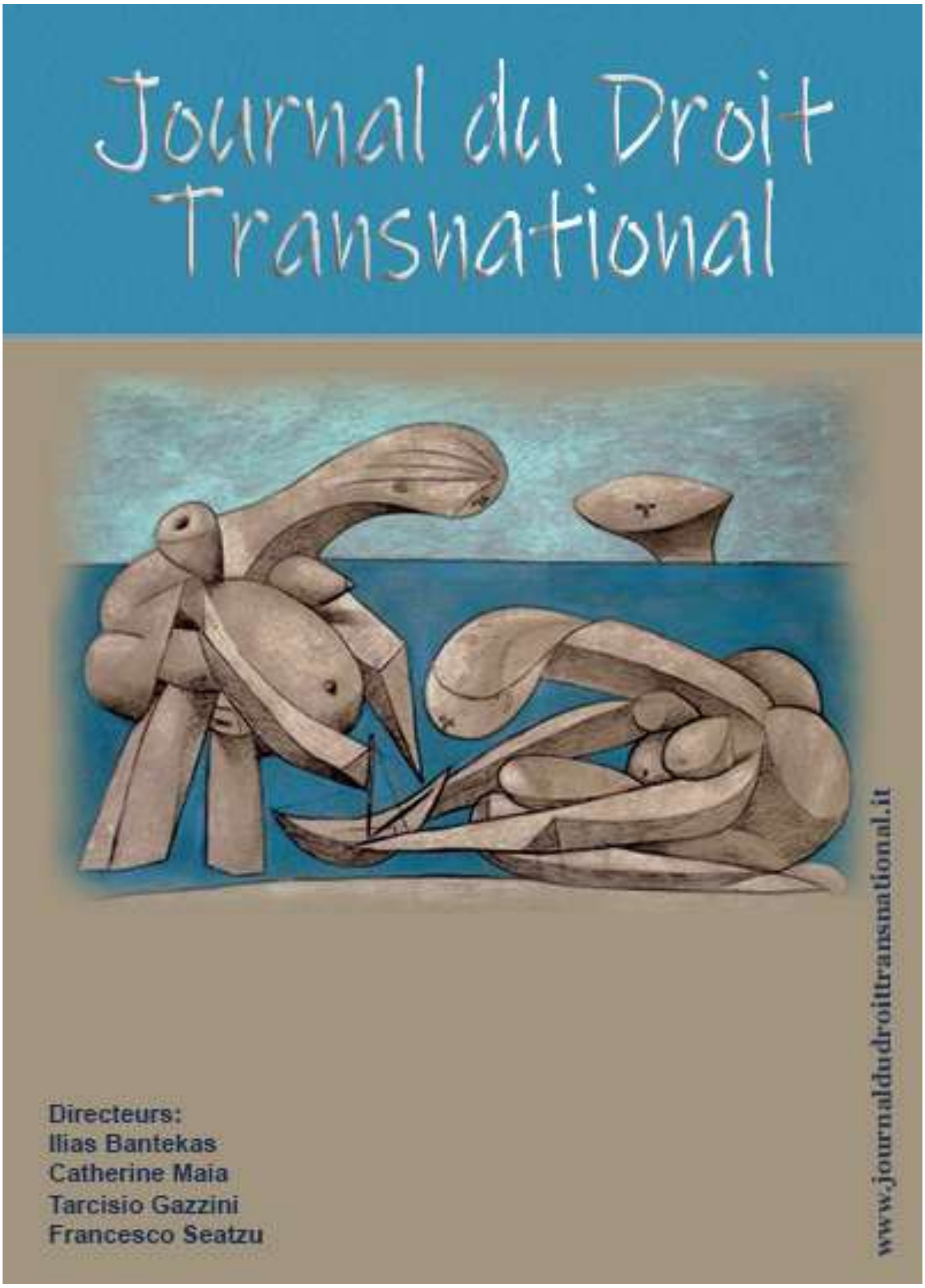

DEFERENCE DEFERRED:

THE ECOWAS COURT, NIGERIA'S CYBERCRIME ACT, AND THE ENFORCEMENT PROBLEM IN REGIONAL CYBER LAW HARMONISATION

Obongodu Paul Unanam

Abstract
In July 2020, the ECOWAS Community Court of Justice ordered Nigeria to repeal or amend Section 24 of its Cybercrime (Prohibition, Prevention, etc.) Act 2015, finding that the provision violated Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the International Covenant on Civil and Political Rights. Nigeria did not comply for four years. A second ruling in 2022 reinforced the order. During the interval, Section 24 continued to be used to arrest journalists, bloggers, and critics of the government. The Cybercrimes (Amendment) Act 2024 eventually addressed some of the language, though disputes remain about whether the changes achieve full compliance.

