OPEN ACCESS

ARTICLE HISTORY
Received: 01-10-2026
Accepted: 20-11-2026
Published: 25-11-2026

Journal Access By QR

Journal homepage: https://ssarpublishers.com/ssarjahss
Abbreviated Key Title: SSAR J Arts Humanit Soc Sci
Volume 3, Issue 6, (Nov-Dec) 2026, Page 431-443 (Total PP.13)
E-mail: ssarpublishers@gmail.com

Digital Privacy Practices and Freedom of Expression in Kenya: A Communication Law Analysis of Data Protection Enforcement, Cybercrime Legislation and Internet Disruptions, 2019–2026

By
Author: Tonny Odhiambo Phd
Assistant Lecturer, Department of Communication, PhD (Business Management), MA (Communication Studies), Presbyterian University of East Africa, P.O. Box 968-00521, Nairobi, Kenya.

ABSTRACT: Digital communication in Kenya depends on the interaction of two constitutional rights, privacy under Article 31 and freedom of expression under Article 33, yet few studies assess how privacy practices and restrictions on expression have evolved together since the Data Protection Act of 2019. This study analyses how data protection enforcement, cybercrime legislation, internet disruptions and judicial review shaped digital privacy practices and freedom of expression in Kenya between 2019 and 2026. A doctrinal and secondary-data design combined analysis of constitutional provisions, statutes and judgments with regulator statistics, press reports and the Freedom on the Net index, and four propositions were assessed through pattern analysis. Complaints to the Office of the Data Protection Commissioner rose from 7,128 in March 2025 to 9,061 in January 2026, an increase of 27.1 percent, and compensation orders rose from 103 to 184, an increase of 78.6 percent, while digital lenders featured prominently among respondents. Kenya's Freedom on the Net score fell from 64 in 2024 to 58 in 2025, the largest decline among 72 countries assessed, after an internet disruption of about seven hours in June 2024 and repeated blocking of Telegram, before recovering to 59 in 2026. In July 2026 the High Court struck down two provisions of the Computer Misuse and Cybercrimes (Amendment) Act of 2025, while dozens of other provisions survived on grounds of res judicata. The findings indicate that privacy enforcement has expanded mainly against commercial data handlers, that expression is restricted mainly through infrastructure and criminal-law channels, and that courts have been the principal check on both.

KEYWORDS: Digital privacy, freedom of expression, data protection, communication law, internet shutdowns, cybercrime law, Kenya.
Abbreviations: CMCA, Computer Misuse and Cybercrimes Act, DPA, Data Protection Act, FOTN, Freedom on the Net, KCSE, Kenya Certificate of Secondary Education, KICA, Kenya Information and Communications Act, ODPC, Office of the Data Protection Commissioner.

INTRODUCTION

Background and Problem

Communication law governs who may say what, to whom and by what means, and who may collect, keep and use the information that communication generates. In digital environments these two concerns converge, because the same networks, platforms and devices that carry expression also record it. A person who posts, messages or searches leaves data that can be processed by companies, intercepted by state agencies or used to identify and intimidate speakers. The relationship between privacy and expression is therefore not simply one

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

of balance between competing rights; privacy protects the conditions under which people can form and share opinions without fear, while expression gives meaning to the autonomy that privacy secures (Emerson, 1963; Solove, 2006).

Kenya presents a revealing case. The Constitution of 2010 guarantees privacy in Article 31 and freedom of expression in Article 33, and it sets criteria for limiting any right in Article 24 (Republic of Kenya, 2010). The Data Protection Act of 2019 created a regulator and a rights-based regime modelled largely on European law (Otele, 2021; Republic of Kenya, 2019). At the same time, successive cybercrime laws, the blocking of platforms and the disruption of connectivity during protests have placed pressure on online expression (Freedom House, 2025; Global Voices, 2026). Freedom House recorded the largest decline in internet freedom among 72 countries in its 2025 assessment, driven by a nationwide disruption in June 2024, the blocking of Telegram and arrests of online activists (Freedom House, 2025; tech-ish, 2026). Yet during the same period, the regulator issued more determinations and compensation orders each year, and the courts suspended or struck down key provisions of the Computer Misuse and Cybercrimes (Amendment) Act of 2025 (Capital FM, 2026; The Standard, 2026).

The problem addressed is that privacy enforcement and restrictions on expression are usually analysed separately, by data protection specialists on one side and by media freedom and digital rights organisations on the other. Little research examines them together as a single system of communication regulation, or asks which institutions actually constrain each. This study treats the two as parts of one system and asks how digital privacy practices and freedom of expression have evolved in Kenya since 2019, which instruments and institutions drive each, and what the courts have done to restrain them.

1.2 Theoretical Framework

Four bodies of theory frame the analysis. First, privacy theory. The early account of privacy as a right to be let alone (Warren & Brandeis, 1890) has been extended by a taxonomy that identifies harms from information collection, processing, dissemination and invasion (Solove, 2006), and by the account of privacy as contextual integrity, which holds that information flows are appropriate when they conform to the norms of the context in which they arise (Nissenbaum, 2004). Privacy has also been defined as control over the circulation of information about oneself (Westin, 1967). These accounts suggest that digital privacy practices should be evaluated by the flows of information they permit and by the actors who control them.

