OKUMU KUBAI & CO. ADVOCATES

IMEI Registration and the right to Privacy:

What the High Court's Ruling means for every Kenyan

8th August 2025

Introduction

In a digital-first Kenya, your phone is more than just a gadget; it's your bank, your social hub, your ID, and even your wallet. So, when the government moves to collect and store information from your mobile device, you're right to ask: Is my privacy at risk?

This very question was at the heart of the decision by the High court in ***Katiba Institute v Communications Authority of Kenya & 2 others (Petition No. E647 of 2024).*** The court was invited to determine whether the mass registration of International Mobile Equipment Identity (IMEI) numbers under a regulatory framework violated Kenyans' constitutional right to privacy.

Background

On 24th October 2024, the Communications Authority of Kenya (CAK) issued a public notice mandating all mobile device importers, assemblers, and retailers to register their devices' IMEI numbers with the Kenya Revenue Authority (KRA) through a centralized digital portal. The policy extended beyond commercial entities and introduced additional compliance measures. Notably, passengers arriving in Kenya were required to declare the IMEI numbers of their devices as part of customs procedures. Furthermore, Mobile Network Operators (MNOs) were directed to restrict network access exclusively to devices listed on a government-approved whitelist, with devices not in compliance slated for grey-listing or eventual blacklisting.

The stated objective of these regulatory measures was to safeguard the integrity of Kenya's mobile device ecosystem, curtail the importation and distribution of counterfeit or untaxed devices, and enhance revenue collection

through improved tax compliance within the telecommunications supply chain. The measures, it was stated, were part of a broader government strategy to align digital infrastructure with regulatory and fiscal accountability.

The Legal Challenge

Petitioner's case

Katiba Institute filed a constitutional petition challenging the legality of the IMEI registration framework. They argued that it violated Article 31 of the Constitution (the right to privacy); breached the Data Protection Act, 2019 (DPA) by failing to conduct a Data Protection Impact Assessment (DPIA) as required under section 31 of the DPA; usurped Parliament's legislative role by imposing a policy framework without tabling it as a statutory instrument and lacked public participation and sufficient legal safeguards against mass surveillance.

The petitioner contended that the IMEI number, once tied to an individual's name, passport, and mobile usage, qualifies as personal data under Section 2 of the DPA and must be processed lawfully and transparently.

Respondents' position

The Communications Authority of Kenya (CAK) and the Kenya Revenue Authority (KRA), the respondents in that matter mounted a firm defense of the IMEI registration framework, arguing that it was a legitimate administrative measure grounded in their respective regulatory mandates. They contended that IMEI numbers are purely technical device identifiers and not inherently linked to any individual's personal information. As such, they argued, the numbers fell outside the scope of data protected by privacy laws.

Additionally, the respondents maintained that the primary objective of the framework was to enhance compliance with excise and customs laws, targeting tax evasion and the circulation of counterfeit mobile devices. Since the IMEI numbers were collected at the point of importation, assembly, or retail before the devices were sold to end users, the process did not, in their view, involve the processing of personal data within the meaning of the DPA.

The CAK and KRA also emphasized that the regulatory notices issued were administrative instruments, not legislative in character. Consequently, they argued that the notices did not require tabling before Parliament under the Statutory Instruments Act, nor were they subject to the same level of procedural scrutiny as formal regulations.

Finally, the respondents defended the use of a whitelist system as a necessary and proportionate measure to ensure that only compliant and type-approved devices are connected to Kenyan mobile networks. In their view, the whitelist, along with grey-listing and blacklisting mechanisms served consumer protection, market integrity, and revenue assurance goals and did not pose any real or imminent threat to constitutional rights.

The High Court's Findings

The judge, before whom the petition was heard found merit in the petition. He made several critical findings that underscore the importance of constitutional safeguards in regulatory processes involving personal data.

Firstly, the court held that IMEI numbers constitute personal data when linked to an individual's identity. Although an IMEI number in isolation may not reveal the identity of the user, its combination with customs declarations, SIM registration information, or telecom usage records renders it personally identifiable. As such, IMEI numbers fall within the scope of data protected under Article 31 of the Constitution and the DPA.

Secondly, the court found that the state had failed to conduct a Data Protection Impact Assessment (DPIA) as required under Section 31 of the DPA. A DPIA is mandatory where the data processing presents a high risk to the rights and freedoms of individuals. The absence of this assessment meant that the data collection and processing regime introduced by the notices lacked a crucial layer of accountability and risk mitigation, thereby rendering the notices legally defective.

Thirdly, the Court held that the notices were ultra vires and procedurally flawed. By imposing binding obligations on importers, manufacturers, network operators, and even individual consumers, the notices assumed the force of law. Consequently, they fell within the definition of statutory instruments, which by law must be tabled before Parliament pursuant to the Statutory Instruments Act. Their issuance without public participation also violated Article 10 of the Constitution, which mandates inclusivity and transparency in governance, and breached Section 4 of the Fair Administrative Action Act, which requires affected persons to be consulted before administrative actions are implemented.

Lastly, the court addressed the risks of surveillance and discriminatory outcomes inherent in the IMEI registration framework. It warned that the ability to tie IMEI numbers to specific individuals could facilitate tracking, profiling, and state-led monitoring of citizens' activities that undermine democratic rights and freedoms. Furthermore, the exclusion of non-whitelisted devices from mobile networks disproportionately impacts the poor and digitally marginalized, potentially entrenching digital exclusion in an increasingly connected society.

Implications for Stakeholders

For government agencies, the judgment affirms that administrative efficiency cannot trump constitutional requirements. Even when regulatory measures are grounded in legitimate public interest objectives such as enhancing tax compliance, eliminating counterfeit products, or safeguarding national revenue, those measures must still adhere to both procedural and substantive constitutional safeguards. The decision sends a clear message that the rule of law must guide every stage of policy formulation and implementation, particularly where fundamental rights are at stake.

For businesses, particularly those involved in the importation, assembly, distribution, and retail of mobile devices, the ruling signals a shift toward increased regulatory oversight on data handling practices. Companies must now integrate data protection compliance into their operational frameworks, especially in areas such as customs declarations, supply chain logistics, and regulatory reporting. The expectation going forward is that businesses will conduct robust due diligence to ensure their data processing activities align with the requirements of the DPA.

For individuals and civil society, the judgment serves as a powerful reaffirmation of digital rights. It empowers data subjects and advocacy groups to demand transparency, accountability, and constitutional fidelity from both public and private actors involved in digital governance. Importantly, the decision sets a progressive benchmark for evaluating the legality of emerging technologies such as device identity management systems and ensures that innovation proceeds within the framework of constitutional rights, particularly privacy, dignity, and equality.

Conclusion

The *Katiba Institute* judgment is a significant victory for privacy and constitutional governance. It confirms that regulatory goals, however well-meaning, must be pursued within the framework of legality and fundamental rights. As our digital infrastructure evolves, this case offers timely guidance on how to regulate without infringing on individual rights.

By: Eugene Khaika – *Legal Intern*

Michael Okumu – *Senior Partner*

8th August, 2025