

Régulation du numérique au Sahel : État des lieux et perspectives pour un modèle centré sur l'humain

Mars 2025



À propos du Forum de Bamako sur le numérique et la cohésion sociale

Ce rapport est issu du Forum de Bamako sur le Numérique et la Cohésion sociale, un réseau réunissant des universitaires et des praticiens issus d'institutions gouvernementales, non gouvernementales et de la société civile. Son objectif est de créer un espace de collaboration multipartite, multidisciplinaire et plurisectoriel pour faire progresser le numérique et renforcer la cohésion sociale en Afrique de l'Ouest et au-delà. Le Forum est coordonné par Search for Common Ground et ses partenaires. Visitez son site ici : <https://bamakoforum.sfcg.org/page-daccueil/>

À propos des auteurs

Dr. Ilo Allaye Diall, Enseignant-Chercheur en Droit public à l'Université des Sciences Juridiques et Politiques de Bamako, Membre du Forum de Bamako sur le numérique et la cohésion sociale.

Francis Sala-Diakanda, Directeur Régional pour l'Afrique de l'Ouest, Search for Common Ground.

Lena Slachmuis, Conseillère Principale, Digital Peacebuilding, Search for Common Ground, Co-Présidente du Council on Tech and Social Cohesion.

Habibou Bako, Chargé de plaidoyer pour l'Afrique de l'Ouest, Search for Common Ground, Facilitateur du Forum de Bamako sur le Numérique et la cohésion sociale.

Remerciements

Les auteurs remercient tous ceux qui ont contribué à cet article en facilitant les entretiens et la révision. Ils expriment leur gratitude aux membres du Forum de Bamako sur le Numérique et la Cohésion sociale, ainsi qu'au personnel de Search for Common Ground, notamment les équipes Global Affairs and Partnerships (GAP) et Afrique de l'Ouest, incluant les bureaux du Burkina Faso, du Mali et du Niger. Cette publication a été rendue possible grâce à une subvention de la Carnegie Corporation of New York.

Notice

L'analyse présentée dans ce document ne reflète pas nécessairement la politique ou la position officielle des organisations auxquelles les auteurs sont affiliés. Les opinions exprimées relèvent de la seule responsabilité des auteurs.

Table des matières

1) Introduction	4
<hr/>	
2) Pourquoi réguler l'espace numérique au Sahel ?	6
<hr/>	
3) Panorama du cadre légal et réglementaire	9
Régulation de la cybercriminalité	10
Régulation de la protection des données personnelles	11
Régulation des communications électroniques	12
Une régulation numérique en quête de cohérence	13
<hr/>	
4) Vue d'ensemble du cadre institutionnel	14
<hr/>	
5) Initiatives de régulation portées par la société civile	16
<hr/>	
6) Co-construire une régulation numérique centrée sur l'humain	18
<hr/>	
7) Recommandations pour un modèle de régulation efficace centré sur l'humain	20
<hr/>	
8) Références	22

1) Introduction

L'essor des technologies numériques a permis à des millions de personnes d'échanger et de s'engager sur des enjeux locaux et mondiaux. Dans les pays sahéliens¹, cette tendance est très visible avec un taux croissant de pénétration d'internet qui est de 33,1% au Mali, 19,9% au Burkina Faso et 16,9% au Niger². Ces chiffres sont faibles comparativement à l'ensemble de la population des pays concernés, mais ils restent dans la moyenne africaine³ et celle des populations alphabétisées⁴.

Les réseaux sociaux, avec environ 6 millions d'utilisateurs sahéliens et une diaspora influente, modifient les dynamiques politiques, sociales et sécuritaires de la région.⁵ Cependant, cet espace numérique est devenu un champ de tensions et d'opportunités, où s'entrelacent les espoirs de connectivité avec des défis complexes en matière de sécurité, de paix, et de cohésion sociale⁶. Les plateformes numériques, initialement perçues comme des moteurs de dialogue et de partage, sont rapidement devenues des espaces de

dynamiques conflictuelles⁷.

Face à cette situation, plusieurs stratégies ont été adoptées pour mitiger les défis et amplifier les opportunités, comme la régulation, le fact-checking, l'éducation au numérique, et les initiatives communautaires de lutte contre la désinformation. Le fact-checking s'est imposé comme l'approche la plus connue. C'est l'ensemble des pratiques et outils permettant de vérifier l'exactitude d'une information, qu'il s'agisse de textes, images, vidéos ou rumeurs diffusées sur les réseaux sociaux⁸. Dans le contexte sahélien, le fact-checking est essentiellement mené par les associations des blogueurs⁹, les organes de presse, ou des associations plus spécialisées comme Africacheck¹⁰.

Une autre approche pour répondre aux défis est l'éducation aux médias et au numérique. Elle vise à développer les compétences des individus pour les rendre autonomes, critiques, et créatifs dans leur utilisation des médias¹¹. Elle englobe les contenus médiatiques et les langages (écrits, sonores, visuels), les formes et genres utilisés, ainsi que les contextes sociaux, économiques et culturels de la production, diffusion et réception des médias. Elle inclut également la compréhension des outils et plateformes médiatiques et de leurs enjeux. L'éducation aux médias est aussi assurée par les associations de blogueurs et les centres spécialisés, comme l'École de Journalisme et des Sci-

1. Par Sahel nous parlons du Burkina Faso, du Mali et du Niger. Plusieurs autres appellations existent et sont pertinentes comme le Sahel central, le Liptako Gourma ou de l'Alliance (la Confédération) des Etats du Sahel. Notre appellation n'occulte en rien la pertinence de ces appellations ou de l'étendue géographique qui peuvent inclure d'autres pays de l'atlantique à la méditerranée.

2. DataReportal : <https://datareportal.com/>

3. Internet penetration in Africa January 2024, by country, <https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/>

4. Niger (38,1% en 2022), Mali (30,76% en 2022), Burkina (34,49% en 2022), selon voir <https://atlasocio.com/classements/education/alphabetsation/classement-etats-par-taux-alphabetsation-afrique.php>, voir aussi : <https://www.datapandas.org/ranking/literacy-rate-by-country>

5. Johannes Bhanye and al., Social Media in the African Context: A Review Study on Benefits and Pitfalls, https://www.researchgate.net/publication/372382503_Social_Media_in_the_African_Context_A_Review_Study_on_Benefits_and_Pitfalls

6. Johannes Bhanye and al., *op. cit.*

7. Jiaxuan Yue et al., Conflit et espace en ligne au Sahel : défis et recommandations, Search for Common Ground, Juillet 2022, <https://documents.sfcg.org/wp-content/uploads/2022/07/Note-D-Analyse-Conflit-et-espace-en-ligne-au-Sahel-Juillet-2022.pdf>

8. Conseil de journaliste, <https://conseilsdejournalistes.com/fact-checking/01-le-fact-checking-quest-ce-que-cest/>

9. Search for Common Ground, You've been fact-checked: Malian media engaged for truth and peace, December 19, 2022, <https://documents.sfcg.org/youve-been-fact-checked/>

10. Site d'AfricaCheck, <https://africacheck.org/fr>

11. UNESCO, Media and Information Literacy, <https://www.unesco.org/en/media-information-literacy>

ences de la Communication du Mali.

La mobilisation des communautés¹² est un pilier essentiel dans la lutte contre la désinformation et les discours de haine en ligne. À travers des initiatives locales et internationales, les *cyber-gardiens*¹³ et *community stewards*¹⁴ jouent un rôle clé en modérant les contenus et en sensibilisant les utilisateurs aux risques du numérique. Leur travail repose sur une surveillance active des plateformes, le signalement des contenus problématiques et la promotion d'un dialogue constructif. Ces actions participatives ont démontré leur efficacité dans la réduction des tensions et la préservation de la cohésion sociale.

Enfin, la régulation du numérique, qui nous concerne dans le cadre de cette analyse, est une approche très répandue, mais peu comprise du fait de sa complexité et de la centralité de l'Etat dans l'approche. Elle fait référence aux lois, politiques et lignes directrices qui régissent l'utilisation, le contenu et les opérations des plateformes numériques, y compris les réseaux sociaux.

Au Sahel, la régulation des espaces numériques traite de la cybersécurité, les discours haineux en ligne, la désinformation, la protection des données et la vie privée. Cette étude vise à identifier les approches de régulation adoptées et à comprendre le contexte de leur mise en œuvre ainsi que des recommandations pour développer un cadre réglementaire adapté.

