Research Note

Authoritarian Alliances and the Politicking of Data in Africa

Beverley Townsend and Arthur Gwagwa

Abstract. This research note explores the need for further research into increasing accounts of the unregulated acquisition, use, and control of personal data by foreign states in collaboration with certain African states. Limited local research on the acquisition of large-scale digital data by African authoritarian governments, with the backing of certain foreign actors, has meant that African civil society has insufficiently confronted the human rights implications. Yet these practices are not new and are a continuation of authoritarian influence into the digital era.

1 Introduction

Africa has of late been the target of pervasive and unregulated digital practices. This research note identifies two interrelated and emergent issues within Africa: first, the collection, processing, repurposing, and sharing of personal data by both state and non-state actors, and second, the use of data-capturing technologies, including various surveillance and facial recognition systems. These are practices that directly challenge human well-being and human rights: rights to self-determination (of either individuals or groups), rights to autonomy, and privacy rights.

The current extraction of data for political and economic value is fueled by the technological trend known as "datafication," which turns many aspects of human life into data that is then realized as a new form of value. Personal data—information related to an identifiable person—is collected without the data subject's knowledge or consent, and often contrary to the user's expectations. Such data is recorded and stored in digital formats, can be distributed widely across platforms, and, with the assistance of digital technologies, is vulnerable to forms of user exploitation and harm. Unlawful and unethical collection and processing is not only an affront to the user's autonomy and right to self-determination, but also can have the deleterious effect of shifting the balance of power in favor of the party controlling the data. Control equates to power that, in turn, translates into financial or other advantages and promotes the controlling party's interests (Véliz 2021).

Aligned with various data privacy violations, including the collection and processing of data, is the interrelated and increasingly widespread use of data-capturing technologies: technologies that intentionally or inadvertently capture and record data. While

doi:10.54501/jots.v2i1.111

data-capturing technologies, such as surveillance, facial recognition, and monitoring technologies, may be used for lawful purposes, they have recently been implicated in enabling human rights abuses by allowing certain states a measure of social control and enabling them to “exert increasing levels of influence over industries and governments around the world” (ASPI 2019).

Invasive data collection is also achieved through weak legal standards. Surveillance and monitoring technologies, although country specific, are being deployed and operated within the ambit of developing, underdeveloped, onerous, or vague legal and policy frameworks. The full impact on individual and group rights from such novel digital methods is yet to be ascertained; however, as historical events have demonstrated, the impact on Africans’ right to self-determination resulting from the arising geopolitical power asymmetries can be immense. As foreign states, often with the support from industry, enter into collaboration with African governments to extract data for strategic political reasons, the reach of online, digitized information creates novel challenges to African peoples’ human rights (Gwagwa and Townsend 2024).

2 Privacy challenges of data protection and data-capturing technologies

By 2022, 162 countries worldwide had enacted data privacy laws. Africa has been the region of fastest global data protection expansion (Greenleaf 2023), with an increase in adoption of data protection laws, the most recent of which was by eSwatini (Swaziland) and Tanzania in 2022. However, reports suggest that there have been mass biometric data collections in 23 African countries by various third-party state and non-state actors amid largely inadequate data protection safeguards (CIPESA 2022). Countries affected are, among others, Algeria, Angola, Benin, Burkina Faso, Cape Verde, Congo, Gabon, Lesotho, Madagascar, Niger, Togo, and Sierra Leone (ICTWorks 2022). A confluence of factors, including the limitation and fragmentation of data protection laws and surveillance regulation in certain African countries, together with disparate and ineffective oversight and enforcement mechanisms, exacerbates the data privacy position in Africa. Greater awareness and monitoring is required, as is the call for data-unregulated African countries to urgently provide data protection.

To facilitate data collection, foreign actors engage in a form of regulatory arbitrage that enables them to arrange and structure their communications and transactions to evade more restrictive national regulations, in favor of the advantages offered by less stringent foreign regulatory regimes (Froomkin 1997). As many African countries adopt biometric digital identity systems for public services improvement, the personal biometric data of entire populations is collected, processed, and used. Arising threats brought about by such acquisition pose serious risks to the people of certain African countries—by either or both governments themselves or, directly or indirectly, third-party actors (be they from industry, commerce, private corporations, or the like)—who gain access to such data and are granted the freedom to use data-capturing technologies.

