



PRESENTED BY

NKOPANE TSHEHLA

Managing Director, Larocure Advisory

Gambling and Lottery Regulatory Advisor

PhD Candidate

25+ Years' Experience in Gambling Regulation and Operations

LAROCURE
ADVISORY

Opening: The case for regulatory modernisation

Bom dia

Programme Director, GRAF representatives, distinguished regulators, policymakers, industry leaders, fellow speakers, ladies and gentlemen.

It is a privilege to join you here at the Centro de Conferências Joaquim Chissano for a conversation that is increasingly important to the future of gambling regulation across our continent.

Mozambique's founding President, Samora Machel, once observed that "The state must be the first to be organised and fully committed to serving the interests of the people."

That organisational imperative is where our challenge begins today. I want to begin with the problem, in one sentence. A gambling transaction can occur in seconds, while the regulatory response can take weeks or months.

That gap is what I want to talk about today, through this simple proposition:

A regulator cannot effectively govern what it cannot independently see.

For much of its history, gambling regulation was designed around activities with a physical location. The regulator could identify the casino, betting shop, lottery outlet or gaming machine. It could inspect the premises, examine records, verify equipment and determine which activities were taking place within its jurisdiction.

That model was appropriate for the market it was designed to govern. But the market has changed.

Today, a single gambling transaction affecting an African jurisdiction may involve a player using a mobile phone, an operator licensed elsewhere, a platform hosted in another country, a payment intermediary working across several markets and data stored in a cloud environment over which the regulator has limited visibility.

The transaction may occur within seconds, while the regulatory response may take weeks or months. This creates a widening gap between market speed and regulatory speed.

The evidence already reflects this transition.

The wider digital context is equally important. According to the World Bank, 40 per cent of adults in Sub-Saharan Africa had a mobile-money account in 2024, compared with 27 per cent in 2021. The GSMA reports that almost two-thirds of Africans live within mobile-broadband coverage but do not yet use mobile internet. This combination of expanding financial access and uneven digital participation creates both opportunity and regulatory risk. The same mobile infrastructure that improves access to payments and services can also allow gambling products to reach consumers faster than traditional supervisory systems can respond.

In South Africa, regulated gambling turnover exceeded R1.5 trillion in the year ending March 2025. Total gross gambling revenue reached R74.5 billion. Betting accounted for almost 70 per cent of national GGR, while reported online betting alone generated R44.46 billion, approximately 60 per cent of the national total.

In Mozambique, government budget execution data shows casino tax receipts fell to MZN359.5 million in 2025, 7.3 per cent below the previous year and only 54 per cent of the budget target. The Ministry of Finance linked this performance partly to the growth of online gambling.

These figures tell us something important. Economic activity is moving from infrastructure the regulator can physically inspect to digital channels that may not be visible with the same clarity.

The central challenge is therefore no longer simply whether our laws recognise online gambling, mobile betting or new forms of digital wagering. The deeper question is whether our institutions possess the infrastructure to exercise meaningful authority over them.

Can the regulator independently determine what is happening in its market? Can it verify information an operator submits? Can it identify the companies, platforms and payment channels behind an unlawful gambling website? Can it follow an operator when it changes its domain name, application, payment account or corporate identity? Can it detect risk before consumer harm or revenue loss becomes widespread?

If the answer is no, the jurisdiction may have legal authority on paper but lack effective authority in practice.

The strategic question I want to address today is therefore this:

What regulatory and digital infrastructure do African jurisdictions require to govern gambling effectively in an increasingly digital and cross-border environment?

My argument is that this infrastructure must begin with a practical understanding of digital sovereignty.

What digital sovereignty means for an African gambling regulator

Digital sovereignty is sometimes presented as national ownership of technology, compulsory data localisation or withdrawal from international platforms. That is not what I mean.