12. Search for Common Ground, RAPPORT D'ACTIVITÉS 2022: L'espoir perdue, https://www.sfcg.org/wp-content/uploads/2023/08/2022-Impact-report_EU_FR.pdf

13. Search for Common Ground, Final Evaluation, Cyber Guardians: Empowering youth to combat online hate speech in Sri Lanka, February 2020, https://documents.sfcg.org/wp-content/uploads/2020/05/SFCG-Sri_Lanka_Cyber_Guardians_Final_Evaluation_2020.pdf

14. Institutional Learning Team, "Community Stewards and Social Cohesion in Digital Spaces." Search for Common Ground (January 2023), <https://cnxus.org/wp-content/uploads/2023/02/SFCG-Community-Stewards-and-Social-Cohesion-in-Digital-Spaces.pdf>

2) Pourquoi réguler l'espace numérique au Sahel ?

L'espace numérique désigne l'ensemble des environnements virtuels interconnectés par les technologies de l'information et de la communication (TIC)¹⁵. Il comprend des plateformes en ligne telles que les réseaux sociaux, les sites web, les applications mobiles et les services de communication électronique. Dans le contexte sahélien, cet espace numérique est devenu un terrain d'expression politique et sociale où se croisent opportunités et défis¹⁶. Il joue un rôle central dans la diffusion d'informations, la mobilisation citoyenne et l'échange d'idées, mais il est également marqué par des phénomènes de désinformation, de discours haineux et de manipulation de l'opinion publique¹⁷.

En effet, depuis une décennie et demie, le Sahel fait face à des crises sociopolitiques et sécuritaires exacerbées par des narratifs polarisants^{18 19}. La place des réseaux sociaux, et de l'espace numérique de manière générale, comme amplificateurs est particulière-

ment notable²⁰. Par exemple dans les protestations et débats populaires ayant conduit aux changements de régimes au Mali (2020, 2021), au Burkina Faso (2022) et au Niger (2023) ont largement été amplifiées par l'espace numérique²¹. Les tensions diplomatiques régionales et internationales, ainsi que l'aggravation de la situation sécuritaire avec la montée des groupes armés extrémistes, font l'objet de nombreux messages partagés. Ainsi, les réseaux sociaux deviennent un espace privilégié pour les débats politiques, les critiques sociales, mais aussi pour la désinformation, la manipulation et la propagation de discours haineux

La désinformation, qui se définit comme la diffusion intentionnelle d'informations fausses ou déformées, a pris une ampleur considérable au Sahel²². Les acteurs cherchant à manipuler l'opinion publique, qu'ils soient locaux ou transnationaux, utilisent les réseaux sociaux pour promouvoir des récits biaisés, enflammer les tensions ethniques et politiques, ou encore miner la confiance des populations envers leurs gouvernements²³. Cette propagation de fausses nouvelles est souvent accompagnée d'un autre phénomène inquiétant : la montée des discours haineux et des incitations à la violence, en particulier de la part de groupes armés violents qui exploitent ces plateformes pour recruter, diffuser leur propagande et exacerber les tensions locales.

L'espace numérique peut aussi favoriser les violences basées sur le genre²⁴. Étant donné que Facebook et WhatsApp sont les plateformes les plus couram-

15. Admire Mare aborde "les espaces/platformes numériques comme des infrastructures planétaires (réseaux, systèmes, technologies) avec des affordances, des cultures, des logiques opérationnelles et des caractéristiques sociotechniques distinctes. Les espaces numériques tels que YouTube, Facebook, MySpace, WhatsApp et Twitter sont des infrastructures planétaires compatibles caractérisées par une convergence de différents systèmes, protocoles et réseaux. Les espaces numériques favorisent de nouvelles formes de connectivité, de communication dialogique, d'engagement politique, de transactions économiques et de production culturelle." Voir, Admire Mare, *Espaces numériques, droits et responsabilités*, Friedrich Ebert- Stiftung, Janvier, 2023, https://library.fes.de/pdf-files/bue-ros/africa-media/20189.pdf?utm_source=chatgpt.com

16. Jiaxuan Yue et al., *op.cit.*

17. Dalanda Moukala et Fatima Al-Ansar, *Les femmes sahéliennes dans les espaces numériques*, Search for Common Ground, June 2024, <https://www.sfcg.org/wp-content/uploads/2024/09/20240909-Sahelian-women-in-Digital-Spaces-final-copy-FRE.pdf>

18. UNDP, *Sahel human development report 2023*, January 2024, <https://www.undp.org/africa/publications/sahel-human-development-report-2023>

19. Eduardo Albrecht, Eleonore Fournier-Tombs, and Rebecca Brubaker, *Disinformation and Peacebuilding in Sub-Saharan Africa: Security Implications of AI-Altered Information Environments* (New York: United Nations University and Interpeace, 2024)

20. Habibou Bako, *Réseaux sociaux et désinformation au Sahel*, Bulletin Francopaix, Vol. 7, n° 10, Décembre 2022, <https://dandurand.uqam.ca/wp-content/uploads/2022/12/2022-12-Bulletin.pdf>

21. Habibou Bako, *op. cit.*

22. Eduardo Albrecht, *et al. op. cit.*

23. Habibou Bako, *op. cit.*

24. Dalanda Moukala et Fatima Al-Ansar, *op. cit.*

ment utilisées dans la région, elles représentent des espaces propices à la propagation de violences basées sur le genre facilitées par la technologie (VBGFT)²⁵. La VBGFT fait référence aux actes de violence, de harcèlement ou d'abus commis à l'encontre de personnes, surtout des femmes et des filles, à travers l'utilisation des technologies numériques telles que les réseaux sociaux, les applications de messagerie, les mails et autres plateformes en ligne. Cela inclut notamment le cyberharcèlement, la diffusion non consentie de contenus intimes en ligne (souvent désigné sous le terme « revenge porn ») ainsi que la coercition numérique. Ces exemples sont édifiants à ce sujet²⁶.

Exemple 1 (violence communautaire) : En 2016, après une attaque contre des chasseurs par des groupes armés, une des victimes, Théodore Somboro, gravement blessé, a envoyé un message audio via un groupe WhatsApp dans lequel il exprimait des appels à la vengeance. Ce message, relayé sur les réseaux sociaux, a été amplifié par certains acteurs violents, contribuant à intensifier les tensions entre les communautés peules et celles liées à la confrérie des chasseurs, notamment les Dogons et les Bambaras. Ces événements ont alimenté un conflit avec une forte dimension communautaire dans le centre du pays²⁷.

Exemple 2 (tension politique) : Le 10 février et le 5 avril 2019, la retransmission en direct des propos tenus par l'imam Dicko lors de ses meetings, respectivement au stade du 26 mars et à la place de l'Indépendance, a largement contribué à attiser le climat politique. Lors de ces événements, l'imam avait publiquement appelé le Président de la République à révoquer le Premier ministre Soumeylou Boubèye Maïga, l'accusant d'instrumentaliser le conflit au Centre du pays. Il avait également évoqué le déplacement forcé de certaines commu-

nautés autochtones, contraintes d'abandonner les terres de leurs ancêtres au profit d'autres groupes. Ces déclarations ont rapidement été diffusées et amplifiées sur les réseaux sociaux, notamment sur Facebook, où elles ont été interprétées et commentées par des chroniqueurs d'obédience communautaire. Ce phénomène a contribué à la montée des tensions politiques et sociales, et est l'une des causes ayant mené au renversement du régime du Président Ibrahim Boubacar Keita.

Exemple 3 (harcèlement sexuel) : Voici le témoignage d'une jeune femme nigrienne : « Récemment, j'ai partagé sur ma page Facebook un message que j'ai reçu d'un inconnu : on m'a proposé de me prostituer pendant le mois sacré du Ramadan pour 50 000 francs CFA. J'ai partagé les captures d'écran sur ma page et de nombreuses autres jeunes femmes ont répondu dans les commentaires avec des captures d'écran de messages similaires provenant de la même personne. Une plainte a été déposée. »²⁸

Face aux défis posés par la désinformation, les discours haineux et la manipulation de l'opinion publique et les VBGFT, les États sahéliens ont dû adapter leurs réponses en exploitant le principal levier institutionnel à leur disposition : la régulation. La régulation du numérique désigne l'ensemble des lois, politiques et mécanismes mis en place pour encadrer l'usage des technologies de l'information et de la communication²⁹. Elle englobe plusieurs domaines clés : la cybersécurité, la protection des données personnelles, la modération des contenus et la gouvernance des plateformes numériques³⁰.