While not the only reason, this is in large part due to the absence, or inadequacy, of data protection laws; the lack of restriction on cross-border data exchanges; and insufficient oversight and enforcement of the collection, processing, and access to personal data, which fall short of prescribed safeguards under international human rights law. Such instances of data collection show patterns of informational privacy and data abuse, and in the case of certain African countries, demonstrate the development of alliances between authoritarian governments and foreign state and non-state data brokers. Pauwels (2020) describes, for example, how ruling governments are repurposing biometric data for manipulative electoral campaigns and agreeing to massive data collection and management arrangements outside the national democratic accountability structure. These governments have been reluctant to pass legislation that constrains foreign activities and protects their citizens. The difficulty too is that such developments are part of a broader trend of placing political interests ahead of national and continental security interests, which, for example, is seen in the slow pace at which the African bloc agreed to ratify and adopt data protection and cyber governance policies such as the now in force African Union Malabo Convention (African Union 2014).

The privacy challenge of data collection is also exacerbated by data-capturing technologies, such as surveillance cameras, deployed in cities and at borders, ostensibly to improve service delivery and public security. The risk is that this data may also be used for other purposes, such as influencing political campaigns and inflaming tensions for strategic political reasons. Data collected can also be used to surveil political opponents, dissidents, and human rights defenders as well as to limit civil liberties such as privacy, free speech, and free association. Stevens et al. (2023) demonstrate how rights, essential to the development of personal identity and effective functioning of participatory democracy, are implicated by surveillance technologies in Zimbabwe.

While data-capturing technologies are dual use—that is, for legitimate counterterrorism initiatives and law enforcement—the allegation is that certain countries are creating a future of technology-driven authoritarianism in countries that have low regulatory thresholds, are non-privacy preserving, and lack the rule of law, and where the technology is deployed to limit the organic expression and development of democracy. These countries are unfortunately not isolated anomalies but are symptomatic of a broader precedent-setting trend.

3 Foreign authoritarian influences

International procurement of surveillance technologies has long been a target of certain exporting states (Feldstein 2019), and with the expansion of AI surveillance comes the acquisition of vast datasets in countries that Cheeseman, Lynch, and Willis (2018) suggest “lack the political will and institutional framework necessary for it to function effectively.”

While trade links with the US are concentrated to mature democracies, authoritarian states and weak democracies are substantially more likely to import AI from China relative to mature democracies (Beraja et al. 2023). In 2022, China was the largest exporter of AI-enabled technologies worldwide, with 201 export deals involving facial recognition systems. A staggering 45% of China’s facial recognition exports are to authoritarian states and weak democracies (using the polity score in Marshall, Gurr, and Jaggers (2016)), including many in Africa (Beraja et al. 2023). Given the escalating trend in the use of digital identifiers and data analytics in Africa, and the utter unwillingness or inability to provide adequate citizen safeguards, China’s motivation to export AI technology to non-democratic, underregulated regimes should be a cause for concern.

States with poor digital rights records, declining democracy, and rising digital authoritarianism stand to be targeted and implicated the most—casting doubt on the integrity of biometric data collection programs and their resultant databases. By way of illustration, in 2017, China entered into an agreement with Zimbabwe to deploy facial recognition software in Harare. Ostensibly, similar agreements have been signed in Angola and Ethiopia (HRW 2014; Gwagwa and Garbe 2018). Ethiopia, for example, while one of the poorest countries in the world, has the capabilities of a highly technologically advanced, online censored and surveillance state (Wilson, Lindberg, and Tronvoll 2021).

The difficulty is also that China is exporting its technologies along with a very particular ideological worldview. It envisages an internet that forms part of a broader digital ecosystem of its making and in a way that enables and supports digital authoritarianism (ASPI 2019). Russia and China promote internet control by controlling norms in regional and international institutions through, inter alia, filtering or blocking websites, using counterinformation campaigns and surveillance technologies, and censoring and controlling content (Deibert et al. 2010; Ebert and Maurer 2013; Flonk 2021). The power asymmetries created by the Chinese normative influence on Africa have a long-term impact on groups' rights to self-determination.

These developments have serious geopolitical implications. First, a weaker and cyber-insecure Africa has important implications for the US and other established democracies, if only because Africa can be used as a launch pad for global cyberterrorism and cybercrime (INTERPOL 2021). Second, China's AI technology exports are leading to the emergence of new power structures outside the control of existing governance and accountability frameworks and have an impact on the rules-based global order and geopolitical alliances (see also Freyburg and Garbe (2018) and Meservey (2018)).

