Heralding Privacy concerns in AfCFTA's proposed E-commerce Protocol

By:

Megan Kathure

November 8, 2022

One social order of living facing contestation is the remit of international economic law and human rights. An attempt at assemblage–*co-existence or subsistence*–of these two orderings has been strewn with triumphs and defeat alike, with the most notable incidents being the Seattle protests[1] in the run-up to WTO's Ministerial Conference of 1999. This trade and human rights tension unmistakably subsists in digitally-enabled trade, otherwise classed as e-commerce, where concerns of surveillance, consumer protection, and identity theft abound.

With the growth of e-commerce, a core human right concern pervading this "novel" (un-explored) form of trade is the right to privacy. The right, perceived by privacy evangelists as an enabler of digital transactions, is lamentably seen as onerous by traders, who often, in the case of mediating e-commerce transactions, are big technology companies[2]. E-commerce, with no settled

definition or agreement over terminology- similarly referenced as digital trade, is defined by the OECD as the sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders[3].

This blog piece makes a case for recognising privacy and its derivative, data protection in the AfCFTA's E-Commerce Protocol and subsequent e-commerce related agreements concluded by Africa's Regional Economic Communities (RECs) and states. Recognising privacy in RECs' and African states' e-commerce related agreements following the Protocol's enactment is necessary amidst the untapped potential of e-commerce in Africa, especially in light of the greater economic integration envisioned by the AfCFTA. This blog proceeds by highlighting areas necessitating minimum data privacy standards in e-commerce. It will then compare the performance of RECs in e-commerce frameworks whilst casting challenges formed by an enduring inconsistent legal landscape. Finally, the blog concludes and provides recommendations.

AfCFTA's E-commerce potential to usher a new privacy paradigm in Africa's e-commerce?

Despite the growth of e-commerce in Africa and the greater intra-African trade envisioned by AfCFTA's economic integration, there are few minimum data protection standards amongst African states when it comes to e-commerce. This is particularly the case for cross-border online transactions, online payment security and data collection.

Digital cross-border transactions of any nature are acutely reliant on data. With regard to online payment systems, consumers divulge more information, unlike in conventional payment systems. This, in turn, has enlarged the scale of vulnerability as witnessed by increased data breach incidents of stolen credit and debit card numbers. In a typical online payment transaction, which payment processors often facilitate, a consumer will disclose their identity details such as their real name, email address, shipping address and other personally identifiable information for purposes of verification, financial information such as credit card number, expiration date, and verification code, to process purchases and authorise sales online[4].

As a general practice in e-commerce sales, girded in the prevalent norm of web tracking, the following types of data are often collected[5] by different actors: browsing patterns, purchase history, location data, and a unique identifier for mobile or computer devices, among others. Such consumer data is often collected and sold without users' consent, and notification for marketing and legal requirements such as the use of privacy policies have been deemed inefficient , noting the wordiness and amount of legalese contained in these policies. Other mitigations, such as the use of anonymous communication tools[6], serve as a reminder that systems without provable (or at least well-defined) privacy properties may have information leaks and privacy breaches in unexpected ways[7].

From the foregoing, it is manifestly plain that a wide array of data is collected. Alive to the absence of a global privacy standard and hortatory commitments to privacy in free trade agreements[8] (FTAs), there is a need for the AfCFTA e-commerce protocol to define and harmonise data privacy requirements and laws in the continent's e-commerce activities.

Legislative attempts on e-commerce by RECs

Out of Africa's eight Regional Economic Communities (RECS), only three RECs, namely; SADC, EAC, and ECOWAS, have operational legislative instruments facilitating and/or guiding E-commerce. Out of the three, ECOWAS only has the most robust of laws. This includes a Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Supplementary Act on Electronic Transactions, Directive C/DIR/1/08/11 on cybercrime, and Supplementary Act A/SA.3/01/07 on the legal regime applicable to network operators and service providers. The SADC landscape consists of an e-commerce model law and an e-commerce Strategy[9]. Noting the paucity of facilitating frameworks within RECs on e-commerce, it behoves the continent's leaders to fast-track the design and actualisation of AfCFTA's e-commerce Protocol and, consequently, regional and national strategies in a bid to realise the Digital Transformation Strategy for Africa[10].

The Supplementary Act on Personal Data Protection within ECOWAS, formulated in 2010, has striking relevant provisions for present e-commerce transactions. To highlight a few of its provisions:

- It possesses an elaborate definition of personal data to mean any information relating to an identified individual who may be directly or indirectly identified by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity (Article 1);
- It prescribes in mandatory terms, by use of the term “shall”, that each ECOWAS Member State shall establish its own data protection authority who, shall be an independent administrative authority responsible for ensuring that personal data is processed in compliance with the provisions of the Supplementary Act (Article 1,14); and
- It allows a data controller to transfer personal data to a non-member ECOWAS country only where such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data (Article 36).