Dès lors, l'efficacité de la régulation dépend non seulement de son cadre juridique, mais aussi de sa capacité à être appliquée de manière équilibrée et

25. Dalanda Moukala et Fatima Al-Ansar, *op. cit.*

26. Voir la rubrique « An k'a sègèsègè » de l'Association des Blogueurs du Mali, <https://assoblog.org/category/verification-des-faits/>

27. Modibo Galy Cissé, Les enjeux de la violence dite communautaire au Centre du Mali comme facteur important dans la crise actuelle, CODESRIA Bulletin, Nos 5&6, 2020 Page 26, <https://journals.codesria.org/index.php/codesriabulletin/article/view/129/112>

28. Dalanda Moukala et Fatima Al-Ansar, *op. cit.*

29. Tahirou Koné l'aborde comme « une science des règles, de la manière dont les règles peuvent permettre à un groupe de structurer et de mettre en œuvre une action collective ». Voir, Tahirou Koné, « Plateforme numérique et (de) régulation sociale en Afrique francophone », Communication, technologies et développement [En ligne], 13 | 2023, mis en ligne le 08 octobre 2023, consulté le 26 janvier 2025. URL : <http://journals.openedition.org/ctd/8659> ; DOI : <https://doi.org/10.4000/ctd.8659>

30. UNESCO, Principes pour la gouvernance des plateformes numériques, 2023, <https://unesdoc.unesco.org/ark:/48223/pf0000387359/PDF/387359fre.pdf.multi>

adaptée aux réalités locales, en impliquant tous les acteurs concernés, y compris la société civile et les entreprises technologiques³¹. Ces régulations visent à limiter les abus, tout en protégeant les libertés fondamentales. Cependant, leur application soulève parfois des préoccupations quant aux risques de restrictions excessives de la liberté d'expression³².

31. Tahirou Koné, « Plateforme numérique et (de) régulation sociale en Afrique francophone », Communication, technologies et développement [En ligne], 13 | 2023, mis en ligne le 08 octobre 2023, consulté le 26 janvier 2025. URL : <http://journals.openedition.org/ctd/8659> ; DOI : <https://doi.org/10.4000/ctd.8659>

32. Visite au Niger - Rapport du Rapporteur spécial sur les droits à la liberté de réunion pacifique et à la liberté d'association, Clément Nyaletossi Voule (A/HRC/50/23/Add.2) (Advance Unedited Version), <https://reliefweb.int/report/niger/visite-au-niger-rapport-du-rapporteur-special-sur-les-droits-la-liberte-de-reunion-pacifique-et-la-liberte-dassociation-clement-nyaletossi-voule-ahrc5023add2-advance-unedited-version>

3) Panorama du cadre légal et réglementaire

De manière générale, les États sahéliens se sont appuyés essentiellement sur les cadres communautaires et continentaux établis par la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO)³³, l'Union économique et monétaire ouest-africaine (UEMOA)³⁴ et l'Union Africaine (UA)³⁵ pour formuler leurs propres lois en matière de cybercriminalité, de protection des données personnelles, et de régulation des communications électroniques. Ces législations visent à la fois à lutter contre les dérives en ligne et à promouvoir un environnement numérique sécurisé et inclusif.

Lois	<p>Principaux textes portant sur la cybercriminalité</p> <ul style="list-style-type: none"> • Loi N° 2019-056 sur la cybersécurité et la protection des données personnelles en 2019 au Mali • Loi N° 2019-33 sur la répression de la cybercriminalité en 2019 au Niger • Loi N°045-2009 visant à la protection des infrastructures et les données sensibles contre les menaces numériques croissantes en 2019 au Burkina Faso • Loi n° 025-2018 du 31 mai 2018 portant code pénal au Burkina Faso • Loi N°2024-027 du 13 décembre 2024 portant code pénal du Mali • Code pénal et code de procédure pénale du Niger, Ministère de la justice, 2018
	<p>Principaux textes portant sur la protection des données à caractère personnel</p> <ul style="list-style-type: none"> • Loi N°010-2004 en 2004 pour protéger les droits des personnes en matière de données personnelles au Burkina Faso • Loi N°2013-015 portant sur la protection des données à caractère personnel au Mali • Loi N°2017-28 en 2017 encadre la collecte, le traitement, et l'utilisation des données personnelles, établissant des normes pour le traitement des informations sensibles et leur protection au Niger • Loi n° 025-2018 du 31 mai 2018 portant code pénal au Burkina Faso • Loi N°2024-027 du 13 décembre 2024 portant code pénal du Mali • Code pénal et code de procédure pénale du Niger, Ministère de la justice, 2018
	<p>Principaux textes portant sur la communication électronique</p> <ul style="list-style-type: none"> • Décret N° 2019-0521, modifiant la loi de 2008 sur la réglementation des réseaux et services de communications électroniques au Burkina Faso • Loi N° 2017-016 sur les services postaux régulant les activités postales au Mali • Loi N°2018-45 de 2018 sur les communications électroniques au Niger • Loi n° 025-2018 du 31 mai 2018 portant code pénal au Burkina Faso • Loi N°2024-027 du 13 décembre 2024 portant code pénal du Mali • Code pénal et code de procédure pénale du Niger, Ministère de la justice, 2018

33. ECOWAS Cybersecurity Agenda "Enhancing Cybersecurity ECOWAS Region", <https://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/ECOWAS-Cybersecurity-Agenda-GFCE.pdf>

34. UEMOA, Evaluation des usages numériques et politiques nationales en matière d'utilisation de masse du numérique dans l'espace UEMOA, Rapport provisoire 10 juillet 2020, https://www.uemoa.int/sites/default/files/bibliotheque/evaluation-des-usages-numeriques-et-politiques-nationales-en-matiere-dutilisation-de-masse-du_0.pdf

35. AU Policy and Regulation Initiative for Digital Africa (PRIDA), Convention de l'Union Africaine du 27 juin 2014 sur la cybersécurité; Déclaration d'Abidjan du 22 février 2012; Déclaration d'Addis Abeba du 22 juin 2012 sur l'harmonisation des cyber législations en Afrique

Régulation de la cybercriminalité

La régulation des réseaux sociaux et de l'espace numérique est un domaine en pleine évolution au Sahel, souvent en décalage avec les défis posés par la croissance rapide de ces technologies³⁶. La plus récente catégorie de la régulation concerne la cybercriminalité. Avec l'essor d'Internet et la numérisation croissante des services, les cyberattaques sont devenues une menace majeure, touchant aussi bien les particuliers que les institutions publiques et privées. C'est dans ce cadre que les États ont mis en place des dispositifs législatifs et réglementaires sur la cybersécurité. La cybercriminalité englobe un large éventail d'infractions pénales commises à l'aide de réseaux de télécommunication ou de systèmes d'information, ou contre ces réseaux et systèmes³⁷. Ces infractions peuvent inclure l'accès illégal à des systèmes informatiques, l'interception de données, la diffusion de contenus illicites, et bien plus. Les législations nationales cherchent à encadrer ces activités, tout en respectant les droits et libertés individuelles.

En la matière, il existe des cadres juridiques distincts pour les trois pays sahéliens. Au Niger, la loi n°2019-33 du 03 juillet 2019 portant répression de la cybercriminalité au Niger³⁸ sanctionne les infractions spécifiques aux technologies de l'information et de la communication, incluant les atteintes aux systèmes informatiques et aux données, ainsi que d'autres abus. Au Mali, la loi n°2019-056 du 05 décembre 2019 portant répression de la cybercriminalité³⁹ transpose la directive de la

36. APDP Mali, Rencontre des présidents des autorités de protection des données personnelles et les ministres de la communication et de l'économie numérique du Burkina Faso, Mali et Niger, 16 Décembre 2024, <https://apdp.ml/en/rencontre-des-presidents-des-autorites-de-protection-des-donnees-personnelles-et-les-ministres-1>, ou MaliActu, Le ministre de la communication appelle les régulateurs des télécommunications à accorder une attention au développement du secteur, 22 novembre 2023, <https://maliactu.net/le-ministre-de-la-communication-lassemble-gnrale-des-rgulateurs-de-tlcommunications-de-lafrique-de-louest-jinvite-les-rgulateurs-des-tlcommunications-accorder-une-attention-au-dveloppement-de-ce-se/>

37. ECOWAS Directive and related texts on Cyber legislation, <https://rm.coe.int/-3148-3-2-3-nigeria-ecowas-o-3-auc-moctar-yedaly-pdf/1680748652>

38. Loi n° 2019-33 du 03 juillet 2019, portant répression de la cybercriminalité au Niger, <https://www.africa-laws.org/Niger/criminal%20law/Loi%20n%202019-33%20portant%20répression%20de%20la%20cyber%20criminalité%20au%20Niger.pdf>

39. Loi n°2019-056 du 05 décembre 2019 loi 2019-056 portant répression de la cybercriminalité, <https://amrtp.ml/download/loi-n2019-056-du-05-decembre-2019-portant-repression-de-la-cybercriminalite/>

CEDEAO et s'applique à toute infraction commise au moyen des technologies de l'information et de la communication. Au Burkina Faso, la loi n°045-2009 du 10 novembre 2009⁴⁰ régleme les services et les transactions électroniques, en mettant l'accent sur la protection des données et la sécurité des transactions.

