RAPPORT

TROMPERIE NUMÉRIQUE

Les escroqueries à l'emploi en ligne et la cybercriminalité au Cameroun et au Tchad

Ado Adamou Abba Ari

CENTRAL AFRICA OBSERVATORY ON ORGANIZED CRIME AND VIOLENCE

AOÛT 2026

© 2026 Institute for Security Studies.
Tous droits réservés.

Les droits d'auteur sur la publication dans son ensemble appartiennent aux auteurs et à l'Institute for Security Studies, et aucune partie de la présente publication ne peut être reproduite, en totalité ou en partie, sans l'autorisation écrite expresse des auteurs et de l'éditeur. Les opinions et analyses exprimées dans cette publication sont celles des auteurs et ne reflètent pas nécessairement celles de l'ISS, de ses administrateurs, des membres de son conseil consultatif ou de ses donateurs. Les auteurs contribuent aux publications de l'ISS à titre personnel.

Couverture : *© Adrienne Surprenant/Bloomberg via Getty Images*

À propos de l'ISS
L'Institute for Security Studies (ISS) établit des partenariats afin de développer les connaissances et les compétences nécessaires pour assurer l'avenir de l'Afrique. L'ISS est une organisation africaine à but non lucratif disposant de bureaux en Afrique du Sud, au Kenya, en Éthiopie et au Sénégal. Grâce à ses réseaux et à son influence, l'ISS fournit des recherches stratégiques fiables et opportunes, ainsi que des formations pratiques et une assistance technique aux gouvernements et à la société civile.

www.issafrica.org

SOMMAIRE

Sigles et abréviations ii

Résumé exécutif **1**

Méthodologie 2

Principales conclusions 3

Connectivité numérique et accès à Internet en Afrique **4**

L'essor de la connectivité numérique et les vulnérabilités qui en découlent en Afrique centrale **7**

Mode opératoire des auteurs d'escroqueries à l'emploi en ligne au Cameroun et au Tchad **10**

Anatomie d'une escroquerie à l'emploi en ligne : une approche en plusieurs étapes 10

Le cas du Cameroun : une approche numérique bien rodée 11

Le cas du Tchad : le désespoir comme levier 12

Les différences entre les arnaques en ligne au Cameroun et au Tchad 13

Acteurs, réseaux et outils de la cybercriminalité **18**

Les acteurs de l'écosystème de la cybercriminalité 18

Structures des réseaux et liens transnationaux 19

Outils et technologies numériques 20

Victimisation, vulnérabilité et exploitation **21**

Ampleur et impact économique de la fraude en ligne 21

Profil des victimes et conséquences sociales 22

De la fraude à l'exploitation : un continuum de l'exploitation 23

Liens entre la cybercriminalité, les conflits régionaux et les migrations irrégulières **24**

Les conflits et l'instabilité, facteurs favorisant la cybercriminalité 24

Déplacements forcés, désespoir et cycles d'exploitation 25

Cybercriminalité, migrations irrégulières et traite des êtres humains 26

Vulnérabilités systémiques et réponses à la cybercriminalité **27**

L'essor du numérique sans préparation adéquate 27

Des réponses juridiques et institutionnelles fragiles 28

Lacunes technologiques et déficit de données 28

Les réseaux sociaux et le déficit de responsabilité 29

Des réponses nationales divergentes 29

Coopération régionale et sous-régionale : des ambitions sans mise en œuvre 30

Coopération internationale et contraintes structurelles persistantes 30

Défis techniques et réglementaires liés au traçage des téléphones utilisés par les escrocs 31

Conclusions et recommandations **33**

Recommandations 35

Notes 38

Sigles et abréviations

ANSICE	Agence nationale de sécurité informatique et de certification électronique
ANTIC	Agence nationale des technologies de l'information et de la communication
CEEAC	Communauté économique des États de l'Afrique centrale
CERT	Équipe d'intervention en cas d'urgence informatique
FCFA	Franc CFA (franc de la Communauté financière africaine)
IA	Intelligence artificielle
ONUDC	Office des Nations Unies contre la drogue et le crime
UE	Union européenne