This external influence and imposition of values on African peoples has a long history. We identify too that several African countries inherited surveillance laws from the past, in particular those that legalize surveillance and allow the criminalization of legitimate conduct in the interest of public order and safety, child protection, national security, morality, and health. As shown in the case of Belgian national IDs in Rwanda leading to the 1994 genocide, the invasive collection of biometric data lead to the marginalization and elimination of population groups so identified. Therefore, in many ways, surveillance in the digital age does not merely advance the normative influence by major illiberal powers (Pauwels 2020), but also supports preexisting regimes of monitoring that political activists and African citizens faced in daily life prior to the onset of the digital age. Any research into the local position must be informed by an understanding of these important historical influences.

4 Conclusions and future research questions

In this research note we have given a broad overview of the challenges and risks of digital repression brought about by the increasing unregulated acquisition, use, and control of personal data by foreign state and non-state actors in Africa and the politics that underpin it. Fragile asymmetrical power dynamics already exist in certain parts of Africa, which may be aggravated with the advent of data-informed power imbalances and a deepening digital divide (see WEF (2020)). We need to ask: (1) where and how data and data-capturing technologies are benefiting and compromising privacy interests across Africa; (2) how this occasions harms to groups and to individuals; (3) what legacy and present influences inform these harms; and (4) how digital constitutionalism can be reimagined as a constitutional architecture or framework that is cognizant and protective of rights and fundamental freedoms in a digital age.

There is limited academic research that critically examines the issues we have raised in this paper. This failure highlights a lack of capacity by local researchers in utilizing mixed methods approaches to understand this complex and evolving area often shrouded in secrecy. Further quantitative and qualitative research is required. While research has been limited to date because of logistical challenges, we believe that local researchers must harness and foster international collaborations and consider the research methods and issues we raise below:

- Through case study analysis and process-tracing methodology, explore how the

Sino-Russian model of cybernationalism (Bolt and Cross 2018) and the normative influence founded on such close ties are developing between Africa and China and how they diffuse and influence African cybernorms.

- By focusing on a few qualitative case studies over a longer period, consider how the challenges brought about by the large-scale data collection by authoritarian African governments compare between countries without data protection laws, such as Mozambique, Libya, the Central African Republic, Sudan, and South Sudan, and those that have adopted data protection laws, such as South Africa, Ghana, and Kenya.
- Through empirical field quantitative and qualitative studies, consider the impact of AI-enhanced technologies, and how such technologies are designed in theory and practice, what their capacities are, and where they are located. Consider also what governance models are suitable for oversight and for safeguarding human rights, and how historical data governance structures influence the current governance frameworks.
- And lastly, consider the criteria and heuristics African governments should use to measure the value of personal and non-personal data and its cross-border transfer and to understand lessons that might be adopted from other global regions.

References

African Union. 2014. “African Union Convention on Cyber Security and Personal Data Protection, Declaration of Principles on Freedom of Expression and Access to Information.” https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Australian Strategic Policy Institute. 2019. “Mapping China’s Tech Giants.” https://www.aspi.org.au/report/mapping-chinas-tech-giants.

Beraja, Martin, Andrew Kao, David Y. Yang, and Noam Yuchtman. 2023. *Exporting the Surveillance State via Trade in AI.* Technical report. Working Paper. Brookings. https://www.brookings.edu/wp-content/uploads/2023/01/Exporting-the-surveillance-state-via-trade-in-AI_FINAL-1.pdf.

Bolt, Paul J., and Sharyl N. Cross. 2018. “The Sino, Russian Military, Security Relationship: Emerging Trends and Challenges.” In *China, Russia, and Twenty-First Century Global Geopolitics.* Oxford University Press, February. https://doi.org/10.1093/oso/9780198719519.003.0003. eprint: https://academic.oup.com/book/0/chapter/193836768/chapter-ag-pdf/44622703/book_25992_section_193836768.ag.pdf.

Cheeseman, Nic, Gabrielle Lynch, and Justin Willis. 2018. “Digital dilemmas: The unintended consequences of election technology.” *Democratization* 25 (8): 1397–418. https://doi.org/10.1080/13510347.2018.1470165.

Collaboration on International ICT Policy for East and Southern Africa. 2022. *Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa.* Technical report. CIPESA. https://cipesa.org/wp-content/files/reports/Privacy-Imperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-Africa-Report.pdf.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* MIT Press. ISBN: 978-0-262-26603-1. https://doi.org/10.7551/mitpress/8551.001.0001.