This article uses that four-year delay as its subject. The argument is not that Nigeria was wrong to delay. The question is what the delay reveals about how regional cyber law harmonisation actually works when a member state has no financial incentive to comply and its executive has a political interest in retaining the statute. The article draws on the transnational law literature, the sociology of international adjudication compliance, and the institutional architecture of the ECOWAS system to identify three structural factors: the absence of any coercive mechanism in the ECOWAS Treaty framework, the political economy of cybercrime legislation in Nigeria, and the mismatch between how long international adjudication takes and how fast digital rights violations accumulate. It concludes with proposals for a compliance monitoring committee, more specific provisional measures, and linkage between cyber rights compliance and the ECOWAS digital trade framework.

Keywords: ECOWAS Court of Justice; cybercrime legislation; freedom of expression; West Africa; transnational law; compliance; regional human rights systems; digital rights

I. INTRODUCTION

In 2015, Nigeria's National Assembly enacted the Cybercrime (Prohibition, Prevention, etc.) Act. Section 24 of that statute, titled 'cyberstalking,' criminalised any message sent via computer that a recipient or third party found grossly offensive, indecent, obscene, or menacing. No meaningful threshold of intent was required. No harm had to be shown. A post that someone found annoying was potentially a crime.

What followed was predictable. Journalists were arrested for tweets critical of state governors. Social media users were prosecuted for sharing unflattering coverage of public officials. A blogger in Kano spent weeks in detention after a post that referred to a local politician as corrupt. The law did not distinguish between harassment and accountability journalism, and the police did not try to draw the line themselves.

In 2018, the Incorporated Trustees of Laws and Rights Awareness Initiative filed an application before the ECOWAS Community Court of Justice challenging Section 24's compatibility with the African Charter on Human and Peoples' Rights and the International Covenant on Civil and Political Rights.[1] On 10 July 2020, the Court found Nigeria liable for violating the right to freedom of expression and ordered it to repeal or amend the provision.[2]

Nigeria did nothing for four years. Arrests under Section 24 continued. A second case by the Socio-Economic Rights and Accountability Project produced a reinforcing order from the same Court in 2022.[3] The Cybercrimes (Amendment) Act was eventually passed in 2024, addressing some of the vague language, though civil society organisations and legal commentators have questioned whether the changes fully satisfy what the Court required.[4]

This article is about that gap. Not about whether the Court was right, it was, but about why a legally sound, clearly grounded international order produced four years of non-compliance from a state that had the institutional capacity to comply. The answer has less to do with bad faith, though bad faith was present, than with structural features of the ECOWAS enforcement system, the political incentive landscape in Abuja, and the temporal architecture of international adjudication.

The analysis proceeds as follows. Part II situates the ECOWAS Court's jurisprudence on digital rights within the framework of transnational law. Part III identifies three structural factors that explain the compliance delay. Part IV offers three proposals for improving the system. Part V concludes.

II. THE ECOWAS COURT AND CYBER RIGHTS

Philip Jessup defined transnational law in 1956 as all law which regulates actions or events that transcend national frontiers, including public and private international law and other rules that do not fit neatly into those categories.[5] He was writing about commercial arbitration and shipping disputes. But the definition describes, with some accuracy, the situation that arises when a domestic cybercrime statute produces rights

[1]Incorporated Trustees of Laws and Rights Awareness Initiative v. Federal Republic of Nigeria, Application No. ECW/CCJ/APP/53/18, filed 6 November 2018.

[2]Judgment No. ECW/CCJ/JUD/11/20 (10 July 2020). The Court found Nigeria liable under Art 9 of the African Charter on Human and Peoples' Rights and Art 19 of the ICCPR and ordered repeal or amendment of Section 24.