Second, free expression theory. The classic defence of free expression rests on the search for truth (Mill, 1859), while a systems account treats expression as the foundation of self-fulfilment, participation in decision-making, the balance between stability and change, and the discovery of truth (Emerson, 1963). Both accounts imply that restrictions must be tested against the purposes that expression serves and not only against the interests of those who wish to limit it. Third, theories of surveillance and chilling effects explain the link between the two rights. Empirical studies show that awareness of government surveillance reduces the willingness to express minority opinions online and alters information-seeking behaviour (Penney, 2016; Stoycheff, 2016). Surveillance is also embedded in commercial data extraction, which concentrates information power in firms and states (Lyon, 2014; Zuboff, 2015).

Fourth, theories of digital repression and proportionality. Digital repression refers to the use of technology by states to monitor, restrict or punish citizens, including through surveillance, disinformation, censorship and shutdowns (Feldstein, 2021). The standard legal tool for judging restrictions is the proportionality test, which asks whether a limitation pursues a proper purpose, is rationally connected to it, uses the least restrictive effective means, and is balanced against the harm to the right (Barak, 2012). Kenya's Article 24 writes a version of this test into the Constitution, and Article 19(3) of the International Covenant on Civil and Political Rights requires restrictions on expression to be provided by law and necessary for a legitimate aim (Republic of Kenya, 2010; United Nations, 1966).

1.3 Legal Framework

Table 1 summarises the instruments. Article 31 of the Constitution protects privacy and specifically the privacy of communications, and Article 33 protects freedom of expression while excluding propaganda for war, incitement to violence, hate speech and advocacy of hatred (Republic of Kenya, 2010). The Data Protection Act implements Article

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

31 by setting principles of lawful processing, creating the Office of the Data Protection Commissioner (ODPC) and providing remedies, including compensation and administrative fines (Republic of Kenya, 2019). Its journalistic exemption in section 52 has been criticised as narrow and inadequately balanced against expression (ARTICLE 19, 2019; ARTICLE 19 Eastern Africa, 2024). The Computer Misuse and Cybercrimes Act of 2018 created offences, including cyber harassment, and powers to intercept communications (Republic of Kenya, 2018), and the High Court upheld most of it in 2020 (Bloggers Association of Kenya v Attorney General, 2020). Kenyan courts also held in 2020 that the national digital identity programme could proceed only with a proper data protection framework in place (Nubian Rights Forum v Attorney General, 2020). At the regional level, the African Union Convention on Cyber Security and Personal Data Protection of 2014 links data protection to cyber security (Abdulrauf & Fombad, 2016; African Union, 2014), and research on African data privacy laws documents wide variation in their design and enforcement (Makulilo, 2016).

Table 1. Constitutional and statutory instruments governing privacy and expression

Instrument	Key provision	Communication function
Constitution, Article 31	Privacy, including privacy of communications	Protects the confidentiality of messages and personal information
Constitution, Article 33	Expression, media and information; exclusions in 33(2)	Protects speech and journalism; limits incitement and hate
Constitution, Article 24	Criteria for limiting rights	Proportionality test for restrictions
Data Protection Act 2019	Principles; ODPC; section 52 journalistic exemption; remedies	Regulates processing by public and private actors
Computer Misuse and Cybercrimes Act 2018 and Amendment Act 2025	Offences; interception; section 6 blocking; section 27 cyber harassment	Criminalises online conduct; enables blocking and interception
International Covenant, Articles 17 and 19; Malabo Convention	Privacy; expression; data protection and cyber security	Supplies international and regional standards

Note. Compiled from the sources cited in Section 1.3.

1.4 Aim and Propositions

The aim of the study is to establish how data protection enforcement, cybercrime legislation, internet disruptions and judicial review have shaped digital privacy practices and freedom of expression in Kenya between 2019 and 2026. The analysis tests four propositions. P1: Privacy enforcement has expanded in volume and in remedies but is concentrated on commercial data handlers. P2: Restrictions on expression operate mainly through infrastructure and criminal-law channels and not through data protection channels. P3: Surveillance and the narrow journalistic exemption create tensions between privacy and expression that the legal framework has not resolved. P4: Courts have been the principal institutional check, but their rulings have been partial.

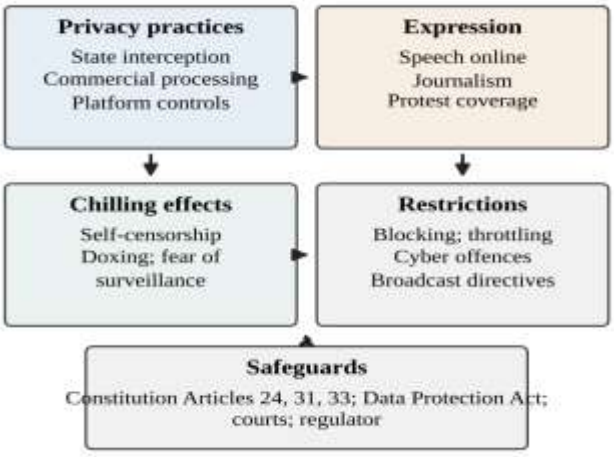

Figure 1. Conceptual framework linking privacy practices, expression, chilling effects, restrictions and safeguards

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

2. Materials and Methods

2.1 Research Design

The study uses a doctrinal analysis supplemented by secondary data analysis. Doctrinal legal research identifies, analyses and synthesises the content of legal rules, principles and authorities and applies them to a defined problem (Hutchinson & Duncan, 2012). Secondary data analysis adds indicators drawn from regulators and independent monitors, and document analysis supplies the procedure for selecting and interpreting the documents (Bowen, 2009). The unit of analysis is the legal measure or enforcement event, and the period is from the entry into force of the Data Protection Act in November 2019 to November 2026.