Ebert, Hannes, and Tim Maurer. 2013. “Contested cyberspace and rising powers.” *Third World Quarterly* 34 (6): 1054–74. https://doi.org/10.1080/01436597.2013.802502.

Feldstein, Steven. 2019. *The Global Expansion of AI Surveillance.* Vol. 17. Carnegie Endowment for International Peace Washington, DC.

Flonk, Daniëlle. 2021. “Emerging illiberal norms: Russia and China as promoters of internet content control.” *International Affairs* 97 (6): 1925–44. https://doi.org/10.1093/ia/iiab146.

Freyburg, Tina, and Lisa Garbe. 2018. “Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa.” *International Journal of Communication* 12:3896–916. https://ijoc.org/index.php/ijoc/article/view/8546.

Froomkin, A Michael. 1997. “The Internet as a source of regulatory arbitrage.” *Borders in Cyberspace (Brian Kahin & Charles Nesson, eds.)(1997).*

Greenleaf, Graham. 2023. “Global data privacy laws 2023: 162 national laws and 20 Bills.” *Privacy Laws and Business International Report (PLBIR),* https://doi.org/10.2139/ssrn.4426146.

Gwagwa, Arthur, and Lisa Garbe. 2018. “Exporting repression? China’s artificial intelligence push into Africa.” *Council on Foreign Relations,* https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa.

Gwagwa, Arthur, and Beverley Townsend. 2024. “Re-imagining Africa’s sovereignty in a digitally interdependent world.” https://www.globalpolicyjournal.com/blog/10/05/2023/re-imagining-africas-sovereignty-digitally-interdependent-world.

Human Rights Watch. 2014. “Ethiopia: Telecom Surveillance Chills Rights.” https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights.

ICTWorks. 2022. “Unsafe National Biometric Data Collection in 23 African Countries.” https://www.ictworks.org/national-biometric-data-collection/#.Y7z5s3bMI2w.

INTERPOL. 2021. “INTERPOL report identifies top cyberthreats in Africa.” https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.

Marshall, Monty G., Ted Robert Gurr, and Keith Jaggers. 2016. “Polity IV project: Political regime characteristics and transitions, 1800–2015.” *Center for Systemic Peace* 13. https://www.systemicpeace.org/polityproject.html.

Meservey, Joshua. 2018. “Implications of China’s presence and investment in Africa.” *Testimony before the Subcommittee on Emerging Threats and Capabilities, US Senate,* https://www.armed-services.senate.gov/imo/media/doc/Meservey_12-12-181.pdf.

Pauwels, Elenore. 2020. “Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention Opportunities and Challenges for the International Community.” *Global Center on Cooperative Security,* accessed January 13, 2023. https://www.jstor.org/stable/pdf/resrep27551.pdf.

Stevens, Amy, Pete Fussey, Daragh Murray, Kuda Hove, and Otto Saki. 2023. “‘I started seeing shadows everywhere’: The diverse chilling effects of surveillance in Zimbabwe.” *Big Data & Society* 10 (1). https://doi.org/10.1177/20539517231158631.

Véliz, Carissa. 2021. *Privacy is Power.* Melville House New York. ISBN: 978-1-61219-915-3.

Wilson, Steven Lloyd, Staffan Lindberg, and Kjetil Tronvoll. 2021. “The best and worst of times: The paradox of social media and Ethiopian politics.” *First Monday,* https://firstmonday.org/ojs/index.php/fm/article/view/10862.

World Economic Forum. 2020. “Africa must act now to address cybersecurity threats. Here’s why.” https://www.weforum.org/agenda/2022/08/africa-must-act-to-address-cybersecurity-threats.

Authors

Bev Townsend is a South African researcher at the University of York, England, who works in the law and ethics of data and digital technologies and in AI and resilient autonomous systems.

(bev.townsend@york.ac.uk)

Arthur Gwagwa is based at the Utrecht University Ethics Institute. His research interests are on the geopolitics and intercultural ethics of AI.

(arthurgwagwa@gmail.com)

Funding statement

The work of Beverley Townsend was funded by the UKRI project EP/V026747/1 "Trustworthy Autonomous Systems Node in Resilience." The content of this article is solely the responsibility of the authors and does not necessarily represent the official views of the funding bodies.

Ethical standards

The authors have no competing interests to declare that are relevant to the content of this article.

Keywords

Africa; digital repression; data-capturing technologies; data protection.