LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Togo

Country Report

PARADIGM INITIATIVE

LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Report produced and published by Paradigm Initiative
April 2026

374 Borno Way, Yaba, Lagos, Nigeria.
media@paradigmhq.org
www.paradigmhq.org

ISBN: 978-978-68-6631-4

Togo

By Emmanuel Elolo Agbenonwossi,
Fronts Numériques, Togo

Executive Summary

Togo's 2025 digital rights landscape sits at a crossroads between accelerated state modernisation and a sharp contraction of civic space. Since 2016, the country has invested in submarine cables, backbone networks, digital identity, data protection, and cybersecurity institutions, as well as in artificial intelligence strategies and global initiatives, such as the Giga for school connectivity by the International Telecommunications Union (ITU) and United Nations Educational, Scientific and Cultural Organization (UNESCO). This positioning has enabled it to become an ambitious digital reformer in West Africa. In 2025, this ambition was reinforced by the elevation of the Ministry of Public Service Efficiency and Digital Transformation, and the operationalisation of the data protection authority, new oversight for video surveillance and a more active national cyber defence through Cyber Defense Africa and CERT.tg.

At the same time, the year was marked by massive protests against the 2024 constitutional reform and socio-economic pressures, met by lethal force. There were

more than 100 arrests for online expression, disruptions[1] of major platforms, the suspension of France 24 and Radio France Internationale, and a climate of fear shaped by the unresolved Pegasus scandal[2] and the expanded use of cybercrime provisions to police digital speech.

Connectivity improved but remained unequal, with high costs and rural gaps only partially offset by initiatives such as the first community network in Atti Akakpé. People with disabilities, women and low-income groups continued to face structural barriers and digital literacy gaps. Access to information stayed constrained by the non-implementation of the 2016 law and weak proactive disclosure, limiting the ability of media, lawyers and civil society to scrutinise State action.

Against this backdrop, the report finds that Togo's overall compliance with the African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa declined compared to 2024, despite progress on data protection, digital inclusion and emerging technologies. The report recommends that the government prioritises legal reform of the cybercrime law, full operationalisation of the access to information framework, stronger guarantees for internet openness, independent oversight of surveillance and data systems, and targeted investments in inclusive connectivity and digital literacy. The report further highlights the need for media, civil society and the private sector to deepen their roles in monitoring rights, expanding digital skills and embedding privacy and accessibility in digital services.

1. Open Observatory of Network Interference (OONI). (2025). Togo: Network disruptions measurement data, June–July 2025., (Accessed 5 February 2026)https://ooni.org
2. Reporters Without Borders (RSF). (2024). Togo: Pegasus spyware used against journalists.https://rsf.org/en/togo, (Accessed 5 February 2026)

Introduction

Since 2016, Togo has pursued an ambitious digital transformation agenda aimed at strengthening state capacity, improving public service delivery and positioning the country as a digital reformer in West Africa. This period saw sustained investment in connectivity infrastructure, including submarine cables and fibre backbone expansion, alongside the rollout of digital public platforms. The adoption of a data protection law in 2019 and the creation of cybersecurity and digital regulatory institutions provided an initial legal and institutional framework for digital governance. The subsequent deployment of a biometric digital identity system marked a decisive shift, embedding digital technologies at the core of public administration and state authority.

Parallel to these reforms, persistent concerns emerged regarding civic space, freedom of expression and privacy in the digital sphere. The 2017 internet shutdown during political protests signalled early on that digital infrastructure could be constrained in moments of political tension, a practice later deemed incompatible with regional human rights standards by the ECOWAS Court[3]. In the years that followed, criminal law and cybercrime provisions were increasingly used to police online expression, including criticism of public officials and governance practices. Independent media and journalists operated under growing pressure, shaped by judicial harassment, economic vulnerability and surveillance risks, gradually narrowing the space for critical digital discourse.

These structural tensions culminated between 2024 and 2025, when constitutional reform heightened political uncertainty and digital platforms became central arenas for civic mobilisation, particularly among youth, artists, influencers and diaspora networks. Social media evolved into a primary space for political organisation and public debate, prompting a restrictive State response marked by arrests, platform disruptions and the

3. Amnesty International Togo, & 7 Ors v. The Togolese Republic, ECOWAS Community Court of Justice, Suit No. ECW/CCJ/APP/61/18, Judgment No. ECW/CCJ/JUD/09/20 (25 June 2020), (Accessed 5 February 2026)

suspension of international broadcasters. At the same time, the government continued advancing its digital agenda, including biometric identity expansion and AI policy development, underscoring a core paradox. While digital systems are promoted as tools for modernisation and efficiency, their deployment within fragile governance contexts has intensified concerns over accountability, concentration of power and the long term sustainability of rights based digital transformation.

Internet Access and Disruptions

Togo's connectivity profile in 2025 illustrates a country that has advanced considerably in building its digital infrastructure but still grapples with the deeper governance questions that accompany the expansion of the digital sphere. Over recent years, the arrival of new submarine cable capacity, the reinforcement of national fibre links, and the rise in mobile broadband adoption have helped strengthen the country's digital foundations. In major urban centres, connectivity is increasingly reliable and digital services are gaining prominence in administrative, commercial and educational settings. Yet these gains remain uneven. Rural communities continue to face lower quality coverage, higher effective costs in relation to household income, and persistent constraints linked to limited electrification. As a result, the distribution of digital opportunity in the country remains structurally imbalanced.

