

LONDA 2025

Rapport sur les droits numériques et l'inclusion en Afrique

Togo

Rapport national



PARADIGM
INITIATIVE



LONDA 2025

Rapport sur les droits numériques et l'inclusion en Afrique

Rapport produit et publié par Paradigm Initiative
Avril 2026

Cette publication peut être reproduite à des fins non commerciales sous n'importe quelle forme, à condition que le crédit approprié soit accordé aux éditeurs et que l'œuvre soit présentée sans aucune déformation.

Copyright ©2026 Paradigm Initiative

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



Licence Creative Commons Attribution
- Pas d'Utilisation Commerciale - Pas de
Modification (CC BY-NC-ND)

ISBN: 978-978-68-6631-4



Togo

Par Emmanuel Elogo Agbenonwosi, Fronts Numériques, Togo

Résumé exécutif

Le paysage numérique du Togo en 2025 se situe à la croisée des chemins, entre une modernisation accélérée de l'État et une forte réduction de l'espace civique. Depuis 2016, le pays a investi dans des câbles sous-marins, des réseaux dorsaux, l'identité numérique, la protection des données et les institutions de cybersécurité, ainsi que dans des stratégies d'intelligence artificielle et des initiatives mondiales, telles que le projet Giga pour la connectivité scolaire de l'Union internationale des télécommunications (UIT) et de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO). Ce positionnement lui a permis de devenir un

acteur ambitieux de la réforme numérique en Afrique de l'Ouest. En 2025, cette ambition s'est concrétisée par la création du ministère de l'Efficacité du service public et de la Transformation numérique, l'opérationnalisation de l'autorité de protection des données, un nouveau contrôle de la vidéosurveillance et une cyberdéfense nationale plus active, notamment grâce à Cyber Defense Africa et CERT.tg.

Parallèlement, l'année a été marquée par des manifestations massives contre la réforme constitutionnelle de 2024 et les pressions socio-économiques, réprimées avec violence.

On a dénombré plus de 100 arrestations pour expression en ligne et troubles à l'ordre public¹ de grandes plateformes, la suspension de France 24 et de Radio France Internationale, et un climat de peur alimenté par le scandale Pegasus non résolu² et le recours accru aux dispositions relatives à la cybercriminalité pour contrôler la liberté d'expression numérique.

La connectivité s'est améliorée, mais reste inégale : les coûts élevés et les disparités en milieu rural ne sont que partiellement compensés par des initiatives telles que le premier réseau communautaire d'Atti Akakpé. Les personnes handicapées, les femmes et les groupes à faibles revenus continuent de se heurter à des obstacles structurels et à des lacunes en matière de compétences numériques. L'accès à l'information demeure limité par la non-application de la loi de 2016 et une faible transparence, ce qui restreint la capacité des médias, des juristes et de la société civile à contrôler l'action de l'État.

Dans ce contexte, le rapport constate que le respect par le Togo de la Déclaration de principes de la Commission africaine sur la liberté d'expression et l'accès à l'information en Afrique a globalement diminué par rapport à 2024, malgré les progrès réalisés en matière de protection des données, d'inclusion numérique et de technologies émergentes.

Le rapport recommande au gouvernement de donner la priorité à la réforme de la loi sur la cybercriminalité, à la pleine mise en œuvre du cadre d'accès à l'information, au renforcement des garanties d'ouverture d'Internet, à la supervision indépendante des systèmes de surveillance et de traitement des données, ainsi qu'à des investissements ciblés dans la connectivité inclusive et l'alphabétisation numérique. Le rapport souligne également la nécessité pour les médias, la société civile et le secteur privé de renforcer leur rôle dans la surveillance des droits, le développement des compétences numériques et l'intégration du respect de la vie privée et de l'accessibilité dans les services numériques.

1. Observatoire ouvert des interférences de réseau (OONI). (2025). Togo : Données de mesure des perturbations de réseau, juin-juillet 2025. (Consulté le 5 février 2026)<https://ooni.org>
2. Reporters sans frontières (RSF). (2024). Togo: Le logiciel espion Pegasus utilisé contre des journalistes.<https://rsf.org/en/togo> (Consulté le 5 février 2026)

Introduction

Depuis 2016, le Togo poursuit une ambitieuse politique de transformation numérique visant à renforcer les capacités de l'État, à améliorer la prestation des services publics et à positionner le pays comme un acteur majeur de la réforme numérique en Afrique de l'Ouest. Cette période a été marquée par des investissements soutenus dans les infrastructures de connectivité, notamment les câbles sous-marins et l'extension du réseau de fibre optique, ainsi que par le déploiement de plateformes publiques numériques. L'adoption d'une loi sur la protection des données en 2019 et la création d'institutions de cybersécurité et de régulation numérique ont fourni un cadre juridique et institutionnel initial pour la gouvernance numérique. Le déploiement ultérieur d'un système d'identité numérique biométrique a constitué un tournant décisif, plaçant les technologies numériques au cœur de l'administration publique et de l'autorité de l'État.

Parallèlement à ces réformes, des préoccupations persistantes ont émergé concernant l'espace civique, la liberté d'expression et le respect de la vie privée dans la sphère numérique. La coupure d'Internet en 2017 lors des manifestations politiques a rapidement montré que l'infrastructure numérique

pouvait être restreinte en période de tensions politiques, une pratique jugée ultérieurement incompatible avec les normes régionales relatives aux droits de l'homme par la Cour de justice de la CEDEAO.³ Dans les années qui suivirent, le droit pénal et les dispositions relatives à la cybercriminalité furent de plus en plus utilisés pour contrôler l'expression en ligne, notamment les critiques à l'encontre des responsables politiques et des pratiques de gouvernance. Les médias et les journalistes indépendants subirent une pression croissante, marquée par le harcèlement judiciaire, la précarité économique et les risques de surveillance, ce qui réduisit progressivement l'espace du discours numérique critique.

Ces tensions structurelles ont culminé entre 2024 et 2025, lorsque la réforme constitutionnelle a accentué l'incertitude politique et que les plateformes numériques sont devenues des espaces centraux de mobilisation citoyenne, notamment pour les jeunes, les artistes, les influenceurs et les réseaux de la diaspora. Les médias sociaux se sont transformés en un espace privilégié d'organisation politique et de débat public, provoquant une réponse étatique restrictive marquée par des arrestations, des perturbations de plate

3. [Amnesty International Togo et 7 autres c. la République togolaise Cour de justice de la CEDEAO, affaire n° ECW/CCJ/APP/61/18, arrêt n° ECW/CCJ/JUD/09/20 \(25 juin 2020\), \(consulté le 5 février 2026\)](#)

formes et la suspension de diffuseurs internationaux. Parallèlement, le gouvernement a poursuivi son programme numérique, incluant l'extension de l'identité biométrique et le développement de politiques en matière d'intelligence artificielle, soulignant un paradoxe fondamental. Si les systèmes numériques sont présentés comme des outils de modernisation et d'efficacité, leur déploiement dans des contextes de gouvernance fragiles a intensifié les inquiétudes concernant la responsabilité, la concentration du pouvoir et la viabilité à long terme d'une transformation numérique fondée sur les droits.