[3]SERAP v. Federal Republic of Nigeria, Judgment No. ECW/CCJ/JUD/09/24 (ECOWAS Court of Justice, 2024).

[4]Prince Ederagobor, 'Digital Speech on Trial: Section 24 of Nigeria's Cybercrime Act and its Impact on Civil Liberties' (2025) SSRN Working Paper 5315568.

[5]Philip Jessup, Transnational Law (Yale University Press 1956) 2.

violations affecting communications that routinely cross borders, and a regional court attempts to adjudicate the result.

The ECOWAS Community Court of Justice has human rights jurisdiction by virtue of the 2005 Supplementary Protocol.[6] That jurisdiction is declaratory. The Court can find a violation, order a remedy, and issue provisional measures. It cannot execute its own judgments. There is no ECOWAS bailiff, no regional property seizure, no automatic referral to a political organ when a state does nothing after losing a case. The 2005 Protocol requires member states to comply; it provides no mechanism for ensuring they do.[7]

This design was deliberate. The drafters of the Protocol were operating in a political environment where West African states were not going to accept coercive judicial enforcement of human rights orders. The model they chose, a court with authority to declare violations but no power to compel correction, was the minimum viable jurisdiction available at the time. It was better than nothing. But it is not adequate for the kind of rights violations at issue in the Section 24 cases, where harm accumulated daily at the speed of digital communication while the legal process moved at the pace of international litigation.

The Laws and Rights Awareness Initiative judgment is methodologically straightforward. The Court applies the standard three-part proportionality test, legality, legitimate aim, necessity in a democratic society, to Section 24 and finds the provision fails the first step.[8] The statutory language is too vague to constitute a clear legal prohibition of the kind required under international human rights law when restricting freedom of expression. There was no novel doctrine here, no contested legal question. The Court applied settled norms to a domestic statute that failed them.

What makes the case a transnational law problem is not the substantive finding but the pathway from judgment to compliance. That pathway runs through multiple institutional actors: the Court, the Nigerian Attorney General's office, the National Assembly, civil society organisations monitoring implementation. Each actor operates on a different timeline and responds to different incentives. The Court issued an order. The rest was politics.

[6]Supplementary Protocol A/SP.1/01/05 Amending the Preamble and Articles 1, 2, 9, 22 and 30 of Protocol A/P.1/7/91 on the Community Court of Justice.

[7]Supplementary Protocol A/SP.1/01/05, Art 24: member states 'shall take all necessary measures to comply with the judgments of the Court and ensure their execution within their national legal system.'

[8]ECW/CCJ/JUD/11/20 (n 2) paras 90 to 126, applying the proportionality framework drawn from the UN Human Rights Committee's General Comment No. 34 on freedom of expression.

III. WHY FOUR YEARS? THREE STRUCTURAL FACTORS

A. The ECOWAS Treaty Has No Coercive Compliance Mechanism for Human Rights Orders

The enforcement architecture of the ECOWAS system was built for trade disputes, not human rights remedies. The primary compliance incentive is the threat of sanctions in the economic integration context: tariff retaliation, suspension from preferential trade arrangements, exclusion from ECOWAS organs. The 1999 Protocol on the Mechanism for Conflict Prevention adds further tools for security matters. Neither applies when a member state ignores a human rights judgment from the Community Court.[9]

Article 24 of the 2005 Supplementary Protocol provides only that member states shall take all necessary measures to comply with the judgments of the Court and ensure their execution within their national legal system.[10] There is no compliance monitoring body, no reporting obligation, no automatic referral to the ECOWAS Authority of Heads of State when a state fails to act. Compare this to the Council of Europe's Committee of Ministers process, which tracks compliance with European Court of Human Rights judgments, publishes leading case files for significant non-compliance situations, and can initiate infringement proceedings against states that persistently refuse to comply.[11] The ECOWAS system has none of these mechanisms.

From a rational-choice perspective, the cost of non-compliance with an ECOWAS human rights judgment was low. Reputational damage was real but diffuse. Economic sanctions were not available. Regional diplomatic pressure was mild. Against these costs, the Nigerian government had to weigh the domestic political cost of amending legislation it had publicly defended, legislation its security agencies actively used, legislation whose amendment would be read by those agencies as a concession to regional judicial interference.