African gambling ecosystems will continue to use global payment processors, cloud services, platform providers, game suppliers and specialist technology companies. The test of sovereignty is not whether every component is locally owned. It is whether the regulator retains control of the regulatory relationship.

Digital sovereignty means that a regulator can exercise effective authority over gambling activities affecting its jurisdiction, even when the operator, platform, payment system, supplier or data infrastructure is located elsewhere.

I understand this through four connected dimensions.

The first is **regulatory sovereignty**. A licence must establish more than permission to enter the market. It must create an enforceable, ongoing relationship between the regulator and the operator, including accountability for critical suppliers and outsourced services. Outsourcing a function cannot mean outsourcing regulatory responsibility.

The second is **data sovereignty**. The regulator must have timely, reliable and usable access to the information required to understand the market. That access cannot depend entirely on the operator's goodwill or interpretation. When the operator is the only party that can see the complete transaction, generate the report and explain what it means, oversight is not independent.

The third is **revenue sovereignty**. Digital gambling funds move through player wallets, banks, mobile-money services, payment gateways, aggregators and offshore entities. If gambling activity cannot be connected to financial flows, the regulator may be unable to verify GGR, assess tax obligations or understand the true scale of the market.

The fourth is **consumer sovereignty**. African players must remain protected regardless of where the operator or its technology is based. The regulator must be able to assess identity controls, player-fund arrangements, complaints, product fairness and responsible-gambling interventions.

These dimensions depend on one another. Data visibility enables regulatory authority. Regulatory authority enables revenue verification and consumer protection.

This leads to the principle that should guide modernisation:

Visibility precedes authority.

The law grants authority, but visibility enables that authority to be exercised in a digital market.

The regulatory infrastructure required

If digital sovereignty is the objective, regulatory infrastructure is the means of achieving it. This infrastructure is not a single platform or database. It is an integrated capability combining law, institutional arrangements, data standards, technology, skilled people and operational processes.

I propose seven connected capabilities.

1. A clear legal mandate for digital supervision

The first capability is legal, not technological.

A regulator needs an unambiguous mandate to obtain information, access relevant systems, inspect digital records, preserve evidence and require cooperation from operators and material suppliers.

A digital operator may use one company for its platform, another for payments, another for identity verification, another for cloud hosting and several others for games, odds, marketing and customer communication. The regulator may license the operator while remaining legally separated from much of the infrastructure through which the licensed activity occurs.

Modern frameworks should therefore identify critical suppliers, place accountability on the licensee and give the regulator appropriate access to information held across the operational chain.

2. A common regulatory data standard

Before discussing artificial intelligence or predictive monitoring, regulators must answer a more basic question: what information should every operator provide, in what format, at what frequency and according to which definitions?

If operators define active players, bonuses or GGR differently, the regulator cannot compare their reports reliably. If one reports daily, another monthly and another only when asked, the regulator lacks a coherent market view.

A national data standard should define essential information on registrations, deposits, withdrawals, wagers, winnings, bonuses, GGR, complaints, self-exclusions, suspicious activity, and material system incidents. It should also provide reliable identifiers for operators, beneficial owners, suppliers, brands, products and payment channels.

The objective is not to collect everything. Each data requirement must serve a lawful and clearly defined regulatory purpose.

3. Continuous visibility across licensed and unlicensed markets

Traditional supervision focuses mainly on licensed entities. Digital regulation must also observe what is being promoted, accessed and paid for within the jurisdiction.

This requires a capability to identify relevant websites, applications, social-media advertising and payment instructions, and to distinguish licensed activity from unauthorised activity. It also requires persistence. Blocking one domain is inadequate if the same operation returns under another domain, application or payment channel.

The regulator must shift from monitoring websites to understanding operators and the networks that support them.

4. Regulatory intelligence and risk assessment

Collecting data is not the same as understanding the market.

Regulatory intelligence connects operator submissions, transactions, complaints, inspections, payment patterns, advertising, licensing records and open digital information. It identifies relationships, anomalies and changes in risk.