Les infractions phares abordées dans les différentes lois incluent l'accès frauduleux ou illégal à un système informatique, le maintien frauduleux dans un système, l'entrave au fonctionnement d'un système informatique, l'introduction frauduleuse de données, l'interception illégale de données, l'atteinte à l'intégrité des données, la falsification informatique et l'usage de données falsifiées. Les lois traitent également de la fraude informatique, de l'usurpation d'identité numérique, et des infractions liées à la pornographie enfantine. De plus, des infractions telles que l'escroquerie, l'abus de confiance, le recel, l'extorsion et le chantage portant sur des données informatiques sont également criminalisées. Les lois abordent aussi les délits de presse commis par voie électronique, les actes racistes, xénophobes, les menaces et injures proférées par le biais de systèmes d'information.

« Quiconque crée, télécharge, diffuse ou met à disposition, sous quelque forme que ce soit, du matériel raciste et xénophobe, par le biais d'un système d'information est puni de la réclusion de cinq à dix ans et d'une amende de 1 000.000 à 10.000.000 de francs CFA. Article 19, Loi N° 2019-056 du 5 décembre 2019 portant répression de la cybercriminalité au Mali.

« Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et de un million (1 000 000) à cinq millions (5 000 000) de francs CFA d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information. » Article 31, Loi n° 2019-33 du 3 juillet 2019 sur la répression de la cybercriminalité au Niger.

40. Loi n° 045-2009/AN du 10 novembre 2009 portant réglementation des services et des transactions électroniques au Burkina Faso, <https://www.arcep.bf/download/loi-10-11-2009-n045-2009/>

Régulation de la protection des données personnelles

Le deuxième domaine de la régulation concerne la protection des données personnelles. La protection des données à caractère personnel vise à garantir que les informations relatives à une personne physique identifiée ou identifiable soient traitées de manière transparente, sécurisée et conforme à la loi⁴¹.

Au Niger, la protection des données personnelles est encadrée par la loi n° 2017-28 du 3 mai 2017, modifiée et complétée par la loi n° 2019-71 du 24 décembre 2019⁴². Cette législation a institué la Haute Autorité de Protection des Données à caractère Personnel (HAPDP), une autorité administrative indépendante chargée de veiller au respect des droits des personnes en matière de traitement des données. Au Mali, la loi n° 2013-015 du 21 mai 2013⁴³ régit la protection des données personnelles, et l'Autorité de Protection des Données à caractère Personnel (APDP) est l'organisme responsable de son application. Au Burkina Faso, la loi n° 001-2021 du 30 mars 2021⁴⁴ a été adoptée pour renforcer la protection des personnes à l'égard du traitement des données à caractère personnel, remplaçant ainsi la précédente loi n° 010-2004 du 20 avril 2004. La Commission de l'Informatique et des Libertés (CIL), créée en 2004, est l'autorité chargée de veiller à la conformité des traitements de données dans le pays.

Les législations de ces trois pays sahéliens définissent plusieurs infractions majeures liées à la protection des données personnelles. Parmi celles-ci figurent le traitement illicite des données, c'est-à-dire la collecte, l'utilisation ou la divulgation de données sans consen-

tement ou sans base légale appropriée, et l'atteinte à la vie privée par la divulgation non autorisée d'informations sensibles. De plus, le non-respect des obligations de sécurité, telles que l'absence de mesures adéquates pour protéger les données contre les accès non autorisés ou les violations, constitue une infraction notable. Ces lois prévoient des sanctions pour les responsables de traitement qui ne respectent pas les principes établis, afin de garantir une protection effective des données personnelles des citoyens.

« Hors les cas prévus par la loi, le fait de mettre ou de conserver en mémoire informatisée les données nominatives qui, directement ou indirectement, font apparaître les origines raciales, ethniques ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes est puni d'un emprisonnement de trois (03) mois à cinq (05) ans et d'une amende de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA. » L'article 51 de la loi sur la protection des données à caractère personnel du Burkina Faso (LOI N° 010-2004/AN).

« Les données à caractère personnel doivent : être collectées et traitées, de manière loyale, licite et non frauduleuse pour des finalités déterminées, explicites et légitimes ; être adéquates, proportionnées et pertinentes au regard des finalités pour lesquelles elles sont collectées ou utilisées ; être exactes, complètes et si nécessaire mises à jour ; être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées ou utilisées. » Article 7, Loi n° 2013-015 du 21 mai 2013 portant protection des données à caractère personnel en République du Mali

41. ECOWAS, Supplementary Act on personal data protection within ECOWAS, 16th February 2010 <https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf>

42. Loi n° 2019-71 du 24 décembre 2019 relative à la protection des données à caractère personnel, <https://www.hapdp.ne/legislation-nationale>

43. Au Mali, la loi n° 2013-015 du 21 mai 2013 régit la protection des données personnelles, <https://amrtp.ml/download/loi-n2013-015-du-21-mai-2013-portant-protection-des-donnees-a-caractere-personnel-en-republique-du-mali/>

44. Loi n°001-2021/An du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel, <https://academiedepolice.bf/index.php/telechargement/category/43-cybercriminalite?download=190:loi-portant-protection-des-personnes-a-l-egard-du-traitement-des-donnees-a-caractere-personnel>

Régulation des communications électroniques

Enfin, la communication électronique désigne quant à elle l'ensemble des moyens technologiques permettant la transmission, l'émission et la réception de signaux, de sons, d'images, de données et de messages par le biais de réseaux de télécommunications⁴⁵. Elle englobe divers services tels que la téléphonie mobile, internet, la radiodiffusion et les services numériques associés. Dans un monde de plus en plus connecté, ces technologies jouent un rôle crucial dans le développement économique, l'accès à l'information et l'amélioration des interactions sociales. Les États s'efforcent donc de réguler ce secteur stratégique en garantissant l'accès universel aux services de communication tout en veillant à la protection des données, à la cybersécurité et à la concurrence équitable entre les acteurs du marché.

Les cadres législatifs du Niger, du Mali et du Burkina Faso ont été mis en place pour réguler le secteur des communications électroniques et garantir un accès équitable aux services de télécommunications. Au Niger, la Loi n°2018-45 du 12 juillet 2018 établit les conditions d'exploitation des réseaux et de fourniture des services électroniques⁴⁶, en mettant l'accent sur la libéralisation du secteur et la promotion d'un environnement concurrentiel. Au Mali, la Loi n°2017-016 du 12 juin 2017 encadre la régulation du secteur postal et de la communication⁴⁷, en précisant les obligations des opérateurs en matière de couverture territoriale et de qualité de service. Au Burkina Faso, la Loi n°061-2008, modifiée par la Loi n°09-2019 du 23 avril 2019, régit les réseaux et services de communication électronique⁴⁸ en précisant les conditions d'attribution des licences et

les responsabilités des fournisseurs.

Les législations des trois pays définissent plusieurs infractions majeures liées aux communications électroniques. Parmi celles-ci figurent l'exploitation illégale de réseaux et services de télécommunications sans autorisation préalable, la fraude aux communications (telle que la revente illégale de services ou la manipulation frauduleuse de données), ainsi que les atteintes à la cybersécurité et à la protection des données personnelles. Au Niger, la réglementation prévoit des sanctions contre la diffusion de contenus illicites, la cybercriminalité et l'utilisation frauduleuse des infrastructures de communication. Au Mali, la législation met particulièrement l'accent sur le respect du secret des correspondances et la protection des consommateurs contre les pratiques abusives. Enfin, au Burkina Faso, les infractions incluent l'utilisation non autorisée de ressources rares (comme les fréquences et numéros), ainsi que la violation des règles d'interconnexion entre opérateurs. Ces lois s'inscrivent dans un cadre de protection des utilisateurs et de régulation efficace du marché des télécommunications.