The events of mid-2025 demonstrated how quickly these technical gains can become vulnerable when political tensions rise. As youth-led demonstrations expanded across Lomé and other urban centres, several independent monitoring organisations recorded consistent disruptions affecting the platforms most widely used for communication and information sharing. Measurements conducted by the Open Observatory of Network Interference, corroborated by Internet Society monitoring tools, revealed repeated connection failures on WhatsApp, Facebook, Signal, Telegram, YouTube, and other high-traffic services beginning on June 26. These disturbances were documented across multiple operators, including Moov Africa, Togo Cellulaire, CanalBox and YAS Telecom, and their timing coincided with the most visible episodes of civic mobilisation in the country.

National observers confirmed the pattern. Internet Society Togo reported unusual

service degradation that disproportionately affected platforms central to civic communication. Journalists and civil society organisations described significant difficulty in uploading videos, verifying incidents on the ground, or coordinating support for families seeking information about detained or injured relatives. Human rights defenders noted that the disruptions delayed the documentation of allegations of ill treatment and complicated emergency coordination with legal counsellors and partner organisations outside Togo.

The broader economic and social ramifications extended well beyond the immediate political context. Small businesses that rely on messaging applications to maintain customer engagement experienced rapid declines in activity. Students preparing for examinations found that collaborative study channels and online learning tools were intermittently inaccessible. Drivers, delivery workers and other service providers who depend on platform-based communication saw their daily operations disrupted. These consequences underscore the extent to which digital connectivity has become essential to economic participation and social coordination and how even targeted restrictions can generate cascading effects across multiple sectors of society.

The interruptions also had implications for public trust in the digital environment. The restrictions echoed earlier concerns raised across the region about the use of network management tools during periods of political sensitivity. Domestic organisations, including the Internet Society Togo chapter and Association Togolaise des Consommateurs (a consumer rights association), called for the restoration of full access and emphasised the importance of maintaining open communication channels during times of national uncertainty. Regional actors referenced the 2020 judgment of the ECOWAS Court of Justice, which affirmed that restrictions on internet access must comply with principles of legality, necessity and proportionality. These interventions reflected a growing regional consensus that reliable connectivity is a matter of public interest and not merely a technical service.

Although the disruptions in 2025 did not take the form of a complete nationwide outage, their targeted nature raises important policy questions. They point to the need for transparent decision-making processes governing the management of digital networks and stronger institutional safeguards to ensure that measures affecting access do not inadvertently restrict fundamental freedoms. The experience of 2025 suggests that the credibility

of Togo's digital transformation will depend not only on the expansion of infrastructure but also on the establishment of governance practices that protect the resilience of the digital ecosystem in periods of political stress.

Access to Information

In 2025, access to information and freedom of expression in Togo continued to be constrained by longstanding structural deficiencies that have been documented by national and international observers over several years. While a legal framework governing access to public information formally exists, its implementation remains weak, limiting transparency and directly affecting the ability of journalists, civil society organisations and citizens to exercise freedom of expression on the basis of verified and authoritative information.

The legal basis for access to information is provided by the 2016 law on access to public information[4] and its 2017 implementing decree, which establishes procedures for submitting requests, designates information officers within public institutions, and provides for recourse through the Office of the Mediator of the Republic. However, assessments by civil society organisations and governance experts, including findings referenced in parallel reporting to international anti-corruption mechanisms, indicate that these provisions are rarely operational in practice. Requests for information are often unanswered, response timelines are not respected, and refusals are generally not formalised or justified in writing. As a result, the access to information framework remains largely ineffective as a practical tool for transparency and accountability.

This limited access to official information has direct implications for freedom of expression. Journalists interviewed for recent monitoring exercises have consistently reported difficulties obtaining official documents, budgetary data and regulatory decisions, particularly in areas related to public finance, procurement, security and governance. These con-

4. République togolaise. 2017. Décret n° 2017 104 PR du 10 août 2017 portant application de la loi sur l'accès à l'information publique. Gouvernement du Togo. https://communication.gouv.tg/wp-content/uploads/2020/11/decret-n%C2%B02017-104.pdf, (Accessed 5 February 2026)

straints weaken investigative journalism and reduce the capacity of media outlets to provide evidence based reporting. Civil society organisations engaged in public policy analysis similarly report[5] relying on informal networks rather than institutional disclosure mechanisms, which increases vulnerability to pressure and undermines the quality of public debate.

Developments during 2025 further highlighted the interdependence between access to information and freedom of expression. During civic mobilisations between May and July, public demand for timely and accurate information increased sharply, particularly regarding demonstrations, arrests, injuries and government responses[6]. At the same time, the space for independent information narrowed. On June 16 2025, the High Authority for Audiovisual and Communication suspended[7] the broadcasting of France 24 and Radio France Internationale for a period of three months, a decision reported by international media outlets and widely criticised by press freedom organisations. This measure significantly reduced access to international independent reporting at a moment of heightened political sensitivity.

