common good. According to him, 'privacy is not an absolute value and does not trump all other rights or concerns for the common good' (pp. 196). He further elaborates on how privacy can sometimes interfere with greater social interests and often contends that, though not always, privacy should be secondary in the balance of societal needs (Etizioni, 1999).

The real-world implications of this philosophical divide are evident in the legal realm. Additionally, one cannot overlook the European Court of Human Rights' verdict in *Marper v The United Kingdom* where it was held that the retention of innocent individuals' fingerprints and DNA samples violated their right to privacy under Article 8 of the European Convention on Human Rights (*Marper v The United Kingdom, 2008*).

Drawing inspiration from these intricate philosophical debates and their resonance in global legal precedents, it becomes imperative to examine a real-life manifestation of this tension within the African context. The Huduma Namba initiative in Kenya stands as a poignant case study, epitomizing the complex interplay between privacy rights and security imperatives in the era of digitization. This paper therefore delves deeper into the nuances of this landmark initiative.

1. Huduma Namba: A Kenyan case study

The introduction of the National Integrated Identity Management System (NIIMS), colloquially known as the Huduma Namba, in Kenya initially emerged as a pivotal element of the national security strategy (Huduma Namba Admin, 2019). One of its goals was to fortify border control and elevate overall security by implementing a comprehensive biometric identity system (Huduma Namba Admin, 2019; Nyakundi, 2020, pp.17).

The system was designed to collect, process, and analyze vast amounts of data, including biometric information and real-time location details of individuals (Huduma Namba Admin, 2019). The government highlighted the system's prowess in offering unparalleled surveillance capabilities, especially at crucial points like airports and physical border checkpoints. By harnessing the power of AI, the Huduma Namba was positioned to dynamically adapt to evolving security challenges, predict potential threats, and facilitate rapid response at these critical junctures (Huduma Namba Admin, 2019; Nyakundi, 2020, pp.17).

However, the Huduma Namba initiative encountered pronounced resistance from multiple quarters. Concerned citizens, data security experts, and human rights activists raised alarms over the potential risks associated with the program. Prominent international human rights organizations, including Human Rights Watch and Amnesty International, pointed out the latent risks of the program, emphasizing the necessity for stringent data protection measures and transparency (Allen & Zyl, 2020). A particularly grave concern emerged when the Nubian community in Kenya reported cases of discrimination and exclusion during the Huduma Namba registration process, further underscoring the potential for misuse and prejudice embedded in such a wide-reaching program (Kenya Human Rights Commission, 2021).

In a momentous turn of events, the High Court of Kenya delivered a landmark judgment in January 2020, discontinuing the NIIMS program. The court's decision stemmed from the absence of proper legislation to guarantee the security of biometric data within the program. It deemed it imperative for the program to align with Kenya's Data Protection Act and undergo a comprehensive data impact assessment, consequently imposing a temporary halt on its implementation (*Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology and other ex parte Katiba Institute and Yash Pal Ghai, 2020*).

One may ponder why a state, charged with safeguarding its citizens' rights, would adopt AI-driven security measures that seemingly bypass established data protection laws and regulations. This situation can be interpreted through the lens of 'Legal Realism', a concept articulated by Roscoe Pound (1922). Legal Realism suggests that law is not a fixed set of rules but is deeply influenced by social and political factors. It proposes that the actual practice of law often diverges from written statutes, influenced by contemporary needs and pressures. In the context of emerging nations, this might manifest in states prioritizing immediate security needs, driven by political and social imperatives, even when these actions conflict with preexisting legal frameworks (Pound, 1922).

This approach, reflecting Pound's insights on how law functions in society, indicates that the swift adoption of AI for security purposes, without fully considering its implications on existing rights, is not just a technological issue but also a legal and sociopolitical one. It reveals a tendency to value the immediate, tangible benefits of modern technology over the nuanced application of laws. However, this overlooks the complexity of each context and underlines the necessity for a more deliberate and context-sensitive integration of technology, to safeguard individual rights and uphold democratic principles.

The Huduma Namba case illuminates the intricacies nations face when implementing technological solutions for security purposes. This pivotal concern, emanating directly from the Huduma Namba experience, sets the stage for a deeper exploration of Kenya's Data Protection Act, emphasizing the need for robust legislation in a world where technology, border security, and individual privacy rights are increasingly intertwined.