Accès à Internet

et interruptions

Le profil de connectivité du Togo en 2025 illustre un pays qui a considérablement progressé dans la construction de son infrastructure numérique, mais qui reste confronté aux questions de gouvernance plus profondes liées à l'expansion du numérique. Ces dernières années, l'arrivée de nouvelles capacités de câbles sous-marins, le renforcement des liaisons nationales en fibre optique et la montée en puissance du haut débit mobile ont contribué à consolider les fondements numériques du pays. Dans les grands centres urbains, la connectivité est de plus en plus fiable et les services numériques prennent une place prépondérante dans les sphères administratives, commerciales et éducatives. Cependant, ces progrès de-

meurent inégaux. Les communautés rurales continuent de faire face à une couverture de moindre qualité, à des coûts effectifs plus élevés par rapport au revenu des ménages et à des contraintes persistantes liées à une électrification limitée. De ce fait, la répartition des opportunités numériques dans le pays reste structurellement déséquilibrée.

Les événements de la mi-2025 ont démontré la fragilité de ces avancées technologiques face à la montée des tensions politiques. Alors que les manifestations menées par les jeunes s'étendaient à Lomé et à d'autres centres urbains, plusieurs organisations de surveillance indépendantes ont constaté des perturbations récurrentes affectant les plateformes de communication et de partage d'informations les plus utilisées. Les mesures effectuées par l'Observatoire ouvert des interférences de réseau, corroborées par les outils de surveillance de l'Internet Society, ont révélé des coupures de connexion répétées sur WhatsApp, Facebook, Signal, Telegram, YouTube et d'autres services à fort trafic à partir du 26 juin. Ces perturbations ont été constatées chez plusieurs opérateurs, dont Moov Africa, Togo Cellulaire, CanalBox et YAS Telecom, et leur survenue a coïncidé avec les épisodes les plus visibles de mobilisation citoyenne dans le pays.

Des observateurs nationaux ont confirmé cette tendance. L'Internet Society Togo a signalé une dégradation inhabituelle du service, affectant de manière disproportionnée les plateformes essentielles à la communication citoyenne. Des journalistes et des or-

ganisations de la société civile ont fait état de difficultés importantes pour télécharger des vidéos, vérifier les incidents sur le terrain et coordonner l'aide aux familles cherchant des informations sur leurs proches détenus ou blessés. Les défenseurs des droits humains ont noté que ces perturbations ont retardé la documentation des allégations de mauvais traitements et compliqué la coordination d'urgence avec les conseillers juridiques et les organisations partenaires hors du Togo.

Les répercussions économiques et sociales plus larges ont largement dépassé le contexte politique immédiat. Les petites entreprises qui dépendent des applications de messagerie pour maintenir le contact avec leurs clients ont subi une baisse rapide de leur activité. Les étudiants préparant leurs examens ont constaté que les plateformes de travail collaboratif et les outils d'apprentissage en ligne étaient parfois inaccessibles. Les chauffeurs, les livreurs et autres prestataires de services qui dépendent de la communication via des plateformes numériques ont vu leurs activités quotidiennes perturbées. Ces conséquences soulignent à quel point la connectivité numérique est devenue essentielle à la participation économique et à la coordination sociale, et comment même des restrictions ciblées peuvent engendrer des effets en cascade dans de nombreux secteurs de la société.

Ces interruptions ont également eu des répercussions sur la confiance du public dans l'environnement numérique. Les restrictions ont fait écho aux préoccupations déjà exprimées

dans la région quant à l'utilisation des outils de gestion de réseau en période de sensibilité politique. Des organisations nationales, dont la section togolaise de l'Internet Society et l'Association togolaise des consommateurs, ont appelé au rétablissement d'un accès complet et ont souligné l'importance de maintenir des canaux de communication ouverts en période d'incertitude nationale. Les acteurs régionaux ont fait référence à l'arrêt de 2020 de la Cour de justice de la CEDEAO, qui a affirmé que les restrictions d'accès à Internet doivent respecter les principes de légalité, de nécessité et de proportionnalité. Ces interventions témoignent d'un consensus régional croissant selon lequel une connectivité fiable est d'intérêt public et non un simple service technique.

Bien que les perturbations de 2025 n'aient pas entraîné de coupure générale à l'échelle nationale, leur caractère ciblé soulève d'importantes questions politiques. Elles mettent en évidence la nécessité de processus décisionnels transparents pour la gestion des réseaux numériques et de garanties institutionnelles renforcées afin d'éviter que les mesures d'accès ne restreignent involontairement les libertés fondamentales. L'expérience de 2025 montre que la crédibilité de la transformation numérique du Togo dépendra non seulement du développement des infrastructures, mais aussi de la mise en place de pratiques de gouvernance garantissant la résilience de l'écosystème numérique en période de tensions politiques.

Accès à

l'information

En 2025, l'accès à l'information et la liberté d'expression au Togo restaient entravés par des carences structurelles persistantes, documentées depuis plusieurs années par des observateurs nationaux et internationaux. Si un cadre juridique régissant l'accès à l'information publique existe formellement, sa mise en œuvre demeure insuffisante, limitant la transparence et affectant directement la capacité des journalistes, des organisations de la société civile et des citoyens à exercer leur liberté d'expression sur la base d'informations vérifiées et fiables.

Le cadre juridique de l'accès à l'information est défini par la loi de 2016 sur l'accès à l'information publique et son décret d'application de 2017,⁴ qui établissent les procédures de soumission des demandes, désignent les responsables de l'information au sein des institutions publiques et prévoient un recours auprès du Bureau du Médiateur de la République. Cependant, les évaluations menées par les organisations de la société civile et les experts en gouvernance, notamment les conclusions citées dans les rapports parallèles transmis aux mécanismes internationaux de

lutte contre la corruption, indiquent que ces dispositions sont rarement appliquées dans la pratique. Les demandes d'information restent souvent sans réponse, les délais de réponse ne sont pas respectés et les refus ne sont généralement ni formalisés ni justifiés par écrit. De ce fait, le dispositif d'accès à l'information demeure largement inefficace comme outil concret de transparence et de responsabilité.

Cet accès limité à l'information officielle a des conséquences directes sur la liberté d'expression. Les journalistes interrogés lors de récents exercices de suivi ont systématiquement fait état de difficultés à obtenir des documents officiels, des données budgétaires et des décisions réglementaires, notamment dans les domaines des finances publiques, des marchés publics, de la sécurité et de la gouvernance.

Ces contraintes fragilisent le journalisme d'investigation et réduisent la capacité des médias à fournir des reportages étayés par des preuves. Les organisations de la société civile qui analysent les politiques publiques indiquent également qu'elles s'appuient sur des réseaux informels plutôt que sur des mécanismes institutionnels de divulgation,⁵ ce qui accroît leur vulnérabilité aux pressions et nuit à la qualité du débat public.

4. République du Togo 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>(Consulté le 5 février 2026)
5. Coalition UNCAC.2023. Rapport parallèle sur le Togo. Coalition pour la Convention des Nations Unies contre la corruption. https://uncaccoalition.org/wp-content/uploads/FINAL_Parallel-Report-TOGO-UNCAC_EN.pdf(Consulté le 5 février 2026)

Les événements survenus en 2025 ont encore accentué l'interdépendance entre l'accès à l'information et la liberté d'expression. Lors des mobilisations citoyennes entre mai et juillet, la demande du public pour une information rapide et précise a fortement augmenté, notamment concernant les manifestations, les arrestations, les blessés et les réactions des pouvoirs publics.⁶ Dans le même temps, l'espace pour l'information indépendante s'est réduit. Le 16 juin 2025, la Haute⁷ Autorité de l'audiovisuel et de la communication a suspendu la diffusion de France 24 et de Radio France Internationale pour une durée de trois mois, une décision relayée par les médias internationaux et largement critiquée par les organisations de défense de la liberté de la presse. Cette mesure a considérablement restreint l'accès à une information internationale indépendante à un moment où le contexte politique était particulièrement tendu.

