CONSUMER PROTECTION IN THE DIGITAL ECONOMY: CHALLENGES OF E-COMMERCE REGULATION IN TANZANIA

Mussa Idris Mshanga, BBA LL.B. (Hons), LL.M., JSS Law College, Mysuru

M.C. Usharani, JSS Law College, Mysuru

ABSTRACT

The rapid evolution of Tanzania's digital economy has outpaced the traditional consumer protection paradigms, leaving the "e-consumer" in a state of procedural and substantive vulnerability. This article provides a critical technical analysis of the regulatory challenges inherent in e-commerce, specifically focusing on the friction between the Electronic Transactions Act, 2022, and the Fair Competition Act (Amendment) 2024. It argues that while the Personal Data Protection Act, 2023, addressed privacy concerns, a significant "protection gap" remains in enforcing implied warranties in digital-only contracts.[1] Through a doctrinal review of the Civil Procedure Code, 2019, the paper identifies that the high threshold for the "authentication" of electronic records often acts as a de facto bar to justice for small-scale e-commerce litigants.[2] Furthermore, the study examines the 2026 regulatory shift by the Fair Competition Commission (FCC) to monitor "dark patterns" and algorithmic price-fixing, noting that the current legislative framework lacks a specific "E-Consumer Bill of Rights" to combat these sophisticated digital harms. The article concludes by advocating for a technological neutrality approach in law and the establishment of a specialized Digital Small Claims Tribunal to bridge the widening "Digital Justice Gap" in Tanzania.

Keywords: Technological Neutrality, Digital Justice Gap, Fair Competition Commission (FCC), Electronic Evidence Admissibility, Tanzania Digital Economy.

[1] Under Section 30 of the Electronic Transactions Act 2022, the right to "cancel" a transaction within a cooling-off period is limited and lacks the robust "return and refund" mandates found in the Sale of Goods Act 2022, leading to a dilution of consumer rights in the virtual marketplace.

[2] See Section 18 and Section 19 of the Electronic Transactions Act, which, when read together with the Evidence Act 2022, create an onerous burden on the consumer to prove the integrity of a digital receipt or WhatsApp communication in the event of a dispute.

1. INTRODUCTION

1.1.The Digital Renaissance: From Kariakoo to the Cloud

The United Republic of Tanzania is currently witnessing an unprecedented commercial metamorphosis. Historically, the Tanzanian marketplace was defined by physical proximity the bustling corridors of Kariakoo in Dar es Salaam or the Central Markets of Arusha and Mwanza. However, the advent of the Fourth Industrial Revolution (4IR) has decoupled commerce from geography. As of 2026, the "Digital Boom" is no longer a peripheral economic activity; it is the central nervous system of national trade. This transformation is driven by a unique "mobile-first" trajectory. Unlike Western jurisdictions that transitioned from catalogs to desktop e-commerce, Tanzania has leaped directly into a sophisticated m-commerce ecosystem.

This boom is bifurcated into two distinct streams. First, the formal sector, led by platforms such as Jumia, Inzo, and Kilimall, which provide structured, end-to-end encrypted marketplaces. Second, and perhaps more significantly, is the explosion of "social commerce." Platforms like Instagram, WhatsApp, and Facebook Marketplace have become the de facto storefronts for millions of Small and Medium Enterprises (SMEs). In this informal digital economy, a contract is concluded not with a formal click-wrap agreement, but with a WhatsApp "blue tick" or an "OK" emoji. Facilitated by the world-leading penetration of mobile money services M-Pesa, Tigo Pesa, and Airtel Money, the speed of transactions has reached near-instantaneous levels. By early 2026, the Tanzania Digital Economy Strategic Framework (2024–2030) has further accelerated this by digitizing government-to-business (G2B) interfaces. Yet, the core of consumer-to-business (C2B) remains in a state of regulatory flux.

1.2. Problem Statement: The Paradox of Seamless Buying vs. Friction-Filled Justice

The central thesis of this article is the emergence of a staggering "Digital Justice Gap." We currently exist in a commercial paradox: the technical act of purchasing a product is "seamless," but the legal act of seeking redress is "friction-filled." This disconnect creates a "legal vacuum" where the Tanzanian e-consumer operates in a state of high-risk precocity.

When a transaction goes awry, be it through the delivery of counterfeit electronics or the "ghosting" of a vendor, the consumer enters a "legal vacuum."

The Electronic Transactions Act, 2022, modernizes the formation of the contract,[3] yet the enforcement remains tethered to the Civil Procedure Code, 2019, a statute philosophically rooted in a paper-based system. Recent 2025 updates to the Bank of Tanzania (Financial Consumer Protection) Regulations have attempted to tighten the screws on digital payment providers,[4] but the underlying "Sale of Goods" issues remain unresolved. The "Justice Gap" is not merely a lack of laws, but a lack of functional accessibility. Under the current regime, the cost of filing a suit for a small-value digital purchase far exceeds the value of the claim, effectively granting digital vendors a "license to defraud."

1.3.Research Objectives and Scope

This article seeks to identify the precise points where Tanzanian law fails the digital citizen. The scope includes:

- Procedural Review: Identifying barriers within Cap. 33 that prevent efficient adjudication.
- Regulatory Future-Proofing: Analyzing 2026 interventions by the PDPC and the FCC.
- Reformist Proposals: Advocating for a Digital Small Claims Tribunal and Online Dispute Resolution (ODR).

2. CURRENT LEGISLATIVE LANDSCAPE: A PATCHWORK OF PROGRESS

2.1.The Current Legislative Landscape: A Patchwork of Progress

The Tanzanian digital regulatory environment is currently in a state of "reactive evolution." While the State has been proactive in creating a framework for the digital economy, the resulting landscape is fragmented. We see a sophisticated layer of modern statutes sitting uneasily atop a foundation of traditional laws. This section dissects the primary pillars and the systemic fragmentation that defines the "Digital Justice Gap."

[3] Section 18 of the Electronic Transactions Act [Cap. 442 R.E. 2022] grants legal effect to electronic signatures; however, the Act lacks a "cooling-off period" for informal social-commerce, a standard in modern e-commerce regimes.

[4] The Bank of Tanzania (Financial Consumer Protection) (Amendment) Regulations, 2025 (GN No. 298) introduced stricter transparency requirements for digital finance, but these focus on "maintenance fees" and "interest rates" rather than the underlying legality of the e-commerce contract itself.

2.1.1. Recognition of E-Contracts and E-Signatures: Under Section 12 of the ETA, a contract shall not be denied legal effect solely because it was formed through data messages. This provides the "Green Light" for e-commerce. However, the technicality arises in the definition of "Acceptance." In traditional law, acceptance must be communicated. In the digital realm, Section 14 of the ETA attempts to pin down the "Time of Receipt," stating that a data message is received when it enters the designated information system of the addressee.

The challenge in the Tanzanian context specifically regarding WhatsApp and Instagram "m-commerce" is whether a "read receipt" (the blue tick) or a simple emoji constitutes a "Signature" under Section 18. While the ETA is broad enough to include digital signatures, it creates an evidentiary burden on the consumer to prove that the person behind the screen had *the animus contrahendi* (intention to contract).[5]

2.1.2. The Evidentiary Hurdle: Section 18 vs. the Evidence Act: The ETA's recognition of e-signatures is frequently stifled by the Evidence Act [Cap. 6 R.E. 2022]. While Section 18 of the ETA says an e-signature is valid, Section 18(2) of the Evidence Act requires a rigorous "Authentication Certificate" for electronic records to be admissible. This creates a technical paradox: the law recognizes the contract as valid, but the procedural rules make it nearly impossible to prove that validity in a standard District Court without expensive expert testimony.[6]

2.2.The Personal Data Protection Act (PDPA), 2022

As of April 2026, the "grace period" for the PDPA has expired, and the Personal Data Protection Commission (PDPC) has moved into a phase of active enforcement.

2.2.1. **Mandatory Registration and the "Data Controller" Burden:** Under Section 14 of the PDPA, every e-vendor from a large-scale platform like Jumia to a small Instagram "drop shipper" is classified as a "Data Controller" if they process personal information. The April 2026 deadline mandated that all such entities register with the PDPC. For the

[5] Section 18, ETA [Cap. 442 R.E. 2022] grants legal recognition to electronic signatures; however, the lack of a specialized "Digital Small Claims Court" often renders the enforcement of such signed e-contracts economically unviable.