Domestic media outlets attempted to compensate for this loss of external sources, but continued to face structural challenges documented by press freedom organisations, including limited access to official sources, financial fragility and increased risks of administrative or judicial pressure. Reports by international journalist protection bodies indicate that these conditions contributed to heightened self censorship and reduced on the ground coverage of sensitive events.

The digital information environment was also affected during this period. According to monitoring by regional media freedom organisations, disruptions to internet connectivity and online services were reported in late June 2025, coinciding with protest related events[8]. These dis-

5. UNCAC Coalition. 2023. Parallel report on Togo. United Nations Convention against Corruption Coalition. https://uncaccoalition.org/wp-content/uploads/FINAL_Parallel-Report-TOGO-UNCAC_EN.pdf, (Accessed 5 February 2026)
6. Amnesty International. 2025. Togo. Protesters tortured as authorities crack down on dissent. Amnesty International. https://www.amnesty.org/en/latest/news/2025/06/togo-protesters-tortured/ (Accessed 5 February 2026)
7. Reuters. 2025. Togo suspends RFI and France 24 for three months, communications authority says. Reuters. https://www.reuters.com/business/media-telecom/togo-suspends-rfi-france-24-three-months-communications-authority-says-2025-06-16/, (Accessed 5 February 2026)
8. Media Foundation for West Africa. 2025. Internet disruptions amid post protest repression in Togo. Media Foundation for West Africa. https://mfwa.org/country-highlights/togo-internet-disruptions-amid-post-protest-repression/, (Accessed 5 February 2026)

ruptions limited the ability of journalists and citizens to communicate, document events in real time and access independent sources of information. As a consequence, public discourse increasingly relied on fragmented and unverified information circulating through social media platforms rather than on transparent institutional communication.

Arbitrary arrests linked to the exercise of freedom of expression were documented by multiple credible sources throughout 2025[9]. International media reported approximately 80 arrests during protest related events in June alone. Human rights organisations documented a broader pattern extending beyond the immediate protest period, reporting that at least 133 young activists were arbitrarily arrested between June and October 2025 in connection with protest participation, online expression or public criticism of authorities[10]. In several cases, detainees were reportedly held without prompt access to legal counsel, raising concerns among legal practitioners regarding due process guarantees.

Several emblematic cases illustrate the broader pattern observed. In May 2025, a prominent musician was arrested following critical public statements and online publications[11]. His subsequent appearance in a video apology circulated on social media was described by media freedom organisations as indicative of coercion. In early June 2025, a journalist working for an international broadcaster was detained while covering demonstrations and reportedly forced by security forces to delete recorded footage, an incident documented by international journalist protection organisations[12]. These cases, combined with the suspension of international broadcasters, contributed to a climate of intimidation and had a chilling effect on journalistic activity and public expression.

9. Associated Press. 2025. Togo arrests dozens after protests over constitution change. Associated Press. https://apnews.com/article/e61f8334f1dc4483d446770b35aa9549, (Accessed 5 February 2026)
10. Front Line Defenders. 2025. Repression of Gen Z in Togo. 48 activists must be urgently released. Front Line Defenders. https://www.frontlinedefenders.org/en/statement-report/repression-gen-z-togo-48-activists-must-be-urgently-released, (Accessed 5 February 2026)
11. Media Foundation for West Africa. 2025. Arrested rapper reappears in viral apology video on social media. Media Foundation for West Africa. https://mfwa.org/country-highlights/togo-arrested-rapper-reappears-in-viral-apology-video-on-social-media/, (Accessed 5 February 2026)
12. Committee to Protect Journalists. 2025. Togo detains TV5 Monde journalist, forces deletion of protest videos. Committee to Protect Journalists. https://cpj.org/2025/06/togo-detains-tv5-monde-journalist-forces-deletion-of-protest-videos/(Accessed 5 February 2026)

The continued digitalisation of public administration did not offset these constraints. While online platforms expanded access to administrative services, independent assessments indicate that proactive disclosure of public information remained limited. Data on budget execution, infrastructure projects, regulatory decisions and policy implementation were not published systematically. As already observed in earlier research cycles, digital transformation improved administrative efficiency without strengthening transparency, public oversight or the right to information.

Overall, developments in 2025 confirmed and, in some respects, intensified concerns identified in previous reporting. The absence of an effective access to information regime, combined with restrictions on media freedom, digital disruptions and arrests linked to public expression, continued to limit access to verified information and weaken the conditions for free, informed and pluralistic public debate. In the absence of sustained institutional reforms and stronger protections for freedom of expression, administrative modernisation has not translated into greater transparency or increased public trust in state institutions.