2. Unpacking Kenya's Huduma Namba and Data Protection Act

The case of Huduma Namba provides a compelling example that underscores the critical issue at hand – the safety and integrity of data. In the complex terrain of data management, ensuring the utmost protection of this data stands as an imperative of paramount importance (Kenya Human Rights Commission, 2021). Robust infrastructure, encryption, anonymization techniques, and secure servers emerge as indispensable components of this equation. However, as the exploration delves deeper, the focal point invariably shifts to the question of access control. Who should wield the keys to this treasure trove of data? While African governments undoubtedly shoulder a significant responsibility in safeguarding national security interests, this responsibility must be tempered with a judicious and legally sound approach to data access. The question arises: how can it be ensured that access remains the province of authorized personnel, thus avoiding the potential for misuse and violations of individual privacy?

The tenets of data protection and privacy rights underscore the necessity of a meticulous and legally sound framework for access control (Solove, 2011). The principle of data minimization dictates that access should be granted solely for the purposes for which it was collected, with clear limitations in place. This is in line with the fundamental precept of data protection – that data should only be utilized for specified, explicit, and legitimate purposes. Unfortunately, the application of this prudent approach has, in practice, faced inconsistencies.

The examination of Kenya's Data Protection Act is instructive in this context. The Act explicitly mandates that data should be confined to what is strictly necessary in relation to its intended processing purposes. It emphasizes that data should not be retained in a form that identifies data subjects for any longer than is necessary and underscores the importance of explicitly defining the purposes for which data will be used and processed (Data Protection Act, 2019).

However, a critical juncture arises when delving into the exemptions provided within the Act. Section 51 of the Act introduces a departure from these data protection principles and safeguards when matters of national security or public interest come into play (Data Protection Act, 2019). Essentially, it allows entities collecting or processing data exclusively in the name of national security or public interest to operate outside the confines of the safeguards meticulously outlined in the Data Protection Act.

Exemptions provided within data protection laws, such as those seen in Section 51 of the Kenya Data Protection Act, can be perceived as double-edged swords. On the one hand, there is a palpable rationale behind them which is to equip states with the necessary agility to respond to immediate and unforeseen security threats, and to protect the greater public good. In a world where cyber threats, terrorism, and transnational crimes are increasingly sophisticated, governments might argue the need for more flexible access to data (Bernal, 2016). However, the other edge of the sword presents a series of vulnerabilities. Such exemptions, in the absence of rigorous oversight, can serve as potential avenues for overreach, leading to breaches in citizens' privacy rights. History is replete with instances where governments, under the guise of national security, have encroached upon individual rights (Greenwald, 2014). This becomes especially concerning in the digital age, where data represents an extension of one's identity, autonomy, and dignity.

The ambiguity rooted in these exemptions is glaringly evident in the case of the Huduma Namba initiative. There is an augmented risk of data breaches, both intentional (misuse by authorized personnel) and unintentional (cyberattacks), by interlinking various databases and consolidating vast amounts of personal information. Such a centralized system, while efficient for governmental purposes, becomes a high-value target for malicious actors, both internal and external (Richards, 2013).

Furthermore, there is the looming specter of function creep – a term used to describe the scenario when data collected for one specific purpose gets used for an entirely different and often unforeseen purpose (Koops, 2011). The Huduma Namba, originally touted as a tool for national security, could easily morph into a mechanism for political surveillance, control, and suppression, especially in the absence of clear definitions of its 'ultimate purpose'.

The contention, therefore, lies in striking a delicate balance. Governments need to be equipped with tools and data to ensure national security, but this should not come at the expense of fundamental human rights. Crafting a more refined legislative framework that narrows down exemptions, coupled with the establishment of independent oversight bodies and periodic reviews, can serve as a starting point to navigate this conundrum (Bygrave, 2017). Moreover, fostering a culture of transparency and engaging in consistent dialogue with stakeholders, including the general public, can ensure that any national security measures undertaken are proportionate, necessary, and in line with democratic principles.

C. Can a balance be achieved?

Daniel Solove (2011), a prominent author, offers a critical examination of the oft-debated tension between privacy and security (Solove, 2011, pp. 17). Solove critiques the commonly held notion that pits privacy against security in an antagonistic relationship, arguing that such a dichotomy is overly simplistic and potentially misleading (Solove, 2011). Solove (2011) observes that:

> 'Privacy often loses out to security when it shouldn't. Security interests are readily understood, for life and limb are at stake, while privacy rights

> remain more abstract and vaguer. Many people believe they must trade privacy in order to be more secure. And those on the security side of the debate are making powerful arguments to encourage people to accept this tradeoff. These arguments, however, are based on mistaken views about what it means to protect privacy and the costs and benefits of doing so. The debate between privacy and security has been framed incorrectly, with the tradeoff between these values understood as an all or-nothing proposition. But protecting privacy need not be fatal to security measures; it merely demands oversight and regulation. We can't progress in the debate between privacy and security because the debate itself is flawed' (pp.2).