Les médias nationaux ont tenté de compenser cette perte de sources extérieures, mais ont continué de se heurter à des difficultés structurelles documentées par les organisations de défense de la liberté de la presse, notamment un accès limité aux sources officielles,

une fragilité financière et des risques accrus de pressions administratives ou judiciaires. Les rapports des organismes internationaux de protection des journalistes indiquent que ces conditions ont contribué à une autocensure accrue et à une réduction de la couverture sur le terrain des événements sensibles.

L'environnement informationnel numérique a également été affecté durant cette période. Selon le suivi réalisé par des organisations régionales de défense de la liberté des médias, des perturbations de la connexion internet et des services en ligne ont été signalées fin juin 2025, coïncidant avec des événements liés aux manifestations.⁸ Ces perturbations ont limité la capacité des journalistes et des citoyens à communiquer, à documenter les événements en temps réel et à accéder à des sources d'information indépendantes. De ce fait, le débat public s'est de plus en plus appuyé sur des informations fragmentées et non vérifiées circulant sur les réseaux sociaux, au détriment d'une communication institutionnelle transparente.

Des arrestations arbitraires liées à l'exercice de la liberté d'expression ont été documentées par de multiples sources crédibles tout au long de l'année 2025.⁹ Les médias in

6. Amnesty International. 2025. Togo. Des manifestants sont torturés lors de la répression des autorités contre la dissidence. Amnesty International. <https://www.amnesty.org/en/latest/news/2025/06/togo-protesters-tortured/> (Consulté le 5 février 2026)
7. Reuters. 2025. Le Togo suspend RFI et France 24 pour trois mois, annonce l'autorité de régulation des communications. Reuters. <https://www.reuters.com/business/media-telecom/togo-suspends-rfi-france-24-three-months-communications-authority-says-2025-06-16/> (Consulté le 5 février 2026)
8. Fondation des médias pour l'Afrique de l'Ouest. 2025. Perturbations d'Internet suite à la répression des manifestations au Togo. Fondation des médias pour l'Afrique de l'Ouest. <https://mfwa.org/country-highlights/togo-internet-disruptions-amid-post-protest-repression/> (Consulté le 5 février 2026)
9. Associated Press. 2025. Le Togo arrête des dizaines de personnes après des manifestations contre la réforme constitutionnelle. Associated Press. <https://apnews.com/article/e61f8334f1dc4483d446770b35aa9549/Con->

ternationaux ont fait état d'environ 80 arrestations lors des manifestations du mois de juin seulement. Les organisations de défense des droits humains ont constaté un phénomène plus général, s'étendant au-delà de la période de protestation immédiate : au moins 133 jeunes militants auraient été arrêtés arbitrairement entre juin et octobre 2025 pour avoir participé à des manifestations, exprimé leurs opinions en ligne ou critiqué publiquement les autorités.¹⁰ Dans plusieurs cas, des détenus auraient été maintenus en détention sans accès rapide à un avocat, ce qui a suscité des inquiétudes parmi les praticiens du droit quant aux garanties d'une procédure régulière.

Plusieurs cas emblématiques illustrent la tendance générale observée. En mai 2025, un musicien de renom a été arrêté suite à des déclarations publiques critiques et à des publications en ligne.¹¹

Son apparition ultérieure dans une vidéo d'excuses diffusée sur les réseaux sociaux a été qualifiée de coercition par les organisations de défense de la liberté de la presse. Début juin 2025, un journaliste travaillant pour une

chaîne de télévision internationale a été arrêté alors qu'il couvrait des manifestations et aurait été contraint par les forces de sécurité d'effacer les images enregistrées ; un incident documenté par des organisations internationales de protection des journalistes.¹² Ces affaires, conjuguées à la suspension des diffuseurs internationaux, ont contribué à instaurer un climat d'intimidation et ont eu un effet dissuasif sur l'activité journalistique et la liberté d'expression.

La numérisation continue de l'administration publique n'a pas permis de lever ces obstacles. Si les plateformes en ligne ont élargi l'accès aux services administratifs, des évaluations indépendantes ont montré que la diffusion proactive d'informations publiques restait limitée. Les données relatives à l'exécution budgétaire, aux projets d'infrastructure, aux décisions réglementaires et à la mise en œuvre des politiques n'étaient pas publiées de manière systématique. Comme l'ont déjà constaté des études précédentes, la transformation numérique a amélioré l'efficacité administrative sans pour autant renforcer la transparence, le contrôle public ni le droit à l'information.

sulté le 5 février 2026)

10. Défenseurs de première ligne.2025. Répression de la génération Z au Togo. 48 activistes doivent être libérés d'urgence. Défenseurs de première ligne. <https://www.frontlinedefenders.org/en/statement-report/repression-gen-z-togo-48-activists-must-be-urgently-released>(Consulté le 5 février 2026)
11. Fondation des médias pour l'Afrique de l'Ouest.2025. Un rappeur arrêté réapparaît dans une vidéo d'excuses devenue virale sur les réseaux sociaux. Fondation des médias pour l'Afrique de l'Ouest. <https://mfwa.org/country-highlights/togo-arrested-rapper-reappears-in-viral-apology-video-on-social-media/>(Consulté le 5 février 2026)
12. Comité pour la protection des journalistes.2025. Le Togo arrête un journaliste de TV5 Monde et l'oblige à supprimer des vidéos de manifestations. Comité pour la protection des journalistes. <https://cpj.org/2025/06/togo-detains-tv5-monde-journalist-forces-deletion-of-protest-videos/>(Consulté le 5 février 2026)

Globalement, l'évolution de la situation en 2025 a confirmé, et même accentué à certains égards, les préoccupations soulevées dans les rapports précédents. L'absence d'un régime d'accès à l'information efficace, conjuguée aux restrictions de la liberté des médias, aux perturbations numériques et aux arrestations liées à l'expression publique, a continué de limiter l'accès à une information vérifiée et d'affaiblir les conditions d'un débat public libre, éclairé et pluraliste. Faute de réformes institutionnelles durables et d'une protection renforcée de la liberté d'expression, la modernisation administrative ne s'est pas traduite par une plus grande transparence ni par un renforcement de la confiance du public envers les institutions étatiques.

Protection des données

et cybersécurité

Le cadre de gouvernance des données du Togo est entré dans une phase plus active en 2025 avec l'opérationnalisation progressive de l'Instance de Protection des Données à Caractère Personnel.¹³ L'autorité, créée en vertu de la loi de 2019 sur la protection des données personnelles, a entamé sa transi-

tion hors de sa phase initiale et a affirmé sa présence réglementaire au sein de l'écosystème numérique national. Son activation est intervenue à un moment où les services publics, les institutions financières et les entreprises privées s'appuient de plus en plus sur la collecte et le traitement des données personnelles. Le programme d'identité biométrique a étendu sa portée, les services administratifs numériques se sont généralisés et une part croissante des interactions quotidiennes des citoyens avec l'État s'est déplacée vers les plateformes numériques. Ces évolutions ont renforcé l'importance d'un organisme de contrôle capable d'orienter la gestion responsable des données, de clarifier les obligations de conformité et de définir les droits des individus concernant leurs données personnelles.