The Act further affords data subjects a host of expansive rights concerning their collected data, a set of rights which foregrounds control and privacy of the data subject and which, when enforced, addresses privacy concerns in e-commerce transactions[11]. Additionally, these rights and the corresponding obligations on data controllers appear to have large underwritings of privacy by design. Thus, a data subject, for instance, *inter alia*, has the right to be informed no later than at the time of collection of the data and irrespective of the means and media: the defined purpose{s) for which the data is to be processed; the categories of data involved; the recipient or recipients to whom the data is likely to be disclosed; the period of preservation of the processed data (Article 38). Data subjects’ rights also include the right of access[12], the right to object[13], and the right to rectification and destruction[14].

The vision of the (SADC) E-commerce Strategy, adopted in 2012, is to enhance business to business (B2B) trade between countries and promote business to consumer (B2C) e-commerce inside countries. It consists of an action plan of 4 pillars: an enabling e-commerce environment[15], developing capacity for e-commerce in each member state[16], strengthening e-commerce sub-regional and national infrastructure[17] and establishing an institutional and governance structure to undertake capacity building, support data collection and setting up a database[18].

Making up for the shortfall in e-commerce frameworks at the regional level, African countries are developing national strategies and policy harmonisation in ICT or data protection laws[19]. Prudence must, however, be exercised in crafting and implementing such laws to ensure that they enable e-commerce transactions. Imposing absolute data localisation[20] requirements, for instance, impedes cross-border online transactions because stringent requirements for data collection or processing deter market entry by potential businesses wishing to make their services available to such highly restricted markets.

While Africa is witnessing greater adoption of data protection laws, RECs should be wary of adopting regional frameworks stricken with fault lines of present national laws, such as the disproportionate exclusions allowed to governments or vague rights or limitations credited to data subjects. Foreign and national entities should be subjected to the same national or regional data protection frameworks save for uniquely limited circumstances because the effectiveness of data protection legislation is undermined if a significant number of entities are excluded from complying with its requirements[21]. A disparate form of compliance to data protection governance lays open the framework to abuse, ultimately weakening the utility of the said framework. This unevenness in compliance is exacerbated when countries legislate data protection laws with varying data transfer requirements. In addition to data subjects' rights, the principal focus of such legislation is undermined.

A plea for harmonisation

Trade and human rights have long had a troubled relationship and the advent of new technologies such as the internet further complicates the relationship[22]. Human rights and economic regulation have evolved in splendid isolation despite the fact that the concern for human rights started with the need to address slavery, and thus a trade issue, in the nineteenth century. The difficulty in integrating human rights and economic theory will undoubtedly gain traction in e-commerce regulation owing to increased invocation by public and private actors to integrate human rights concerns such as privacy in trade agreements. Whether such invocations will hold is largely a question of the willingness and ability of nation-states to cede mercantilist logic to what is deemed by some as non-economic goals.

The invocation for harmonisation in Africa's data protection framework is augmented by the emergence of new data realms[23] facilitated by bilateral and regional FTAs whose scale and popularity point towards standard settings outside international consensus-building bodies. In Africa, lurking in this lure of singular assignment of obligations are agreements concluded with Morocco, Mauritius and the Africa-Europe Digital Economy Partnership, which I opine should be treated with caution because of the ease in which such foreign interests may shape Africa's digital trade policy. This position is buttressed and made more urgent with the proposed US-Kenya FTA, whose negotiations are steeped in demand for unfettered cross border data flows between the two countries, in line with the interest of US companies[24]. Thus, possibilities of coherence to Africa's data protection landscape are stymied owing to risks of dissonance such as those fronted by the US-Kenya FTA, whose conclusion seems to loom before the operationalisation of the AfCFTA.

Moreover, commentators have noted that the US-Kenya FTA is likely to inform agreements concluded by the US with other African countries[25], which might have broader and ongoing consequences on data transfer rules in the AfCFTA's e-commerce protocol. Further practical challenges may ensue from a lack of harmonisation in policies regulating e-commerce. Africa's efforts in regional integration are uncannily characterised by States overlapping subscriptions to different regional economic communities and trade agreements, and this status quo has stalled integration. The same state of play is likely to be witnessed in data protection if the African States fail to achieve a considerable level of harmonisation in data protection rules.

Conclusion

The thrust of the traditional debate pitting international trade law against human rights law suggests that the two systems are inherently incompatible [26]. As technology disrupts traditional business models, it becomes clear that realising the full gains from e-commerce necessitates the incorporation of certain human rights, such as privacy. Privacy, after all, may subsist as an economic goal. Laudable are the efforts to increase intra-African trade, but Africa's digital policy landscape may seem to be ailing from perennial legislation devoid of substantial actionable progress. A case in point is the frequently cited Malabo Convention[27] yet to enter into force.

Risk of abuse of gathered data by its recipients or other malicious third parties such as hackers and ensuring that such recipients such as data controllers lawfully appropriate collected data is a testament to the need for effective privacy commitments in e-commerce laws. Ultimately, with the underpinning architecture of e-commerce at the B2C level running on trust[28], centring privacy in a facilitative legal framework within Africa's digital trade ecosystem proves timely.