Drawing from Solove's perspective, it becomes evident that the clash between security and privacy requires a more nuanced approach. Instead of treating them as competing interests in a zero-sum game, there should be a focus on their potential harmonious coexistence. Particularly in this age of technological advancements, AI technologies have significantly boosted border security, emphasizing the need for strategies that ensure security imperatives do not arbitrarily trample on privacy rights.

The pathway to this equilibrium, as articulated by Solove, hinges on the effective application of oversight and regulation. Security measures, especially those pertinent to border security, need to be constrained by regulatory frameworks to prevent potential power abuses and privacy violations. Such regulatory structures must also dictate the breadth of personal data collection and its subsequent uses, ensuring security initiatives operate within predefined limits.

Taking a practical viewpoint, consider the legal challenges faced by Kenya. While its Constitution upholds the right to privacy, it confronted obstacles in preserving these rights during the Huduma Namba initiative rollout. Yet, this scenario also highlighted the role of regulatory intervention, as seen when the High Court intervened, demanding the program's compliance with the Data Protection Act (*Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology and other ex parte Katiba Institute and Yash Pal Ghai, 2020*).

Regulatory bodies and data protection authorities across Africa, too, have a monumental role in maintaining the equilibrium between security and privacy. Their tasks encompass providing unambiguous guidelines, executing regular audits, and confirming that security mechanisms abide by prevailing legal standards. This rigorous approach not only ensures public safety but also respects individual privacy rights.

A call to action for African nations is the inception of autonomous data protection authorities. These entities must possess the technical prowess to impartially arbitrate between the imperatives of national security and privacy rights (Mavedzege, 2020). While collecting biometric data for border security is not inherently objectionable, Solove's insights urge a critical assessment of such security protocols. This rigorous assessment can lead to not just enhanced privacy protections but also more effective security implementations. Solove (2011) presents a series of questions for consideration: does the measure work well? Does it infringe on privacy and civil liberties? What oversight can rectify these issues? If there is a privacy-security tradeoff, to what extent should security measures be curtailed to safeguard privacy? These inquiries should guide independent entities in their operational mandates.

D. International precedents in balancing privacy and security

Solove's perspective is not merely a theoretical assertion; it mirrors the direction already undertaken by some countries in the global North. The European Union, for instance, offers a shining testament to this balance with its General Data Protection Regulation (GDPR). This landmark regulation, while prioritizing stringent data protection norms for citizens, does not inherently stifle security initiatives. Instead, it mandates transparency, accountability, and proportionality when handling personal data for security objectives. Specifically, Article 23 of the GDPR grants member states the latitude to curtail certain data protection rights, provided it is done necessarily and proportionately to safeguard national interests, including security.

Shifting the gaze to the United Kingdom, post-Brexit developments brought forth the Investigatory Powers Act (IPA) of 2016. This legislation, while sanctioning bulk data collection for safeguarding national security, simultaneously instituted a 'double lock' mechanism. This dual approval process, necessitating the concurrence of both the Secretary of State and an independent Judicial Commissioner for surveillance warrants, underscores the very ethos of oversight that Solove advocates.

Moreover, Canada offers yet another compelling blueprint. Its Privacy Act, in tandem with the Personal Information Protection and Electronic Documents Act (PIPEDA), embodies the principles of data minimization and purpose specificity. Even when it comes to the delicate terrain of national security, entities like the Canadian Security Intelligence Service (CSIS) operate within meticulously defined parameters. Any deviations from these guidelines are subjected to stringent scrutiny by the Privacy Commissioner, thus reinforcing the indispensable nature of checks and balances.

These international paradigms underscore that the interplay between privacy and security is not an anomaly restricted to African shores. Instead, it is the methodology with which these challenges are negotiated that distinguishes the democratic fabric of nations. By extrapolating insights from these best practices, African states can customize solutions tailored to their distinct socio-political landscapes. The ultimate objective remains unwavering ensuring that while the state's legitimate security concerns are judiciously addressed, the inherent dignity and rights of its citizenry remain sacrosanct. In this harmonious coexistence of technological evolution and human rights, as encapsulated in Solove's philosophy, nations can envision a future where both realms flourish symbiotically.