2.2 Data Sources and Selection

Table 2 lists the sources. Primary legal sources comprise the Constitution, statutes, international instruments and judgments. Regulator data comprise statements and award entries of the ODPC and press reports of its figures. Independent monitoring data comprise the Freedom on the Net assessments of Kenya and civil society reports. Press reports of court rulings were used for judgments that could not be retrieved directly, and they were checked against at least one other outlet. A figure or event entered the dataset only if it came from an official source or was reported consistently by two independent outlets. Conflicts were flagged and not resolved silently. For example, the ODPC reported 7,611 complaints received by 31 May 2025 (ODPC, 2025b), whereas a statement of March 2025 reported 7,128 (ODPC, 2025a) and a report of January 2026 reported 9,061 (Capital FM, 2026); the series is consistent in direction and the dates are shown.

Table 2. Secondary data sources and indicators

Source type	Examples	Indicators
Legal sources	Constitution; Data Protection Act; cybercrime statutes; judgments	Rights, duties, tests, rulings
Regulator statements	ODPC statements, award entry, guidance notes; press reports	Complaints, determinations, orders, penalties
Independent monitors	Freedom on the Net 2025 and 2026; civil society reports	Scores; documented disruptions; surveillance practices
Press reports	The Standard, The Star, Citizen Digital, Capital FM, Business Daily	Court rulings; timeline of events

Note. Full citations appear in the reference list.

2.3 Analytical Procedure

Three analytical steps were used. First, each restriction on expression was assessed against the Article 24 criteria and the proportionality test, using the reasoning and outcome of the courts where available. Article 24(1) of the Constitution requires that a limitation be provided by law, be reasonable and justifiable in an open and democratic society, and take account of the nature of the right, the importance of the purpose, the nature and extent of the limitation, the need to ensure the enjoyment of rights by others, and the relation between the limitation and its purpose, including whether less restrictive means exist (Republic of Kenya, 2010). These criteria were operationalised as four questions: whether the measure had a published legal basis, whether its aim was legitimate, whether it was necessary, and whether its extent was proportionate. The assessment is the author's doctrinal judgment, and it is presented as such. Second, enforcement indicators were computed from the regulator series: relative change between observations, the number of determinations per 100 complaints, and the number of compensation orders per 100 determinations. Third, the four propositions were assessed by comparing the predicted pattern with the pattern in the evidence. Relative change is computed as $(X_T - X_0)$ divided by X_0, multiplied by 100, where X_0 and X_T are the first and last observations. Because the series contain two or three observations and the data are aggregate counts, no inferential statistics were computed. Figures were produced with Python 3 and matplotlib. All data are public, and no human participants were involved.

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

2.4 Strengths and Limitations of the Method

The doctrinal approach allows direct engagement with the legal texts and the courts' reasoning, and the use of regulator and monitor data provides external indicators of practice. The limitations are that the enforcement series have few observations and different definitions across sources, that press reports were used for some rulings, that the index scores measure perceived conditions and not individual experiences, and that the analysis does not observe private data processing or covert state surveillance directly. The findings should therefore be read as a structured assessment of the legal and enforcement record and not as proof of causal effects.

3. Results and Discussion

3.1 Privacy Enforcement: Expansion and Concentration

The ODPC series shows steady expansion. Complaints received rose from 7,128 on 18 March 2025 to 9,061 in January 2026, an increase of 27.1 percent, and determinations rose from 215 to 357, an increase of 66.0 percent (Capital FM, 2026; ODPC, 2025a). Compensation orders rose from 103 to 184 (78.6 percent), alternative dispute resolutions from 39 to 84 (115.4 percent), and penalties from ten entities to 20 penalty notices (Table 3 and Figure 2). The intake of complaints has been steady at roughly 185 to 200 a month: 483 complaints arrived in the 74 days between 18 March and 31 May 2025, about 199 a month, and 1,450 arrived between 31 May 2025 and late January 2026, about 184 a month (Capital FM, 2026; ODPC, 2025a; ODPC, 2025b). The ODPC also reported that 7,497 of 7,611 complaints received by 31 May 2025 had been resolved, a resolution rate of 98.5 percent (ODPC, 2025b), although resolution includes dismissals, withdrawals and mediated outcomes and so is a looser measure than determinations.

Table 3. Data protection enforcement indicators

Indicator	Mar 2025	Jan 2026	Change
Complaints received	7,128	9,061	+27.1%
Determinations	215	357	+66.0%
Alternative dispute resolutions	39	84	+115.4%
Compensation orders	103	184	+78.6%
Penalties (entities; notices)	10	20	+100.0%
Determinations per 100 complaints	3.0	3.9	+0.9
Compensation orders per 100 determinations	47.9	51.5	+3.6

Note. Sources: ODPC (2025a); Capital FM (2026). The penalty figures count entities in March 2025 and penalty notices in January 2026 and are not strictly comparable.

