

Kenya's Cybercrimes Law Faces Its *Broadest* Constitutional Test Yet

Nine petitioners, eighteen respondents, and eight interested parties collide over a single amendment clause — and a website-blocking power nobody voted on.

BY PATRICK MUCHANGI, FOUNDER & ADVOCATE — MUCHANGI PATRICK & CO. ADVOCATES

CASE DOCKET

COURT

High Court of Kenya, Constitutional & Human Rights Division — Nairobi

JUDGE

Hon. Justice P. M. Nyaundi

CITATION

[2026] KEHC 9453 (KLR)

JUDGMENT DATE

2 July 2026

CONSOLIDATED PETITIONS

E671, E673, E677, E698, E705 & E716 of 2025 — lead file E671

STATUTE UNDER FIRE

Computer Misuse and Cybercrimes (Amendment) Act, 2025

On 6 November 2025, the High Court folded six separate petitions — filed by, among others, the Law Society of Kenya, the Kenya Human Rights Commission, ICJ-Kenya, Article 19 East Africa, and MP Babu Owino — into one consolidated challenge. Before the merits were even argued, the court had already suspended the most contentious phrase in the amendment: the words **"is likely to cause them to commit suicide."** That conservatory order is the reason this case has been watched so closely since last year, and it's worth understanding exactly what is — and isn't — being fought over.

01 The Three Provisions on Trial

SECTION 27(1)(B) — THE "EMOTIONAL HARM" CLAUSE

Criminalises electronic communication that is "grossly offensive," causes "serious emotional distress," or is "likely to cause" the recipient to commit suicide. Petitioners say these are subjective, unmeasurable standards; a conviction carries up to **Kshs 20 million in fines or 10 years' imprisonment.**

SECTION 6(1)(JA) — NC4'S WEBSITE-BLOCKING POWER

Lets the National Computer and Cybercrimes Co-ordination Committee (NC4) restrict access to websites or apps linked to "unlawful activities," "religious extremism," or "cultism" — **without a prior court order.** This is the provision petitioners call administrative "prior restraint."

SECTION 6(1)(J) — CONTENT MORALITY CLAUSE

Criminalises "pornographic, immoral or sexually explicit content" online, which petitioners frame as unconstitutional moral paternalism reaching into private digital consumption.

02 Where the Two Sides Actually Disagree

Strip away the procedural noise and the fight comes down to two irreconcilable readings of the same words.

PETITIONERS ARGUE

- The law criminalises *speculative psychological outcomes*, not conduct — turning criminal law into a tool of intimidation.
- Blocking a website without judicial sign-off hands a court's job to an administrative committee, breaching separation of powers.
- The Bill touched county functions and needed Senate approval under Article 110(1) — it never got it.
- Public participation was inadequate before passage.
- Penalties are grossly disproportionate to a harm that is, by the law's own language, only "likely."

STATE RESPONDENTS ARGUE

- Section 27 was already tested and upheld in *BAKE v Attorney-General (2020)* — this fight is **res judicata** and belongs to a pending Court of Appeal case, not a fresh petition.
- Cyberspace is borderless and needs calibrated regulation to protect national security, dignity, and children.
- The statute targets conduct, with intent and causation as objective anchors — not opinion.
- Statutes carry a presumption of constitutionality that petitioners haven't rebutted with concrete evidence.
- Parliament followed proper procedure; claims of arbitrary enforcement are hypothetical.

WHAT MOST COVERAGE MISSED

The State's entire *res judicata* defence rests on treating the 2025 amendment as old news. But petitioners point out the 2020 *BAKE* case tested the **2018 wording** of Section 27 — the suicide clause, the NC4 blocking power, and the identity-verification dispute didn't exist yet. Courts generally can't be barred from reviewing a provision that wasn't even law the last time they looked. Whether Justice Nyaundi accepts that distinction is arguably the single most consequential threshold question in the entire case — more consequential, procedurally, than the vagueness arguments that dominate the headlines.

03 The Correction Nobody Reported

Here is the detail that separates a court filing from a headline. A central plank of the petitioners' privacy argument is that the amendment imposes **mandatory identity**

verification for social media users — a surveillance risk to whistleblowers and activists.