V. A CALL FOR TRANSPARENCY AND ACCOUNTABILITY IN AI-DRIVEN BORDER SECURITY

In the rapidly evolving landscape of AI-driven border security, the urgency for ethical oversight intensifies, particularly in the context of Africa's rich and varied socio-political milieu. This part of the paper is dedicated to illuminating key ethical principles that should be integral to the deployment of AI technologies in border security. It offers a detailed exploration of the necessity and implementation of Transparency and Accountability as foundational pillars in this domain. Additionally, this discourse provides strategic recommendations aimed at striking an equitable balance between the imperatives of heightened security and the preservation of individual privacy rights.

A. Transparency in global echoes

Refocusing the discussion on transparency in AI systems within a legal and scholarly context underscores its significance in AI-driven border security, using established frameworks and perspectives. Legal doctrines and scholarly consensus converge on the principle that transparency is a fundamental legal and ethical necessity in the deployment of AI technologies, particularly in sensitive areas like border security.

The need for transparency is rooted in making AI decision-making processes accessible and understandable, aligning them with societal norms and legal standards. Scholars in the field of AI ethics, such as Lawrence Lessig (2006) emphasize transparency's importance for the ethical application of technology. Lessig's (2006) framework advocates for technology to be open to inspection and auditing, ensuring compliance with ethical and legal norms.

The European Union’s General Data Protection Regulation (GDPR) exemplifies a legal framework mandating transparency in AI systems. It insists on individuals' right to understand the logic behind significant automated decisions impacting them.

This stance underscores the necessity for AI systems in border security to operate transparently, allowing for accountability and public scrutiny.

Academic voices like Cathy O’Neil (2017) have argued for the need for more interpretable and transparent AI systems. O'Neil highlights the risks of opaque algorithms leading to biased and discriminatory outcomes, advocating for AI systems that are open to examination and critique. Similarly, Frank Pasquale (2015) champions transparent audit trails in AI systems to enable accountability for harmful decisions or practices. This perspective is particularly crucial for AI applications in border security, where decisions have significant implications for individual rights and freedoms.

The adoption of transparency as a core principle in AI legal frameworks is gaining traction in various countries and regions, demonstrating its effectiveness in balancing privacy and security. For instance, the GDPR emphasizes the transparency of AI systems and mandates the right to explanation for affected individuals. Canada's Directive on Automated Decision-Making, applicable to AI systems in federal departments, requires AI technologies to undergo assessments for their impact on privacy and human rights (OECD. AI Policy Observatory, 2023). Singapore’s Model AI Governance Framework also highlights transparency, providing guidelines for transparent AI operations in areas with significant societal impacts, like border security (Personal Data Protection Commission Singapore, 2020).

These examples show that embracing transparency in AI governance fosters a more responsible and trustful use of technology. Transparent AI systems in border security enable stakeholders, including the public and policymakers, to understand and trust the decisions made by these systems, a vital component for their successful integration into security operations.

In conclusion, transparency serves as a crucial bridge, connecting the advanced capabilities of AI in enhancing border security with the imperative of protecting individual privacy. By adopting transparent AI practices, countries can foster an environment where security and privacy coexist harmoniously, balancing the effectiveness of AI in security with the sanctity of individual rights. This approach is not only a legal and ethical necessity but also a practical solution to the challenges posed by integrating AI into border security, leading to technology that is as responsible as it is revolutionary.

B. Accountability in an AI-driven world

Accountability is pivotal in AI deployments, particularly when considering the profound societal impacts, they can have. Instances such as South Africa's collaboration with Huawei for advanced urban surveillance, although not directly border-related, reflect potential implications of similar technologies at border checkpoints (Reuters, 2019). Uganda's experience, where Huawei reportedly assisted in hacking opposition politicians, further illustrates the dangers of unchecked AI power, potentially leading to the misuse of technology for political surveillance (Mozur, 2019).

This scenario underscores the dangers of unchecked power, leading to the potential misuse of technology for political ends. Global initiatives, like Canada's Directive on Automated Decision-Making, emphasize the need for risk assessments and bias reviews (Government of Canada, 2019). Such guidelines serve as a reminder that while AI's capabilities can be harnessed for efficiency, it is essential to weave in stringent safeguards to ensure the technology remains accountable.

In summary, strict accountability measures are essential in AI deployments for border security. Learning from the experiences of South Africa and Uganda and guided by frameworks like the EU's AI Act and international human rights standards, it becomes clear that accountability must be foundational in AI deployment. Such measures ensure that AI technologies not only enhance border security efficiency but also uphold fundamental human rights and freedoms, maintaining ethical integrity and public trust in AI applications.

C. Bridging the gap with collaborative policies

In light of the paper's focus on Africa's transition from traditional border security measures to the integration of Artificial Intelligence (AI), this paper recommends the development and implementation of collaborative policies as a pivotal strategy for achieving a harmonious balance between security imperatives and the safeguarding of fundamental human rights and freedoms.

