GVG speaks out on controversial "spy" tender

- insists system cannot be used to spy on citizens' private calls . . .
- but ensures effective regulatory protocols and revenue collection . . .

AMID the raging M500 million tender dispute over the Lesotho Communications Authority (LCA)'s Compliance Monitoring and Revenue Assurance (CMRA) system, widely criticised as a potential "spy" tool, the ***Lesotho Times*** (**LT**) sat down with Global Voice Group (GVG) Communications Manager, **Susana G. Hiernaux**, to discuss the company's operations, ethics and the concerns surrounding its technology.

The government is strongly opposed to former LCA Chief Executive Officer Mamarame Matela's 2020 decision to award the tender to GVG and has since escalated the case to the Court of Appeal to have the contract nullified.

GVG refutes allegations that the CMRA system enables mass surveillance, insisting it merely enhances regulatory compliance and revenue collection.

Below are excerpts:


SUSANA G. Hiernaux.

LT: Your website states that you work "exclusively for government institutions and regulatory bodies", which seems like a unique business model in the technology space. Why do you deliberately exclude other sectors, such as civil society organisations, human rights groups, and private entities and individuals from your client base? How do you ensure your work serves the interests of all citizens, and not just the governments of the day?

HIERNAUX: GVG works exclusively with governments and regulators because our solutions address compliance, taxation, and governance challenges that only regulators are mandated to oversee. Our systems are designed to help states capture revenue, ensure fair competition, and protect consumers. While we do not sell to civil society or private companies, the ultimate beneficiaries of our work are citizens — because better oversight ensures that more public resources are available for healthcare, education, and infrastructure.

Our exclusive focus on public institutions is what guarantees our independence. For over 25 years, we've worked with regulators, ministries, and agencies across diverse contexts, always avoiding conflicts of interest with the private sector.

By doing so, we preserve trust, strengthen institutions, and ensure our solutions serve citizens through transparency and accountability.

LT: How do you vet the "digital agenda" of a government client? How do you define a government's "point of view" in a context where, for example, the government's agenda may include suppressing political dissent, monitoring journalists, or tracking human rights activists? What safeguards do you put in place to ensure that your technology is not used to facilitate such activities?

HIERNAUX: When we say we see things from a government's point of view, we only mean that we understand their regulatory and fiscal mandate, not their political agenda. Before engaging, we carefully assess the project scope to ensure it is limited to compliance and regulatory oversight.

GVG's solutions do not enable governments to monitor private citizens, political activities, or journalists. Safeguards are built into our systems so that data is anonymized, aggregated, and relevant only for regulatory purposes.

Integrity is at the heart of our operations. We strictly adhere to the data privacy laws of every country in which we operate, and we reinforce this commitment through internationally recognized standards such as ISO 27001.

This certification ensures that our internal systems are designed to protect data confidentiality, integrity, and availability, and that we operate with the highest level of security and ethical responsibility.

In fact, in most of our projects, the national data protection authority is a key stakeholder within the working group. Their involvement ensures that privacy safeguards are embedded from the outset and that our solutions align with both local and global standards.

LT: There is growing evidence from human rights organisations and academic studies suggesting that many governments, particularly in Africa, are using technologies framed as "RegTech" and "GovTech" to build comprehensive surveillance infrastructures. These systems are often used for political control and regime survival under the guise of national security and economic stability. How does GVG ensure that its systems are not aiding human rights violations?

HIERNAUX: We understand the concerns raised by human rights organisations and academic studies regarding the potential misuse of RegTech and GovTech solutions. At GVG, we take these issues seriously and have built both our mission and operational model around the principles of integrity, transparency, and accountability.

Our contracts clearly define the intended purpose of each platform we deploy. We work exclusively with government institutions and regulatory bodies, and the vast majority of the projects we support in Africa are launched through public tenders and funded by reputable international entities such as the World Bank and the United Nations. These frameworks provide an additional layer of oversight and help ensure that technologies are used in alignment with the public interest and international standards.

Beyond implementation, we invest heavily in capacity building in every country where we operate. We train local teams not only in the technical operation of our systems but also in the ethical standards and guiding principles that underpin them. This approach empowers institutions to manage the platforms independently and responsibly, ensuring continuity and integrity long after our direct involvement has ended.

LT: Given the sensitive nature of your work, and the potential for misuse, what other measure of transparency do you offer? Do your contracts with governments include clauses that prohibit your technology from being used for surveillance that violates human rights? Do you publish any transparency reports or annual human rights impact assessment of your work in the countries where you operate? Does GVG have a responsibility to pull out of contracts with governments that abuse your technology for purposes other than what is explicitly stated in the contract?

HIERNAUX: At GVG we provide every possible safeguard to ensure our tools are used responsibly and ethically. If a system were ever misused to commit a crime — such as a human rights violation — that would fall under the jurisdiction of legal authorities which is beyond our control. What we can affirm with confidence is that, in over 25 years of global operations, GVG has never received a complaint of that nature, nor have we ever encountered any evidence suggesting that our solutions have been used for unlawful purposes after deployment.