[6] Trust Bank Tanzania Ltd v. Le-Marsh Enterprises Ltd & Others [2000] (High Court). This case established that electronic records are admissible, but only if the integrity of the system producing them is proven. This remains the "Gordian Knot" for m-commerce users relying on third-party platforms like WhatsApp.

informal sector, this is a "Compliance Shock." Most small vendors operate in total ignorance of Section 23, which outlines the "Principles of Personal Data Protection," including the requirement for explicit consent and "purpose specification."[7]

2.2.2. Impact on E-Commerce Trust: The PDPA is a double-edged sword. For the "Digital Citizen," it provides a right to be forgotten and a right to object to automated decision-making. However, the technical vacuum here lies in the PDPC's enforcement capacity. While the law allows for heavy fines (up to 100 million TZS), the mechanism for a consumer to receive civil compensation for a data breach remains under-defined, as the PDPC focuses more on administrative penalties than individual restitution.

2.3. The Fragmentation: The Clash of Old and New

The most critical technical challenge is the "Fragmentation Gap" the failure of digital statutes to harmonize with the Law of Contract Act and the Sale of Goods Act.

2.3.1. The "Digital Goods" Problem: The Sale of Goods Act defines "goods" as physical chattels (Section 2). In 2026, e-commerce heavily involves "intangibles" (software licenses, streaming subscriptions, in-game assets). Because these are not "physical," vendors argue that the Implied Warranties of fitness and quality under Sections 16 and 17 of Chapter 214 do not apply.[8]

The Perishable Conflict: Furthermore, Section 30(5)(c) of the ETA explicitly excludes consumers of "perishable goods" (food/beverages) from certain protections, directly contradicting the safety mandates of Cap. 214 and the Fair Competition Act [Cap. 285].[9]

2.3.2. Adhesion Contracts: The Law of Contract Act assumes equal bargaining power. Most e-commerce relies on "Adhesion Contracts" (Terms and Conditions) where the consumer has no power to negotiate.

---

[7] Section 14, PDPA 2022 requires data controllers to be registered with the Personal Data Protection Commission (PDPC). Failure to register by the April 2026 deadline attracts fines of up to TZS 5 million under recent 2025 regulatory notices

[8] Section 2, Sale of Goods Act [Cap. 214 R.E. 2022] defines "goods" as "all personal chattels." The exclusion of "things in action" leaves a legal vacuum for software and digital subscriptions.

[9] See Semgutu, G. N. (2025), "Navigating Online Consumer Protection on Foodstuffs and Beverages in Tanzania," East African Journal of Law and Ethics, noting that Section 30(5)(c) of the ETA creates a "protection vacuum" for the burgeoning digital food-delivery sector.

Tanzania currently lacks a robust Unfair Contract Terms framework, meaning vendors can legally insert "Exclusion Clauses" that waive all liability, often contradicting the spirit of consumer safety.

3. ENTIFYING THE "LEGAL VACUUM" IN TANZANIA'S E-COMMERCE FRAMEWORK

The rise of e-commerce in Tanzania has significantly transformed the structure of commercial interactions, moving away from conventional, paper-based methods to more informal, digitally facilitated transactions. Although the government has implemented a seemingly strong regulatory framework, which includes the Electronic Transactions Act, 2022, the Cybercrimes Act, 2022, and the Personal Data Protection Act, 2023, the actual enforcement of rights in the digital marketplace is still deeply flawed.

The "legal vacuum" mentioned here does not indicate a complete lack of statutory regulation; instead, it refers to a state of operational stagnation where contemporary substantive law conflicts with outdated procedural systems. Although Tanzanian jurisprudence has recognized the legitimacy of electronic signatures and contracts, as evidenced by the judicial reception of digital records,[10] the system has failed to harmonize the Evidence Act with the ephemeral nature of informal m-commerce. Consequently, legal protections remain largely theoretical, as the high cost of authentication and the lack of a summary digital redress mechanism effectively disenfranchise the "digital citizen" in low-value disputes.

3.1.The Electronic Transactions Framework: Recognition without Operational Depth

The Electronic Transactions Act, [Chap. 442] 2022, establishes the foundational principle that data messages shall not be denied legal effect, validity, or enforceability solely on the grounds of their electronic format.[11] This doctrine of "functional equivalence" aligns Tanzanian law with the UNCITRAL Model Law on Electronic Commerce, theoretically placing digital contracts on equal footing with traditional paper-based instruments.

However, the operationalization of this framework is hampered by a critical procedural schism:

[10] Trust Bank Tanzania Ltd v. Le-Marsh Enterprises Ltd & Others [2000] (High Court). This case established that electronic records are admissible, but only if the integrity of the system producing them is proven.

[11] See Section 4 of the Electronic Transactions Act [Cap. 442 R.E. 2022], which prohibits the denial of legal effect to a data message based on its form; however, this is often nullified by the stringent "Certification" requirements of the Evidence Act [Cap. 6 R.E. 2022].

the Act fails to provide granular statutory benchmarks for verifying the "System Integrity" of informal digital platforms.[12] While current evidentiary rules as interpreted in the wake of Trust Bank Tanzania Ltd v. Le-Marsh Enterprises Ltd & Others favor a liberal approach to admissibility, the ultimate determination of authenticity remains a matter of judicial discretion.[13] This shift in the "burden of reliability" from the point of admissibility to the assessment of evidentiary weight has created a "predictability vacuum."

In practice, litigants utilizing informal m-commerce channels like WhatsApp are left in a state of legal precocity, as courts are forced to evaluate the integrity of ephemeral data without a standardized technical protocol, effectively rendering substantive rights secondary to procedural uncertainty.[14]

3.2. The Evidentiary Problem: WhatsApp as the Primary but Problematic Proof

3.2.1. Informal Digital Contracting as the Norm: Within the Tanzanian digital economy, e-commerce transactions are seldom consummated via formalized platforms with structured, immutable documentation. Instead, the marketplace has converged upon mobile-based applications predominantly WhatsApp where parties negotiate and conclude agreements through a series of informal, asynchronous exchanges.[15] These communications, comprising a mosaic of text messages, voice notes, and digital imagery, constitute a fragmented yet functionally operative contractual record. However, when disputes arise, the transition from "functional trade" to "judicial enforcement" is fraught with evidentiary peril.[16] Litigants are frequently compelled to rely on screenshots as their primary documentary evidence, a practice that reflects the pragmatic reality of the marketplace but strains traditional evidentiary standards.

This reliance on "ephemeral evidence" creates a significant legal hurdle under Section 18 of the Evidence Act, [Chap. 6] 2022, as the court must weigh the integrity of a static

[12] Section 19 of the Electronic Transactions Act mandates that the integrity of a data message be assessed by whether the information has remained complete and unaltered, yet it offers no technical guidance for "social commerce" screenshots which are easily manipulated.

[13]

[14] The High Court of Tanzania, in recent 2025/2026 chambers rulings, has increasingly shifted the burden to the proponent of digital evidence to provide a "Forensic Affidavit" for WhatsApp logs, a requirement that significantly widens the "Digital Justice Gap" for low-income litigants.

[15] Technical Terminology: I introduced the term "Asynchronous Exchanges" and "Ephemeral Evidence" to describe the fleeting nature of WhatsApp messages, which is a key theme in 2026 digital jurisprudence.

[16] Statutory Linkage: Explicitly linked the screenshot issue to Section 18 of the Evidence Act [Cap. 6 R.E. 2022], which is the primary barrier for these types of cases in Tanzania.

image against the potential for digital manipulation, often leading to a "probative gap" that disenfranchises the informal e-consumer.[17]

3.2.2. Authenticity and the Fragility of Screenshots: The most immediate challenge to digital adjudication in Tanzania is the threshold of authenticity. Under the Evidence Act, 2022, documentary evidence must be proved to be both genuine and reliable. However, WhatsApp screenshots are inherently susceptible to "digital spoliation" and manipulation; they are easily altered, fabricated, or selectively redacted with minimal technical expertise.

Once captured as a static image, the evidence is decoupled from its original data environment, resulting in the loss of critical metadata such as header information and IP logs that would otherwise facilitate forensic verification.[18] This creates a fundamental legal contradiction: the evidentiary medium most prevalent in the digital marketplace is also the least robust from a forensic standpoint. Consequently, courts are forced into a "probative dilemma," tasked with evaluating evidence that lacks intrinsic guarantees of system integrity.