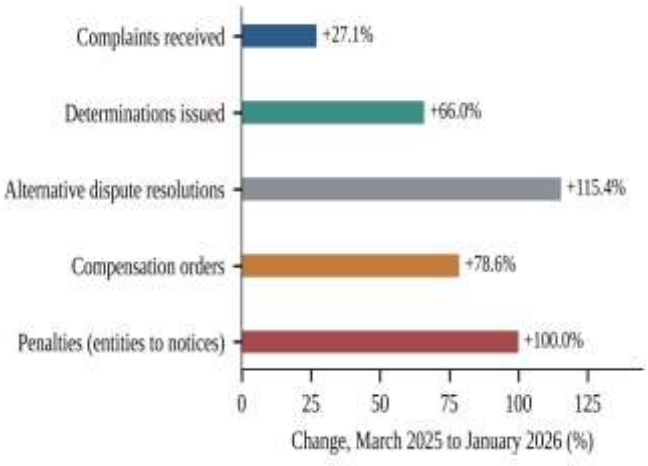

Figure 2. Change in enforcement indicators, March 2025 to January 2026

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

Data: ODPC (2025a); Capital FM (2026).

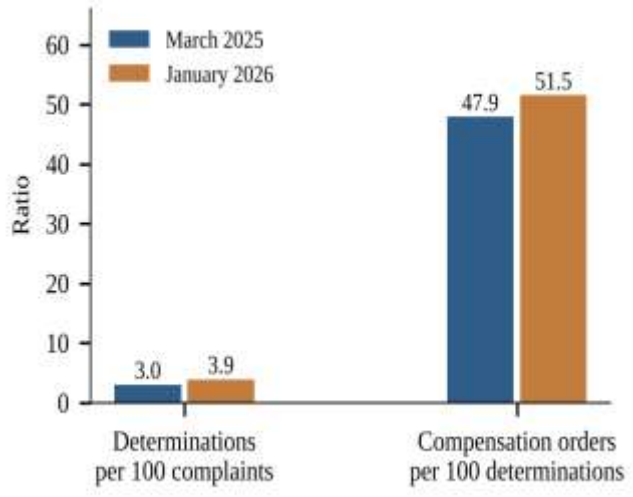

Figure 3. Enforcement conversion ratios

Data: Calculated from Table 3.

Two features of the series stand out. The first is the low conversion of complaints into formal determinations: only 3.0 determinations were issued per 100 complaints in March 2025 and 3.9 in January 2026. Most complaints are therefore closed through other routes, which may be efficient for the complainant but leave little formal precedent. The second is that remedies have become more individual: compensation orders per 100 determinations rose from 47.9 to 51.5, so that about half of formal decisions carry a payment to the data subject, which is consistent with the rights-based design of the Act (Republic of Kenya, 2019). The scale of the regime is also growing, with more than 15,000 entities reported as registered with the ODPC in 2026 (The Kenya Times, 2026). The concentration of enforcement on commercial actors, which is the substance of P1, is visible in the sectors that feature in determinations. Digital lenders feature prominently, with complaints about unsolicited messaging, consent violations and the disclosure of borrowers' contacts, and the press reports that tighter rules have turned the spotlight on lenders and on the doxing of defaulters (Business Daily, 2025). Reported penalties include a fine of KES 5 million on a smartphone manufacturer and an order against a financial technology company (Digital Policy Alert, 2024; Digital Policy Alert, 2025). By contrast, none of the reported determinations concerns interception or surveillance by state agencies. Allegations of police access to telecommunications data, including a media investigation of 2024 that the operator denied, have been pursued through civil society letters and journalism and not through ODPC adjudication (Freedom House, 2025; ICNL, n.d.). A study of surveillance regulation concludes that the Kenya Information and Communications Act and the National Intelligence Service Act lack safeguards for privacy and related rights (ICNL, n.d.). P1 is therefore supported: enforcement has expanded and is concentrated on commercial processing, while state surveillance remains largely outside the regulator's visible case law.

3.2 Restrictions on Expression: Infrastructure and Criminal Law

Table 4 sets out the main restrictions and the responses to them. Kenya imposed what civil society described as its first internet shutdown in November 2023, when Telegram was blocked during national examinations, and the pattern was repeated in the examination periods of 2023 and 2024 (Access Now, 2024; tech-ish, 2026). On 25 June 2024, during protests against the Finance Bill, connectivity was disrupted for about seven hours, and at least three networks blocked the web version of Telegram (Freedom House, 2025; Global Voices, 2026). In May 2025 the High Court barred the State from shutting down the internet in a case brought by civil society (The Star, 2025), yet Telegram was blocked again on 25 June 2025 and a directive ordered media houses to stop live broadcasts of the unrest (Global Voices, 2026). These measures acted on infrastructure and broadcast channels, and no published legal basis for them was identified in the sources reviewed, which raises doubt about their compatibility with the legality requirement of the Article 24 and Covenant tests, because a limitation must be prescribed by law and its reasons made accessible (Republic of Kenya, 2010; United Nations, 1966).