Data Protection And Cybersecurity

Togo's data governance framework entered a more active phase in 2025 with the gradual operationalisation of the Instance de Protection des Données à Caractère Personnel[13]. The authority, established under the 2019 personal data protection law, began to transition beyond its foundational phase and assumed a more pronounced regulatory presence within the national digital ecosystem. Its activation came at a time when government services, financial institutions and private companies increasingly rely on the collection and processing of personal information. The biometric identity programme expanded its coverage, digital administrative services became more widely used, and a broader part of citizens' daily interactions with the state moved onto digital platforms. These de-

13. Togo First. (2025, April 1). Togo: National Data Protection Authority launches as Cyber Defence Africa strengthens cyber resilience. https://www.togofirst.com/en/itc/0104-16053-togo-national-data-protection-authority-launches (Accessed 5 February 2026)

velopments elevated the importance of an oversight institution capable of guiding responsible data management, clarifying compliance obligations and articulating the rights of individuals in relation to their personal information.

The authority's work in 2025 focused on issuing guidance to public and private operators, improving public understanding of data rights and clarifying the obligations that accompany the handling of personal information. This was particularly important in the context of expanding digital public services and centralising biometric identifiers. Many citizens expressed a growing expectation that data collected for public service delivery be handled transparently, securely and with clear limitations on secondary use. The authority's emergence offered an initial reference point for these expectations, although its limited resources and modest operational capacity underscored the scale of the challenge that lies ahead.

A significant regulatory development concerned the governance of video surveillance in public and semi-public spaces. The proliferation of cameras in commercial centres, residential compounds and public institutions had outpaced the existence of a formal oversight mechanism. In 2025, the data protection authority introduced a requirement that any installation of video surveillance systems in locations accessible to the public must undergo a formal notification and authorisation process. Operators must register surveillance systems, demonstrate that their purpose complies with national privacy standards and visibly display proof of authorisation. Recordings produced by systems that do not comply with these requirements may not be admissible in legal procedures. This measure signalled an effort to introduce order and accountability into an expanding surveillance ecosystem and to ensure that public security objectives do not erode the privacy rights of individuals.

While these institutional developments marked progress, they occurred within a cybersecurity environment that was becoming increasingly active and increasingly sophisticated. Cyber Defence Africa, established in 2019 through a public-private partnership, continued to serve as the national centre for cyber defence operations, functioning both as the national Security Operations Centre and as CERT.tg. Throughout 2025, CDA expanded its technical capacity, broadened its analytical functions and worked closely with public administrations, banks and service providers to detect intrusions and mitigate risks. Its public alerts on phishing at-

tacks, fraudulent payment schemes, data theft attempts, and vulnerabilities affecting corporate and government systems have become more frequent, reflecting the growing exposure of the country to cyber threats.

CERT.tg's activities played an important preventive role by helping organisations recognise emerging threats and by encouraging citizens to adopt basic digital hygiene practices. These interventions were particularly relevant given the parallel expansion of digital identity, digital financial services and electronic platforms for administrative procedures. As more users engage in digital transactions, the risk of identity theft, fraud and manipulation of personal or financial data increases.

The visibility of CERT.tg in 2025 helped address these vulnerabilities and contributed to a more informed public conversation about digital security.

Cyber Defence Africa also deepened its cooperation with regional and international partners. Through capacity-building exercises, joint analysis initiatives, and cooperation agreements with peer institutions, the organisation participated in efforts to strengthen Africa's collective cyber resilience. The cooperation agreement signed in 2025 with a southern African state illustrated this outward engagement and signalled Togo's intention to position itself as an emerging actor in African cybersecurity.

These institutional developments took place in a political and social environment that remains sensitive to issues of surveillance and digital monitoring. Past allegations involving intrusive technologies created an enduring perception of risk among journalists, civil society organisations and political actors. Although no confirmed cases emerged in 2025, this perception shaped how many individuals interacted with digital platforms and how they interpreted the growing presence of cybersecurity institutions.

The overlap between cyber defence mandates, national security interests and data governance responsibilities requires careful management to avoid reinforcing concerns about privacy and undue monitoring.

The developments observed in 2025 highlight both the consolidation and the structural tensions inherent in the construction of a contemporary data and cybersecurity governance architecture within a rapidly digitalising environment.

Beyond the existence of Law No. 2019 014, the operationalisation[14] of the Instance de Protection des Données à Caractère Personnel marked a decisive institutional shift, transforming a statutory framework into an active supervisory mechanism capable of issuing guidance, framing compliance obligations and serving as a reference point for the protection of private life and personal data processing.

The introduction in 2025 of a formal declaration and authorisation regime for video surveillance systems[15] further translated abstract rights into enforceable administrative procedures. By requiring prior notification, documented justification and visible proof of authorisation for surveillance devices installed in publicly accessible spaces, the authority embedded legality and proportionality tests into everyday security practices, thereby strengthening procedural safeguards for individuals.

Taken together, these elements position Togo with a structured legal base, an identifiable oversight authority[16], a defined regulatory mechanism for surveillance technologies and an operational cyber defence infrastructure capable of responding to systemic risks. This integration constitutes a foundational condition for sustaining digital transformation while anchoring it within a framework attentive to rights, security and institutional accountability.