A regulator should be able to build a persistent profile of an operator or unlicensed network. That profile should survive changes in branding, domains, or corporate structures and should direct limited regulatory resources to the matters requiring the most attention.

The cycle is simple:

Observe. Understand. Predict. Act. Learn.

The regulator observes the market, converts observations into intelligence, anticipates likely risks, acts through lawful powers and learns from the result.

5. Integration with the wider public regulatory system

A gambling regulator may identify unlawful activity but still depend on other institutions to address it. Payment disruption may require a bank or payment provider. Advertising intervention may require a communications authority or platform. Suspicious flows may require a financial-intelligence body. Cyber incidents may require specialist agencies.

A memorandum of understanding is useful, but it is insufficient on its own. Cooperation must become an operational procedure. Institutions should know what information may be shared, who receives it, what evidence is required, what action is available and how the outcome is reported back.

6. Skilled people and institutional knowledge

Digital regulation cannot be completely outsourced to a vendor.

Technology companies can provide important systems and specialist expertise, but the regulator must retain the ability to understand the system, question its conclusions and decide how regulatory powers are exercised.

This does not mean every regulator must employ a large team of software engineers. It means the institution needs sufficient capability in regulatory data, digital investigations, payments, cybersecurity, analytics and platform governance. When a technology contract ends, the regulator should not lose the knowledge required to supervise its own market.

7. Governance, accountability and public trust

The use of advanced monitoring and analytics creates responsibilities for the regulator itself.

Digital supervision must operate within clear legal limits, appropriate data-protection requirements, access controls, audit trails and human oversight. Where analytics or automated tools contribute to a decision, the regulator should understand the basis of that conclusion.

Digital sovereignty cannot be built by weakening the rule of law. It must strengthen the regulator's capability while preserving fairness, accountability and public trust.

How the architecture operates in practice

Consider a practical example.

Consumers begin receiving social-media advertisements for an unlicensed mobile gambling platform. A reactive regulator may wait for a complaint, investigate the website, issue a warning and request that access to the domain be restricted.

A modern system would go further.

The monitoring capability would identify the advertisement, website and application. The intelligence function would compare their digital characteristics with existing profiles. It might discover that the brand uses the same infrastructure, payment instructions or support channels as an operator investigated elsewhere.

The regulator could identify the financial and technological entities enabling the activity. Structured alerts could be sent to payment, telecommunications, financial-intelligence and advertising authorities. Evidence would be preserved according to an agreed procedure. If the operator moved to another domain, application or payment account, its persistent risk profile would allow the regulator to recognise it.

Where lawful and appropriate, that intelligence could also be shared with other African regulators.

In this model, regulation does not end when a website disappears. It continues until the regulator understands the operator, the supporting network and the risk presented to the market.

Uganda and Kenya demonstrate how parts of this architecture can operate.

Uganda reports that industry turnover increased from UGX500 billion in FY2021/22 to UGX8 trillion in FY2024/25. During the broader reform period, annual gaming revenue increased from UGX50.6 billion to UGX323 billion. The regulator links this progress to formalisation measures and the introduction of its National Central Electronic Monitoring System, which supports real-time oversight.

Kenya integrated betting companies into the tax system, creating daily visibility of transaction data and improving remittance verification. In FY2024/25, excise tax on betting services reached KSh13.23 billion, and betting tax reached KSh5.70 billion, with both exceeding their targets.

Ghana provides a different illustration. The Gaming Commission's gross receipts increased from approximately GHS106.7 million in 2024 to GHS115.9 million in 2025, a growth of about 9 per cent. The aggregate figure, however, conceals an important shift. Casino-related receipts rose by approximately 31 per cent, from GHS46.7 million to GHS61.4 million, while sports-betting receipts declined by approximately 14 per cent, from GHS52.7 million to GHS45.4 million. The Commission attributes the casino performance largely to increased online casino operations.