En 2025, l'autorité a axé ses travaux sur la publication de lignes directrices à destination des opérateurs publics et privés, l'amélioration de la compréhension par le public des droits relatifs aux données et la clarification des obligations liées au traitement des données personnelles. Ce travail s'avérait particulièrement important dans le contexte du développement des services publics numériques et de la centralisation des identifiants biométriques. De nombreux citoyens ont exprimé une attente croissante

13. Togo d'abord.(1er avril 2025). Togo : Lancement de l'Autorité nationale de protection des données tandis que Cyber Defense Africa renforce sa cyber-résilience. <https://www.togofirst.com/en/itc/0104-16053-togo-national-data-protection-authority-launches> (Consulté le 5 février 2026)

quant à la gestion transparente et sécurisée des données collectées pour la prestation de services publics, ainsi qu'à la limitation claire de leur utilisation secondaire. La création de cette autorité a constitué un premier point de repère pour répondre à ces attentes, même si ses ressources limitées et sa capacité opérationnelle modeste ont souligné l'ampleur du défi à relever.

Un changement réglementaire majeur a concerné la gouvernance de la vidéosurveillance dans les espaces publics et semi-publics. La prolifération des caméras dans les centres commerciaux, les complexes résidentiels et les institutions publiques avait pris de court l'existence d'un mécanisme de contrôle formel.

En 2025, l'autorité de protection des données a instauré l'obligation, pour toute installation de systèmes de vidéosurveillance dans des lieux accessibles au public, de faire l'objet d'une procédure formelle de notification et d'autorisation. Les opérateurs doivent enregistrer leurs systèmes de surveillance, démontrer que leur finalité est conforme aux normes nationales de protection de la vie privée et afficher clairement la preuve de leur autorisation. Les enregistrements produits par des systèmes non conformes à ces exigences peuvent être irrecevables devant les tribunaux. Cette mesure témoigne d'une volonté d'instaurer un cadre réglementaire rigoureux et de responsabiliser les acteurs d'un écosystème de surveillance en pleine expansion, afin de garantir que les objectifs de sécurité publique ne portent pas atteinte au droit à la

vie privée des individus.

Bien que ces évolutions institutionnelles aient marqué un progrès, elles se sont déroulées dans un contexte de cybersécurité de plus en plus actif et sophistiqué. Cyber Defense Africa (CDA), créée en 2019 dans le cadre d'un partenariat public-privé, a continué de jouer le rôle de centre national des opérations de cyberdéfense, fonctionnant à la fois comme centre national des opérations de sécurité et comme CERT.tg. Tout au long de l'année 2025, CDA a renforcé ses capacités techniques, élargi ses fonctions d'analyse et collaboré étroitement avec les administrations publiques, les banques et les fournisseurs de services afin de détecter les intrusions et d'atténuer les risques. Ses alertes publiques concernant les attaques de phishing, les fraudes aux paiements, les tentatives de vol de données et les vulnérabilités affectant les systèmes des entreprises et des administrations sont devenues plus fréquentes, témoignant de l'exposition croissante du pays aux cybermenaces.

Les activités de CERT.tg ont joué un rôle préventif important en aidant les organisations à identifier les menaces émergentes et en encourageant les citoyens à adopter des pratiques de sécurité numérique de base. Ces interventions étaient particulièrement pertinentes compte tenu du développement parallèle de l'identité numérique, des services financiers numériques et des plateformes électroniques pour les démarches administratives. À mesure que le nombre d'utilisateurs effectuant des transactions

numériques augmente, le risque d'usurpation d'identité, de fraude et de manipulation des données personnelles ou financières s'accroît. La visibilité de CERT.tg en 2025 a permis de remédier à ces vulnérabilités et a contribué à un débat public plus éclairé sur la sécurité numérique.

Cyber Defense Africa a également approfondi sa coopération avec ses partenaires régionaux et internationaux. Par le biais d'exercices de renforcement des capacités, d'initiatives d'analyse conjointe et d'accords de coopération avec des institutions homologues, l'organisation a participé aux efforts visant à renforcer la cyber-résilience collective de l'Afrique. L'accord de coopération signé en 2025 avec un État d'Afrique australe illustre cet engagement international et témoigne de la volonté du Togo de se positionner comme un acteur émergent de la cybersécurité africaine.

Ces évolutions institutionnelles se sont déroulées dans un contexte politique et social toujours sensible aux questions de surveillance et de contrôle numérique. Les allégations passées concernant les technologies intrusives ont durablement ancré un sentiment de risque chez les journalistes, les organisations de la société civile et les acteurs politiques. Bien qu'aucun cas confirmé n'ait été recensé en 2025, cette perception a influencé la manière dont de nombreuses personnes interagissaient avec les plateformes numériques et interprétaient la présence croissante des institutions de cybersécurité. Le chevauchement entre les mandats de cy-

berdéfense, les intérêts de sécurité nationale et les responsabilités en matière de gouvernance des données exige une gestion rigoureuse afin d'éviter d'alimenter les craintes relatives au respect de la vie privée et à la surveillance abusive.

Les évolutions observées en 2025 mettent en lumière à la fois la consolidation et les tensions structurelles inhérentes à la construction d'une architecture contemporaine de gouvernance des données et de la cybersécurité dans un environnement en pleine numérisation. Au-delà de l'existence de la loi n° 2019 014,¹⁴ l'opérationnalisation de l'Instance de Protection des Données à Caractère Personnel a marqué un tournant institutionnel décisif, transformant un cadre légal en un mécanisme de surveillance actif capable d'émettre des orientations, de définir des obligations de conformité et de servir de point de référence pour la protection de la vie privée et le traitement des données personnelles.

L'introduction en 2025 d'un régime formel de déclaration et d'autorisation pour les systèmes de vidéosurveillance¹⁵ a permis de traduire davantage les droits abstraits en procédures administratives exécutoires. En exigeant une notification préalable, une justification documentée et une preuve visible de l'autorisation pour les dispositifs de surveillance installés dans les espaces publics, elle a intégré les critères de légalité et de proportionnalité dans les pratiques de sécurité quotidiennes, renforçant de ce fait les garanties procédurales pour les particuliers.

Ensemble, ces éléments confèrent au Togo un cadre juridique structuré, une autorité de contrôle identifiable,¹⁶ un mécanisme de régulation des technologies de surveillance clairement défini et une infrastructure de cybersécurité opérationnelle capable de répondre aux risques systémiques. Cette intégration constitue une condition essentielle à la pérennité de la transformation numérique, tout en l'ancrant dans un cadre respectueux des droits, de la sécurité et de la responsabilité institutionnelle.

Vie privée et

surveillance de l'État

La surveillance étatique a façonné la vie numérique au Togo tout au long de l'année 2025, de manière à la fois visible et insidieuse, instaurant un contrôle strict sur un paysage politique déjà marqué par les tensions. Le pays abordait cette année avec les séquelles non résolues du scandale du logiciel espion Pegasus. En 2021, l'analyse forensique du Security Lab d'Amnesty International et les révélations des médias internationaux ont confirmé que les téléphones

du journaliste d'investigation Ferdinand Ayité et d'autres journalistes togolais avaient été ciblés pour une potentielle infection par Pegasus, un outil de surveillance sophistiqué conçu par la société israélienne NSO Group. Ces investigations ont suscité l'inquiétude internationale, mais aucune enquête publique n'a été menée au Togo.

Dans une interview accordée au Monde, Ayité lui-même a averti que les autorités togolaises avaient investi dans des systèmes d'écoute et entretenaient des relations privilégiées avec des réseaux israéliens composés d'anciens agents du renseignement. Ces déclarations sont devenues un point de référence important pour de nombreux journalistes et militants, influençant leur perception de la vulnérabilité numérique jusqu'en 2025.