WHAT MOST COVERAGE MISSED

The Data Protection Commissioner, joined as the 4th Interested Party, says that provision does not exist. In sworn testimony from John Walubengo, the Commissioner states that a textual review of the *actual assented statute* reveals no such identity-verification requirement anywhere in it. What the Act does contain are narrower cybersecurity definitions — of "access," "identity theft," and "virtual account" — which is a materially different thing from compelling every user to verify who they are.

That doesn't kill the petitioners' broader privacy case, but it means one of their most-quoted claims may be arguing against a law that isn't actually on the books. It's the kind of factual correction that only surfaces when someone reads the interested-party affidavits rather than the press statement.

04 The Doctrines Doing the Real Work

Both sides reach for the same three constitutional tests, and how the court weighs them will decide the case far more than any single fact will:

- **Void for vagueness:** can an ordinary citizen tell, in advance, what "likely to cause suicide" actually forbids? Petitioners lean on *Geoffrey Andare v Attorney-General* and the American cases *Papachristou v Jacksonville* and *Grayned v Rockford* to argue no.
- **Prior restraint:** is blocking a site before any court examines it a "drastic interference," as Kenyan courts previously warned in the *Wanuri Kahiu* Film Classification Board case? Petitioners say NC4's power fits that description exactly.
- **Article 24 proportionality:** even a legitimate goal — protecting mental health, curbing harassment — has to be pursued by the least restrictive means available. Petitioners argue a blanket criminal statute with 10-year sentences fails that test; the state says the law is already narrowly tailored.

Interested parties widened the lens further than either side alone: the Kenya National Commission on Human Rights argued that suicide-related harm needs a **public health response, not criminalisation**, and cited an ECOWAS ruling and European Court of Human Rights precedent treating internet access itself as a derivative right that arbitrary shutdowns impermissibly chill.

| [Geoffrey Andare v AG & 2 Others \[2016\] eKLR](#)

| [National Assembly v Katiba Institute \[2023\] KECA 1174](#)

| [Wanuri Kahiu v KFCB \[2020\] KEHC 6500](#)

| [BAKE v AG & 3 Others \[2020\] KEHC 7924](#)

| [Senate v Speaker of National Assembly \[2025\] KESC 49](#)

| [Ahmet Yildirim v Turkey \(ECHR, 2012\)](#)

| [Amnesty Int'l Togo v Togolese Republic \(ECOWAS\)](#)

| [Grayned v City of Rockford, 408 U.S. 104 \(1972\)](#)

05 What the Petitioners Actually Want

Beyond striking down individual clauses, the consolidated petition asks the court to go further than most cybercrime challenges typically do:

- a) Declare NC4's website-blocking power (6(1)(ja)) and the morality clause (6(1)(j)) unconstitutional and void.
- b) Declare the impugned provisions vague, overbroad, and contrary to the principle of legality.
- c) Declare the Kshs 20 million / 10-year penalties manifestly excessive.
- d) Quash any blocking directives already issued under the Act.
- e) Find the Act void for lack of Senate involvement and inadequate public participation.
- f) Issue an order of mandamus compelling Parliament to bring the Act back in line with the Constitution.

WHERE THINGS STAND

This record captures the introduction, the parties' full pleadings, and their written and oral submissions — the argument, not yet the outcome. The suicide-clause wording remains suspended under the November 2025 conservatory order while the court weighs its decision. Anyone citing a "ruling" on the substantive questions at this stage is getting ahead of the record.

HOW THIS TOUCHES YOUR DATA PROTECTION EXPOSURE

Whichever way the court rules on Section 6(1)(ja) and the identity-verification question, the underlying compliance exposure for Kenyan businesses is already live: what data you collect, how you verify users, and what you're obliged to disclose if NC4 or the ODPC comes calling.

Muchangi Patrick & Co. Advocates advises boards, fintechs, and platforms on exactly this intersection — data protection compliance under Kenya's Data Protection Act, cybercrimes exposure, and how to respond if a regulator or law enforcement request lands on your desk. If this case affects how your business handles user data or content moderation, we can help you get ahead of it rather than react to it.

[Book a Consultation](#)

[Chat on WhatsApp](#)

[See Our Data Privacy Practice](#)

Source: Kenya Law — [2026] KEHC 9453 (KLR), Judgment of 2 July 2026
Public domain record, National Council for Law Reporting

For essential site functionality and to remember your preferences, we use a small number of cookies. With your consent, we also use cookies to understand how visitors use this site. See our [Cookie Notice](#).

Essential Only

Accept All