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

Table 4. Timeline of measures affecting online expression and judicial responses

Date	Event	Response
Nov 2023	Telegram blocked during national examinations	No court response until 2025
25 Jun 2024	About seven hours of disrupted connectivity during protests; Telegram web blocked on three networks	Civil society litigation; High Court order against shutdowns, May 2025
Nov 2024	Telegram blocked during KCSE	Documented by monitors
25 Jun 2025	Telegram blocked again; live broadcast directive	Contrary to court order
15 Oct 2025	Amendment Act assented	Suspension of key provisions, 22 Oct 2025
3 to 4 Nov 2025	Kerugoya court extends suspension of section 27; new petition filed	Petitions by civil society and legislator
2 Jul 2026	High Court strikes down sections 6(1)(jA) and 27(1)(b)	Other provisions survive res judicata

Note. Sources: Access Now (2024); Freedom House (2025); The Star (2025a, 2025b); Citizen Digital (2025); Bloggers Association of Kenya (2025); Global Voices (2026); The Standard (2026); Dawan Africa (2026).

The second channel is criminal law. The Computer Misuse and Cybercrimes (Amendment) Act of 2025, assented to on 15 October 2025, empowered the National Computer and Cybercrimes Coordination Committee to direct the blocking of websites and widened the offence of cyber harassment (Bloggers Association of Kenya, 2025; The Standard, 2025). The High Court suspended key provisions within a week (The Star, 2025b), the Kerugoya High Court extended orders against section 27 in November 2025 (Citizen Digital, 2025), and a civil society petition challenged sections 3 and 4 (Bloggers Association of Kenya, 2025). Civil society petitioners argued that the provisions threatened expression and media freedom (Bloggers Association of Kenya, 2025), which is the chilling effect that theory predicts (Penney, 2016; Stoycheff, 2016). On 2 July 2026 the High Court declared sections 6(1) (jA) and 27(1)(b) unconstitutional because they limited expression and media freedom without justification, while leaving dozens of other provisions, including sections 3, 5, 16, 17 and 22, in force because they had been upheld earlier in the Bloggers Association case and were res judicata (Bloggers Association of Kenya v Attorney General, 2020; Dawan Africa, 2026; The Standard, 2026). P2 is supported: restrictions on expression have operated through connectivity and platform blocking, broadcast directives and cyber offences, and not through the Data Protection Act.

3.3 Assessment Against Article 24

Table 5 applies the four questions to selected measures. The assessment is doctrinal and is based on the information available in the sources reviewed. Where a court has ruled, the ruling is reported; where it has not, the assessment indicates the doubts that the criteria raise. The pattern is clear. Measures that acted on infrastructure, such as platform blocking and connectivity disruptions, shared a lack of an identified legal basis and an indiscriminate reach, since they affected all users of a platform or network and not only those suspected of wrongdoing, so that less restrictive means, such as targeted action against specific content or users, were available (Barak, 2012). Measures embodied in statutes, namely sections 6(1)(jA) and 27(1)(b), had a legal basis but were struck down in July 2026 because their breadth and the absence of judicial oversight limited expression without adequate justification (The Standard, 2026). By contrast, the penalties and compensation orders of the data protection regime have a statutory basis, and they are generally consistent with the proportionality criteria, with the caveat that the journalistic exemption remains narrow (ARTICLE 19 Eastern Africa, 2024; Republic of Kenya, 2019).

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

Table 5. Assessment of selected measures against Article 24 criteria

Measure	Legal basis; aim	Necessity and proportionality	Outcome
Telegram blocking during examinations	None identified; examination security	Blocks a whole platform for all users	Doubtful
Connectivity disruption, 25 June 2024	None identified; no published aim	Nationwide effect on all users	Doubtful; later court order against shutdowns
Section 6(1)(jA), blocking power	Statute; control of unlawful content	Blocking without court approval	Struck down, 2 July 2026
Section 27(1)(b), cyber harassment	Statute; protection from online harm	Broad wording limiting expression	Struck down, 2 July 2026
Data protection penalties and orders	Statute; protection of privacy	Statutory limits; case-by-case decisions	Generally consistent

Note. Assessment by the author from the sources in Table 4 and the Data Protection Act.

3.4 Interaction of Privacy and Expression

The two rights interact in three ways. First, surveillance and data exposure suppress speech. A commentary on the period argues that platforms and technology firms were used as instruments of state control during protests (Global Voices, 2026), and a regional report documents how interception and unlawful surveillance create a chilling effect on human rights defenders, journalists and activists (ICNL, n.d.). The ODPC's own enforcement shows that doxing, the publication of personal information to shame or intimidate, is a recognised harm in digital lending (Business Daily, 2025), and the same technique is available against political speakers. These patterns illustrate the harms of exposure and aggregation identified in the taxonomy of privacy (Solove, 2006) and the logic of chilling effects (Penney, 2016).

Second, data protection law can constrain journalism. The Data Protection Act contains a journalistic exemption whose definition has been criticised as narrow (ARTICLE 19, 2019), and a study of 2024 recommends clarifying its scope, including which derogations it permits (ARTICLE 19 Eastern Africa, 2024). The ODPC responded with guidance notes on processing for journalistic purposes in 2025, which stress that Article 33 secures freedom of expression and the media, while Article 31 secures privacy (ODPC, 2025c). Third, the enforcement structure is asymmetrical. A regulator that can fine and order compensation against firms has no equivalent public record against state interception, and the legal basis for interception in the cybercrime statute is the subject of a separate petition before the Supreme Court (The Standard, 2026). P3 is supported in part: the tensions exist and are partly acknowledged by guidance, but the exemption remains contested and surveillance accountability is weak.