References

[1] World Trade Organization Protests in Seattle< https://www.seattle.gov/cityarchives/exhibits-and-education/digital-document-libraries/world-trade-organization-protests-in-seattle > On 12th January 2022

[2] A Dynamic and Static Analysis of the Uber Mobile Application from a Privacy Perspective < http://jisar.org/2018-11/n1/JISARv11n1p11.pdf> ; Dr. Darren R. Hayes, 'Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application', Law; Z Zoom Agrees to Settle Lawsuit Over 'Zoombombing' New York Times 1st August 2021 < https://www.nytimes.com/2021/08/01/technology/zoom-lawsuit-zoombombing.html > See also settlement in the class action suit against Zoom over privacy concerns ; Amazon devices will soon automatically share your Internet with neighbors < https://dig.watch/updates/amazons-ring-doorbell-strengthen-privacy-following-concerns-over-data-sharing/ https://arstechnica.com/gadgets/2021/05/amazon-devices-will-soon-automatically-share-your-internet-with-neighbors/ >

[3] OECD Guide to Measuring the Information Society, 2011 < https://stats.oecd.org/glossary/detail.asp?ID=4721 >

[4] Anna Myers, 'Cross-Border Commerce without Constraint: Shifting from TerritorialBased Regulation to an IndustryBased Code of Conduct for the Online Payment Processing Industry' Federal Communications Law Journal Vol. 67 < http://www.fclj.org/wp-content/uploads/2016/01/67.3.3-Myers.pdf >

[5] Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1879, 1885 (2013)

https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/ >

[6] Aleecia M. Mcdonald & Lorrie Faith Cranor, ‘ The Cost Of Reading Privacy Policies’* < Https://Kb.Osu.Edu/Bitstream/Handle/1811/72839/Isjlp_V4n3_543.Pdf >

[7] Steven Goldfeder et al, ‘ When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies’ < https://arxiv.org/pdf/1708.04748.pdf?source=post_page---------- >

[8] Mira Burri, ‘Interfacing Privacy and Trade’ < https://scholarlycommons.law.case.edu/jil/vol53/iss1/5/ >

[9] E-Commerce in the SADC Sub-Region Strategy Framework < https://www.skylineuniversity.ac.ae/pdf/ecommerce/SADC_e-commerce_Strategy_FINAL_Oct18-FINAL.pdf >

[10] The Digital Transformation Strategy For Africa (2020-2030) < https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf >

[11] See Article 38-41

[12] Article 39 of the Supplementary Act on Personal Data Protection within ECOWAS,

[13] Article 40 the Supplementary Act on Personal Data Protection within ECOWAS,

[14] Article 41 of the Supplementary Act on Personal Data Protection within ECOWAS,

[15] E-Commerce in the SADC Sub-Region Strategy Framework, pg 9

[16] E-Commerce in the SADC Sub-Region Strategy Framework, page 12

[17] E-Commerce in the SADC Sub-Region Strategy Framework, pg 16

[18] E-Commerce in the SADC Sub-Region Strategy Framework, pg 17

[19] What is Africa’s Digital Agenda? Africa Policy Research Institute https://afripoli.org/uploads/publications/Africas_Digital_Agenda_final.pdf

[20] Anupam Chander, Uyen P. Le, ‘ Breaking the Web: Data Localization vs. the Global Internet’ < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858# >

[21] Tara Davis, ‘Data Protection in Africa: A Look at OGP Member Progress < https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf >

[22] GAO, Henry S. ‘Google’s China problem: A case study on trade, technology and Human Rights under the GATS’. (2011). Asian Journal of Wto and International Health Law and Policy. 6, 347-385. Research Collection School Of Law. < https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4142&context=sol_research >

[23] Susan Ariel Aaronson, Patrick Leblond, ‘ Another Digital Divide: The Rise of Data Realms and its Implications for the WTO’ < https://doi.org/10.1093/jiel/jgy019 >

[24] Melissa Omino and Isaac Rutenberg, ‘Why the US-Kenya Free Trade Agreement Negotiations Set a Bad Precedent for Data Policy’ June 1, 2021 < https://www.cgdev.org/blog/why-us-kenya-free-trade-agreement-negotiations-set-bad-precedent-data-policy >

[25] James Thuo Gathii, An Early Assessment of the Prospective Kenya-United States Trade Agreement < https://www.afronomicslaw.org/2020/02/13/an-early-assessment-of-the-prospective-kenya-united-states-trade-agreement/ >

[26] Kent Jones, ‘The WTO core agreement, non-trade issues and institutional integrity’ < http://www.personal.reading.ac.uk/~les05am/ec246/Jones02WTR1Nov.pdf >

[27] African Union Convention on Cyber Security and Personal Data Protection < https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection >

[28] Ghada El Haddad et al, ‘Universite de Montreal, Montreal, QC, CAUnderstanding Trust, Privacy and Financial Fears in Online Payment, < https://ieeexplore.ieee.org/abstract/document/8455883 >

View online: Heralding Privacy concerns in AfCFTA’s proposed E-commerce Protocol