Résumé exécutif

Le présent rapport analyse les arnaques à l'emploi et à l'intégration socio-économique facilitées par les technologies numériques en Afrique centrale, à travers une étude de cas comparative centrée sur le Cameroun et le Tchad. L'enquête met en évidence un écosystème criminel adaptable et de plus en plus transnational, qui tire parti des aspirations d'une jeunesse de la région connectée au numérique, mais vulnérable sur le plan socio-économique. Les criminels exploitent les réseaux sociaux et les plateformes de messagerie, principalement WhatsApp et Facebook, pour mener des stratagèmes d'ingénierie sociale. Ces arnaques, reposant principalement sur des mécanismes de fraude aux frais anticipés, entraînent des pertes financières pour les victimes et s'accompagnent de la collecte de données à caractère personnel. Dans certains cas, ces arnaques conduisent au recrutement de victimes par des réseaux de traite des êtres humains, qui les exploitent ensuite dans le cadre du travail forcé et de l'exploitation sexuelle dans les États du Golfe et au-delà.

L'étude met en évidence un lien entre cette forme de cybercriminalité et le contexte plus large d'instabilité régionale. L'analyse montre comment des conflits, tels que la crise anglophone au Cameroun et l'insurrection de Boko Haram dans le bassin du lac Tchad, créent des conditions propices au développement de ces arnaques en favorisant les déplacements forcés, les difficultés économiques et l'affaiblissement des institutions. Elle indique également que les produits de ces activités peuvent contribuer à accentuer l'instabilité et à renforcer les dynamiques de violence et d'exploitation dans la région. En outre, les offres frauduleuses peuvent encourager les migrations irrégulières vers l'Europe et les États du Golfe, établissant un lien entre la tromperie numérique et la traite des êtres humains.

Les réponses nationales et régionales actuelles sont insuffisantes et se révèlent dépassées par l'ampleur du phénomène. Les cadres juridiques sont obsolètes et peu appliqués, tandis que les capacités institutionnelles des services répressifs et de l'appareil judiciaire sont limitées par le manque de ressources techniques et de formations spécialisées, ainsi que par l'insuffisance des mécanismes de coopération transfrontalière. Les politiques et les stratégies peinent à être mises en œuvre.

Le rapport analyse le fonctionnement de ces arnaques en ligne, les acteurs et les réseaux impliqués, ainsi que les outils et les plateformes qu'ils utilisent. Il évalue leur ampleur, leurs répercussions sur les victimes, ainsi que l'efficacité des réponses actuellement apportées. L'analyse met également en

évidence d'importantes lacunes en matière de capacités juridiques, institutionnelles et opérationnelles. Le rapport est structuré en six sections, qui portent respectivement sur le mode opératoire des arnaques, les acteurs, les réseaux et les outils impliqués, le profil des victimes et les conséquences des arnaques, les liens avec les conflits et les migrations, ainsi que les faiblesses des systèmes de prévention et des réponses nationales, régionales et internationales, avant de s'achever sur une série de recommandations.

Méthodologie

L'étude porte sur le Cameroun et le Tchad, retenus comme études de cas comparatives. Si les deux pays sont confrontés à des pressions socio-économiques et politiques similaires, ils se distinguent par leurs infrastructures numériques et leur niveau de connectivité, ce qui permet de comparer l'influence de ces facteurs sur les dynamiques des arnaques. L'analyse porte sur les arnaques liées à l'emploi et à l'intégration socio-économique, tout en prenant en compte leurs implications plus larges pour l'Afrique centrale.