Cette histoire a pris toute son importance car une grande partie de la vie politique et sociale du pays s'est déplacée vers les plateformes numériques. Les jeunes, les artistes, les journalistes et les acteurs de la société civile ont de plus en plus recours à TikTok, Facebook, Instagram et WhatsApp pour exprimer leurs opinions, documenter leurs griefs et organiser des manifestations. Face à l'intensification des inquiétudes concernant la réforme constitutionnelle de 2024, les espaces

14. CIO Mag. (2025, 29 mars). Togo: L'Autorité de protection des données personnelles entame sa mission. <https://cio-mag.com/protection-des-donnees-personnelles-au-togo-lipdcp-entame-sa-mission/> (Consulté le 5 février 2026)
15. Médias civiques. (27 juillet 2025). Togo : L'IPDCP lance le processus de déclaration officielle des systèmes de vidéosurveillance. <https://civicmedias.info/cv/index.php/2025/07/27/togo-ipdcp-lancement-officiel-du-procesus-de-declaration-des-dispositifs-de-videosurveillance/> (Consulté le 5 février 2026)
- 16.

numériques sont devenus le principal lieu de débat et de mobilisation. Lorsque les manifestations menées par les jeunes ont débuté fin mai et ont rapidement pris de l'ampleur tout au long du mois de juin, l'expression en ligne a acquis une importance politique accrue.

La riposte de l'État s'est largement appuyée sur la surveillance des activités numériques et sur l'application de dispositions légales générales issues de la loi de 2018 sur la cybercriminalité. Des organisations de défense des droits humains ont signalé l'arrestation de plus de 100 personnes entre le 5 juin et le 31 octobre pour des faits liés à l'expression en ligne. Environ 48 personnes étaient encore détenues à la fin de l'année. Les témoignages de détenus et d'avocats ont indiqué que les interrogatoires portaient fréquemment sur l'activité sur les réseaux sociaux. Les personnes interrogées étaient confrontées à des captures d'écran de sessions TikTok en direct, de commentaires Facebook ou de messages partagés via des groupes WhatsApp, et devaient justifier leurs liens avec des comptes, des organisateurs ou des personnalités de la diaspora. Ce schéma a démontré que les autorités utilisaient systématiquement les traces en ligne comme un élément central pour identifier les participants et les sympathisants à la mobilisation.

L'arrestation et le traitement infligés au rap-

peur Aamron ont mis en lumière ces dynamiques.¹⁷ Aamron, qui utilisait TikTok et d'autres plateformes pour critiquer des dirigeants politiques, a été assigné à résidence, transféré dans un établissement psychiatrique, puis est apparu dans une vidéo pour présenter ses excuses dans des circonstances floues. Son cas a profondément marqué les jeunes car il illustre comment la visibilité numérique pouvait rapidement engendrer une grande vulnérabilité. Pour beaucoup, il a confirmé que l'expression en ligne n'offrirait plus aucune protection contre l'intervention de l'État.

L'expérience de Traoré Leïla a renforcé cette perception. Les médias nationaux et des militants ont rapporté qu'elle avait été arrêtée alors qu'elle allaitait son nourrisson et qu'elle était restée en détention pour des motifs liés à la sécurité. Bien que les détails de son affaire soient incomplets, elle est largement décrite comme une détenue arrêtée en raison de ses liens supposés avec des réseaux d'opposition. Sa situation met en lumière la vulnérabilité des personnes soupçonnées d'être liées à des critiques politiques, que ce lien se fasse par le biais d'interactions numériques ou par proximité sociale.

Ces pratiques s'inscrivent dans un contexte de cybersécurité plus large, dont les capacités n'ont cessé de se développer, comme expliqué précédemment avec la création de

17. The Guardian. (10 juillet 2025). Un de trop : l'arrestation d'un rappeur déclenche des manifestations contre la dynastie au pouvoir au Togo. <https://www.theguardian.com/world/2025/jul/10/rapper-aamron-arrest-protests-togo-ruling-dynasty>

Cyber Defense Africa, du Centre national des opérations de sécurité et de CERT.tg. Tout au long de l'année 2025, l'institution a surveillé les réseaux nationaux en temps réel, émis des alertes sur les campagnes d'hameçonnage et les cybermenaces, et renforcé son infrastructure technique. Ces compétences sont essentielles à la protection des systèmes critiques, mais elles contribuent également à l'impression, partagée par le public, que l'État exerce une surveillance accrue des communications numériques. La frontière entre cybersécurité et surveillance n'est pas toujours claire pour les utilisateurs, notamment au cours d'une année marquée par des arrestations et des interrogatoires liés à des activités en ligne.

L'effet cumulatif de ces dynamiques a influencé les comportements en ligne tout au long de l'année 2025. Les journalistes ont fait preuve d'une prudence accrue lorsqu'ils abordaient des sujets politiquement sensibles, évitant souvent les plateformes de messagerie traditionnelles pour les échanges de fond.

Les acteurs de la société civile ont réorienté les discussions stratégiques vers des canaux de communication plus discrets, conscients des risques liés à l'exposition dans les espaces numériques ouverts. Les commentateurs de la diaspora, notamment le journaliste d'investigation exilé Ferdinand Ayité, qui a continué d'analyser l'actualité politique nationale par le biais d'émissions régulières en direct sur Internet, étaient conscients que leurs interactions avec des contacts restés au pays

pouvaient, involontairement, les exposer à une surveillance accrue. Chez les jeunes utilisateurs en particulier, les efforts délibérés pour réduire leur visibilité numérique se sont multipliés, témoignant d'une prise de conscience que la surveillance des traces numériques était désormais intégrée au dispositif de sécurité national.

Ce qui caractérisait la surveillance étatique au Togo en 2025, ce n'était pas l'existence d'un système unique, mais la convergence de l'autorité légale, des capacités techniques et de la volonté politique. L'expression numérique était étroitement surveillée, les traces en ligne étaient utilisées pour identifier et arrêter les dissidents, et les révélations passées concernant les logiciels espions continuaient d'influencer les attentes du public. Dans ce contexte, la frontière entre sphère privée et sphère publique s'est considérablement estompée et l'espace numérique, loin d'offrir une protection, est devenu l'un des principaux vecteurs par lesquels l'État exerçait sa présence sécuritaire.

Évolutions des TIC

et des technologies

émergentes

Au Togo, en 2025, le développement des TIC a été marqué par la consolidation des infrastructures publiques numériques et une orientation délibérée vers les technologies émergentes comme instruments de modernisation de l'État. Le gouvernement a continué de faire de la transformation numérique une priorité nationale, en insistant sur le rôle des données, de la connectivité et de l'innovation pour améliorer l'efficacité administrative et stimuler le développement économique.

L'année a été marquée par des avancées notables dans les travaux nationaux sur l'intelligence artificielle (IA). Les autorités ont intensifié les consultations sur la future stratégie nationale en matière d'IA, la présentant comme un outil pour renforcer l'administration publique, appuyer la prise de décision et moderniser des secteurs prioritaires tels que l'agriculture, la santé et l'éducation. Des instituts de recherche, des experts techniques et des instances gouvernementales ont participé à des ateliers visant à définir les fondements d'un écosystème d'IA capable de s'appuyer sur des données locales, un capital humain qualifié et des principes de gouvernance clairs. Une série de réunions nationales a permis de donner de la visibilité à ces débats et d'inscrire l'IA dans une réflexion

plus large sur la compétitivité économique et la réforme des services publics.