« Les opérateurs des réseaux et services ouverts au public ainsi que leurs personnels sont tenus de respecter le secret des correspondances. Toutes les transmissions par les moyens de communications électroniques devront garantir la confidentialité, sans préjudice des pouvoirs d'investigation de la justice et de la sûreté de l'Etat. Article 35, de la Loi N° 061-2008/AN, Burkina Faso.

« La présente loi a pour objet: de garantir un meilleur fonctionnement et une meilleure exploitation du service public des postes afin d'offrir aux usagers/clients des services de qualité à un prix accessible sur l'ensemble du territoire national; d'améliorer la densité du réseau postal public existant, l'élargissement de la couverture géographique du pays et le développement des services postaux dans les zones rurales; d'assurer la séparation entre la fonction de régulation et celle d'établissement et/ou d'exploitation des réseaux et services postaux; d'assurer le respect des principes d'égalité de traitement des usagers/clients, de

45. CEDEAO - Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, <https://www.droit-afrique.com/upload/doc/uemoa/CEDEAO-Acte-2010-02-transactions-elec-troniques.pdf>

46. Loi n°2018 45 du 12 juillet 2018 portant réglementation des communications électroniques, <https://ictpolicyafrica.org/en/document/f9bpankdsa>

47. Loi N°2017-016 du 12 juin 2017 portant Règlementation du secteur Postal, <https://amrtp.ml/download/loi-n2017-016-du-12-juin-2017-portant-reglementation-du-secteur-postal/>

48. Loi n° 061 – 2008/an du 27 novembre 2008 portant réglementation générale des réseaux et services de communications électroniques au Burkina Faso, https://www.arcep.bf/download-category/loi_n061-2008/

continuité et d'adaptabilité du service public des postes; d'assurer la fourniture du service postal universel; de renforcer le rôle du secteur postal dans le développement économique; d'assurer la transparence des comptes des opérateurs postaux; d'assurer le respect des règles d'une concurrence saine et loyale; de garantir le secret de la correspondance; d'assurer le respect des conventions et accords internationaux ratifiés par le Mali en matière postale. Article 5 de la Loi N°2017-016 portant sur les services postaux en République du Mali.

Une régulation numérique en quête de cohérence

Les législations en matière de cybercriminalité, de protection des données personnelles, et de communication électronique s'articulent souvent de manière complémentaire au sein d'un même pays. Elles s'appuient généralement sur les codes pénaux, qui servent de cadre juridique de référence. Toutefois, cette complémentarité se transforme parfois en un facteur de fragmentation, rendant l'application des textes complexe et peu cohérente.

L'un des principaux défis de cette régulation réside dans son inadaptation à l'évolution rapide des technologies, notamment avec l'essor de l'intelligence artificielle et des nouvelles formes de criminalité numérique. Face à ces transformations, les législations peinent à suivre le rythme des innovations, entraînant des lacunes et des incohérences dans leur mise en œuvre.

En outre, la méconnaissance des textes juridiques, la fracture numérique et les limites infrastructurelles exacerbent ces difficultés, rendant l'application uniforme des régulations particulièrement ardue. Ces obstacles sont d'autant plus marqués dans les zones rurales et instables, où l'accès aux technologies est

limité et les moyens de contrôle insuffisants.

Ces réglementations sont fréquemment critiquées par les utilisateurs de l'espace numérique, notamment en ce qui concerne leur impact sur la liberté d'expression⁴⁹. De nombreuses pratiques gouvernementales soulèvent des préoccupations en la matière, comme les coupures d'Internet lors des périodes électorales, la censure de certaines pages sur les réseaux sociaux ou encore l'emprisonnement de journalistes, blogueurs et autres acteurs du numérique⁵⁰.

L'incrimination de la cybercriminalité dans les codes pénaux des pays du Sahel constitue également un enjeu sensible. En effet, la préservation de l'ordre public, souvent évoquée dans ces textes, demeure une notion floue et sujette à interprétation pour beaucoup d'utilisateurs de l'espace numérique. Cette ambiguïté juridique ouvre la porte à des restrictions excessives et à un usage détourné des lois pour limiter la liberté d'expression sous couvert de sécurité⁵¹.

L'analyse du cadre légal et réglementaire révèle ainsi une diversité de lois et de régulations, adaptées à des contextes locaux spécifiques mais parfois insuffisantes pour répondre aux défis actuels. Une meilleure harmonisation et une approche plus concertée de la régulation numérique apparaissent donc nécessaires pour garantir un équilibre entre sécurité, respect des droits fondamentaux et innovation technologique. La mise en œuvre de ce cadre légal a largement été l'œuvre d'institutions étatiques spécialisées.

49. AFD, Rapport 2023 sur les libertés numériques dans les pays d'Afrique francophone, <https://cnxus.org/wp-content/uploads/2023/06/rapport-libertes-numeriques-pays-franco-phones-afrique.pdf>

50. Sandrine Blanchard, La liberté d'expression en danger dans le Sahel, 13 juin 2024, <https://www.dw.com/fr/mali-niger-burkina-repression-de-la-liberte-de-la-presse-et-dexpression-bocoum/a-69355843>

51. Sandrine Blanchard, *op. cit.*

4) Vue d'ensemble du cadre institutionnel

En plus du dispositif légal, la régulation et les textes sur le numérique au Sahel s'appuient sur plusieurs institutions créées pour encadrer, protéger et accompagner le développement du secteur numérique. Chaque institution joue un rôle spécifique, mais leur coexistence soulève à la fois des opportunités et des défis.

<p>Communication et postes</p> <ul style="list-style-type: none"> • Autorité de Régulation des Communications Électroniques et de la Poste (ARCEP) au Burkina et au Niger • Autorité Malienne de Régulation des Télécommunications/TIC et Postes (AMRTP) au Mali 	<p>Données personnelles</p> <ul style="list-style-type: none"> • Commission de l'Information et des Libertés (CIL) au Burkina Faso • Autorité de Protection des Données à Caractère Personnel (APDP) au Mali; • Haute Autorité de Protection des Données à Caractère Personnel (HAPDP) au Niger
<p>Communication et média</p> <ul style="list-style-type: none"> • Conseil Supérieur de la Communication (CSC) au Burkina Faso et au Niger • Haute Autorité de la Communication (HAC) au Mali • Conseil supérieur de la communication • Maison de la presse 	<p>Cybercriminalité</p> <ul style="list-style-type: none"> • Brigade Centrale de Lutte contre la Cybercriminalité au Burkina faso • Pôle spécialisé en cybercriminalité au Mali • Pôles et procureurs spécialisés au Niger et au Mali

Tout d'abord, il faut noter que les autorités de régulation des communications électroniques sont des acteurs clés dans la gestion de l'espace numérique. Au Burkina Faso et au Niger, cette mission est assurée par l'Autorité de Régulation des Communications Électroniques et de la Poste (ARCEP), tandis qu'au Mali, c'est l'Autorité Malienne de Régulation des Télécommunications et Postes (AMRTP) qui en est responsable⁵². Ces institutions délivrent les licences, régulent les opérateurs télécoms, supervisent les services postaux et disposent d'un pouvoir de sanction pour garantir le respect des normes. Elles jouent ainsi un rôle central dans le maintien de la compétitivité et l'adaptation du cadre juridique à un secteur numérique en expansion.

« Notre mission est triple et elle consiste à : veiller sur l'intérêt de l'État dans le domaine des télécommunications et des technologies de l'information et de la communication ; veiller au respect des textes légaux et à l'égalité de traitement des opérateurs en assurant une concurrence saine et loyale; et à veiller au droit des consommateurs dans la délivrance des services ». (Propos d'un haut cadre d'institution de régulation, 2024).