The transformative potential of AI in border security, with its advanced techniques like biometric data processing, facial recognition, and iris scanning, brings forth a spectrum of ethical considerations, chief among them being transparency and accountability. The burgeoning use of these technologies in Africa underscores the need for robust frameworks to manage the complexities of personal information, addressing concerns over data storage, accessibility, and the risk of misuse.

To navigate these challenges effectively, Africa can look towards global initiatives as models for developing collaborative policies. The European Union's AI Act proposal, for instance, sets a precedent in establishing harmonized regulations for high-risk AI applications, including those in border security. Such frameworks emphasize transparency, data governance, and accountability, aligning with the need for ethical AI deployment.

Furthermore, regional initiatives within Africa, such as the African Union's Digital Transformation Strategy and the Smart Africa Initiative, lay the groundwork for collaborative digital policymaking. These strategies, while broad, provide a foundation upon which specific AI governance frameworks for border security can be built, tailored to the unique socio-political contexts of the continent.

In practice, these collaborative policies should encompass rigorous risk assessments, bias reviews, and strict guidelines for data handling and security. They should ensure that AI systems used in border security are not only efficient but also operate within a framework that respects privacy and human rights.

VI. CONCLUSION

In Africa's ambitious journey to harness AI's potential for border security, the balance between innovative advancements and the protection of human rights stands out as a central concern. This paper underscores the profound ethical and privacy challenges that emerge alongside the promises of heightened security and efficiency. The digital fingerprints and biometric traces left at border crossings, while essential for security, possess inherent vulnerabilities that could be exploited if mismanaged or abused. The narrative of Africa's border security evolution emphasizes the necessity for both technological advancement and the upholding of individual rights, transparency, and ethical governance.

Achieving a harmonious balance between these objectives, though intricate, is achievable. This equilibrium requires ongoing policy evaluation, introspection, and broad stakeholder engagement to ensure technological progress respects foundational societal principles.

Furthermore, the adoption and integration of AI in border security across the African continent present extensive research opportunities. Potential studies could delve into the legislative frameworks guiding AI adoption in various African nations or spotlight the socio-political repercussions of such systems on marginalized communities. As the global landscape becomes increasingly interconnected, there is an imperative for transparent, accountable, and rights-respecting AI systems. This drive goes beyond technological integration. It is an endeavor to ensure every advancement not only uplifts but also safeguards every individual, without prejudice.

In conclusion, this paper posits that achieving a harmonious balance between enhancing security and protecting individual rights in Africa is attainable through the adoption of collaborative policies in AI governance. By drawing on global models and building upon regional initiatives, African nations can forge a path that harnesses the benefits of AI in border security while upholding the ethical principles of transparency and accountability. Such an approach will not only facilitate the continent's commitment to efficiency and innovation but will also ensure that the deployment of AI technologies respects and protects fundamental human rights and freedoms.

REFERENCES

Adebajo, A., & Rashid, I. (2004). West Africa's Security Challenges: Building Peace in a Troubled *Region. Lynne Rienner Publishe*r. https://doi.org/10.1017/S0022278X05210984.

Adi-Ibijola, A., Okonkwo, C. (2023). *Artificial Intelligence in Africa: Emerging Challenges In Responsible AI in Africa: Challenges and Opportunities. Social and Cultural Studies of Robots and AI.* Palgrave Macmillan. 10.1007/978-3-031-08215-3_5

Africa Defence Forum. (2018 May 25) *Surveillance technology helps secure border zones.* Defenchttps://adf-magazine.com/2017/12/the-invisible-wall/

African Union Migration Policy Framework for Africa, (2006).

Akinyemi, O., (2013). Globalization and Nigeria Border Security: Issues and Challenges. *International Affairs and Global Strategy*, *11*. https://www.files.ethz.ch/isn/168769/01.pdf

Allen, K., Zyl, I, (2020). Who's watching who? Biometric surveillance in Kenya and South Africa. *enact,* 17. https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf.

Amoako-Gyampah. K., Salam. A (2004). An extension of the technology acceptance model in an ERP environment. *Information & Management. 41*(6). https://doi.org/10.1016/j.im.2003.08.010

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

Balasubramaniam, N. Kauppinen, M, Rannisto, A. Kari,H., Kujala,S. .(2023) *Transparency and explainability of AI systems: From ethical guidelines to requirements, Information and Software Technology, 159.*[Paper Presentation] https://doi.org/10.1007/978-3-030-98464-9_1.