L'innovation dans le secteur de l'éducation s'est poursuivie grâce à l'association du Togo à l'initiative Giga, le programme mondial de connectivité scolaire piloté par l'UNICEF et l'UIT. Giga utilise l'intelligence artificielle, la cartographie satellitaire et la modélisation des infrastructures pour identifier les écoles non connectées et concevoir des stratégies d'extension rentables. Pour le Togo, la participation à Giga représente bien plus qu'un simple exercice de connectivité. Elle fournit une méthodologie structurée pour cartographier les lacunes nationales en matière d'infrastructures et encourage l'intégration des écoles dans la planification plus large du haut débit rural. Elle renforce également la coopération avec les partenaires internationaux et soutient une vision à long terme où la connectivité devient un pilier fondamental du développement éducatif. Giga ayant désormais cartographié plus d'un million d'écoles dans le monde et développé des modèles de financement basés sur la demande agrégée, cette approche offre aux pays, dont le Togo, des outils pratiques pour concevoir des plans nationaux de connectivité scolaire réalistes.

L'administration publique numérique a également progressé en 2025, grâce à des efforts continus visant à renforcer l'interopérabilité entre les systèmes gouvernementaux et à élargir l'accès aux services publics en ligne. Les acteurs institutionnels se sont employés à moderniser leurs systèmes d'information internes et à réorganiser les processus admin

istratifs autour des plateformes numériques. Plusieurs organismes gouvernementaux ont commencé à s'appuyer davantage sur des systèmes de données intégrés pour suivre la prestation de services et améliorer leur efficacité opérationnelle. Ces efforts ont été soutenus par des partenaires internationaux à travers des programmes axés sur la gouvernance numérique du secteur public, le développement des infrastructures et le renforcement des capacités institutionnelles.

Les technologies émergentes ont occupé une place prépondérante dans les discussions sur la transformation économique et la compétitivité nationale. Les autorités ont examiné comment l'innovation en matière d'analyse de données, de cartographie géospatiale et d'automatisation pourrait être appliquée à des domaines tels que l'aménagement du territoire, les transports, l'agriculture et l'adaptation au changement climatique. Les projets pilotes menés dans ces domaines témoignent d'un intérêt croissant pour le recours aux technologies afin de relever les défis structurels de longue date. Les organisations régionales et les partenaires au développement ont offert des plateformes d'échange supplémentaires sur l'innovation responsable, l'inclusion numérique et le développement du capital humain pour le secteur technologique.

Le Togo a également poursuivi la coopération régionale en matière de cybersécurité et de résilience numérique, reconnaissant que les technologies émergentes nécessitent une infrastructure stable et sécurisée. Les agences

gouvernementales ont conclu des accords de collaboration avec d'autres États africains, axés sur le partage d'informations, le soutien mutuel en matière de réponse aux incidents et le renforcement conjoint des capacités. Ces partenariats ont mis en évidence la volonté d'inscrire les progrès nationaux dans un cadre régional plus large et de renforcer la préparation collective de l'Afrique à l'économie numérique.

Inclusion numérique

En 2025, l'inclusion numérique au Togo était marquée par des progrès, mais aussi par des contraintes structurelles persistantes. Si la connectivité urbaine continuait de s'améliorer, l'accès restait inégal selon les régions, les groupes de revenus et les catégories sociales. Les communautés rurales, en particulier, souffraient d'une couverture plus faible, d'une électrification limitée et de coûts élevés, ce qui freinait l'utilisation régulière des services numériques. Ces disparités influençaient l'accès quotidien à l'information, à l'éducation et aux services administratifs.

Un événement marquant s'est produit en novembre 2025 avec l'inauguration du premier réseau communautaire du pays à Atti Akakpé, mis en œuvre par l'Internet Society of Togo en partenariat avec les acteurs locaux. Cette initiative a introduit un modèle de connectivité géré localement, conçu pour les zones où les opérateurs commerciaux sont peu présents. Elle a offert une voie alternative d'accès à Internet en milieu rural, combinant infrastructure, participation communautaire et possibilité de formation numérique locale. L'expérience a démontré que des solutions ciblées, portées par les communautés, peuvent compléter les stratégies numériques nationales, notamment dans les régions où les lacunes en matière d'infrastructures demeurent importantes.

L'accessibilité financière a continué d'influencer l'accès aux services numériques. Le

coût des appareils et des données mobiles est resté élevé par rapport au revenu moyen, limitant ainsi la connectivité pour de nombreux ménages. Les étudiants, les travailleurs du secteur informel et les familles à faibles revenus dépendaient souvent d'appareils partagés ou d'un accès intermittent, ce qui restreignait leur capacité à profiter pleinement de l'apprentissage en ligne, des plateformes financières ou des services gouvernementaux de plus en plus numérisés.

Les personnes handicapées rencontraient des obstacles supplémentaires pour accéder aux plateformes numériques. Les systèmes du secteur public n'étaient pas systématiquement conçus en tenant compte des exigences d'accessibilité. Les technologies d'assistance, telles que les lecteurs d'écran ou le sous-titrage, n'étaient pas toujours compatibles avec les interfaces gouvernementales. Les associations de défense des droits des personnes handicapées continuaient de réclamer une meilleure intégration des normes de conception universelle dans les services numériques, tant publics que privés.

L'accès au numérique est également influencé par le genre. Les femmes, notamment en milieu rural, possèdent moins d'appareils, utilisent moins fréquemment Internet et ont un accès réduit aux formations numériques. Les contraintes sociales, les difficultés économiques et les préoccupations liées à la sécurité limitent leur participation aux espaces en ligne. Les périodes de forte activité politique engendrent des risques accrus de harcèlement et d'intimidation en ligne à l'en

contre des femmes qui s'expriment publiquement sur les plateformes numériques.

Les enfants et les jeunes occupent une place de plus en plus centrale dans les débats nationaux sur les opportunités numériques.

Le Fonds de service universel demeurait un instrument important pour réduire la fracture numérique, mais la transparence de son fonctionnement restait limitée. Faute de rapports clairs sur l'allocation et la mise en œuvre des fonds, il était difficile de déterminer dans quelle mesure il soutenait les communautés mal desservies, les personnes handicapées ou les utilisateurs à faibles revenus.

La société civile a continué de plaider pour une plus grande transparence afin de garantir que le fonds joue pleinement son rôle dans la réduction des inégalités d'accès au numérique.

Le niveau de compétences numériques variait considérablement selon les groupes de population. Les jeunes apprenaient souvent de manière informelle grâce aux réseaux sociaux, tandis que les personnes âgées et les habitants des zones rurales rencontraient davantage de difficultés à naviguer sur les plateformes en ligne ou à utiliser les outils numériques nécessaires aux services publics. Avec la numérisation croissante des

systèmes administratifs, le besoin de compétences numériques généralisées est devenu de plus en plus évident à travers le pays.

Ces facteurs conjugués ont façonné le paysage de l'inclusion numérique en 2025. La connectivité s'est développée, mais l'accès réel dépendait des moyens financiers, de la situation géographique, des compétences et du contexte social. L'émergence de modèles communautaires, tels que le réseau Atti Akakpé, a apporté une dimension,¹⁸ prometteuse au paysage national, démontrant comment les initiatives locales peuvent contribuer à combler les lacunes que les infrastructures nationales ne peuvent à elles seules résoudre immédiatement.

18. République togolaise.(29 novembre 2025). L'Internet Society déploie son premier réseau communautaire. République togolaise. <https://www.republicoftogo.com/toutes-les-rubriques/high-tech/l-internet-society-deploie-son-premier-reseau-communautaire>(Consulté le 5 février 2026)

Conclusion

La trajectoire numérique du Togo en 2025 a révélé un pays progressant rapidement dans la construction d'infrastructures publiques modernes, tout en faisant face aux limites d'un environnement de gouvernance soumis à de fortes tensions. Les investissements dans l'identité numérique, les plateformes de services publics, les initiatives de connectivité et les premiers travaux sur l'intelligence artificielle ont confirmé le rôle central croissant de la technologie dans le développement national. Ces réformes ont élargi les capacités administratives de l'État et jeté les bases d'une transformation à long terme.