This demonstrates why a regulator needs visibility at product and channel level. An overall increase may conceal substantial migration within the market. A regulator that sees only the total may know that revenue has grown without knowing which products are expanding, which channels are contracting or where new consumer risks are emerging.

Nigeria illustrates regulatory complexity. Within the Federal Capital Territory alone, the official register contains 7 lottery, 26 sports-betting, 20 casino and 31 interactive or mobile-gaming licence entries. Some companies appear in more than one category, so these are not 84 unique operators. They still show the number of licences, products, brands, and channels one jurisdiction must connect and supervise.

Tanzania adds a broader institutional perspective. Its Gaming Board reports collections of TZS260.21 billion over four years, almost twice the amount collected during the preceding period. It separately reports that the sector contributed TZS922.25 billion in taxes and supported more than 30,000 direct and indirect jobs. The distinction between the Board's collections and wider sector taxes matters, but both figures demonstrate why gambling information is relevant to fiscal planning and economic policy.

These examples do not prove that technology alone caused the revenue changes. Market growth, licensing, formalisation, tax policy and enforcement also matter. They do show that regulatory and

fiscal authorities gain meaningful capability when they can independently access and analyse timely data.

African cooperation and regulatory alignment

No African jurisdiction can achieve full digital sovereignty through national infrastructure alone.

An operator may be licensed in one country, accept players in another, advertise from a third and process payments through several others. A regulator acting alone may see only one part of the operation.

Cooperation should not weaken national sovereignty. It should strengthen each regulator's ability to exercise it.

This does not require identical gambling laws, licensing structures or tax rates. Our constitutional arrangements, market histories and policy priorities differ. What Africa needs is not uniformity but regulatory alignment.

I propose four practical starting points.

First, regulators should establish a common regulatory vocabulary. Shared definitions for operators, critical suppliers, beneficial owners, material incidents and suspicious activity would make exchanged information more useful without displacing national law.

Second, we need consistent identifiers for operators, owners, platforms and suppliers. A business may use different corporate entities and brands across markets. If every regulator records only the local trading name, the wider continental network may remain invisible.

Third, regulators need a standard cross-border alert. It should identify the entity, explain the risk, present the evidence, state the action already taken and clarify what information or response is requested. Information-sharing cannot depend solely on personal relationships between officials. It must be institutionalised, secure and lawful.

Fourth, jurisdictions should develop capability together. Regulators can share data standards, procurement lessons, training material and implementation experience. Joint development in digital evidence, payment tracing, cybersecurity and platform governance would reduce duplication and build a common professional language.

Over time, this could support a federated African regulatory intelligence capability. Federated does not mean transferring every country's data into one continental database. National regulators would retain control of their information and determine what may legally be shared. The system would allow participating regulators to identify common entities, exchange defined intelligence and coordinate risk alerts without surrendering decision-making authority.

Africa does not necessarily need a single regulator. It needs connected regulators.

GRAF can provide the institutional foundation for this work. A small group of participating jurisdictions could begin with a limited pilot: a minimum data dictionary, common operator and supplier identifiers, and a secure cross-border alert procedure.

The principle should be simple:

Information should move between African regulators at least as effectively as gambling activity moves between African markets.

Practical lessons from the Eastern Cape

My experience in the Eastern Cape, and in working with regulators, licensed operators and applicants across African markets, has reinforced several practical lessons.

The first is that modernisation begins with governance, not technology. Before procuring a system, the regulator must determine what it needs to see, why it needs that information, who will analyse it and what action should follow. Technology should support a defined regulatory operating model; it cannot create that model for the regulator.

The second lesson is that the regulatory perimeter extends beyond the applicant company and its physical premises.

Consider the assessment of a cloud-based bookmaker. The licence may be legally anchored in one province. At the same time, the platform is hosted elsewhere, employees work from different locations, payments move through national systems, and customers access the service by mobile phone.