Benjamin, R. (2019). Assessing risk, Automating Racism. *Science, 366*(64). https://doi.org/10.1126/science.aaz3873

Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. *Journal of Cyber Policy, 1*(2), 243-264. https://doi.org/10.1080/23738871.2016.1228990

Bianco, M., (2021). *Overcoming the social barriers of AI adoption. [Masters Thesis, Eindhoven University of Technology] https://research.tue.nl/en/studentTheses/overcoming-the-social-barriers-of-ai-adoption*

Borenstein, J., Howard, A. (2021). Emerging challenges in AI and the need for AI Ethics Education. *AI Ethics* 1. https://doi.org/10.1007/s43681-020-00002-7

Burt, C. (2019 October 7). *NEC facial recognition border tech for Kenya as airport biometrics rollouts continue.* Biometric.com. https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue

Bygrave, L. A. (2017). *Data privacy law: An international perspective.* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Canada's Privacy Act Canada. (1985). Privacy Act, R.S.C., 1985, c. P-21. Justice Laws Website.

Chome, N. (2021). Borderland infrastructure and livelihoods: a review of implications for the development of formal border crossings in Mandera County, Kenya. *Research & Evidence Facility.* https://blogs.soas.ac.uk/ref-horn-research/2021/04/12/borderland-infrastructure-and-livelihoods-a-review-of-implications-for-the-development-of-formal-border-crossings-in-mandera-county-kenya/

Coetzee, J.,(2018). Strategic implications of Fintech on South African retail banks. South African *Journal of Economic and Management Sciences 21*(1).https://doi.org/ 10.4102/sajems.v21i1.2455

Constitution of the Republic Kenya. (2010).

Dahshan, M., Masbah, M. (2020). Synergy in the North: Furthering Cooperation. *Chatham House.* https://www.chathamhouse.org/sites/default/files/2020-01-2020-Synergy-North-Africa.pdf

Darch, C, Majikijela, Y. Adams, R. Rule, S. (2020 March). AI, Biometrics and Securitization in Migration Management: Policy Options for South Africa. *Policy Action Network.* http://hdl.handle.net/20.500.11910/15281

Data Protection Act (2019). Kenya

Data Protection Act, 2012 Ghana.

Data Protection Regulation (NDPR), 2019 Nigeria.

Dugbazah, J. Glover, B. Mbuli, B. Kungade, C. (2021 October 5). Enhancing Border Security in Africa Using Smart Border Contril Technologies. *African Union Development Agency. https://www.nepad.org/blog/water-sanitation-and-hygiene-revolution-africa-using-smart-technologies*

East African Community (EAC). (2010). Common Market Protocol.

Edwards, D. (2023 May 23). *AI and Identity Verification: Revolutionizing Security and User Experience.* Robotics & Automation News. AI and Identity Verification: Revolutionizing Security and User Experience – Robotics & Automation News (roboticsandautomationnews.com)

Effoduh, J. (2020 October 20). *7 ways that African states are legitimizing artificial intelligence.* Openair.Africa. 7 Ways that African States are Legitimizing Artificial Intelligence | Open AIR

Etzioni, A. (1999). The Limited of Privacy. 196

European Court of Human Rights. Marper v. the United Kingdom. Applications nos. 30562/04 and 30566/04, 2008.

Future Travel Experience. (2013 April). *Ghana airports adopt biometric border management system in eGhana project* Future travel experience. https://www.futuretravelexperience.com/2013/04/ghana-airports-adopt-biometric-border-management-system-in-eghana-project/

General Data Protection Regulation (GDPR) European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.

Geoghegan, S. (2023 May 4). *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers Epic.org.* https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/

Gituanja, N. (2013). *Border Management and National Security: An Analysis of the Implementation of Border Policies in Kenya.(Publication No: R50/68470/2011) [Master's Thesis, University of Nairobi].http://erepository.uonbi.ac.ke/bitstream/handle/11295/60490/Gituanja_Border%20management%20and%20national%20security.pdf;sequence=3*

Government of Canada. (2019). Directive on Automated Decision-Making.

Goyal, A., Anandamurthy, B., Dash, P., (2020). *Automatic Border Surveillance Using Machine Learning in Remote Video Surveillance Systems. Emerging Trends in Electrical, Communications, and Information Technologies*. Springer. https://doi.org/10.1007/978-981-13-8942-9_64

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Journal of Strategic Security 9(3).L: https://www.jstor.org/stable/10.2307/26473340

Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg,I., and De Beer, J., (2020). Artificial Intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. *The African Journal of Information and Communication, 26*. 10.23962/10539/30361

Herbst, J. (2000). *States and Power in Africa*. Princeton University Press.