3.5 Independent Indicators and the Role of the Courts

Freedom House scored Kenya's internet freedom at 64 in 2024, 58 in 2025 and 59 in 2026, as Figure 4 shows (Freedom House, 2025; Freedom House, 2026; tech-ish, 2026). The 2025 decline of six points was the largest of any country assessed that year and was attributed mainly to the June 2024 shutdown, the blocking of Telegram and the arrest of online activists (Freedom House, 2025; tech-ish, 2026). Figure 5 shows the composition of the 2025 score: Kenya obtained 14 of 25 points for obstacles to access (56.0 percent), 24 of 35 for limits on content (68.6 percent) and 20 of 40 for violations of user rights (50.0 percent) (Freedom House, 2025). The weakest category is therefore the one most closely tied to the interplay of privacy and expression, namely the violation of user rights through arrests, surveillance and intimidation. A report on the same period concluded that Kenya's digital progress was overshadowed by surveillance and rights violations (Eastleigh Voice, 2025).

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

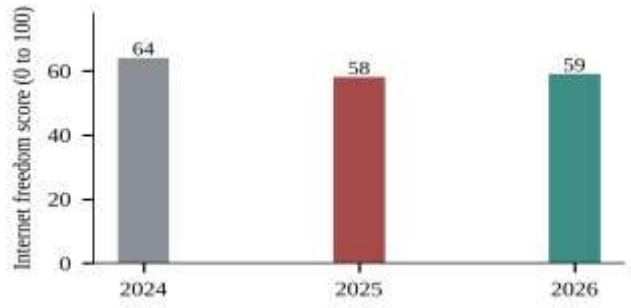

Figure 4. Kenya internet freedom score, 2024 to 2026
Data: Freedom House (2025, 2026); tech-ish (2026).

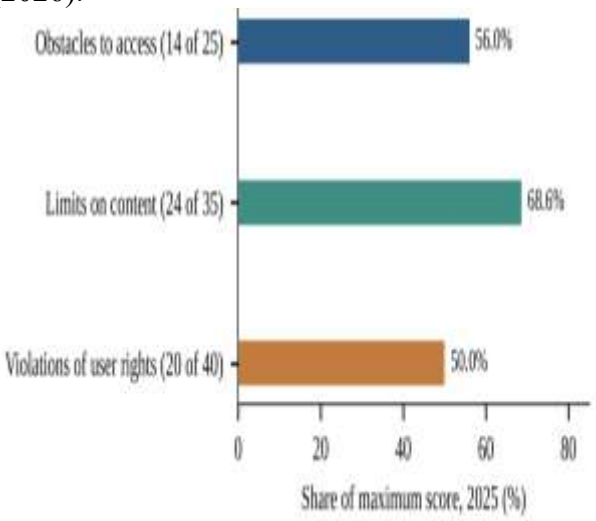

Figure 5. Components of Kenya's 2025 internet freedom score

Data: Freedom House (2025).
The courts emerge as the principal check, which is the substance of P4. They suspended provisions of the 2025 amendment within a week, barred shutdowns in May 2025, and struck down the two most contested provisions in July 2026 (The Standard, 2026; The Star, 2025; The Star, 2025b). However, the rulings have been partial. The judgment left most of the Act intact on res judicata grounds, the Telegram block of June 2025 occurred after the court order against shutdowns, and the challenge to interception powers in the 2018 Act awaits the Supreme Court (The Standard, 2026). Courts therefore function as a brake and not as a comprehensive guarantee. This outcome is consistent with the proportionality framework, in which courts examine the necessity of specific provisions without necessarily redesigning the regulatory architecture (Barak, 2012), and with the broader finding that states adapt their instruments when one is blocked, moving from broadcast to connectivity to platforms (Feldstein, 2021; Global Voices, 2026).

Table 6. Assessment of propositions

Proposition	Main evidence	Assessment
P1: enforcement concentrated on commercial actors	Complaints +27.1%; compensation orders +78.6%; digital lenders prominent; no reported state-surveillance determinations	Supported
P2: restrictions through infrastructure and criminal law	Telegram blocks; seven-hour disruption; broadcast directive; sections 6 and 27 of the Amendment Act	Supported
P3: unresolved tension between privacy and expression	Narrow section 52 exemption; guidance notes 2025; surveillance gaps; chilling effects	Supported in part
P4: courts as partial check	Suspension in a week; two provisions struck down; most provisions res judicata; Telegram block after court order	Supported

Note. Assessments express consistency with the evidence, not statistical significance.
A further consideration is the position of platforms and intermediaries. Blocking and throttling orders are executed by network operators and platforms, and the private companies that carry them out hold information about users and traffic that can also be requested by state agencies. This dual role, as carrier of speech and holder of data, places intermediaries at the junction of privacy and expression, and it explains why the same operators appear in discussions of both shutdowns and surveillance (Freedom House, 2025; Global Voices, 2026). From the standpoint of contextual integrity, data collected

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

to provide a communication service are shared under norms that do not include handing them over for purposes of political monitoring (Nissenbaum, 2004), and this is the standard by which intermediary disclosure should be judged. The regional framework reinforces the point by linking data protection with cyber security, but it leaves open how to protect expression when security arguments are used to justify restrictions (Abdulrauf & Fombad, 2016; African Union, 2014). The Kenyan record suggests that transparency obligations on operators, such as publishing the number and legal basis of government requests, would be a practical complement to judicial review.