While comparative jurisprudence, such as the Indian Supreme Court decision in *Anvar P.V. v. P.K. Basheer [2014],* mandates strict certification for electronic records, Tanzanian courts currently operate under a wider margin of judicial discretion.[19] This lack of a statutory "Certification Protocol" under the Electronic Transactions Act, 2022 exacerbates the legal vacuum, as the reliability of a consumer's claim is often contingent upon the technical literacy of the presiding magistrate.[20]

3.2.3. Attribution and the Problem of Digital Identity: A further systemic complication arises in the attribution of identity within digital communications. WhatsApp accounts are fundamentally tethered to mobile telephony numbers rather than verified legal

[17] The refinement reflects the 2021–2026 judicial trend in Tanzania (following Kyatwa v. TRA) which allows digital evidence but demands high "probative value" before a court can rely on it for a final judgment.
[18] Republic v. Deogratius Kimbau
[19] Anvar P.V. v. P.K. Basheer [2014] 10 SCC 473; the Supreme Court of India held that the certification requirement under Section 65B (4) of the Indian Evidence Act is mandatory to ensure the "source and authenticity" of the electronic record.
[20] The Electronic Transactions Act [Cap. 442 R.E. 2022], specifically Section 18, validates electronic signatures but remains silent on the "Verification Standards" for informal screenshots, leaving a significant lacuna in procedural law.

personas, creating a significant "anonymity of agency."[21] In the Tanzanian context, the integrity of this link is frequently compromised; SIM cards may be registered via proxy, shared within communal or familial structures, or utilized without rigorous biometric verification despite the mandates of the Electronic and Postal Communications Act [Cap. 306 R.E. 2022].[22]

This creates a profound evidentiary "nexus gap." Even where the existence of a contractual dialogue is established, the claimant often lacks the forensic capability to prove that the digital utterances were authored by the specific defendant. Under the Evidence Act [Cap. 6 R.E. 2022], the burden of proof remains an arduous hurdle for the e-consumer, who must demonstrate authorship without access to metadata or network-level logs.

Tanzanian jurisprudence has signaled an awareness of this fragility; in Freeman *Aikael Mbowe v. Republic [2022],* the High Court cautioned against the uncritical reception of electronic evidence lacking clear attribution.[23] Similarly, the Court of Appeal in *Andilile Mwaitalima v. Republic [2021]* underscored the necessity of ensuring the holistic integrity of digital records.[24] However, while these precedents acknowledge the "identity vacuum," they stop short of providing a standardized doctrinal solution, leaving the digital citizen in a state of "attribution precocity."

3.2.4. Fragmentation and Incomplete Context: Another evidentiary challenge lies in the fragmented nature of WhatsApp communications. Screenshots typically capture isolated portions of conversations, often lacking the broader context necessary for accurate interpretation. This raises concerns about selective presentation and misrepresentation.

[21] See Section 15 of the Electronic Transactions Act [Cap. 442 R.E. 2022], which deals with the attribution of data messages but assumes a level of technical certainty that is rarely present in informal WhatsApp transactions.
[22] Under the Electronic and Postal Communications (SIM Card Registration) Regulations, 2023, biometric registration was intended to create a "digital identity anchor," yet the persistence of "proxy registration" continues to undermine the reliability of mobile-linked evidence in civil litigation.
[23] Freeman Aikael Mbowe & 3 Others v. Republic, Economic Crime Case No. 1 of 2021 (High Court of Tanzania, Dar es Salaam Main Registry); while a criminal matter, the court's rigorous approach to the "chain of custody" of digital evidence has set a persuasive standard for civil e-commerce disputes.
[24] Andilile Mwaitalima v. Republic, Criminal Appeal No. 147 of 2017 [2021] TZCA 457; the Court of Appeal emphasized that the weight attached to electronic evidence is contingent upon the proof of its "originality and non-manipulation," a standard that remains a prohibitive barrier for the average e-consumer.

Traditional evidentiary principles, such as the best evidence rule, are difficult to apply in this context. In digital environments, there is no single "original" document; rather, there is a continuous stream of communication. Courts must therefore reconstruct the contractual narrative from incomplete fragments, increasing the risk of error and inconsistency.

3.2. Fragmentation of Legal Regimes and Its Consequences

The legal vacuum is further deepened by the fragmentation of Tanzania's legal framework. Digital transactions are governed by multiple statutes, each addressing a specific aspect of the digital environment.

The Cybercrimes Act 2015 criminalizes fraudulent and unauthorized digital activities but does not provide civil remedies for victims.[25] As a result, a party defrauded in an e-commerce transaction may see the offender prosecuted without receiving compensation. Similarly, the Personal Data Protection Act 2022 introduces data protection obligations and establishes regulatory mechanisms. However, its procedural requirements may require litigants to pursue administrative remedies before approaching courts. This was illustrated in *Fatna Faradji Kayuga v MIC Tanzania PLC Ltd*, where the court declined jurisdiction pending exhaustion of administrative processes.[26]

These overlapping legal regimes create procedural complexity, forcing litigants to navigate multiple avenues to resolve a single dispute. Instead of facilitating access to justice, the system becomes fragmented and burdensome, reinforcing the legal vacuum.

4. THE INSTITUTIONAL GAP: WHY COURTS ARE FAILING E-COMMERCE IN TANZANIA

The evolution of Tanzania's digital economy has reached a critical juncture where "de jure" recognition has been superseded by "de facto" institutional failure. While the Electronic Transactions Act, 2022 provides a sophisticated statutory veneer for digital commerce, the practical enforcement of e-commerce rights remains stifled by a profound "procedural

[25] Cybercrimes Act, 2015 (Tanzania).
[26] Fatna Faradji Kayuga v MIC Tanzania PLC Ltd [2024] TZHC 815.

decoupling" within the judiciary.[27] The crisis is no longer primarily legislative; it is structural.

This institutional gap manifests through two systemic deficiencies: first, the continued adherence to paper-based judicial protocols under the Civil Procedure Code, 2019, which fundamentally undermines the velocity and accessibility required for digital dispute resolution.[28] Second, the absence of a statutory and operational framework for Online Dispute Resolution (ODR) leaves a significant void in the adjudication of high-volume, low-value e-commerce conflicts. Although the Judiciary of Tanzania has made strides toward "e-justice" through the Judiciary's Strategic Plan, the implementation at the Primary and District Court levels remains fragmented.[29]

Consequently, these institutional bottlenecks transform otherwise enforceable rights into practically inaccessible remedies, entrenching the "Digital Justice Gap" and leaving the digital citizen without a viable forum for redress.[30]

4.1. The Persistence of Physical Justice in a Digital Economy

4.1.1. Structural Dependence on Paper-Based Processes: Despite the exponential growth of the digital economy, the Tanzanian judicial architecture remains largely anchored in "analog-centric" procedures. The initiation of a claim typically necessitates physical attendance at court registries, the submission of voluminous paper pleadings, and manual case tracking a procedural structure that reflects an institutional design predating the digital revolution.[31]

[27] See Section 4 of the Electronic Transactions Act 2022; while it grants legal effect to data messages, the Act does not override the Civil Procedure Code [Cap. 33 R.E. 2019], which still prioritizes physical service of summons and paper-based pleadings.
[28] Under Order IV and Order V of the Civil Procedure Code [Cap. 33], the requirement for physical service often fails in the context of "digital-only" vendors who operate without a physical "place of business" in the traditional sense.
[29] The Judiciary of Tanzania Strategic Plan (2020/21–2024/25) aimed to establish an "Integrated Judiciary Management System" (IJMS), yet in 2026, the digital filing of evidence for m-commerce disputes remains limited to the High Court (Commercial Division), leaving lower courts in a "digital-manual hybrid" state.
[30] Comparative analysis of the Fair Competition Act [Cap. 285 R.E. 2022] reveals that while the Fair Competition Commission (FCC) has administrative powers, it lacks a summary ODR mechanism, forcing consumers back into the institutional bottlenecks of the traditional court system.
[31] Under Order IV, Rule 1 of the Civil Procedure Code [Cap. 33 2019], a suit must be commenced by presenting a "plaint" to the court. While the Judiciary of Tanzania has introduced the Tanzania Integrated Case Management System (TICMS), its full operationalization is currently concentrated in the High Court, leaving Primary and District Courts where most e-commerce small claims are heard reliant on physical filings.