Parallèlement, l'année a mis en lumière les tensions qui surgissent lorsque le progrès technologique s'accompagne d'une dégradation du climat civique et politique. Le recours généralisé à la loi sur la cybercriminalité contre la liberté d'expression en ligne, les arrestations consécutives aux mobilisations numériques, les perturbations affectant les principales plateformes lors des manifestations publiques et la restriction de l'accès à l'information ont tous démontré comment les systèmes numériques peuvent s'imbriquer dans le contrôle politique. Le manque d'accès opérationnel au système d'information et le manque de transparence dans plusieurs domaines de l'administration publique ont encore compliqué la relation entre gouvernance numérique et confiance du public. L'inclusion numérique reste fortement tributaire de la situation géographique, du revenu,

du genre et des compétences. L'inauguration du réseau communautaire Atti Akakpé a illustré le potentiel des solutions portées par les communautés, tandis que l'initiative Giga a proposé une approche structurée de la connectivité scolaire. Cependant, de nombreux citoyens se heurtent encore à des obstacles qui les empêchent de profiter pleinement de la transformation numérique du pays.

Les événements de l'année ont mis en lumière une question centrale pour l'avenir de la gouvernance numérique au Togo. Le pays a bâti d'importantes infrastructures techniques et affiché une ambition claire. Ses prochaines étapes dépendront de sa capacité à opérer dans un cadre garantissant la protection des droits, la transparence et l'utilisation des technologies pour renforcer le lien entre les citoyens et l'État, au lieu de l'affaiblir.

Recommandations

Gouvernement

- Mettre en œuvre la loi de 2016 sur l'accès à l'information en publiant les lignes directrices d'application et en créant un mécanisme fonctionnel pour la réception, le traitement et le recours des demandes d'information.
- Réformer les dispositions de la loi de 2018 sur la cybercriminalité afin de garantir que les infractions liées à l'insulte et à la désinformation ne puissent pas être utilisées pour criminaliser l'expression légitime en ligne.
- Renforcer l'indépendance et les capacités opérationnelles de l'autorité nationale de protection des données, en veillant à ce que son contrôle s'applique aussi bien aux acteurs publics que privés traitant des données à caractère personnel.
- Mettre en place un cadre de garanties cohérent et applicable régissant le déploiement des systèmes d'identification biométrique, des infrastructures de vidéosurveillance, des outils de décision automatisée et l'interception ou l'analyse des communications numériques, y compris les appels téléphoniques. Ce cadre devrait définir des règles transparentes concernant la limitation des finalités, la minimisation des données, la durée de conservation, les contrôles d'accès et le contrôle indépendant, afin de garantir que les objectifs de sécurité et administratifs soient poursuivis dans un cadre juridique clairement défini et soumis à des mécanismes de responsabilisation efficaces.
- Garantir un accès ininterrompu à Internet pendant les périodes de tensions publiques et adopter des procédures claires, conformes aux normes régionales en matière de droits de l'homme, pour toute restriction des services numériques.
- Améliorer la connectivité rurale en publiant des plans transparents pour l'expansion des infrastructures et en assurant une utilisation ciblée du Fonds de service universel.
- Intégrer les normes d'accessibilité dans toutes les plateformes numériques publiques et veiller à ce que les services soient accessibles aux personnes handicapées sans obstacles.

Environnement

- Développer les reportages sur la gouvernance numérique, la protection des données, l'intelligence artificielle et les implications sociétales de la transformation numérique.
- Renforcer le travail d'enquête sur les finances publiques, les marchés publics et les infrastructures numériques tout en maintenant des normes éthiques et éditoriales rigoureuses.
- Engager un dialogue structuré avec les institutions étatiques afin de clarifier les procédures d'accès à l'information publique et de surmonter les blocages administratifs.
- Offrir une formation en sécurité numérique aux journalistes et aux rédactions afin de réduire les risques pendant les périodes de sensibilité politique.

Organisations de la société civile

- Poursuivre la surveillance des droits numériques et la documentation des restrictions à la liberté d'expression en ligne au moyen de méthodes rigoureuses et fondées sur des preuves.
- Développer les programmes d'alphabétisation numérique communautaires, en particulier dans les zones rurales et auprès des femmes, des jeunes et des groupes marginalisés.
- Établir des partenariats avec les communautés universitaires et techniques afin d'analyser l'impact des systèmes d'identité numérique, des technologies de surveillance et des politiques émergentes en matière d'IA.
- Collaborer avec les instances régionales et continentales pour renforcer le plaidoyer transfrontalier et aligner les débats nationaux sur les cadres de gouvernance africains plus larges.

Secteur privé

- Améliorer l'accessibilité financière des services de connectivité et des services numériques en développant des modèles de tarification accessibles, notamment pour les utilisateurs à faibles revenus et en milieu rural.
- Adoptez des politiques internes robustes en matière de protection des données et de confidentialité, garantissant le respect total de la législation nationale et des normes internationales.
- Intégrez l'accessibilité et la conception inclusive dans tous les produits et plateformes numériques.
- Collaborer avec les universités, les centres de formation et les incubateurs pour soutenir le développement des compétences numériques liées aux technologies émergentes telles que l'intelligence artificielle, les services cloud et les systèmes géospatiaux.

Indice de score du Togo pour 2025 comparé à celui de 2024

L'indice de score 2025 affiche un léger recul par rapport à 2024, le score global passant de 29 à 28 sur 60. Si la variation numérique semble limitée, la répartition des indicateurs révèle une divergence persistante entre les progrès réalisés en matière de développement institutionnel et infrastructurel et les pressions continues qui affectent les droits numériques fondamentaux.

Par rapport à 2024, la plupart des baisses concernent les restrictions à la liberté d'expression en ligne, le recours aux dispositions

légales pour réprimer la liberté d'expression numérique et les préoccupations persistantes relatives à la transparence et à la surveillance. En 2024, le pays était déjà confronté à des inquiétudes persistantes concernant les poursuites liées à la liberté d'expression en ligne. La situation s'est considérablement aggravée après la mobilisation citoyenne de juin et juillet 2025. Selon l'Organisation mondiale contre la torture et ses partenaires, au moins 133 jeunes militants togolais ont été arrêtés arbitrairement à partir du 5 juin 2025 pour avoir « exprimé leurs opinions ou manifesté pacifique-

ment », et 48 étaient encore détenus au moment de leur déclaration d'octobre 2025. Ces chiffres illustrent l'ampleur des arrestations consécutives à la mobilisation et témoignent de la tension croissante entre la contestation citoyenne, l'expression numérique et les réponses des forces de sécurité de l'État au cours de l'année.

L'accès à Internet a également connu un déclin. En 2024, le Togo a maintenu une connectivité relativement stable malgré des coupures régionales. En 2025, cependant, des perturbations ciblées des plateformes de communication utilisées lors des manifestations ont réduit la conformité du pays aux principes de la CADHP relatifs à un accès ouvert et ininterrompu. Ce changement n'était pas dû à une faiblesse des infrastructures, mais plutôt au recours à des restrictions d'accès dans un contexte de tensions politiques.