Huduma Namba Admin. (2019). Huduma Namba and Our National Security Strategy.

International Data Corporation. (2023 April 11). *The Middle East & Africa will See the World's Fastest AI spending Growth Through 2026*, trendsmena. https://trendsmena.com/business/middle-east-and-africa-to-see-fastest-ai-spending-growth-in-2022-26-idc/#:~:text=While%20this%20will%20account%20for%20just%202%20percent,billion%20in%202026%2C%20IDC%20said%20in%20a%20statement.

International Organization of Migration. (2020). *Africa Migration Report: Challenging the Narrative.* https://publications.iom.int/books/africa-migration-report-challenging-narrative

Investigatory Powers Act (IPA) of 2016 United Kingdom. (2016). Investigatory Powers Act 2016. Chapter 25. The Stationery Office.

Jili, B. (2020 December 11). *The Spread of Surveillance Technology in Africa Stirs Security Concerns*. Africa Center for Strategic Study. https://africa-center.org/spotlight/surveillance-technology-in-africa-security-concerns/

Kenya Human Rights Commission. (2021 October 18). Consortium Applauds Court Judgement Declaring Huduma Cards Illegal; Calls for Further Reforms. https://citizenshiprightsafrica.org/kenya-consortium-applauds-court-judgement-declaring-huduma-cards-illegal-calls-for-further-reforms/

Koops, B. J. (2011). Forgetting footprints, shunning shadows. A critical analysis of the "Right to Be Forgotten" in big data practice. *Scripted, 8*(3), 229-256. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719

Kris, L. (2019 March 5). *Automated Border Control – Rising Trend Continues, Experts Say*. Adaptive Recognition. https://adaptiverecognition.com/blog/identity-industry/automated-border-control-gates-growth-in-2018/

Landau, L. B., & Segatti, A. (2009). *Human development impacts of migration: South Africa case study. Human Development Research Paper,* UNDP. https://mpra.ub.uni-muenchen.de/19182/1/HDRP_2009_05.pdf

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

Martins, B., Lidén, K. & Jumbert., M. (2022). Border security and the Digitalization of sovereignty: insights from EU borderwork, *European Security, 31*(3). https://doi.org/10.1080/09662839.2022.2101884

Mavedzege, J. (2020). The Right Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance. *African Journal of Legal Studies, 12*(3). https://brill.com/view/journals/ajls/12/3-4/article-p360_7.xml

Mikalef, P. Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information and Management 58*(3). https://doi.org/10.1016/j.im.2021.103434

Mozur, P. (2019). *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*. The New York Times. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times (nytimes.com)

Najibi, A. (2020). Racial Discrimination in Face Recognition Technology. Harvard University. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Nigeria Immigration Services. (2023). NIS History.

NIST (2020). *Biometric Recognition Systems and Their Application.* National Institute of Standards and Technology. https://www.nist.gov/programs-projects/biometrics

Nwadike F, Ekeanyanwu N. (2012). Building sustainable peace in Africa: Nigeria in perspective. *African Media and Democracy Journal; 1*(1). https://www.academia.edu/4883555/BUILDING_SUSTAINABLE_PEACE_IN_AFRICA_NIGERIA_IN_PERSPECTIVE

Nyakundi F. (2020). *Huduma Namba: Kenya's Transformation into an Infor-*

mational State. [Master's Thesis, University of Washington]. Nyakundi_washington_0250O_22269.pdf

O. Bello, P., & A. Olutola, A. (2020). Modern Slavery and Human Trafficking. In Revves J (Ed).*The Conundrum of Human Trafficking in Africa*. IntechOpen. https://www.intechopen.com/chapters/70938

OECD. AI Policy Observatory (2023). Canada's Directive on Automated Decision-Making. Directive on Automated Decision-Making- Canada.ca

Okumu, W. (2011). Border Management and Security in Africa. *The Border Institute*. https://www.researchgate.net/publication/308983535_Border_Management_and_Security_in_Africa#full-text

O'Neil, C. (2017). *Weapons of Math Destruction*. Penguin Books.

Open Society Justice Initiative. (2020). Kenya's National Integrated Identity Management System.

Parliamentary Monitory Group (2019 March 5). HANIS & Automated Biometric Identification System (ABIS).

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. : Harvard University Press.

Pato, J & Millet, L. (2010). *Biometric Recognition: Challenges and Opportunities*. National Academies Press. https://doi.org/10.17226/12720

Personal Data Protection Commission Singapore. (2020). Singapore's Approach to AI Governance.