B. Section 24 Served a Political Function Its Drafters Intended to Preserve

It is tempting to read the compliance delay as bureaucratic inertia. That reading is too charitable. Section 24 was used, in documented cases, to arrest people who criticised state governors, federal ministers, and sitting presidents on social media.[12] The

[9]Protocol Relating to the Mechanism for Conflict Prevention, Management, Resolution, Peacekeeping and Security (Lome, 10 December 1999), Arts 22 to 45.

[10]Supplementary Protocol A/SP.1/01/05 (n 6) Art 24.

[11]Council of Europe, Rules of the Committee of Ministers for the Supervision of the Execution of Judgments and Terms of Friendly Settlements (adopted 10 May 2006, amended 18 January 2017), Rules 9 to 11 (leading cases, infringement proceedings).

[12]Paradigm Initiative and Media Rights Agenda, 'Digital Rights in Nigeria: Annual Assessment 2019 to 2022' (Lagos 2022) 14 to 23, documenting prosecutions under Section 24 in which the alleged conduct consisted of social media criticism of public officials.

vagueness that the ECOWAS Court found incompatible with international human rights law was not a drafting error. It was the feature that made the provision useful.

Research on cybercrime legislation across Sub-Saharan Africa finds a consistent pattern: overbroad speech provisions recur across jurisdictions not because parliaments do not know how to draft narrower statutes, but because those who control the legislative calendar benefit from vague restrictions on online criticism.[13] The Nigerian Cybercrime Act was passed during a period of intensifying social media political discourse, just before the 2015 elections. Its speech provisions reflected anxieties about online mobilisation that were shared across the political establishment.

The mechanism of compliance in this context requires a political coalition capable of outweighing the incumbent interest in retaining the statute. In Nigeria, that coalition existed throughout the 2020 to 2024 period but was not sufficient on its own. What changed by 2024 was the intersection of the ECOWAS Court orders with two additional pressures: the FATF grey listing process, which imposed a financial cost on non-compliance with international governance standards,[14] and a shift in the political administration following the 2023 elections. The 2020 court order alone did not produce compliance. The 2020 order combined with a FATF financial incentive and a change of political administration did.

C. International Adjudication Is Too Slow for Digital Rights Violations

The case that produced the 2020 judgment was filed in 2018. From filing to judgment: approximately two years. If Nigeria had complied immediately, the cycle from legal challenge to remedy would have been two years. Arrests under Section 24 continued until at least 2023. The actual cycle was nine years and counting, since disputes about full compliance with the 2024 amendment remain unresolved.

During those nine years, hundreds of individuals were prosecuted under a provision that the ECOWAS Court had found incompatible with international human rights law. Each prosecution was, in retrospect, a rights violation. None received individual remedy. The 2020 order was declaratory and prospective; it said nothing about reparations for people already harmed.

What makes the cyber context particularly severe is the combination of speed and irreversibility. A tweet takes seconds. An arrest under Section 24 takes hours. A prosecution takes years. A criminal record is permanent, or nearly so. By the time an international court adjudicates the statute that enabled the prosecution, the harm has already been done and cannot be undone by a prospective order to amend legislation. The

[13]Jonathon Penney, 'Internet surveillance, regulation, and chilling effects online: A comparative case study' (2017) 6 Internet Policy Review 1, 15.

[14]FATF, 'Anti-money laundering and counter-terrorist financing measures: Nigeria Mutual Evaluation Report' (FATF 2021) Annex C. Nigeria exited the FATF grey list in June 2023.

enforcement problem in cyber rights is not just about whether states comply; it is about whether compliance, when it eventually comes, means anything for the people who were harmed while it was delayed.

IV. THREE PROPOSALS

None of the proposals below requires amending the ECOWAS Treaty. Each works within existing institutional authority. Taken together, they would change the compliance calculation enough to reduce the kind of four-year gap this article has examined.

A. A Cyber Rights Compliance Monitoring Committee

The ECOWAS Authority of Heads of State and Government can establish subsidiary institutions under Article 15 of the ECOWAS Treaty.[15] A dedicated compliance monitoring committee for cyber rights judgments, established by decision of the Authority rather than by Treaty amendment, could be charged with tracking state compliance with Community Court orders in the digital rights domain. Its membership should include representatives from the ECOWAS Commission, civil society organisations with documented expertise in digital rights monitoring, and the national human rights institutions of member states.