52. Sites de l'ARCEP Niger (<https://arcep.ne/>), de l'ARCEP Burkina Faso (<https://www.arcep.bf/>) et de l'AMRTP Mali (<https://amrtp.ml/>)

La protection des données personnelles est également une priorité pour les États sahéliens, qui ont mis en place des institutions dédiées. Au Mali, c'est l'Autorité de Protection des Données à Caractère Personnel (APDP) qui en a la charge. Au Burkina Faso, cette mission est assurée par la Commission de l'Information et des Libertés (CIL), tandis qu'au Niger, c'est la Haute Autorité de Protection des Données à Caractère Personnel (HAPDP) qui joue ce rôle⁵³. Ces organismes veillent à garantir que les informations privées des citoyens soient protégées et régulent leur utilisation par les entreprises et les services publics. Ils disposent aussi d'un pouvoir de sanction en cas d'infraction aux règles de gestion des données personnelles.

« Je pense qu'au regard des difficultés auxquelles nous sommes confrontés, les institutions nationales ont vocation à se retrouver dans un cadre plus globalisant offrant les moyens nécessaires pour une véritable régulation ». (Propos d'un haut cadre d'une institution de protection des données à caractère personnel, 2024).

En matière de communication, de média et des réseaux sociaux, chaque pays sahélien dispose aussi d'une instance de régulation. La Haute Autorité de la Communication (HAC) est chargée de cette mission au Mali, tandis qu'au Burkina Faso et au Niger, cette responsabilité incombe au Conseil Supérieur de la Communication (CSC)⁵⁴. Ces institutions veillent à garantir la liberté de la presse tout en régulant les médias audiovisuels et numériques pour assurer un équilibre entre la liberté d'expression et la responsabilité des acteurs médiatiques.

« La presse en ligne fait aussi partie du numérique ». (Propos d'un haut cadre d'une institution de communication, 2024).

Les institutions judiciaires ont également un rôle important dans la régulation du numérique. Au Mali, un Pôle spécialisé en cybercriminalité a été mis en place, tandis qu'au Burkina Faso, la Brigade Centrale de Lutte con-

tre la Cybercriminalité est chargée des enquêtes dans ce domaine. Au Niger, les procureurs de la République disposent de prérogatives spécifiques pour traiter les infractions commises par des moyens électroniques. Ces structures permettent de lutter contre diverses menaces numériques, telles que les cyberattaques, la fraude en ligne et d'autres infractions liées à l'utilisation des technologies de l'information.

« Les moyens de sanction dont nous disposons sont administratifs, généralement nous ne judiciaireons que quand les intéressés refusent de s'exécuter ». (Propos d'un haut cadre d'une institution de protection de données, 2024).

Ces différentes institutions offrent de nombreuses opportunités pour les États du Sahel. Elles contribuent à la structuration d'un cadre favorable au développement du numérique, garantissent la protection des citoyens et assurent une régulation adaptée aux évolutions technologiques. Elles participent aussi à la transparence et à l'équité dans la gestion des télécommunications et des données personnelles, tout en renforçant la sécurité face aux menaces numériques.

Cependant, des défis persistent. Le principal problème est la multiplication des organes de régulation, qui entraîne une fragmentation des ressources humaines et financières, déjà limitées. Cette dispersion nuit à l'efficacité des actions de régulation. L'absence de coordination entre les différentes entités peut également engendrer des chevauchements de compétences, rendant la bureaucratie plus lourde et ralentissant les processus décisionnels. Enfin, l'autonomie des institutions reste parfois insuffisante, notamment en raison des pressions politiques, ce qui peut compromettre leur capacité à prendre des décisions indépendantes et impartiales. En plus des structures étatiques, la société civile sahélienne joue un rôle clé dans la mise en place d'une régulation alternative et complémentaire.

53. Sites de l'APDP du Mali (<https://apdp.ml/>), de la CIL du Burkina Faso et de la HAPDP du Niger (<https://www.hapdp.ne/>)

54. Sites de la HAC du Mali (<https://www.hac.ml/>), du CSC du Niger (<https://www.csc-niger.ne/>) et du CSC du Burkina Faso (<https://www.csc.bf/>)

5) Initiatives de régulation portées par la société civile

La régulation de l'espace numérique ne repose pas uniquement sur les cadres législatifs et institutionnels mis en place par les États. La société civile joue un rôle fondamental dans l'élaboration de normes éthiques et de pratiques visant à promouvoir un usage responsable des plateformes numériques⁵⁵. Cette dynamique s'explique par la nécessité de concilier liberté d'expression, protection des droits fondamentaux et lutte contre la désinformation, dans un environnement où les États adoptent parfois des approches coercitives. À travers l'élaboration de chartes et codes de conduite, la société civile sahélienne a mis en place des mécanismes d'autorégulation qui viennent compléter et, dans certains cas, pallier les lacunes des cadres juridiques nationaux⁵⁶.

L'adoption des chartes et codes de conduite des blogueurs au Mali, au Burkina Faso et au Niger illustre la volonté des acteurs du numérique de structurer leur profession et de limiter les dérives sur les réseaux sociaux. Au Mali, la Charte des Blogueurs, adoptée sous l'égide de l'Association des Blogueurs du Mali (ABM) et Doniblog, repose sur des principes fondamentaux tels que la responsabilité, la crédibilité, la diversité des opinions et le respect des droits humains⁵⁷. Ce document encourage les blogueurs maliens à vérifier systématiquement leurs sources, à éviter les propos incitant à la haine et à privilégier une information qui contribue à la cohésion sociale et à la paix.

55. Tahirou Dounda et al., Evaluation finale, Projet « Renforcer la résilience communautaire à la désinformation dans les régions du nord et du centre du Mali » https://www.sfcg.org/wp-content/uploads/2023/09/Search_Rapport_Evaluation_Finale_Tabale_Kunkan.pdf

56. FemininAct, Lutte contre l'incivisme numérique: L'ABB adopte un code de bonne conduite, 24 novembre 2023, <https://www.femininactu.com/actualite/lutte-contre-lincivisme-numerique-labb-adopte-un-code-de-bonne-conduite>

57. Lamissa Diarra, Blogosphère. Les blogueurs disposent désormais d'une charte, 21 avril 2023, <https://benbere.org/terre-dopportunités/blogosphere-blogueurs-disposent-desormais-charte/>

Au Burkina Faso, l'Association des Blogueurs du Burkina (ABB) a instauré un Code de Bonne Conduite des Blogueurs, qui définit des règles éthiques strictes encadrant la pratique du *blogging* et l'usage des réseaux sociaux⁵⁸. Ce code affirme que les blogueurs burkinabè ont le droit d'influencer les politiques publiques, tout en garantissant une information de qualité et en luttant contre la désinformation. Il met en avant des principes tels que l'intégrité journalistique, la protection des sources et le rejet des pressions politiques et financières.

De leur côté, les blogueurs du Niger ont adopté une Charte des Médias Sociaux, qui insiste sur le respect des droits humains et de la dignité individuelle⁵⁹. La charte condamne fermement la diffusion de discours haineux, de propos discriminatoires et d'informations manipulées. Il engage également les blogueurs et influenceurs nigériens à se conformer aux normes éthiques et aux lois en vigueur, en mettant l'accent sur la responsabilité individuelle et collective des acteurs numériques. Quelques dispositions phares des code et charte des blogueurs:

« Les blogueurs du Mali s'engagent à traiter l'actualité et les questions d'intérêt national avec un esprit de responsabilité tout en veillant à contribuer à la paix et au vivre-ensemble au sein de leurs communautés. » Article 4, Charte des Blogueurs du Mali.

58. OuestInfo, Burkina, Autorégulation de l'espace numérique : Des journalistes, blogueurs et web-acteurs de Bobo à l'école de l'ABB, 30 septembre 2024, <https://www.ouestinfo.bf/burkina-autoregulation-de-lespace-numerique-des-journalistes-blogueurs-et-web-acteurs-de-bobo-a-lecole-de-labb/>

59. CSC Niger, Le CSC accompagne les blogueurs dans le processus de l'adoption de leur charte, <https://www.csc-niger.ne/newsarticles/le-csc-accompagne-les-blogueurs-dans-le-processus-de-ladoption-de-leur-charte/>

« *Aucun blogueur ne doit en aucune circonstance verser dans la production et la publication de contenus infondés et « commandités », moyennant une contrepartie financière ou de quelque nature qu'elle soit.* » Article 5, Charte des Blogueurs du Mali.

« *Le/la blogueur(se) a la liberté d'influencer les politiques publiques, de susciter des débats d'intérêt général et scientifique, de promouvoir les valeurs de la démocratie et des droits humains.* » Article 2, Code de Bonne Conduite des Blogueurs du Burkina.