3.6 Implications for Communication Law and Practice

Three implications follow. For regulators, the findings suggest that publishing sector-level determinations and the legal basis of each penalty would strengthen the precedent value of enforcement, and that the narrow conversion of complaints into determinations deserves explanation. For legislators, the experience of the 2025 Amendment Act shows that provisions empowering executive agencies to block content or criminalise broadly defined harms are vulnerable to constitutional challenge because they fail the necessity and proportionality criteria, and that clearer statutory standards and judicial authorisation would reduce litigation risk. For communicators, including journalists, civil society organisations and platforms, the findings imply that compliance with data protection duties and the protection of expression should be planned together: journalistic work that processes personal data benefits from the 2025 guidance, and organisations that rely on messaging platforms need contingency plans for blocking and throttling (Access Now, 2024; ODPC, 2025c).

3.7 Limitations and Further Research

The limitations are the short series and the reliance on press reports for some rulings and enforcement figures. The analysis cannot observe covert surveillance or private data processing, and index scores are perceptual measures. Future research should obtain ODPC determinations and test them for sector and outcome patterns, build a database of court rulings on expression and privacy, survey journalists and activists on self-censorship in Kenya, and compare Kenya with other East African states.

4. Conclusion

The study set out to establish how data protection enforcement, cybercrime legislation, internet disruptions and judicial review shaped digital privacy practices and freedom of expression in Kenya between 2019 and 2026. Privacy enforcement expanded, with complaints rising by 27.1 percent and compensation orders by 78.6 percent between March 2025 and January 2026, but it is concentrated on commercial data handlers and converts only a small share of complaints into formal determinations. Restrictions on expression operated mainly through connectivity disruptions, platform blocking and broadly drafted cyber offences, and contributed to a six-point fall in Kenya's internet freedom score in 2025. The courts were the main safeguard, suspending and then striking down the most contested provisions of the 2025 Amendment Act, although most provisions survived and shutdown-type measures recurred. The study contributes an integrated reading of privacy and expression as one system of communication regulation, and a transparent indicator set for tracking it. Further work should rely on primary enforcement and judicial records and on surveys of speakers.

Acknowledgment

No acknowledgement.

REFERENCES

1. Emerson, T. I. (1963). Toward a general theory of the First Amendment. Yale Law Journal, 72(5), 877–956. https://doi.org/10.2307/794655
2. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564. https://doi.org/10.2307/40041279
3. Republic of Kenya. (2010). Constitution of Kenya, 2010. National Council for Law Reporting.
4. Republic of Kenya. (2019). Data Protection Act, No. 24 of 2019 (Cap. 411C). National Council for Law Reporting. https://new.kenyalaw.org/akn/ke/act/2019/24/eng%402022-12-31/source.pdf
5. Otele, O. M. (2021). Kenya's data protection regime: Challenges and future prospects. Journal of African Politics, 1, 66–88.

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

6. Freedom House. (2025). Freedom on the Net 2025: Kenya. https://freedomhouse.org/country/kenya/freedom-net/2025
7. Global Voices. (2026, October 21). When Big Tech becomes a tool of state control in Kenya. https://globalvoices.org/2026/10/21/when-big-tech-becomes-a-tool-of-state-control-in-kenya/
8. tech-ish. (2026, April 2). Kenya internet freedom score: Cloudwards 2026. https://tech-ish.com/2026/04/02/kenya-internet-freedom-score-cloudwards-2026/
9. Capital FM. (2026, January). ODPC issues 184 compensation orders to data protection complainants. https://www.capitalfm.co.ke/business/2026/01/odpc-issues-184-compensation-orders-to-data-protection-complainants
10. The Standard. (2026). Blow to State as High Court nullifies key cybercrime Act sections. https://www.standardmedia.co.ke/business/crime-and-justice/article/2001551832/blow-to-state-as-high-court-nullifies-key-cybercrime-act-sections
11. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160
12. Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–158.
13. Westin, A. F. (1967). Privacy and freedom. Atheneum.
14. Mill, J. S. (1859). On liberty. John W. Parker and Son.
15. Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. Berkeley Technology Law Journal, 31(1), 117–182. https://doi.org/10.15779/Z38SS13
16. Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. Journalism & Mass Communication Quarterly, 93(2), 296–311. https://doi.org/10.1177/1077699016630255
17. Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 1(2), 1–13. https://doi.org/10.1177/2053951714541861
18. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5
19. Feldstein, S. (2021). The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press. https://doi.org/10.1093/oso/9780190057497.001.0001
20. Barak, A. (2012). Proportionality: Constitutional rights and their limitations. Cambridge University Press. https://doi.org/10.1017/CBO9781139179041
21. United Nations. (1966). International Covenant on Civil and Political Rights. General Assembly resolution 2200A (XXI).
22. ARTICLE 19. (2019). Kenya: Protect the data protection framework. https://article19.org/resources/kenya-protect-the-data-protection-framework
23. ARTICLE 19 Eastern Africa. (2024). Journalistic exemptions under Kenya's data protection framework [Policy brief]. https://www.article19.org/wp-content/uploads/2024/11/ODOV-journalistic-exemptions.pdf
24. Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act, No. 5 of 2018. National Council for Law Reporting.
25. Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR (High Court of Kenya).
26. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society of Kenya & another (Interested Parties) [2020] eKLR (High Court of Kenya).
27. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection. African Union.
28. Abdulrauf, L. A., & Fombad, C. M. (2016). The African Union's data protection convention 2014: A possible cause for celebration of human rights in Africa? Journal of Media Law, 8(1), 67–97. https://doi.org/10.1080/17577632.2016.1176702
29. Makulilo, A. B. (Ed.). (2016). African data privacy laws. Springer. https://doi.org/10.1007/978-3-319-47317-8