The key mechanism is specificity and publication. States subject to a Community Court order in the cyber domain would be required to submit implementation roadmaps within 90 days of judgment and progress reports at six-month intervals. Non-compliance reports would be published and transmitted to the ECOWAS Council of Ministers. The reputational cost of formal, published, institutionally documented non-compliance is not the same as the diffuse reputational cost of simply ignoring a court order.

B. Provisional Measures with Specific Implementation Guidance

The ECOWAS Court can issue provisional measures in urgent cases under Rule 31 of its Rules of Procedure.[16] Its use of this power has been limited, and the provisional measure orders it has issued have tended toward general formulations. In the cyber rights context, where rights violations accumulate at the speed of prosecution decisions, there is a strong argument for provisional measures that specify what compliance looks like in operational terms.

An order directing Nigeria to suspend enforcement of Section 24 pending final judgment, with guidance specifying that suspension means instructing the Nigerian Police Force and the Attorney General's office to issue internal guidance against new Section 24 prosecutions, is more actionable than a general suspension order. It reduces the space for administrative delay and good-faith disagreement about what the order requires.
The Inter-American Court of Human Rights has moved in this direction through detailed reparations orders that sometimes specify draft legislative text, institutional reform

[15]Revised Treaty of ECOWAS (Cotonou, 24 July 1993), Art 15(1).

[16]Community Court of Justice ECOWAS, Rules of Procedure (2005), Rule 31.

timelines, and monitoring conditions.[17] The ECOWAS Court could adapt this approach to the cyber context in collaboration with bodies that have the relevant technical expertise: the African Union's Digital Transformation Strategy team, national human rights institutions, and civil society organisations with legal drafting capacity.

C. Digital Trade Linkage

The ECOWAS Regional Approach to Digital Economy 2024 to 2034 commits member states to harmonising digital trade regulations, data protection frameworks, and e-commerce rules across the region.[18] States that maintain legislation found incompatible with the African Charter by the Community Court operate a digital regulatory environment that creates legal uncertainty for cross-border digital service providers. The relationship between that regulatory uncertainty and the digital trade framework has not been formalised.

Requiring states to certify compliance with outstanding Community Court human rights orders as a condition of access to ECOWAS digital economy harmonisation arrangements would create an economic incentive for cyber rights compliance that the current system lacks. This proposal is the most institutionally complex of the three and is offered as a direction of travel that the ECOWAS Commission could begin developing through technical working groups, without requiring immediate political commitment.

V. CONCLUSION

I grew up in Nigeria. I read about Section 24 arrests in newspaper coverage that was itself threatened with prosecution under the same provision. When the ECOWAS Court issued its 2020 order, people I knew who worked in press freedom organisations celebrated it. When nothing happened, they were not surprised. When the 2022 reinforcing order also produced nothing, they were still not surprised. There was a shared, accurate understanding that the court order and the political reality were operating on different planes.

What this article has tried to do is explain that shared understanding in structural terms. The ECOWAS Court was right. The Court's orders were legally sound. The compliance failure was not because the orders were wrong or ambiguous. It happened because the institutional architecture connecting court judgment to state behaviour was built without coercive mechanisms, the statute being challenged served political interests that outweighed regional reputational pressure, and the harm was accumulating faster than any conceivable adjudication timeline could address.

[17] Dinah Shelton, Remedies in International Human Rights Law (3rd edn, Oxford University Press 2015) 261 to 290.

[18] ECOWAS Commission, 'Regional Approach to Digital Economy 2024 to 2034' (Abuja 2024).

The 2024 amendment is a partial victory. The journalists arrested between 2020 and 2024 under a provision that an international court had found unlawful have no remedy. Their criminal records remain. The vague language that replaced the old Section 24 vague language still produces prosecutorial uncertainty. The compliance clock on the 2022 order runs.

Transnational law scholarship has spent decades documenting the gap between the formal authority of international legal norms and their practical effect in domestic systems. The ECOWAS/Nigeria cybercrime case is a specific, fully documented, real-time instance of that gap. It closes only when the cost of non-compliance, made specific and financial rather than general and reputational, exceeds the cost of reform. The proposals in Part IV are attempts to change that cost structure. They are worth trying.