Privacy And State Surveillance

State surveillance shaped digital life in Togo throughout 2025 in ways that were both visible and subtle, forming a dense layer of control around a political landscape already marked by tension. The country entered the year with an unresolved legacy from the Pegasus spyware scandal. In 2021, forensic analysis by Amnesty International's Security Lab and reporting by international media confirmed that the phones of the investigative journalist Ferdinand Ayité and other

14. CIO Mag. (2025, March 29). Togo: The Personal Data Protection Authority begins its mission. https://cio-mag.com/protection-des-donnees-personnelles-au-togo-lipdcp-entame-sa-mission/ (Accessed 5 February 2026)
15. Civic Medias. (2025, July 27). Togo: IPDCP launches official declaration process for video surveillance systems. https://civicmedias.info/cv/index.php/2025/07/27/togo-ipdcp-lancement-officiel-du-processus-de-declaration-des-dispositifs-de-videosurveillance/ (Accessed 5 February 2026)
16. The Guardian. (2025, July 10). One too many: Rapper's arrest sparks protests against Togo's ruling dynasty. https://www.theguardian.com/world/2025/jul/10/rapper-aamron-arrest-protests-togo-ruling-dynasty

Togolese journalists had been selected for potential infection with Pegasus, a sophisticated surveillance tool designed by the Israeli company NSO Group. The investigations provoked international concern, yet no public inquiry was held within the country. Ayité himself warned in an interview with Le Monde that the Togolese authorities had invested in listening systems and maintained privileged relations with Israeli networks composed of former intelligence operatives. These statements became an enduring reference point for many journalists and activists, shaping their understanding of digital vulnerability through 2025.

This history mattered because much of the country's political and social life has shifted to digital platforms. Young people, artists, journalists and civic actors increasingly relied on TikTok, Facebook, Instagram and WhatsApp to express their views, document grievances, and organise demonstrations. As concerns about the 2024 constitutional reform intensified, digital spaces became the primary arena for debate and mobilisation. When youth-led protests began in late May and gained momentum quickly throughout June, online expression assumed heightened political significance.

The state's response relied heavily on monitoring digital activity and using broad legal provisions from the 2018 cybercrime law. Human rights organisations reported that more than 100 individuals were arrested between June 5 and October 31 for conduct linked to online expression. Approximately 48 remained in detention at the end of the year. Testimonies from detainees and lawyers indicated that interrogations commonly focused on social media activity. People were confronted with screenshots of TikTok live sessions, Facebook comments or messages shared through WhatsApp groups and were asked to explain their links with specific accounts, organisers or diaspora figures. The pattern demonstrated that the authorities systematically used online traces as a central element in identifying participants and sympathisers in the mobilisation.

The arrest and treatment of the rapper Aamron brought these dynamics into sharp relief[17]. Aamron, who used TikTok and other platforms to critique political

17. République Togolaise. (2025, November 29). L'Internet Society déploie son premier réseau communautaire.

leaders, was detained at home, transferred to a psychiatric institution and later appeared in a video expressing apologies under unclear conditions. His case resonated deeply with young people because it illustrated how digital visibility could translate rapidly into personal vulnerability. For many, it confirmed that online expression no longer provided any degree of insulation from State intervention.

The experience of Traoré Leïla reinforced this perception. National media and activists reported that she had been arrested while breastfeeding her infant and remained in detention under security-related charges. Although details about her case are incomplete, she is widely described as a detainee arrested because of her perceived links to opposition networks. Her situation highlights the vulnerability of individuals who are suspected of being connected to political critics, regardless of whether this connection is made through digital interactions or social proximity.

These practices unfolded within a broader cybersecurity environment that continued to expand in capability as explained earlier with the creation of Cyber Defence Africa qnd the the national Security Operations Centre and CERT.tg. Throughout 2025, the institution monitored national networks in real time, issued alerts on phishing campaigns and cyber threats and strengthened its technical infrastructure. These capabilities are essential for protecting critical systems, but they also contribute to a public perception that the State has significant visibility into digital communications. The boundary between cybersecurity and surveillance is not always clear to users, particularly in a year marked by arrests and interrogations stemming from online activity.

The cumulative effect of these dynamics influenced patterns of online behaviour throughout 2025. Journalists exercised heightened caution when addressing politically sensitive subjects, often avoiding mainstream messaging platforms for substantive exchanges. Civil society actors redirected strategic discussions toward more discreet communication channels, mindful of the potential exposure associated with open digital spaces. Diaspora commentators, including exiled investigative journalist Ferdinand Ayité, who continued to analyse national political developments through regular live online programmes, were conscious that interactions with contacts inside the country could inadvertently place those individuals under scrutiny. Among younger users in particular, deliberate efforts to reduce digital visibility became more common,

reflecting an awareness that the monitoring of digital traces had become embedded within the broader security posture of the state.

What defined state surveillance in Togo in 2025 was not the presence of a single system but the convergence of legal authority, technical capacity and political will. Digital expression was closely watched, online traces were used to identify and detain critics, and past revelations about spyware continued to shape public expectations. In this environment, the boundary between the private and the public sphere narrowed considerably and the digital space, far from offering protection, became one of the primary vectors through which the state exerted its security presence.

Developments in ICT and Emerging Technologies

ICT development in Togo in 2025 was characterised by the consolidation of digital public infrastructure and a deliberate shift toward emerging technologies as instruments of state modernisation. The government continued to treat digital transformation as a national priority, with an emphasis on the role of data, connectivity and innovation in improving administrative efficiency and stimulating economic development.