L'étude s'appuie sur une analyse documentaire fondée sur des rapports et des données provenant d'institutions nationales, notamment l'Agence nationale des technologies de l'information et de la communication (ANTIC) au Cameroun et l'Agence nationale de sécurité informatique et de certification électronique (ANSICE) au Tchad, ainsi que d'organisations internationales, dont l'Office des Nations Unies contre la drogue et le crime (ONUDC), l'Organisation internationale de police criminelle (INTERPOL) et l'Union internationale des télécommunications (UIT). Cette analyse est complétée par des entretiens semi-directifs menés auprès de représentants des pouvoirs publics, de représentants d'organisations non gouvernementales et, lorsque cela est possible, de victimes d'arnaques. En outre, une démarche d'ethnographie numérique est mise en œuvre afin d'observer les réseaux sociaux et les forums en ligne, notamment Facebook et WhatsApp, en vue d'analyser les messages frauduleux, les faux profils en ligne et la structure des réseaux virtuels. Ces études de cas détaillées consacrées au Cameroun et au Tchad offrent un éclairage comparatif sur les schémas de fraude et les réponses institutionnelles.

Les données ont été analysées au moyen d'une analyse thématique, combinant le codage qualitatif des entretiens et l'analyse documentaire afin d'identifier les thèmes, les schémas et les tendances récurrents liés aux méthodes d'escroquerie, aux profils des auteurs et aux vulnérabilités systémiques. Les données quantitatives issues d'enquêtes et de rapports ont été utilisées pour trianguler ces résultats et estimer l'ampleur ainsi que l'impact financier des arnaques. L'approche fondée sur une étude de cas comparative permet de mettre en évidence les différences et les points communs entre les contextes camerounais et tchadien, afin de garantir que les résultats reflètent les réalités locales.

Bien que des mesures aient été prises afin d'assurer une représentation aussi large que possible, l'échantillon de 80 répondants ne permet pas de tirer des conclusions définitives concernant les arnaques à l'emploi en ligne au Cameroun et au Tchad. L'étude présente également plusieurs autres limites, notamment la rareté des données due à la sous-déclaration des faits et aux risques liés à la sécurité, les contraintes éthiques associées à la protection des victimes, ainsi que la nature clandestine des activités d'escroquerie. L'étude privilégie par conséquent une approche essentiellement qualitative afin de garantir l'intégrité des données et le respect des exigences éthiques, les principales conclusions étant fondées sur des entretiens avec des informateurs clés. En outre, les témoignages des victimes ont été anonymisés et, dans la mesure du possible, recoupés avec d'autres sources.

Principales conclusions

- **Mode opératoire évolutif.** Les escrocs utilisent un processus en plusieurs étapes (appâtage, accroche, manipulation), adapté aux contextes socio-économiques locaux. Au Cameroun, cela se traduit notamment par l'usurpation de l'identité d'initiatives gouvernementales et par la création de faux sites web. Au Tchad, où le taux de pénétration d'Internet est plus faible, la fraude est plus directe et repose principalement sur le hameçonnage par SMS (« smishing ») et les appels vocaux (« vishing »).
- **Un écosystème d'acteurs diversifié.** Les auteurs vont d'individus opportunistes (par exemple les Yahoo Boys[1]) à des réseaux criminels organisés, dont certains entretiennent des liens avec des organisations criminelles transnationales, notamment au Nigeria. Cet écosystème s'appuie sur des facilitateurs tels que des mules financières, des faussaires spécialisés dans les documents et des agents publics corrompus.
- **Conséquences humaines et économiques.** En 2021, la cybercriminalité a entraîné des pertes financières de 12,2 milliards de FCFA (environ 20,2 millions de dollars des États-Unis) pour l'économie camerounaise[2]. Au-delà de ces pertes financières, les victimes subissent de graves traumatismes psychologiques, une stigmatisation sociale et des atteintes à leur réputation. Dans certains cas, ces arnaques sont étroitement liées à des formes d'exploitation, notamment la traite des êtres humains.
- **Liens avec les conflits et les migrations.** Il existe un lien manifeste entre la cybercriminalité, les conflits et les migrations. De fait, les zones de conflit constituent un vivier de personnes vulnérables, à la fois en tant que victimes et comme recrues potentielles. Les réseaux de traite des êtres humains utilisent également ces arnaques pour déplacer des victimes sous de faux prétextes. En outre, les produits de ces activités criminelles peuvent alimenter l'instabilité et constituer une menace pour la sécurité nationale.
- **Faiblesses systémiques des dispositifs de réponse.** Les réponses demeurent fragmentées et essentiellement réactives. Les principales lacunes concernent un niveau de culture numérique particulièrement faible, des cadres juridiques obsolètes ou inexistants, des services répressifs insuffisamment dotés en ressources et une coopération régionale limitée, ce qui permet aux criminels d'opérer au-delà des frontières.