Les indicateurs relatifs aux fausses informations et aux infractions de sédition sont restés parmi les plus faibles de l'indice. Leur impact s'est fait plus sentir en 2025, les dispositions légales régissant la sédition et la cybercriminalité étant de plus en plus utilisées dans les poursuites liées aux publications en ligne et aux commentaires sur les réseaux sociaux. L'année précédente, ces dispositions étaient surtout perçues comme problématiques en principe. En 2025, elles sont devenues des instruments opérationnels de répression de la liberté d'expression numérique, notamment chez les jeunes utilisateurs actifs sur des plateformes comme TikTok, Instagram et Facebook.

Le score relatif à l'accès à l'information n'a pas

progressé. La limitation structurelle identifiée en 2024 est restée inchangée. La loi de 2016 sur l'accès à l'information a continué de souffrir d'un manque d'application effective, et les ministères n'ont pas publié systématiquement de données ni de rapports publics. La suspension de deux grands diffuseurs internationaux, dans un contexte de tensions politiques, a encore restreint l'accès à une information indépendante.

Les préoccupations relatives à la protection de la vie privée et à la surveillance restent importantes. Bien qu'aucune nouvelle enquête concernant des logiciels espions n'ait été révélée en 2025, la persistance des révélations sur Pegasus, conjuguée au recours aux traces numériques et à la surveillance des médias sociaux dans les enquêtes liées aux manifestations, a renforcé le sentiment de vulnérabilité du public et maintenu l'indicateur à son niveau le plus bas.

Tous les développements n'ont pas été négatifs. La législation sur la protection des données a conservé un score relativement élevé grâce à l'opérationnalisation de l'autorité nationale de protection des données et à la mise en place d'un contrôle réglementaire des systèmes de surveillance. Cette évolution institutionnelle témoigne d'une consolidation de l'architecture de gouvernance des données du pays, même si les capacités de contrôle restent limitées.

Des progrès ont également été observés en matière d'inclusion numérique. L'inauguration du premier réseau communautaire à Atti Akapé a démontré des approches novatrices en matière de connectivité rurale, tandis que la poursuite des efforts de connectivité scolaire





dans le cadre de l'initiative Giga a donné un nouvel élan à l'élargissement de l'accès aux infrastructures numériques.











L'indicateur relatif aux technologies émergentes s'est également amélioré. Bien qu'aucune stratégie nationale en matière d'intelligence artificielle n'ait été officiellement publiée en 2025, les consultations se sont intensifiées et l'écosystème institutionnel entourant la gouvernance de l'IA est devenu plus visible. La signature de la Convention des Nations Unies contre la cybercriminalité en octobre 2025 a par ailleurs confirmé l'engagement pris dans les cadres de gouvernance internationaux émergents liés aux technologies numériques. Globalement, la comparaison avec 2024 met en évidence une tension structurelle persistante au sein de l'environnement numérique togolais. Le développement des infrastructures, les capacités en matière de cybersécurité et la gouvernance des technologies émergentes ont continué de progresser. Parallèlement, les restrictions affectant la liberté d'expression, la transparence et la protection contre la surveillance sont restées importantes. Le léger recul du score global reflète donc l'importance croissante de ces enjeux civiques et liés aux droits dans le cadre plus large de la transformation numérique.








L'indice Score



Togo, 2025

1 = Totalement non conforme; 2 = Légèrement conforme; 3 = Modérément conforme;
4 = Considérablement conforme; 5 = Entièrement conforme

Indicateurs	ACHPR Principe	2024 Score	2025 Score	2025 Justification
Accès à Internet et interruptions	P37			L'infrastructure s'est améliorée, mais les perturbations ciblées de la plateforme lors des manifestations de juin et juillet ont réduit le respect des principes d'accès ouvert et ininterrompu.
Absence de lois, de politiques et d'autres mesures visant à promouvoir un accès universel, équitable, abordable et significatif à Internet	P37			Malgré les améliorations apportées aux infrastructures de connectivité et des initiatives telles que le déploiement des réseaux de fibre optique, la participation au programme Giga et l'émergence de projets de connectivité communautaire, le Togo ne dispose toujours pas d'un cadre politique global visant spécifiquement à garantir un accès universel, équitable, abordable et significatif à Internet. De plus, aucun rapport public ni donnée vérifiée n'est disponible concernant la collecte, la gestion ou l'utilisation effective du Fonds de service universel, ce qui rend difficile l'évaluation de sa contribution à l'expansion de la connectivité ou au soutien des populations mal desservies.

Indicateurs	ACHPR Principe	2024 Score	2025 Score	2025 Justification
Criminalisation des fausses nouvelles	P22(2)	 2	 1	Les dispositions de la loi sur la cybercriminalité ont continué à criminaliser l'expression en ligne et ont été largement utilisées en 2025 pour justifier des arrestations liées à des commentaires sur les affaires publiques.
Législation sur la sédition	P22(2)	 3	 2	La loi sur la cybercriminalité a conservé des infractions générales qui ont facilité la poursuite des critiques en ligne, y compris les vidéos TikTok et les commentaires sur les réseaux sociaux.
Arrestations arbitraires et harcèlement de journalistes, de défenseurs des droits humains et de citoyens	P20(1) et (2)	 1	 1	Plus de 100 personnes ont été arrêtées entre juin et octobre pour avoir exprimé leurs opinions en ligne, et environ 48 étaient encore en détention à la fin de l'année.
Législation sur la protection des données	P42	 4	 4	L'autorité de protection des données est devenue opérationnelle en 2025 et a introduit une réglementation en matière de surveillance, mais sa capacité de contrôle est restée limitée.
Suppression de contenu en ligne sans procédure	P38 et P39(4)	 2	 2	Les restrictions temporaires imposées aux principales plateformes numériques pendant les manifestations n'ont pas été accompagnées de processus transparents ou communiqués publiquement.

Indicateurs	ACHPR Principe	2024 Score	2025 Score	2025 Justification
Atteinte à la vie privée des communications	P41			Les révélations passées concernant Pegasus sont restées sans réponse, et la perception publique de la surveillance a persisté, renforcée par l'utilisation de traces numériques dans les enquêtes.
Défaut de divulgation proactive d'informations	P29(3)			La loi de 2016 sur l'accès à l'information est restée inopérante et les ministères n'ont pas publié de données ni de rapports réguliers.
Gouvernance de l'IA et des technologies émergentes	P39(6)			Les consultations nationales sur l'intelligence artificielle se sont intensifiées et les fondements politiques de sa gouvernance ont commencé à se dessiner grâce à des discussions multipartites et à une collaboration technique avec les institutions de recherche et les autorités publiques. En octobre 2025, le Togo a également signé la Convention des Nations Unies contre la cybercriminalité, témoignant ainsi d'un engagement accru envers les cadres de gouvernance mondiaux émergents relatifs aux technologies numériques et à la cybersécurité. Cependant, aucune stratégie nationale en matière d'intelligence artificielle ni aucun cadre réglementaire formel n'ont été publiés au cours de l'année.
Adoption de mesures de sécurité en ligne pour les enfants	P37(5)			L'éducation numérique s'est développée, mais il n'existait pas de cadre national global pour la protection des enfants en ligne.

Indicateurs	ACHPR Principe	2024 Score	2025 Score	2025 Justification
Inclusion numérique	P38 et P39(4)			La connectivité s'est améliorée et des réseaux communautaires ont émergé, mais les inégalités en matière de ressources, d'accessibilité et de coût sont restées importantes en milieu rural.
Score global	2024: 29	2025 28		Le Togo a réalisé des progrès en matière d'infrastructures et de développement institutionnel, mais a connu une régression importante en ce qui concerne la liberté d'expression, l'accès à l'information et la protection contre la surveillance arbitraire.



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