The year saw notable advancement in national work on artificial intelligence (AI). Authorities intensified consultations on the country's future AI strategy, framing AI as a tool to strengthen public administration, support decision-making, and modernise priority sectors such as agriculture, health, and education. Research institutions, technical experts and government bodies engaged in working sessions aimed at defining the foundations of an AI ecosystem capable of relying on local data, skilled human capital and clear governance principles. A series of national meetings gave visibility to these debates and placed AI within a larger conversation about economic competitiveness and public service reform.

Innovation in the education sector continued through Togo's association with the Giga initiative, the global school-connectivity programme led by UNICEF and the ITU. Giga uses artificial intelligence, satellite mapping and infrastructure modelling to identify unconnected schools and design cost-effective expansion strategies. For Togo, participation in Giga is more

than a connectivity exercise. It provides a structured methodology for mapping national infrastructure gaps and encourages integration of schools into broader rural broadband planning. It also strengthens cooperation with international partners and supports a longer-term vision in which connectivity becomes a fundamental layer of educational development. As Giga has now mapped more than 1 million schools globally and developed financing models based on aggregated demand, the approach provides practical tools for countries, including Togo, to design realistic national school connectivity plans.

Digital public administration also progressed in 2025, with continued efforts to strengthen interoperability between government systems and expand access to online public services. Institutional actors worked to modernise internal information systems and reorganise administrative processes around digital platforms. Several government bodies began relying more heavily on integrated data systems to monitor service delivery and improve operational efficiency. These efforts were supported by international partners through programmes aimed at public-sector digital governance, infrastructure development and institutional capacity building.

Emerging technologies featured prominently in discussions about economic transformation and national competitiveness. Authorities explored how innovation in data analytics, geospatial mapping and automation could be applied in domains such as land management, transport, agriculture and climate adaptation. Pilot projects in these areas reflected a growing interest in using technology to address longstanding structural challenges. Regional organisations and development partners provided additional platforms for exchange on responsible innovation, digital inclusion and the development of human capital for the technology sector.

Togo also pursued regional cooperation in the field of cybersecurity and digital resilience, recognising that emerging technologies require stable and secure infrastructure. Government agencies engaged in collaborative agreements with other African States, focusing on information sharing, mutual support for incident response and joint capacity building. These partnerships highlighted a willingness to situate national advances within a broader regional framework and to enhance Africa's collective preparedness for the digital economy.

Digital Inclusion

Digital inclusion in Togo in 2025 reflected a combination of progress and persistent structural constraints. Urban connectivity continued to improve, yet access remained uneven across regions, income groups and social categories. Rural communities, in particular, faced weaker coverage, limited electrification, and high costs that constrained the regular use of digital services. These disparities shaped daily access to information, education and administrative services.

A notable development occurred in November 2025 with the inauguration of the country's first community network in Atti Akakpé, implemented by the Internet Society of Togo in partnership with local stakeholders. The initiative introduced a locally managed model of connectivity designed for areas where commercial operators have little presence. It offered an alternative path for rural access, combining infrastructure with community participation and the possibility of local digital training. The experience demonstrated that targeted community-driven solutions can complement national digital strategies, especially in regions where infrastructure gaps remain significant.
Affordability continued to influence who could benefit from digital services. The cost of devices and mobile data remained high relative to average income, limiting sustained connectivity for many households. Students, informal workers and low-income families often relied on shared devices or intermittent access, which restricted their ability to engage fully with online learning, financial platforms or government services that increasingly operated digitally.

People with disabilities encountered additional obstacles in accessing digital platforms. Public sector systems were not consistently designed with accessibility requirements in mind. Assistive technologies such as screen readers or captioning were not always compatible with government interfaces. Advocacy groups continued to call for stronger integration of universal design standards in both public and private digital services.

Gender also shaped digital access. Women, especially in rural areas, reported lower device ownership, less frequent internet use and reduced access to digital training opportunities. Social constraints, economic limitations and safety concerns affected their participation in online spaces. Periods of heightened political activity brought additional risks of online harassment and intimidation directed at

women who engaged publicly on digital platforms.

Children and young people occupied an increasingly central position in national discussions about digital opportunity.

The Universal Service Fund remained an important instrument for addressing connectivity gaps, but public visibility into its operations was limited. Without clear reporting on allocation and implementation, it was difficult to determine the extent to which the fund supported underserved communities, persons with disabilities or low-income users. Civil society continued to advocate for greater transparency to ensure that the fund played its intended role in reducing inequalities in digital access.

Digital literacy varied widely among population groups. Young people often learned informally through social networks, while older adults and rural residents faced greater challenges navigating online platforms or using digital tools required for public services. As administrative systems expanded online, the need for broad-based digital competence became more apparent across the country.

These intersecting factors shaped the digital inclusion landscape of 2025. Connectivity expanded, but real access depended on affordability, geography, skills and social circumstances. The emergence of community-driven models, such as the Atti Akakpé network[18], added a promising dimension to the national landscape, demonstrating how local initiatives can help address gaps that national infrastructure alone cannot immediately fill.