Personal Information Protection and Electronic Documents Act (PIPEDA) Canada. (2000). Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. Justice Laws Website.

Peters, U. (2022). Explainable AI lacks regulative reasons: why AI and human decision-making are not equally opaque. *AI Ethics*. https://link.springer.com/article/10.1007/s43681-022-00217-w

Pound, R. (1922). *An Introduction to the Philosophy of Law*. Yale University Press.

Protection of Personal Information Act (POPIA), 2013 South Africa.

Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology and other ex parte Katiba Institute and Yash Pal Ghai, (2020) eKLR.

Reuters Staff (2019). *Huawei 'worked with' China military on research projects*. Reuters. https://www.bing.com/search?pglt=163&q=Reuters+Staff+(2019).+Huawei+%27worked+with%27+China+military+on+research+projects.+Reuters.&cvid=523d08e9f3d34c429d32a0eb0a3fb183&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQRRj8VdIBBzQwM2owajGoAgCwAgA&FORM=ANNAB1&PC=U531

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934-1965. https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

SA Home Affairs (2018). ABIS project progress report. South Africa Department of Home Affairs.

Saddiki, S. (2020). Border Walla in a Regional Context: The Case of Morocco and Algeria. Borders and Border Walls: In-Security, Symbolism, Vulnerabilities. *Routledge*. https://doi.org/10.4324/9780429352508-8

Santoni de Sio, F., Mecacci, G. (2021). Four Responsibility Gaps with Artificial Intelligence: Why they Matter and How to Address them. Philos. *Technol. 34*. https://doi.org/10.1007/s13347-021-00450-x

Solove, DJ. (2011). Nothing to Hide: The False Tradeoff between Privacy and Security. *Yale University Press*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1827982

State Watch. (2019 September 30). Spanish Moroccan borders upgraded with new cameras, facial recognition and a barbed wire swap. Statewatch | Spanish-Moroccan borders upgraded with new cameras, facial recognition and a barbed wire 'swap'

Stobierski, T. (2021 March 2). *5 Key Elements of a Data Ecosystem*. Harvard School of Business. 5 Key Elements of a Data Ecosystem (hbs.edu).

Tech 5. (2023 April 27). *Leveraging AI to Develop Best-in-Class Biometric Algorithms*. https://tech5.ai/leveraging-ai-to-develop-best-in-class-biometric-algorithms/

The Cable. (2023 May 23). *Artificial Intelligence in migration, border control, and security*. https://www.thecable.ng/artificial-intelligence-in-migration-border-control-and-security#google_vignette

Tyler H. (2022 February 2). *The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions*. The Migration Policy Institute. https://www.migrationpolicy.org/article/artificial-intelligence-border-zones-privacy

UN Economic Commission for Africa (2016). The Africa Data Revolution report. https://www.undp.org/africa/publications/africa-data-revolution-report-2016

UNESCO (2021). Recommendations on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

United Nations Human Rights. (2020). *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*. (UN A/77/549) https://www.ohchr.org/en/documents/thematic-reports/a77549-report-special-rapporteur-contemporary-forms-racism-racial

United Nations Human Rights. (2021). Special Rapporteur on contemporary forms of racism. https://www.ohchr.org/en/special-procedures/sr-racism

United Nations Office of Drugs and Crime. (2020) *Global Report on Trafficking in Persons*. https://www.unodc.org/unodc/en/human-trafficking/global-report-on-trafficking-in-persons.html

United Nations Refugee Agency, (2017). Uganda - Refugees and asylum-seekers (urban). https://data.unhcr.org/en/documents/details/80039

Vision-Box, (2019). Pursue for Harmonized ID and Smart Borders Gains Ground in Africa. https://www.id4africa.com/2019/almanac/FR/VISION-BOX.pdf

Westin, F. *Privacy and Freedom*. Atheneum, 1967.

World Economic Forum. (2022 May). Growing Intra-African Trade through Digital Transformation of Border and Customs Service's Regional Action Group for Africa. https://www.weforum.org/press/2022/05/growing-intra-africa-trade-through-digital-transformation-of-customs-and-borders-a9b9b2dcb0/

World Economic Forum. (2022). *Travel & Tourism Competitiveness Report*. https://www.weforum.org/publications/travel-and-tourism-development-index-2021/in-full/

Zandonini, G. (2019) *Biometrics: The new frontier of EU migration policy in Niger*. The New Humanitarian, https://www.thenewhumanitarian.org/news-feature/2019/06/06/biometrics-new-frontier-eu-migration-policy-niger