« *Le/la blogueur(se) doit examiner l'exactitude des informations collectées nonobstant leurs sources et ne publier que celles dont la véracité et l'exactitude sont vérifiées. Tout doute oblige le/la blogueur(se) à s'abstenir de les publier ou à le faire avec prudence en respectant le principe de vérité et de l'intérêt général.* » Article 5, Code de Bonne Conduite des Blogueurs du Burkina.

« *Le/la blogueur(se) travaille au respect et à la protection des droits humains, en général, et des groupes marginalisés, et traite les informations qui s'y rapportent avec humanité et dignité.* » Article 1er, Charte des Médias Sociaux du Niger.

« *Le/la blogueur(se) a le devoir de rectifier toute information qui se révèle soit sortie de son contexte originel à des fins de manipulation, soit fausse.* » Article 1er, Charte des Médias Sociaux du Niger.

Ces initiatives partagent de nombreux points de convergence. Par exemple, la lutte contre la désinformation et la promotion d'une information crédible ressortent dans toutes ces chartes. L'importance de vérifier les faits avant publication et de garantir l'intégrité des informations diffusées est également un point commun. Le respect des libertés fondamentales est aussi reconnu comme une nécessité de garantir la liberté d'expression, tout en définissant un cadre éthique permettant d'éviter les dérives et la manipulation de l'opinion

publique. Ces initiatives mettent aussi de l'avant l'engagement en faveur d'une régulation participative qui encourage une approche inclusive de la régulation, où les blogueurs et citoyens sont acteurs du cadre de régulation, plutôt que de simples sujets des décisions étatiques. Enfin, elles s'opposent à la publication de contenus commandités ou influencés par des intérêts financiers ou politiques, en insistant sur l'indépendance et l'impartialité des blogueurs et des journalistes.

Ces initiatives de régulation des réseaux sociaux par la société civile montrent un engagement profond en faveur d'une utilisation responsable et éthique de l'espace numérique. Elles partagent toutes les préoccupations communes pour la crédibilité et la véracité des informations diffusées.

Par ailleurs, au-delà des blogueurs et journalistes, des structures faitières comme les Maisons de la Presse jouent un rôle clé dans la promotion des normes éthiques et professionnelles. Au Mali, cette institution regroupe plusieurs organes de presse et œuvre pour la professionnalisation du journalisme numérique. Au Burkina Faso, son équivalent, le Centre national de presse Norbert Zongo, promeut une presse indépendante et pluraliste et assure des formations pour les journalistes et les blogueurs. En revanche, au Niger, la Maison de la Presse a été suspendue en février 2024, affaiblissant le cadre d'autorégulation des médias.

6) Co-construire une régulation numérique centrée sur l'humain

Malgré les efforts des gouvernements et de la société civile en matière de régulation et d'autorégulation, le Sahel reste confronté à des défis numériques majeurs tels que la désinformation et les discours haineux. La persistance de ces défis démontre que ces types d'efforts demeurent insuffisants⁶⁰. Il devient crucial d'adopter de nouveaux mécanismes qui ne se contentent pas de modérer les contenus après coup, mais de concevoir des plateformes qui réduisent les risques en amont⁶¹. C'est là tout l'enjeu d'intégrer pleinement les principes de la conception centrée sur l'humain et du "prosocial tech design", en mettant l'accent sur la protection des utilisateurs, l'inclusivité, et l'impact positif des technologies sur les communautés.

Le développement de solutions numériques centrées sur l'humain et adaptées aux réalités locales est une attente forte. Par exemple, le Forum de Bamako sur le numérique et la cohésion sociale a souligné l'impact négatif des modèles économiques des grandes plateformes⁶². Dans une déclaration conjointe, ils ont questionné la logique de maximisation des profits qui favorise l'expansion des utilisateurs et l'engagement, souvent au détriment de la sécurité, de la confiance sociétale et du bien-être collectif⁶³.

Les choix de conception des plateformes numériques

60. The Case for Designing Tech for Social Cohesion: The Limits of Content Moderation and Tech Regulation (by Dr. Lisa Schirch, Yale Journal of Law and Humanities), <https://openyls.law.yale.edu/bitstream/handle/20.500.13051/18411/The%20Case%20for%20Designing%20Tech%20for%20Social%20Cohesion%20-%20final%20proof%207.31.pdf?sequence=1&i-sAllowed=y>

61. UNESCO, Principes pour la gouvernance des plateformes numériques, 2023, <https://unesdoc.unesco.org/ark:/48223/pf0000387359/PDF/387359fre.pdf.multi>

62. Site du Forum de Bamako sur le Numérique et la Cohésion sociale, <https://bamakoforum.sfcg.org/politique/>

63. Conclusions de la troisième édition du Forum de Bamako sur le Numérique et la Cohésion Sociale Thème : Synergie d'action pour des politiques numériques responsables, Bamako, le 26 novembre 2024, <https://drive.google.com/file/d/1f-TDOBvaBvc-WuuEyBttNyoVvuiArelS-/view>

influencent directement la diffusion des contenus nuisibles. Les algorithmes de recommandation privilégient souvent les contenus polarisants, les interfaces encouragent des comportements addictifs, et les mécanismes de viralité facilitent la propagation de la désinformation. Ces dynamiques, loin d'être anodines, aggravent la fragmentation sociale et alimentent les tensions, en particulier dans des contextes sensibles comme le Sahel. Une régulation efficace doit donc aller au-delà de la simple modération des contenus pour s'attaquer aux causes structurelles de ces dérives numériques.

Facebook, par exemple, a été critiqué pour son rôle dans la dissémination de fausses informations, notamment dans des régions en crise⁶⁴. Bien que l'entreprise ait mis en place des mesures de lutte contre la désinformation, son approche reste largement réactive. De même, Twitter a fait l'objet de vives critiques pour avoir facilité la prolifération des discours haineux et la propagation de contenus extrémistes malgré son modèle de modération facilité par l'Intelligence artificielle. Si des efforts de modération ont été entrepris, ces initiatives demeurent insuffisantes pour contenir efficacement ces phénomènes. Par ailleurs, WhatsApp a limité la possibilité de transférer massivement des messages, réduisant ainsi la propagation incontrôlée de rumeurs et de fausses nouvelles, et cela a un impact positif en particulier dans les zones en conflit. Ce type de mesures proactives illustre l'intérêt d'une régulation axée sur la prévention, plutôt que sur une réaction tardive aux abus.

En intégrant le "prosocial tech design", les entreprises technologiques peuvent contribuer à un environnement numérique plus sûr et plus inclusif. Il appartient

64. Julien Figeac, et al., Facebook favorise-t-il la désinformation et la polarisation idéologique des opinions ?, <https://journals.openedition.org/questionsdecommunication/21149#-quotation>

désormais aux décideurs et aux acteurs du numérique de s'appuyer sur ces bonnes pratiques pour concevoir des plateformes respectueuses des droits humains et porteuses de valeurs positives pour les sociétés du Sahel. Cela pourrait combler l'attente de plus en plus évidente des pays pour que les outils technologiques s'adaptent aux besoins et aux contextes des utilisateurs⁶⁵.

À titre d'illustration, le code de protection de l'enfant en Angleterre met en place des pratiques pour les enfants dans le cadre de la loi sur la sécurité en ligne⁶⁶. Bien qu'il ne prohibe ni ne prescrit spécifiquement des actions, il vise à garantir que les enfants peuvent explorer et apprendre en ligne de manière protégée. Son objectif est de transformer la manière dont les lois sur la protection des données veillent à la sécurité des jeunes utilisateurs. Le Digital service acte en Europe peut également servir de piste à explorer dans les pays en conflits.

Les États africains, notamment au Sahel, abordent la question de la souveraineté numérique en cherchant à protéger leurs citoyens des dangers du numérique, tout en participant à une initiative non contraignante de l'Union africaine. Une régulation proactive des plateformes, incluant des modifications algorithmiques et un design éthique, est essentielle pour éviter une simple modération réactive inefficace, inspirée des normes appliquées aux infrastructures publiques pour garantir la sécurité⁶⁷.