18. République Togolaise. https://www.republicoftogo.com/toutes-les-rubriques/high-tech/l-internet-society-deploie-son-premier-reseau-communautaire (Accessed 5 February 2026)

Conclusion

Togo's digital trajectory in 2025 revealed a country advancing rapidly in the construction of modern public infrastructure while confronting the limits of a governance environment under significant strain. Investments in digital identity, public service platforms, connectivity initiatives and early work on artificial intelligence confirmed the growing centrality of technology in national development. These reforms broadened the state's administrative capabilities and offered a foundation for long-term transformation.

At the same time, the year exposed the tensions that arise when technological progress unfolds alongside a deteriorating civic and political climate. The widespread use of the cybercrime law against online expression, the arrests that followed digital mobilisation, the disruptions affecting major platforms during public demonstrations and the constrained information environment all demonstrated how digital systems can become intertwined with political control. The lack of operational access to the information framework and limited transparency in several areas of public administration further complicated the relationship between digital governance and public trust.

Digital inclusion continued to depend heavily on geography, income, gender and skills. The inauguration of the Atti Akakpé community network illustrated the potential of community-driven solutions, while the Giga initiative offered a structured approach to school connectivity. Yet, many citizens still faced barriers that limited their ability to fully benefit from the country's digital transformation.

The developments of the year highlighted a central question for the future of digital governance in Togo. The country has built important technical foundations and signalled a clear ambition. Its next steps will depend on the degree to which these systems can operate within a framework that protects rights, encourages transparency and ensures that technology strengthens the relationship between citizens and the state rather than narrowing it.

Recommendations

The Government should:

- Operationalise the 2016 Access to Information law by issuing the implementing guidelines and creating a functional mechanism for receiving, processing and appealing information requests.
- Reform provisions of the 2018 cybercrime law to ensure that offences related to insult and false information cannot be used to criminalise legitimate online expression.
- Strengthen the independence and operational capacity of the national data protection authority, ensuring that its oversight applies to both public and private actors processing personal data.
- Establish a coherent and enforceable safeguards framework governing the deployment of biometric identification systems, video surveillance infrastructures, automated decision making tools and the interception or analysis of digital communications, including phone calls. Such a framework should define transparent rules on purpose limitation, data minimisation, storage duration, access controls and independent oversight, ensuring that security and administrative objectives are pursued within clearly bounded legal parameters and subject to effective accountability mechanisms.
- Guarantee uninterrupted access to the internet during periods of public tension and adopt clear procedures aligned with regional human rights standards for any restriction on digital services.
- Improve rural connectivity by publishing transparent plans for infrastructure expansion and ensuring targeted use of the Universal Service Fund.
- Integrate accessibility standards into all public digital platforms and ensure that services can be used by persons with disabilities without barriers.

The Media should:

- Expand reporting on digital governance, data protection, artificial intelligence and the societal implications of digital transformation.
- Strengthen investigative work on public finance, procurement and digital infrastructure while maintaining strong ethical and editorial standards.
- Engage in structured dialogue with State institutions to clarify procedures for accessing public information and overcoming administrative blockages.
- Provide digital security training for journalists and newsrooms to reduce risks during periods of political sensitivity.

Civil Society Organisations should:

- Continue monitoring digital rights and documenting restrictions on online expression through rigorous and evidence-based methods.
- Expand community-based digital literacy programmes, particularly in rural areas and among women, youth and marginalised groups.
- Build partnerships with academic and technical communities to analyse the impact of digital identity systems, surveillance technologies and emerging AI policies.
- Engage with regional and continental bodies to strengthen cross-border advocacy and align national debates with broader African governance frameworks.

The Pivate Sector should:

- Improve the affordability of connectivity and digital services by developing accessible pricing models, especially for low-income and rural users.
- Adopt robust internal policies on data protection and privacy, ensuring full compliance with national legislation and global standards.
- Integrate accessibility and inclusive design into all digital products and platforms.
- Collaborate with universities, training centres and incubators to support the development of digital skills relevant to emerging technologies such as artificial intelligence, cloud services and geospatial systems.

Togo's 2025 Score Index Compared to 2024

The 2025 Score Index reflects a slight decline compared to 2024, with the overall score decreasing from 29 to 28 out of 60. While the numerical change appears limited, the distribution of the indicators reveals a continued divergence between progress in institutional and infrastructural development and persistent pressures affecting fundamental digital rights. Compared to 2024, most downward movements relate to restrictions on online expression, the use of legal provisions to prosecute digital speech and ongoing concerns about transparency and surveillance.

In 2024, the country had already faced sustained concerns regarding prosecutions linked to online expression. The situation escalated significantly after the civic mobilisation of June and July 2025. According to the World Organisation Against Torture and partner organisations, at least 133 young Togolese activists were arbitrarily arrested from 5 June 2025 for hav-

ing “spoken out or gathered peacefully,” and 48 remained in detention at the time of their October 2025 statement. These figures illustrate the scale of the arrests following the mobilisation and reflect the increasingly fraught intersection between civic protest, digital expression and state security responses during the year.