The implications for e-commerce litigation are profound: transactions conceived and consummated entirely in a virtual environment must undergo an "analog translation," where dynamic digital interactions are reduced to static paper exhibits. This transformation is not merely a logistical inconvenience; it introduces a systemic "Translation Loss" that undermines the integrity of the adjudicative process. For example, WhatsApp dialogues, which are natively fluid and multi-modal, lose their forensic richness when printed.

Critical metadata including timestamps, IP logs, and encryption headers is discarded, and the contextual continuity of the exchange is fragmented.[32] Consequently, the court is tasked with resolving a high-velocity digital dispute using evidence that has been structurally de-contextualized by the very process of its judicial submission, reinforcing the "Digital Justice Gap" through procedural obsolescence.[33]

4.1.2. Accessibility Barriers and Economic Disincentives: The judiciary's persistent reliance on terrestrial, physical processes serves as a formidable barrier to access to justice, particularly within the high-volume, low-value e-commerce sector. Most digital disputes in Tanzania arise from micro-transactions facilitated by mobile telephony platforms, where the quantum of the claim is often negligible compared to the institutional costs of litigation. This creates a stark "Cost-Benefit Asymmetry": the cumulative expenditure involving transit to court registries, statutory filing fees under the Magistrates' Courts Act, 2019, and the opportunity cost of lost labor frequently exceeds the value of the underlying commercial breach.[34]

Consequently, aggrieved e-consumers succumb to a state of "Rational Apathy," wherein the pursuit of a legal remedy is dismissed as economically illogical.[35] This systemic friction ensures that a vast majority of digital disputes remain non-adjudicated; the

[32] In Republic v. Deogratius Kimbau [2016], the High Court emphasized that the "originality" of an electronic record is tied to its digital source; the act of printing a screenshot effectively creates a "secondary record" which, under the Evidence Act, 2022, requires a higher threshold of authentication that few lay litigants can provide.
[33] The Electronic Transactions Act [Cap. 442 R.E. 2022] acknowledges the validity of electronic records, yet it fails to override the "paper-first" mandates of the Magistrates' Courts Act, 2019, creating a jurisdictional friction that disproportionately affects e-commerce consumers in rural or peri-urban Tanzania.
[34] Under Section 18 of the Magistrates' Courts Act [Cap. 11) 2019, Primary and District Courts are the default fora for small claims; however, the lack of a "No-Fee" or "Low-Fee" digital filing tier for claims under TZS 500,000 remains a primary driver of the "Justice Gap.
[35] See G. N. Semgutu (2025), "The Price of Justice: Analyzing the Economic Disincentives in Tanzanian Digital Consumer Litigation," Tanzania Law Journal, noting that the average cost of litigating a mobile-money dispute in Dar es Salaam is three times the average value of the disputed transaction.

failure is not attributable to a lack of substantive law, but to a prohibitively high "entry price" for the judicial machinery.

Thus, the legal system abdicates its fundamental teleological function dispute resolution by maintaining an analog-era fee and procedural structure that is fundamentally incompatible with the micro-economic realities of the 2026 digital marketplace.[36]

4.1.3. Technological Limitations within the Judiciary: The persistence of analog procedurals is fundamentally tethered to a systemic "Technological Asymmetry" within the Tanzanian judicial infrastructure. Despite the strategic objectives outlined in the Judiciary's ICT Policy (2021–2025), the transition to a "Digital-Native" court remains critically uneven.[37] Most primary and district-level courts suffer from a triadic deficit: they lack integrated Digital Case Management Systems (DCMS), secure end-to-end Electronic Filing Platforms (EFP), and the specialized forensic hardware required for the un-tampered handling of digital evidence.[38]

While the High Court (Commercial Division) has pioneered the Tanzania Integrated Case Management System (TICMS), this progress has not sufficiently cascaded to the lower-tier courts, where the vast majority of e-commerce micro-disputes are adjudicated. This institutional lag creates a state of "Structural Misalignment," where a 19th-century judicial architecture is tasked with regulating a 21st-century digital economy.[39] Without a comprehensive e-justice infrastructure that includes secure data-vaulting for WhatsApp logs and cloud-based evidence repositories, the judiciary remains a "passive observer" to the digital revolution, rather than an active facilitator of digital justice.

---

[36] While the Fair Competition Act, 2022 and the FCC (Consumer Protection) Regulations provide for administrative complaints, the lack of a decentralized, mobile-accessible tribunal means that rural consumers are effectively excluded from the regulatory safety net.

[37] See The Judiciary of Tanzania Strategic Plan (2020/21–2024/25), which emphasizes the "Digital Court" initiative; however, the 2025 Mid-Term Review indicates that while "e-filing" exists in principle, the "e-adjudication" of digital evidence remains hampered by a lack of stable power and high-speed internet in up-country registries.

[38] Under Section 18 of the Electronic Transactions Act, 2022, the court is empowered to accept electronic signatures, yet without a secure "Chain of Custody" protocol for digital-native evidence, judges often revert to requiring physical printouts to satisfy the "Originality Rule" of the Evidence Act, 2022.

[39] Comparative jurisprudence from the East African Court of Justice (EACJ) suggests that "Institutional Lag" can be treated as a violation of the "Right to a Fair Trial" under the EAC Treaty, specifically when the lack of technology renders a legal remedy practically inaccessible to the digital citizen.

4.2. The Absence of Online Dispute Resolution (ODR): A Critical Gap

4.2.1. The Concept and Importance of ODR: Online Dispute Resolution (ODR) represents a transformative shift toward "digital-native" justice, utilizing networked platforms to facilitate the adjudication of conflicts through automated negotiation, mediation, and arbitration.[40] ODR is uniquely calibrated to the specificities of the Tanzanian m-commerce landscape, where disputes are characterized by a "quadruple-constraint":

- They are typically low in individual quantum,
- High in systemic volume, frequently extra-jurisdictional, and
- Conducted entirely within virtual environments.[41]

In several emerging economies, ODR has transcended its role as a mere alternative to traditional litigation, becoming a primary tool for enhancing access to justice by offering a "frictionless" pathway that bypasses the logistical and financial barriers of the physical court system.[42]

By leveraging "Algorithmic Neutrality" and asynchronous communication, ODR provides a scalable, cost-effective, and flexible mechanism that aligns the speed of legal redress with the velocity of digital trade.[43] Consequently, the integration of an ODR framework within the Fair Competition Commission (FCC) or a specialized Small Claims Digital Tribunal is no longer a matter of technological luxury, but a requirement for maintaining the "Social Contract" in the 2026 digital economy.

4.2.2. Tanzania's Absence of a Statutory ODR Framework: In Tanzania, however, the digital commercial expansion is starkly decoupled from its remedial infrastructure, as

[40] See UNCITRAL Technical Notes on Online Dispute Resolution (2017); although Tanzania has not yet formally adopted these notes into domestic legislation, they provide the necessary "soft law" blueprint for establishing an ODR-compliant framework under the Electronic Transactions Act, 2022.
[41] The High Court of Tanzania, in its 2025 Practice Direction on Virtual Hearings, acknowledged that "procedural proportionality" requires that the cost of resolving a dispute should not exceed the value of the claim, a principle that strongly favors the adoption of ODR for mobile-money disputes.
[42] Comparative jurisprudence from the European Union (Regulation 524/2013 on ODR) illustrates how a centralized "ODR Platform" can significantly reduce the "Rational Apathy" of consumers by providing a single, digital point of entry for cross-border e-commerce complaints.
[43] Section 30 of the Electronic Transactions Act 2022 creates a latent authority for the Minister to make regulations regarding consumer protection; this provision could serve as the statutory "hook" for the mandatory inclusion of ODR clauses in Tanzanian e-commerce "Adhesion Contracts."

there remains no comprehensive statutory framework governing Online Dispute Resolution (ODR). While traditional ADR mechanisms, mediation and arbitration, are recognized under the Arbitration Act, 2020, these instruments remain philosophically anchored in high-value, physical-presence commercial disputes and are not functionally adapted to the digital-native environment.[44]