LT: One of your core services is "revenue assurance". While this sounds like a purely financial service, critics argue that these systems, which monitor and analyse all telecommunications traffic, are in fact a form of mass surveillance. How would you respond to such criticism? How do your systems distinguish between legitimate revenue assurance and the collection of private communications data for surveillance purposes?

HIERNAUX: Revenue assurance is about ensuring governments collect the taxes and fees legally due from operators, not about monitoring private communications. Our systems focus only on transaction volumes, operator declarations, and financial flows —never the content of communications.

LT: Your company has a Mobile Money Monitoring (M3) platform. What data points does this platform collect, and how do you ensure that it is used exclusively for financial regulation and not for tracking the financial transactions of political opponents or civil society organisations?

HIERNAUX: For mobile money, our M3 platform tracks parameters such as transaction volumes, values, and settlement consistency. It does not give visibility into individual account holders' identities for political targeting. The objective is to fight fraud, money laundering, and to safeguard financial inclusion.

LT: As a "leading" provider in this space, what ethical obligations do you believe you have beyond your contractual agreements with governments? Does GVG have a formal ethical framework or a code of conduct that guides its operations and, if so, can you please share the key principles? How do you handle a situation where you discover one of your clients is misusing your technology for purposes that contravene international human rights norms?

HIERNAUX: GVG is committed to ethical deployment and responsible innovation. We remain vigilant and proactive in ensuring that our solutions support good governance. If concerns were ever raised about potential misuse, we would engage constructively with all parties involved to assess the situation and take appropriate action. Our goal is to support governments in building secure, transparent, and rights-respecting digital ecosystems, and we take that mission seriously.

LT: The Lesotho government itself has raised concerns that the GVG tender effectively turns the Lesotho Communications Authority (LCA) into a spy agency with intelligence-gathering capabilities. How do you respond to the specific claim that your system provides intelligence capabilities that go beyond revenue assurance?

HIERNAUX: GVG's system in Lesotho is a compliance monitoring and revenue assurance tool — not an intelligence or surveillance platform. Access is restricted to aggregated data relevant to regulatory oversight. Governments cannot use the system to listen to calls, read messages, or track individuals. Data security protocols and audit trails safeguard against unauthorised use.

LT: Your CMRA system provides real-time access to a vast array of telecom data. The Lesotho state has a well-documented history of snooping on and harassing journalists. What specific, auditable safeguards are in place to prevent the misuse of this data for political surveillance, and how can you guarantee that governments, especially in Lesotho and other countries with a history of repression, are not using your tools to target dissidents, journalists or human rights activists?

HIERNAUX: As we mentioned earlier, we apply globally accepted data protection practices, including techniques like pseudonymization and anonymization. These approaches enable us to generate meaningful insights from data while ensuring that individual identities remain protected. That means we don't get concrete personal information.

LT: It has been reported that GVG's contracts are subject to international arbitration, which can make it difficult for host governments to challenge them in local courts, as seen in Lesotho. Why is this clause a standard part of your contracts, and does it not give your company an unfair advantage?

HIERNAUX: We understand the concerns raised regarding international arbitration, and we welcome the opportunity to clarify our position. Far from offering any unfair advantage, international arbitration is chosen precisely because it ensures neutrality and equidistance between the parties involved. It is a widely accepted mechanism that provides a balanced and impartial framework for resolving disputes.

That said, it's important to emphasize that litigation is never our preferred path. At GVG, we view legal proceedings as a last resort. Our approach has always been rooted in dialogue, collaboration, and mutual understanding. We believe that most challenges can be resolved through open communication and a shared commitment to finding constructive solutions.

Just as innovation drives our technological development, flexibility is a core value in how we engage with our partners. We remain open to discussion and to exploring all available options, always with the goal of building sustainable and respectful relationships with the institutions that we serve.

LT: As a leader in the "reg-tech" industry, what is your vision for the future of government-provided technology, and how do you ensure that these systems — designed for a "digital transformation" — do not lead to a "digital repression"?

HIERNAUX: I like that we're ending with a question about the future, because it's precisely where the most urgent challenges and opportunities lie. Technology is transforming our daily lives at an unprecedented pace, and regulation is struggling to keep up. Historically, regulation has always followed innovation, but today the gap is widening. We're witnessing this in real time with artificial intelligence: even in highly developed countries, establishing a regulatory framework that protects users without stifling progress has become a major challenge.

This is exactly where regulatory technology (RegTech) plays a critical role. We're not just observers, we're at the centre of the storm. RegTech provides governments with the tools to respond quickly, transparently, and responsibly to technological change. At GVG, we see this moment as a turning point. Our mission is to support public institutions in building secure, inclusive, and sustainable digital ecosystems.

That means designing systems that are not only technically robust but also aligned with responsible practices. Just as digital transformation is inevitable, so is the need for smart regulation, and RegTech is the bridge between the two.