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

30. Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70
31. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027
32. Office of the Data Protection Commissioner. (2025b). Global Privacy Assembly awards entry: Office of the Data Protection Commissioner, Kenya, dispute resolution and enforcement. https://globalprivacyassembly.org/wp-content/uploads/2025/07/Global-Awards-Entry-Form-2025-Office-of-the-Data-Protection-Commissioner-Kenya-Dispute-Resolution-and-Enforcement.pdf
33. Office of the Data Protection Commissioner. (2025a, March 18). ODPC urges public to report personal data misuse cases to protect their rights. https://www.odpc.go.ke/odpc-urges-public-to-report-personal-data-misuse-cases-to-protect-their-rights/
34. The Kenya Times. (2026). 184 Kenyans to be compensated as ODPC cracks down on data breaches. https://thekenyatimes.com/latest-kenya-times-news/184-kenyans-to-be-compensated-as-odpc-cracks-down-on-data-breaches/
35. Business Daily. (2025). Spam messaging, doxing: Tighter data privacy rules turn spotlight on digital lenders, CBK. https://www.businessdailyafrica.com/bd/corporate/technology/spam-messaging-doxing-tighter-data-privacy-rules-turn-spotlight-on-digital-lenders-cbk-5282752
36. Digital Policy Alert. (2024). Office of the Data Protection Commissioner fined Oppo Kenya KES 5 million for breaches of data protection regulations. https://digitalpolicyalert.org/event/36296-office-of-the-data-protection-commissioner-fined-oppo-kenya-kes-5-million-for-breaches-of-data-protection-regulations
37. Digital Policy Alert. (2025). Data Protection Commissioner order on Ceres Tech for violations of data protection rights. https://digitalpolicyalert.org/change/13756-data-protection-commissioner-order-on-ceres-tech-for-violations-of-data-protection-rights
38. International Center for Not-for-Profit Law. (n.d.). Regulation of digital surveillance and the impact on civil society in Africa: Kenya digital surveillance report. https://www.icnl.org/wp-content/uploads/Kenya-Digital-Surveillance-report-final.pdf
39. Access Now. (2024, June 25). Authorities in Kenya must immediately restore internet access and keep it on throughout protests and unrest. https://www.scoop.co.nz/stories/WO2406/S00325.htm
40. The Star. (2025, May 16). Court blocks State from shutting down internet. https://www.the-star.co.ke/news/2025-05-16-court-blocks-state-from-shutting-down-internet
41. Bloggers Association of Kenya. (2025, November 4). BAKE, ICJ-Kenya and Article 19 challenge the enforcement of the Cybercrime Amendments Act 2025. https://blog.bake.co.ke/?p=10804
42. The Standard. (2025). Court upholds suspension of sections of cybercrime law. https://standardmedia.co.ke/business/amp/national/article/2001534239/court-upholds-suspension-of-sections-of-cybercrime-law
43. The Star. (2025b, October 22). Court suspends key sections of new cybercrime law. https://www.the-star.co.ke/news/2025-10-22-court-suspends-key-sections-of-new-cybercrime-law
44. Citizen Digital. (2025, November 3). Kerugoya High Court suspends implementation of section in new Computer Misuse law. https://citizen.digital/article/kerugoya-high-court-suspends-implementation-of-section-in-new-computer-misuse-law-n372405
45. Dawan Africa. (2026, July 2). High Court blocks government's powers to shutdown websites in Kenya. https://www.dawan.africa/news/high-court-blocks-governments-powers-to-shutdown-websites-in-kenya
46. Office of the Data Protection Commissioner. (2025c). Guidance notes: Processing for journalistic purpose. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-—-

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.

GUIDANCE-NOTES-for-Journalistic-Purpose.docx-.pdf

47. Freedom House. (2026). Freedom on the Net 2026: Kenya. https://freedomhouse.org/country/kenya/freedom-net/2026

48. Eastleigh Voice. (2025). How Kenya's digital progress is overshadowed by surveillance, rights violations: Report. https://eastleighvoice.co.ke/technology/368579/how-kenyas-digital-progress-is-overshadowed-by-surveillance-rights-violations-report

License: Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) Copyright: © 2026 The Author(s). Published by SSAR Publishers.