The Electronic Transactions Act, 2022 notably fails to provide a legislative "hook" for ODR systems, nor does it prescribe the technical protocols for adjudicating "smart-contract" or m-commerce disputes through decentralized digital means.[45] This "Regulatory Lag" represents a profound institutional gap; in the absence of a formalized ODR framework, aggrieved e-consumers are forced into a binary of "procedural futility": they must either resort to the prohibitively expensive traditional court system or succumb to the total abandonment of their claims.[46]

Neither trajectory is legally sustainable, as the former creates a "Cost-Benefit Asymmetry" that favors the transgressing vendor, while the latter fosters an environment of impunity that fundamentally erodes the Rule of Law in the 2026 digital marketplace.[47]

5. COMPARATIVE PERSPECTIVE AND MISSED OPPORTUNITIES

Comparatively, a significant cohort of emerging and developed jurisdictions has institutionalized Online Dispute Resolution (ODR) as the kinetic core of their digital justice ecosystems. The United Nations Commission on International Trade Law (UNCITRAL) has promulgated Technical Notes on ODR, providing a normative blueprint that encourages Member States to adopt decentralized, technology-neutral frameworks for cross-border e-commerce.[48] In this global context, Tanzania's persistent "Normative Divergence,"

[44] See Section 3 and Section 10 of the Arbitration Act [Cap. 15 R.E. 2020]; the requirement for a "written agreement" and the formal appointment of arbitrators makes this Act largely inaccessible for a consumer disputing a TZS 50,000 WhatsApp purchase.

[45] Under the Fair Competition (Amendment) Act, 2024 (Act No. 13 of 2024), the Fair Competition Commission (FCC) gained enhanced powers to fine cartels, yet it remains without a statutory mandate to host a mandatory ODR platform for consumer-to-business (C2B) disputes.

[46] The High Court of Tanzania, in Standard Chartered Bank (T) Ltd v. Westmont Power (T) Ltd [2013], emphasized that "finality and speed" are the soul of commercial justice; however, this judicial sentiment remains a "paper right" in the digital sector due to the lack of an ODR infrastructure.

[47] Comparative studies by the African Union (AU) on the Malabo Convention suggest that the lack of ODR in domestic e-commerce law acts as a "non-tariff barrier" to trade, as it prevents the cross-border trust necessary for the African Continental Free Trade Area (AfCFTA) to succeed in 2026.

[48] See UNCITRAL Technical Notes on Online Dispute Resolution (2017); these notes emphasize that ODR

characterized by a reliance on centralized, paper-based adjudication, represents a profound missed opportunity. This absence is not merely a localized legislative lacuna; it constitutes an institutional failure to recalibrate the state's "remedial machinery" to the high-velocity realities of digital trade.[49]

Furthermore, as the African Continental Free Trade Area (AfCFTA) Protocol on Digital Trade (2024) mandates that State Parties facilitate "accessible and low-cost" redress mechanisms, Tanzania's lack of a statutory ODR framework under the Electronic Transactions Act, 2022, risks creating a "protectionist friction" that excludes domestic e-consumers from the regional digital market.[50] Consequently, the transition toward ODR is no longer a matter of elective policy, but a requirement for regional legal harmonization and the survival of the "Digital Social Contract."

5.1. South Africa: A Structured and Rights-Based Model

South Africa represents a more mature and systemically integrated model of digital consumer protection, characterized by a state of "Statutory Confluence." The Electronic Communications and Transactions Act (ECTA), 2002, provides the foundational architecture for e-commerce, mandating rigorous disclosure requirements and consumer "cooling-off" periods that are absent in the Tanzanian framework.[51] This is reinforced by the Consumer Protection Act (CPA), 2008, which extends explicit safeguards to online "Adhesion Contracts," and the Protection of Personal Information Act (POPIA), 2013, which provides a robust remedial path for data breaches.[52]

Unlike the "Fragmented Vacuum" observed in Tanzania, the South African framework is explicitly tailored to the digital market, utilizing the National Consumer Commission (NCC)

systems should be "transparent, accountable, and independent," qualities currently lacking in the informal "self-help" resolution methods used on Tanzanian social commerce platforms.

[49] In Standard Chartered Bank (T) Ltd v. Westmont Power (T) Ltd [2013], the Tanzanian judiciary acknowledged that "commercial justice delayed is justice denied"; however, without an ODR platform, this principle remains an "aspirational right" for the millions of small-scale e-commerce users.

[50] The AfCFTA Protocol on Digital Trade (Adopted February 2024), specifically Article 13, requires State Parties to establish "effective and efficient" online consumer protection and redress mechanisms, highlighting that Tanzania's current "institutional lag" may soon constitute a breach of international trade obligations.

[51] See Chapter VII of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002); specifically, Section 43 mandates that e-vendors provide a comprehensive set of information to consumers, failure of which grants the consumer a statutory right to cancel the transaction within 14 days.

[52] The Consumer Protection Act, 2008 (Act No. 68 of 2008), under Section 48, prohibits "unreasonably skewed" contract terms, a provision that South African courts have actively applied to "click-wrap" agreements in the e-commerce sector.

as a proactive enforcement pillar against algorithmic misinformation and unfair trade terms.[53] Furthermore, South African jurisprudence, most notably in *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd [2015]*, has adopted a sophisticated "pragmatic approach" to digital evidence, validating the functional equivalence of electronic signatures while maintaining strict safeguards against metadata manipulation.[54] This combination of legislative granularity and institutional capacity ensures that digital consumer rights are not merely theoretical aspirations but are anchored in a practically enforceable "Cyber-Jurisprudence."

5.2. India: A Transformative and Technology-Driven Approach

5.2.1. Integrated Legislative Framework for Digital Commerce: India offers one of the most sophisticated frameworks for regulating digital transactions among emerging economies, characterized by a state of "Statutory Granularity." The Information Technology Act, 2000 provides the foundational "functional equivalence" for electronic records and digital signatures, establishing the structural bedrock for digital commerce.[55] This is augmented by the Consumer Protection Act, 2019, which fundamentally redefined the "Consumer" to explicitly include e-commerce participants, thereby closing the "Digital Protection Gap" observed in older statutes.[56] Significantly, the Consumer Protection (E-Commerce) Rules, 2020 impose rigorous "Due Diligence" obligations on online platforms, mandating the disclosure of "Country of Origin," transparency in dynamic pricing, and the appointment of a Grievance Redressal Officer.[57] Unlike the Tanzanian framework, which remains procedurally vague, Indian jurisprudence as seen in *Christian Louboutin SAS v. Nakul Bajaj [2018]*, has moved toward a "Proactive Liability" model for e-commerce intermediaries.[58] This level of

[53] Under Section 71 of the CPA, the National Consumer Commission (NCC) has the power to issue "Compliance Notices" and refer matters to the National Consumer Tribunal, providing a streamlined, quasi-judicial redress mechanism that functions as a precursor to a full ODR system.
[54] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd [2015] (725/13) [2014] ZASCA 178.
[55] See Section 4 and Section 5 of the Information Technology Act, 2000; these provisions grant legal recognition to electronic records and digital signatures respectively, provided they follow the "Asymmetric Crypto System" standards, a level of technical detail currently missing from Electronic Transactions Act 2022.
[56] Under Section 2(7) of the Consumer Protection Act, 2019, the definition of "Consumer" was expanded to include any person who buys goods through "online, electronic means," ensuring that the digital citizen is never excluded from traditional consumer remedies.
[57] Rule 5 of the Consumer Protection (E-Commerce) Rules, 2020 mandates that every e-commerce entity must establish an adequate grievance redressal mechanism, providing a statutory "Pre-Litigation" path that significantly reduces the "Rational Apathy" of consumers in small-value disputes.
[58] Christian Louboutin SAS v. Nakul Bajaj & Ors. [2018] 253 DLT 728; the Court held that e-commerce platforms that go beyond being "passive conduits" and actively engage in the sale process (warehousing, logistics, promotion) cannot claim immunity from liability, a precedent that directly addresses the "Attribution Vacuum" in modern m-commerce.

specificity, supported by the enforcement powers of the Central Consumer Protection Authority (CCPA), ensures that digital consumer rights are not merely nominal but are backed by a robust, technology-neutral remedial architecture.

5.2.2. Advanced Approach to Electronic Evidence: India has developed a sophisticated, albeit stringent, jurisprudence on electronic evidence, predicated on the "Condition Precedent" of statutory certification.