Internet access also experienced a decline. In 2024, Togo maintained relatively stable connectivity despite regional outages. In 2025, however, targeted disruptions of platforms used for communication during the protests reduced the country’s alignment with the ACHPR principles on open and uninterrupted access. The change was not due to infrastructure weakness but rather to the use of access restrictions in a moment of political tension.

The indicators related to false news and sedition offences remained among the lowest in the index. Their impact became more visible in 2025 as legal provisions governing sedition and cybercrime were increasingly used in prosecutions related to online publications and social media commentary. In the previous year, these provisions were mainly identified as problematic in principle. During 2025 they became operational instruments in the prosecution of digital expression, particularly among young users active on platforms such as TikTok, Instagram and Facebook.

The score on access to information did not improve. The structural limitation identified in 2024 remained unchanged. The 2016 access to information law continued to lack effective implementation, and ministries did not systematically publish public data or reports. The suspension of two major international broadcasters during a period of political tension further constrained access to independent information.

Privacy and surveillance concerns also remained significant. Although no new spyware investigations were disclosed in 2025, the continued resonance of the Pegasus revelations, combined with the use of digital traces and social media monitoring in investigations linked to protest activity, reinforced public perceptions of vulnerability and maintained the indicator at the lowest level.

Not all developments were negative. Data protection legislation maintained a relatively strong score due to the operationalisation of the national data protection authority and the introduction of regulatory oversight for surveillance systems. This institutional development represents a

consolidation of the country's data governance architecture, even though enforcement capacity remains limited.

Some progress was also observed in digital inclusion. The inauguration of the first community network in Atti Akakpé demonstrated innovative approaches to rural connectivity, while the continuation of school connectivity efforts under the Giga initiative provided additional momentum for expanding access to digital infrastructure.

The indicator on emerging technologies also improved. While no national artificial intelligence strategy was formally published in 2025, consultations expanded and the institutional ecosystem around AI governance became more visible. The signature of the United Nations Convention against Cybercrime in October 2025 further signalled engagement with emerging international governance frameworks related to digital technologies.

Overall, the comparison with 2024 highlights a persistent structural tension in Togo's digital environment. Infrastructure development, cybersecurity capabilities and emerging technology governance continued to advance. At the same time, restrictions affecting freedom of expression, transparency and safeguards against surveillance remained significant. The slight decline in the overall score therefore reflects the growing weight of these civic and rights related concerns within the broader digital transformation trajectory.

The Score Index

Togo, 2025

1 = Totally non-compliant; 2 = Mildly compliant; 3 = Moderately compliant;
4 = Considerably compliant; 5 = Fully compliant

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Internet Access and Disruptions	P37			Infrastructure improved, but targeted platform disruptions during June and July protests reduced compliance with principles of open and uninterrupted access.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37			Despite improvements in connectivity infrastructure and initiatives such as the expansion of fibre networks, participation in the Giga programme and the emergence of community connectivity projects, Togo still lacks a comprehensive policy framework specifically aimed at ensuring universal, equitable, affordable and meaningful access to the internet. In addition, no publicly available reports or verified data exist on the collection, management or effective use of the Universal Service Fund, making it difficult to assess its contribution to expanding connectivity or supporting underserved populations.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
False News Criminalisation	P22(2)			Provisions of the cybercrime law continued to criminalise online expression and were used extensively in 2025 to justify arrests linked to commentary on public affairs.
Sedition Legislation	P22(2)			The cybercrime law retained broad offences that facilitated the prosecution of online criticism, including TikTok videos and social media commentary The cybercrime law retained broad offences that facilitated the prosecution of online criticism, including TikTok videos and social media commentary
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)			More than 100 individuals were arrested between June and October for online expression, and approximately 48 remained in detention at the year's end.
Data Protection Legislation.	P42			The data protection authority became operational in 2025 and introduced surveillance regulation, but enforcement capacity remained limited.
Online content Removal Without Process	P38 and P39(4)			Temporary restrictions on major digital platforms during protests were not accompanied by transparent or publicly communicated processes.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Invasion of Privacy of Communications	P41			Past Pegasus revelatons remained unresolved, and public perception of surveillance persisted, reinforced by the use of digital traces in investigations.
Failure to proactively Disclose Information	P29(3)			The 2016 access to information law remained inoperative, and ministries did not publish regular data or reports.
AI and Emerging Technologies Governance	P39(6)			National consultations on artificial intelligence expanded and policy foundations for AI governance began to take shape through multi stakeholder discussions and technical engagement with research institutions and public authorities. In October 2025, Togo also signed the United Nations Convention against Cybercrime, signalling increased engagement with emerging global governance frameworks related to digital technologies and cybersecurity. However, no national artificial intelligence strategy or formal regulatory framework was published during the year.
Adoption of specific Child Online Safety	P37(5)			Digital education expanded, but a comprehensive national framework for child online protection did not exist.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Digital Inclusion	P37(3)			Connectivity improved, and community networks emerged, yet rural, affordability and accessibility gaps remained substantial.
Total (out of 60):	2024: **29**	**2025** **28**		Togo made progress in infrastructure and institutional development but experienced significant regression in freedom of expression, access to information and protection from arbitrary monitoring.

374 Borno Way, Yaba 101245, Lagos, Nigeria.
www.paradigmhq.org