65. Council on Technology and Social Cohesion, The case for designing for social cohesion, https://techandsocialcohesion.org/wp-content/uploads/2023/02/Digital_Tech_SocialCohesion_ExecSummary.pdf

66. UK's Age Appropriate Design Code (AADC, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>)

67. Politique de l'Union Africaine sur la sécurité et l'autonomisation en ligne des enfants, Adoptée par la 44e session ordinaire du Conseil exécutif de l'Union Africaine Février 2024 - Addis-Abeba, Éthiopie, https://5rightsfoundation.com/wp-content/uploads/2024/05/FR_POLITIQUE-DE-LUNION-AFRICAINE-SUR-LA-SECURITE-ET-LAUTONOMISATION-EN-LIGNE-DES-ENFANTS.pdf

7) Recommandations pour un modèle de régulation efficace centré sur l'humain

La régulation du numérique dans le Sahel ne doit pas se limiter à la lutte contre les abus, mais doit être conçue comme un outil de renforcement de la cohésion sociale, de protection des libertés et de consolidation de la confiance entre les citoyens, les gouvernements et les entreprises. Pour cela, une approche centrée sur l'humain et le prosocial tech design est essentielle. Elle peut s'appuyer sur des standards réglementaires globaux équivalents à ceux en vigueur aux États-Unis et en Europe.

- 1. Réguler en amont plutôt que de se contenter d'une modération réactive :** Les restrictions et mesures de modération actuelles sont souvent réactives et inefficaces. Elles doivent être remplacées par une régulation en amont des plateformes. Les États doivent exiger que les entreprises numériques intègrent dès la conception des principes de protection des utilisateurs, notamment en demandant:
 - La désactivation des recommandations algorithmiques pour les mineurs, comme dans le *Code de conception adaptée à l'âge* au Royaume-Uni.
 - La limitation des mécanismes addictifs tels que le défilement infini et les notifications incitatives.
 - La réduction de la viralité des contenus toxiques en encadrant les algorithmes de recommandation qui peuvent affecter négativement la cohésion sociale.
- 2. Harmoniser la régulation numérique pour une gouvernance régionale cohérente :** Les États du Sahel doivent coordonner leurs politiques numériques à l'échelle régionale pour éviter une fragmentation juridique qui nuirait à la confiance des citoyens et à la stabilité politique. En s'appuyant sur les cadres existants, une convergence législative est essentielle sur la cybersécurité, la

protection des données et la lutte contre la désinformation. Cette harmonisation peut également intégrer les exigences réglementaires appliquées en Europe (RGPD, DSA) et aux États-Unis afin d'éviter un traitement différencié des utilisateurs africains par les plateformes numériques.

- 3. Impliquer activement les citoyens et les acteurs locaux dans la gouvernance et la régulation du numérique :** Les États doivent mettre en place des mécanismes de concertation avec la société civile, les chercheurs, les médias et les entreprises technologiques afin de co-construire les politiques numériques. Cette gouvernance participative garantira une meilleure adéquation des régulations aux réalités locales et renforcera la confiance des citoyens.
- 4. Renforcer la protection des consommateurs et la souveraineté numérique :** Les plateformes numériques devraient, en concertation avec les États africains, adopter des normes de sécurité et d'éthique comparables à celles appliquées en Europe et aux États-Unis. Cette collaboration permettrait de garantir un environnement numérique plus sûr pour tous les utilisateurs, notamment les plus jeunes. Il est essentiel que les États africains définissent leurs propres normes en matière de régulation numérique, en travaillant avec les plateformes pour aller au-delà des ajustements volontaires. Une approche coopérative et inclusive favoriserait une souveraineté numérique effective et respectueuse des droits des utilisateurs.

- 5. Intégrer le “Prosocial Tech Design” et des normes technologiques rigoureuses :** Tout comme les bâtiments doivent respecter des normes de sécurité, les produits numériques doivent être conçus pour garantir la sécurité des utilisateurs. Les États doivent exiger que les plateformes :

Rendent transparents leurs algorithmes et ouvrent l'accès aux régulateurs et chercheurs.

Développent des mécanismes de signalement et de contrôle adaptés aux contextes sociopolitiques, culturels et politiques du Sahel.

- 6. Les États et la société civile doivent renforcer l'éducation numérique et médiatique :** Lutter contre la désinformation et la manipulation numérique passe par une meilleure éducation aux médias et aux technologies. Les États doivent intégrer des modules d'éducation numérique dans les écoles et former les enseignants aux enjeux du numérique. Les organisations de la société civile doivent organiser des campagnes de sensibilisation sur les réseaux sociaux et dans les médias communautaires pour aider les citoyens à mieux analyser et vérifier l'information qu'ils consomment.
- 7. La société civile doit promouvoir l'autorégulation et les bonnes pratiques numériques :** Les organisations de la société civile doivent jouer un rôle plus actif dans la sensibilisation aux bonnes pratiques en ligne.

Les organisations de la société civile doivent promouvoir activement les bonnes pratiques en ligne via des chartes de conduite, des initiatives de fact-checking collaboratives et des campagnes de sensibilisation contre la désinformation.

Les mécanismes d'autorégulation existants, tels que les chartes de blogueurs et les initiatives de vérification des faits, sont des opportunités à renforcer et multiplier.

L'éducation aux médias et au numérique doit être renforcée à travers la portée qu'à la société civile afin de doter les citoyens des compétences d'analyse et de vérification de l'information.

- 8. Les donateurs comme les États, les organisations internationales, les acteurs privés doivent assurer un financement durable des initiatives multipartites de régulation :** les donateurs doivent garantir un financement durable et structuré des initiatives multipartites de régulation du numérique. Cela nécessite l'allocation de ressources adéquates pour assurer le bon fonctionnement des institutions de régulation, le renforcement des capacités en cybersécurité et la mise en œuvre de programmes d'éducation numérique. Un soutien financier pérenne, transparent et orienté vers le renforcement des capacités locales est essentiel pour promouvoir une gouvernance numérique inclusive. Par ailleurs, la mise en place de partenariats public-privé doit être encouragée afin de mobiliser des ressources supplémentaires et d'impliquer activement les entreprises technologiques dans la formation des acteurs locaux et l'amélioration des infrastructures numériques.

8) Références

Council on Technology and Social Cohesion, The case for designing for social cohesion, https://techand-socialcohesion.org/wp-content/uploads/2023/02/Digital_Tech_SocialCohesion_ExecSummary.pdf

Dalanda Moukala et Fatima Al-Ansar, Les femmes sahéliennes dans les espaces numériques, Search for Common Ground, June 2024, <https://www.sfcg.org/wp-content/uploads/2024/09/20240909-Sahe-lian-women-in-Digital-Spaces-final-copy-FRE.pdf>

Eduardo Albrecht and al., Disinformation and Peacebuilding in Sub-Saharan Africa: Security Implications of AI-Altered Information Environments, United Nations University and Interpeace, 2024, <https://unu.edu/publication/disinformation-and-peacebuilding-sub-saharan-africa>

Habibou Bako, Réseaux sociaux et désinformation au Sahel, Bulletin Francopaix, Vol. 7, n° 10, Décembre 2022, <https://dandurand.uqam.ca/wp-content/uploads/2022/12/2022-12-Bulletin.pdf>

Institutional Learning Team, “Community Stewards and Social Cohesion in Digital Spaces.” Search for Common Ground (January 2023), <https://cnxus.org/wp-content/uploads/2023/02/SFCG-Community-Stewards-and-Social-Cohesion-in-Digital-Spaces.pdf>

Jiaxuan Yue et al., Conflit et espace en ligne au Sahel : défis et recommandations, Search for Common Ground, Juillet 2022, <https://documents.sfcg.org/wp-content/uploads/2022/07/Note-D-Analyse-Conflit-et-espace-en-ligne-au-Sahel-Juillet-2022.pdf>

Julien Figeac et al., Facebook favorise-t-il la désinformation et la polarisation idéologique des opinions ?, <https://journals.openedition.org/questionsdecommunication/21149#quotation>

Ruvimbo Shayamunda and al., Social Media in the Africa Context : A review study on benefits and pitfalls, Research Gate, July 2023, https://www.researchgate.net/publication/372382503_Social_Media_in_the_African_Context_A_Review_Study_on_Benefits_and_Pitfalls

Tahirou Dounda et al., Evaluation finale, Projet « Renforcer la résilience communautaire à la désinformation dans les régions du nord et du centre du Mali », https://www.sfcg.org/wp-content/uploads/2023/09/Search_Rapport_Evaluation_Finale_Tabale_Kunkan.pdf

Tahirou Koné, Plateforme numérique et (de)régulation sociale en Afrique francophone, OpenEditions Journals, Communication, technologies et développement, 2023, <https://doi.org/10.4000/ctd.8659>