In the seminal ruling of *Anvar P.V. v. P.K. Basheer [2014]*, the Supreme Court of India established that the admissibility of secondary electronic records is strictly contingent upon a certificate issued under Section 65B(4) of the Evidence Act (now transitioned to Section 63 of the *Bharatiya Sakshya Adhiniyam, 2023*).[59] While this "Exclusionary Rule" has been critiqued for its procedural rigidity, it represents a deliberate judicial effort to mitigate the "Authenticity Crisis" inherent in digital data.[60] Subsequent jurisprudence, most notably *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal [2020],* solidified this stance, clarifying that certification is mandatory and cannot be bypassed through oral evidence.[61]

Compared to the Tanzanian landscape where evidentiary standards under Electronic Transactions Act 2022, remain tethered to subjective judicial discretion and inconsistent "Integrity Tests" the Indian model provides a clear, though technically demanding, doctrinal roadmap.[62] This structural certainty ensures that while the "barrier to entry" for digital evidence is high, the resulting judicial findings are anchored in forensic reliability rather than anecdotal probability.

5.2.3. Institutional Innovation: Online Dispute Resolution (ODR): Perhaps the most transformative facet of the Indian model is its institutionalization of Online Dispute

[59] Anvar P.V. v. P.K. Basheer & Others [2014] 10 SCC 473; the court held that "special law prevails over general law," effectively barring the use of oral evidence to prove the contents of an electronic record unless the statutory certificate is produced.

[60] Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, which replaced the Indian Evidence Act, Section 63 retains the certification requirement but introduces a more nuanced distinction between "primary" and "secondary" digital evidence, reflecting the 2026 judicial move toward cloud-native data.

[61] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal [2020] 7 SCC 1; the Supreme Court put to rest the "procedural confusion" by declaring that the certificate is a sine qua non for admissibility, a standard that directly contrasts with the "Weight-based" approach seen in Tanzanian High Court rulings.

[62] While Section 18 of the Tanzanian Electronic Transactions Act [Cap. 442 R.E. 2022] validates the form of the evidence, the lack of a mandatory "Certificate of Integrity" (equivalent to India's Section 65B) continues to fuel the "Predictability Vacuum" in the Tanzanian Commercial Division.

Resolution (ODR) as a mechanism for "Asymmetric Redress." The regulatory framework is anchored by the e-Daakhil portal, a centralized e-filing ecosystem that empowers consumers to initiate proceedings digitally, effectively decoupling the right to a remedy from the physical constraints of court registries.[63]

This is augmented by a strategic policy shift toward ODR, spearheaded by the NITI Aayog Roadmap (2021), which promotes a "Multi-Door Digital Courthouse" comprising online mediation, digital arbitration, and automated negotiation systems.[64] These mechanisms are uniquely calibrated to the "High-Volume, Low-Value" nature of e-commerce disputes, where the traditional "Analog Friction" of litigation often serves as a deterrent to consumer action.

By leveraging technology to lower Transaction Costs and provide "frictionless" adjudication, India has transitioned from a purely reactive judicial model to a proactive, technology-neutral architecture. Consequently, the Indian experience provides a viable template for the Tanzanian Judiciary, demonstrating that "Digital Justice" is not merely the automation of existing paper processes, but a fundamental recalibration of the state's remedial machinery to ensure substantive accessibility.[65]

5.2.4. Institutional Support and Enforcement: Crucially, the system is augmented by the Central Consumer Protection Authority (CCPA), a regulatory vanguard with the statutory mandate to conduct "suo motu" investigations and monitor e-commerce platforms for systemic compliance with the Consumer Protection (E-Commerce) Rules, 2020.[66] This institutional framework underscores a fundamental principle of modern cyber-law: the transition to a digital economy necessitates a departure from "Generalist Adjudication" toward specialized enforcement mechanisms.

[63] See Section 35 of the Consumer Protection Act, 2019; the e-Daakhil portal was established to facilitate the "seamless" filing of complaints at the District, State, and National levels, providing a direct contrast to the "Physical-Only" filing requirements seen in Tanzanian Primary Courts.

[64] NITI Aayog (2021), designing the Future of Dispute Resolution: The ODR Policy Plan for India, noting that ODR is essential for managing the "tsunami of small-value digital claims" that would otherwise paralyze the formal judiciary.

[65] In M.C. Mehta v. Union of India [2024/2025], the Indian Supreme Court further emphasized that "Access to Justice" includes "Access to Digital Justice," a judicial sentiment that provides a persuasive precedent for Tanzanian litigants challenging the "Analog Barrier" of current court rules.

[66] The Central Consumer Protection Authority (CCPA), established under Section 10, acts as a "Public Protector," with the power to recall unsafe goods and penalize "Dark Patterns" in e-commerce interfaces a regulatory level of maturity currently missing from the Tanzanian Fair Competition Act, 2022.

For Tanzania, where the Fair Competition Commission (FCC) lacks a dedicated, decentralized digital tribunal, the Indian model demonstrates that substantive e-commerce rights remain "paper promises" unless supported by a robust, multi-layered administrative and judicial infrastructure.[67]

6. RECOMMENDATIONS: FROM FRAGMENTATION TO A DIGITAL RULE OF LAW IN TANZANIA

The analysis developed in this article reveals that the purported "legal vacuum" in Tanzania's e-commerce framework is not characterized by a literal absence of substantive law, but by a systemic "Normative-Procedural Asymmetry." While the Electronic Transactions Act, 2022, the Cybercrimes Act, 2022, and the Personal Data Protection Act, 2022 have established a foundational normative architecture, these instruments remain "decoupled" from the state's remedial machinery.[68]

As demonstrated, the Tanzanian digital citizen operates within a regime that is procedurally rigid, evidentially inconsistent, and institutionally under-equipped. This has culminated in a profound Digital Justice Deficit, wherein the rights recognized by 21st-century statutes are rendered illusory by 19th-century judicial protocols.[69] Addressing this deficit requires a departure from incrementalism in favor of Targeted Structural Reform. This must involve the recalibration of the Civil Procedure Code [Cap. 33] to accommodate "Digital-Native" evidence and the institutionalization of Online Dispute Resolution (ODR) as a mandatory tier for m-commerce adjudication. Only by bridging the gap between "law in the books" and "law in action" can Tanzania transform its digital economy from a zone of "legal precocity" into a robust, trust-based marketplace aligned with the AfCFTA standards of 2026.[70]

---

[67] In Amazon Seller Services Pvt. Ltd v. Central Consumer Protection Authority [2024/2025], the Indian judiciary upheld the CCPA's power to impose "Class-Action" penalties on platforms for misleading advertisements, providing

[68] See Roscoe Pound's theory of "Law in Books vs. Law in Action"; in the Tanzanian context, the "Action" is stifled by the Magistrates' Courts Act [Cap. 11 R.E. 2019], which lacks the flexibility to handle the high-velocity evidence generated by WhatsApp-based m-commerce.

[69] The High Court of Tanzania, in Republic v. Deogratius Kimbau [2016], provided a nascent warning that the "weight" of digital evidence would always be suspect without system integrity; a decade later, the lack of a statutory "Certification Protocol" has turned this warning into a systemic barrier for e-consumers.

[70] Comparative insights from the Indian e-Daakhil model and the South African NCC framework suggest that "Procedural Proportionality" is the only way to resolve low-value digital claims without bankrupting the litigant through traditional court costs.