A premises inspection remains relevant, but it cannot answer every regulatory question. The assessment must also examine the platform provider, cloud environment, payment architecture, cybersecurity controls, regulatory access to data, business-continuity arrangements and outsourced compliance functions.

The critical question is no longer only: where is the operator located?

It is also: **where does regulatory control lie?**

The third lesson is that periodic reports remain necessary but are insufficient for fast-moving risks—monthly and quarterly submissions support reconciliation and accountability. However, significant changes in deposits, withdrawals, complaints, system availability or responsible-gambling indicators may require attention before the next reporting date. The regulator needs timely indicators that reveal when closer scrutiny is justified.

The fourth lesson is that institutional capability must grow with the market. When regulated businesses understand their technology more deeply than the institution supervising them, a knowledge imbalance affects licensing, compliance and enforcement. Capacity development must therefore be a continuing institutional strategy, not occasional training.

The final lesson is that African models must reflect African conditions. Many of our markets are mobile-led and combine bank transfers, mobile money, digital wallets, vouchers, agents and sometimes informal channels. National regulators may operate alongside provincial, state or sector-specific authorities. We should learn from international systems, but we must design architecture that can operate within our own legal, financial and institutional realities.

For a regulator asking where to begin, I propose five stages.

The first is **diagnosis**: assess what the regulator can currently observe, which risks remain invisible and where the legal, institutional, skills and technology gaps lie.

The second is **foundation**: clarify legal powers, define essential regulatory data, establish reporting standards and set enforceable expectations for operators and critical suppliers.

The third is **controlled implementation**: begin with a defined area of risk, such as online operator reporting, advertising surveillance, player-fund monitoring or unlicensed-platform detection. A focused pilot can test data quality, legal authority and internal procedures before expansion.

The fourth is **integration**: connect licensing, compliance, enforcement, revenue assurance and consumer protection, and establish working links with payment, financial-intelligence, telecommunications and data-protection institutions.

The fifth is **cooperation**: exchange defined intelligence with trusted African counterparts through lawful mechanisms.

This pathway recognises that modernisation is an institutional transformation, not a single procurement exercise. Each stage should leave the regulator with stronger internal knowledge and greater control of its environment.

Conclusion and call to action

Distintos delegados,

Africa's gambling markets are not waiting for our regulatory systems to modernise.

If the market operates continuously while regulation remains periodic, the gap will widen. If operators can see more of the market than regulators, the information imbalance will deepen. If gambling crosses borders while regulatory intelligence remains isolated, unlawful operators will continue to exploit the spaces between our institutions.

The immediate task is practical.

Each jurisdiction should assess what it can currently see, identify what remains invisible and build the legal, data, institutional and human capabilities required to close that gap.

At the continental level, I propose that GRAF encourage four commitments over the next twelve months.

First, develop a minimum African regulatory data dictionary for digital gambling.

Second, agree on common identifiers for operators, beneficial owners, platforms and critical suppliers.

Third, pilot a standard cross-border alert for material licensing and enforcement risks.

Fourth, establish a working group through which participating regulators can assess digital-regulatory maturity and exchange implementation lessons.

These commitments do not require identical laws or a single continental regulator. They provide a practical foundation for compatible capabilities and trusted cooperation.

I will close with the proposition I opened with.

A regulator cannot effectively govern what it cannot independently see.

But when a regulator can observe its market, understand it and act on it, visibility becomes authority. Authority becomes sovereignty. And sovereignty becomes the foundation of public trust.

His Excellency President Daniel Chapo recently captured the essence of this modern challenge when he stated, **"there will be no digital State if technological islands persist—systems that do not communicate and databases that do not integrate."** By building connected regulatory infrastructure across our continent, we eliminate those technological islands, connect our regulators, and secure the digital sovereignty our nations require.

Obrigado por me ouvirem.