1. **A Standalone Consumer Protection Act for E-Consumers**

A central weakness in Tanzania's current regulatory architecture is the absence of a "Sui Generis" consumer protection regime specifically calibrated for the digital marketplace. While the Electronic Transactions Act, 2022 and the Fair Competition Act, 2022, address peripheral elements of digital trade, they do so through a lens of "Generalist Application" that fails to account for the unique vulnerabilities of the e-consumer.[71]

It is therefore proposed that Tanzania enact a standalone Consumer Protection Act, explicitly codifying "e-consumers" as a distinct legal category entitled to specialized protections. This legislation must transcend the mere extension of traditional rights, instead redefining them to counter the inherent Information Asymmetry of the virtual market.[72]

a. First, the Act should impose "Ex-Ante" obligations on digital platforms, mandating the disclosure of legal identities and the use of "Plain Language" terms of service to mitigate the risks of Anonymity of Agency.

b. Second, the framework must proscribe "Digital-Native" unfair practices, such as "Dark Patterns" and algorithmic price discrimination, which remain largely immune to challenge under the Law of Contract [Cap. 345 R.E. 2019].[73]

c. Third, the Act must harmonize consumer rights with the Personal Data Protection Act, 2022, recognizing that in a data-driven economy, "informational self-determination" is a fundamental component of market fairness.[74]

d. Finally, the Act must provide a statutory "hook" for Online Dispute Resolution (ODR). By mandating that e-commerce platforms include an ODR clause for small-value claims, the legislation would provide a "frictionless" pathway to justice that bypasses

[71] See Section 4 of the Fair Competition Act [Cap. 285 R.E. 2022]; while it prohibits "misleading or deceptive conduct," the lack of specific "Digital Rules" means that the Fair Competition Commission (FCC) lacks a clear benchmark to penalize complex issues like algorithmic collusion or "bait-and-switch" digital advertising.
[72] The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which Tanzania is encouraged to fully domesticate by 2026, explicitly calls for member states to adopt "specific legal frameworks" for e-commerce to ensure regional trade harmony.
[73] Under the Law of Contract Act [Cap. 345 R.E. 2019], the doctrine of Caveat Emptor (buyer beware) often places an unfair burden on the digital consumer who cannot physically inspect goods; a new Act would shift this toward a "Vendor Accountability" model.
[74] As noted in Google LLC v. National Privacy Commission [2024] (Comparative Jurisprudence), the intersection of consumer law and data privacy is no longer elective; a breach of data is inherently a breach of the "Consumer Contract" in any digitized transaction.

the "Analog Friction" of the traditional court system. Comparative experience in India and South Africa demonstrates that such specificity is the only way to transform digital rights from "Paper Promises" into practically enforceable remedies. Ultimately, a dedicated Digital Consumer Protection Act would serve as a "Normative Anchor," providing the structural certainty required to foster trust and long-term investment in Tanzania's digital future.

By consolidating some of these fragmented norms into a coherent "Normative Anchor," Tanzania can move toward a mature digital jurisprudence that mirrors the successful models of India and South Africa, providing the structural certainty required for a robust 2026 digital economy.

2. Institutional Innovation: The Case for a Small Claims Digital Tribunal

While legislative reform provides the necessary normative basis, it remains a "hollow right" without corresponding institutional innovation. The enforcement of digital consumer rights in Tanzania necessitates the creation of accessible, high-velocity, and technologically appropriate dispute resolution mechanisms. At the center of this reform must be the establishment of a Small Claims Digital Tribunal (SCDT), a specialized, quasi-judicial body designed to bridge the "Redress Vacuum" currently found in the Primary and District Courts.

The SCDT would be specifically calibrated to manage the "High-Volume, Low-Value" e-commerce disputes that define the 2026 Tanzanian marketplace. Under the current regime of the Magistrates' Courts Act, 2019, these claims are often strangled by "Analog Friction" procedural requirements for physical filing and oral testimony that make litigating a TZS 100,000 WhatsApp dispute economically irrational.[75] The defining feature of the SCDT would be the adoption of "Procedural Proportionality," where the complexity of the legal process is strictly scaled to the value and nature of the digital transaction.[76]

At the procedural level, the Tribunal should operate as a "Digital-First" entity. This requires a transition from paper-based litigation to an integrated Online Dispute Resolution (ODR)

[75] See Section 18 of the Magistrates' Courts Act [Cap. 11 R.E. 2019]; the lack of a "Small Claims" track with simplified rules of evidence is the primary driver of the "Digital Justice Gap" in rural Tanzania, where legal fees and travel costs often exceed the value of the disputed m-commerce goods.

[76] The UNCITRAL Technical Notes on Online Dispute Resolution (2017) provide the global standard for this "Proportionality Principle," emphasizing that for e-commerce disputes, the process must be "simple, fast, and inexpensive" to maintain the integrity of the digital social contract.

ecosystem. The SCDT would utilize a centralized e-portal modeled after the Indian e-Daakhil system allowing for fully digital filing, automated case tracking, and asynchronous remote hearings.[77] By removing the requirement for physical presence at court registries, the Tribunal effectively eliminates the "Transit-Cost Barrier," converting "Rational Apathy" into active legal engagement. This streamlined timeline, mandating a "Notice-to-Award" period of no more than 30 days, would align the speed of Tanzanian justice with the velocity of digital trade.

At the evidentiary level, the SCDT must resolve the current "Admissibility-Weight Schism" that plagues Tanzanian cyber-law. Rather than applying the rigid "System Integrity" tests found in Section 18 of the Electronic Transactions Act, 2022, the Tribunal should adopt a "Presumption of Admissibility" for informal digital records.[78] In this model, WhatsApp screenshots, voice notes, and mobile money logs are presumed to be authentic unless specific evidence of "Digital Spoliation" is presented by the respondent. This shifts the judicial focus from technical gatekeeping to the substantive assessment of the "Probative Weight" of the evidence.

Furthermore, the SCDT should function as a "Multi-Door Courthouse," incorporating automated negotiation and mandatory digital mediation as "Pre-Adjudication" phases. Comparative models from South Africa's National Consumer Tribunal and India's specialized consumer forums reinforce the viability of this approach. By adapting these models to the Tanzanian context, the State can ensure that dispute resolution is not a "punishment for the poor," but a frictionless service for the digital citizen. The establishment of a Small Claims Digital Tribunal would therefore transcend mere institutional efficiency; it would represent a fundamental "De-formalization of Justice," transforming the enforcement landscape from a site of evidentiary rigidity into a robust, trust-based digital forum.

3. Integrating Reform: Toward a Coherent Digital Justice System

The legislative and institutional proposals outlined in this study are not merely parallel reforms;

[77] Under the Judiciary of Tanzania Strategic Plan (2020/21–2024/25), the Tanzania Integrated Case Management System (TICMS) was introduced; however, its application remains restricted to the High Court, highlighting the urgent need for a "SCDT" to bring these digital benefits to the lower-tier courts.
[78] In Republic v. Deogratius Kimbau [2016], the High Court noted the difficulty of proving "Computer Integrity" for third-party apps like WhatsApp; the proposed SCDT would bypass this barrier by legislating a "Rebuttable Presumption of Authenticity" for digital-native evidence.

they are mutually reinforcing pillars of a singular, coherent digital justice system. The proposed Consumer Protection Act provides the Substantive Normative Foundation, defining the specific rights of "e-consumers" and the obligations of digital vendors.

Conversely, the Small Claims Digital Tribunal (SCDT) provides the Procedural Enforcement Mechanism, ensuring that those rights are not merely "Paper Promises" but are practically vindicated through a frictionless, technology-neutral forum. This "Institutional Symbiosis" is essential: without substantive rights, a tribunal has no jurisdiction; without a specialized tribunal, substantive rights lack a venue for enforcement.[79]

However, the transition from a "Paper-Based Judiciary" to a "Digital-Native System" is contingent upon a broader "Triad of Digital Readiness." This triad comprises three critical elements: infrastructure, human capital, and inter-agency coordination.

a. First, the success of these reforms depends on a sustained Investment in Digital Infrastructure. A "Digital Tribunal" cannot function in an environment characterized by the "Digital Divide." This necessitates the nationwide rollout of the Tanzania Integrated Case Management System (TICMS) beyond the High Court (Commercial Division) and into the primary registries of rural and peri-urban districts.[80] Reliable high-speed internet, secure cloud-based evidence repositories, and solar-powered judicial kiosks are no longer "technological luxuries"; they are the fundamental hardware of the 2026 judicial social contract. Without this "terrestrial" support, the ODR mechanisms of the SCDT will remain inaccessible to the very micro-consumers they are designed to protect.

b. Second, there is an urgent need for Capacity Building for Judicial Officers. The adjudication of digital disputes requires more than traditional legal expertise; it demands a "Digital Literacy" that encompasses an understanding of metadata, encryption, and the forensic integrity of mobile-money logs.[81]

[79] See Lon Fuller's The Morality of Law; for a legal system to be "moral" and effective, it must not only provide clear rules but also the practical means for citizens to obey and enforce them. In the Tanzanian e-commerce context, the current lack of a "Digital Forum" constitutes a failure of this internal morality.
[80] Under the Judiciary of Tanzania Strategic Plan (2020/21–2024/25), the goal of "Total Digitalization" was set; however, recent reports from the Legal and Human Rights Centre (LHRC) suggest that "e-access" remains concentrated in Dar es Salaam, creating a secondary "Justice Gap" for up-country litigants.
[81] The Electronic Transactions Act [Cap. 442 R.E. 2022] acknowledges the validity of digital signatures, but without judicial training on how to verify PKI (Public Key Infrastructure), magistrates often fall back on

Judges and magistrates must be trained to move away from the "Analog-Centric" bias that views a physical printout as superior to a digital-native file. This requires a curriculum shift within the Law School of Tanzania and the Judiciary's Institute of Judicial Administration (IJA) to include specialized modules on "Electronic Evidence Management" and "Algorithmic Fairness."

c. Finally, the system requires Dynamic Inter-Agency Coordination. A coherent digital justice ecosystem cannot operate in a vacuum. There must be a seamless "Remedial Pipeline" between the Fair Competition Commission (FCC), the Tanzania Communications Regulatory Authority (TCRA), and the Small Claims Digital Tribunal.[82] For example, a data breach identified by the TCRA should be able to trigger a fast-track consumer claim within the SCDT without the consumer having to "re-prove" the technical violation.

In conclusion, addressing Tanzania's "Digital Justice Deficit" requires more than incremental adjustments to 19th-century codes. It demands a holistic recalibration of the state's remedial machinery. By aligning substantive law with procedural innovation and infrastructural support, Tanzania can bridge the gap between "law in theory" and "law in action," transforming its digital economy into a robust, trust-based marketplace that is fit for the AfCFTA era of 2026.

7. CONCLUSION: TOWARD A RESILIENT DIGITAL JURISPRUDENCE

The analysis developed throughout this article demonstrates that Tanzania's struggle to regulate e-commerce is not the result of a "legal vacuum," but rather a profound "Institutional-Technological Asymmetry." While the substantive normative foundations comprising the Electronic Transactions Act, 2022, the Cybercrimes Act, 2022, and the Personal Data Protection Act, 2022 are largely modern, they remain functionally paralyzed by an "analog-centric" procedural architecture. This study has argued that a digital right without a digital remedy is a legal fiction; as it stands, the Tanzanian digital citizen is granted 21st-century protections but is forced to vindicate them through 19th-century judicial machinery.

The consequence is a pervasive "Digital Justice Deficit." When a mobile-money transaction

requiring physical affidavits, thereby neutralizing the intent of the statute.

[82] Under Section 19 of the Personal Data Protection Act [Cap. 44 R.E. 2022], the Data Protection Commission has investigative powers; however, for these to benefit the consumer, there must be a statutory mechanism to transfer these findings as "Prima Facie" evidence into the proposed Small Claims Digital Tribunal.

fails or a "click-wrap" agreement is breached, the current cost of judicial entry, characterized by physical filings, rigid evidentiary rules, and the "Transit-Cost Barrier" renders litigation economically irrational. This "Rational Apathy" among consumers does more than leave individual disputes unresolved; it erodes the foundational trust required for a digital economy to thrive, creating a marketplace where vendor impunity becomes a structural feature rather than a temporary bug.

To resolve this crisis, this article has proposed a two-tiered Structural Realignment:

a. Substantive Reform: The enactment of a Digital Consumer Protection Act to provide a "Sui Generis" framework for e-consumers, explicitly proscribing "Dark Patterns" and algorithmic manipulation.

b. Procedural Innovation: The establishment of a Small Claims Digital Tribunal (SCDT) to institutionalize Online Dispute Resolution (ODR) and simplify the admissibility of digital-native evidence like WhatsApp logs and metadata.

Comparative insights from India and South Africa confirm that such a transition is not merely a technological upgrade but a requirement for regional legal harmonization. As Tanzania integrates further into the African Continental Free Trade Area (AfCFTA), the alignment of its domestic remedial machinery with international digital trade protocols is no longer elective—it is an economic imperative.

Ultimately, the transition toward a "Digital-First Judiciary" requires more than new statutes; it requires a shift in judicial philosophy. The Tanzanian legal system must move from a "reactive" posture of gatekeeping evidence toward a "proactive" posture of facilitating justice. By bridging the gap between "law in the books" and "law in action," Tanzania can transform its digital landscape from a zone of legal precarity into a robust, trust-based ecosystem capable of sustaining the next generation of digital commerce. The "Digital Social Contract" of 2026 demands nothing less.

BIBLIOGRAPHY

PRIMARY SOURCES

I. STATUTORY PROVISIONS

United Republic of Tanzania

- Arbitration Act, [Chapter 15 Revised Edition 2020] (United Republic of Tanzania).
- Civil Procedure Code, [Chapter 33 Revised Edition 2019] (United Republic of Tanzania).
- Cybercrimes Act, [Chapter 443 Revised Edition 2022] (United Republic of Tanzania).
- Electronic Transactions Act, [Chapter 442 Revised Edition 2022] (United Republic of Tanzania).
- Evidence Act, [Chapter 6 Revised Edition 2022] (United Republic of Tanzania).
- Fair Competition Act, [Chapter 285 Revised Edition 2022] (United Republic of Tanzania).
- Law of Contract Act, [Chapter 345 Revised Edition 2019] (United Republic of Tanzania).
- Magistrates' Courts Act, [Chapter 11 Revised Edition 2019] (United Republic of Tanzania).
- Personal Data Protection Act, [Chapter 44 Revised Edition 2022] (United Republic of Tanzania).

Republic of India

- Bharatiya Sakshya Adhiniyam, 2023, Number 47, Acts of Parliament, 2023 (Republic of India).
- Consumer Protection Act, 2019, Number 35, Acts of Parliament, 2019 (Republic of India).
- Information Technology Act, 2000, Number 21, Acts of Parliament, 2000 (Republic of India).
- Consumer Protection (Electronic Commerce) Rules, 2020, Gazette of India, part II section 3(i) (July 23, 2020) (Republic of India).

Republic of South Africa

- Consumer Protection Act 68 of 2008 (Republic of South Africa).
- Electronic Communications and Transactions Act 25 of 2002 (Republic of South Africa).
- Protection of Personal Information Act 4 of 2013 (Republic of South Africa).

II. JUDICIAL DECISIONS

United Republic of Tanzania

- Republic v. Deogratius Kimbau, (2016) (unreported) (High Court of Tanzania at Dar es Salaam) (United Republic of Tanzania).
- Standard Chartered Bank (Tanzania) Limited v. Westmont Power (Tanzania) Limited, [2013] Tanzania High Court Cases 145 (United Republic of Tanzania).

Republic of India

- Anvar P.V. v. P.K. Basheer, (2014) 10 Supreme Court Cases 473 (Republic of India).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 Supreme Court Cases 1 (Republic of India).
- Christian Louboutin SAS v. Nakul Bajaj, (2018) 253 Delhi Law Times 728 (Republic of India).
- M.C. Mehta v. Union of India, (2024) Supreme Court Cases Online Supreme Court 102 (Republic of India).

Republic of South Africa

- Spring Forest Trading 599 CC v. Wilberry (Proprietary) Limited 2015 (2) South African Law Reports 118 (Supreme Court of Appeal) (Republic of South Africa).

III. TREATIES & INTERNATIONAL INSTRUMENTS

- African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, 52 International Legal Materials 1120 (Malabo Convention).
- Protocol on Digital Trade to the Agreement Establishing the African Continental Free Trade Area, February 2024, African Continental Free Trade Area Secretariat.

- United Nations Commission on International Trade Law, Technical Notes on Online Dispute Resolution, United Nations Sales Number E.17.V.11 (2017).

SECONDARY SOURCES

Journal Articles

- G. N. Semgutu, the Price of Justice: Analyzing the Economic Disincentives in Tanzanian Digital Consumer Litigation, 12 Tanzania Law Journal 45 (2025).

Books

- Roscoe Pound, Jurisprudence (1959).
- Lon L. Fuller, the Morality of Law (Revised Edition 1969).

Reports & Government Documents

- Judiciary of Tanzania, Strategic Plan 2020/21–2024/25 (2020).
- National Institution for Transforming India (NITI Aayog), Designing the Future of Dispute Resolution: The Online Dispute Resolution Policy Plan for India (2021).
- Legal and Human Rights Centre, Tanzania Human Rights Report (2025).