Connectivité numérique et accès à Internet en Afrique

Le paysage numérique de l'Afrique s'est considérablement développé au cours des dernières années, la proportion de personnes utilisant Internet ayant augmenté de manière constante à l'échelle du continent, selon la Banque mondiale[3]. Le taux d'adoption d'Internet en Afrique subsaharienne demeure nettement inférieur à la moyenne mondiale, ce qui met en évidence la persistance d'importantes disparités en matière de connectivité malgré l'expansion des infrastructures de réseau.

Les dernières données de l'Union internationale des télécommunications montrent que l'utilisation d'Internet en Afrique progresse à un rythme supérieur à la moyenne mondiale. Depuis 2005, la connectivité y augmente d'environ 16,7 % par an, soit plus de deux fois le rythme observé à l'échelle mondiale. Pourtant, en 2024, seuls 38 % environ des Africains utilisaient Internet, contre près de 68 % à l'échelle mondiale[4]. Cette croissance témoigne de progrès considérables dans le déploiement des réseaux et l'extension de la couverture du haut débit mobile. Elle met toutefois en évidence des disparités importantes : les hommes (43 %) sont plus nombreux que les femmes (31 %) à utiliser Internet ; les jeunes âgés de 15 à 24 ans (53 %) sont davantage connectés que les adultes plus âgés ; et les habitants des zones urbaines bénéficient d'un accès à Internet nettement supérieur (57 %) à celui des habitants des zones rurales (23 %). Ces tendances montrent que, si la connectivité continue de progresser, des obstacles structurels — notamment le coût de l'accès, le déficit de compétences numériques et les inégalités en matière d'infrastructures — continuent de freiner une participation inclusive au numérique à l'échelle du continent. Dans l'ensemble, l'utilisation d'Internet en Afrique a considérablement augmenté au cours de la dernière décennie, mais le continent demeure en deçà de la moyenne mondiale : selon les données les plus récentes, seule une minorité d'Africains utilisait Internet, même si le nombre absolu d'utilisateurs continue d'augmenter. Cette évolution reflète non seulement le déploiement des infrastructures, notamment du haut débit mobile et de la fibre optique, mais aussi les difficultés persistantes à traduire cette couverture en une utilisation effective.

En complément de ces données macroéconomiques sur la connectivité, les données recueillies par Afrobarometer en 2024 dans 39 pays africains montrent que l'utilisation des médias numériques,

notamment l'accès régulier à Internet et aux réseaux sociaux, a considérablement progressé, mais demeure inégalement répartie entre les différents groupes démographiques[5]. Près de la moitié des Africains (47 %) déclarent s'informer par l'intermédiaire des réseaux sociaux ou d'Internet au moins quelques fois par semaine. Toutefois, cette proportion varie considérablement d'un pays à l'autre, allant de seulement 14 % à Madagascar à 82 % à Maurice, et concerne principalement les populations urbaines, les personnes plus instruites, les ménages les plus aisés, les hommes et les jeunes. Bien qu'ils aient presque doublé en moins de dix ans, ces progrès en matière d'utilisation des médias numériques coexistent avec des fractures numériques persistantes, dont l'ampleur est aujourd'hui comparable à celle observée lorsque le niveau global d'accès était bien plus faible. Cela laisse penser que la croissance, à elle seule, n'a pas permis de lever les obstacles structurels à l'inclusion numérique.

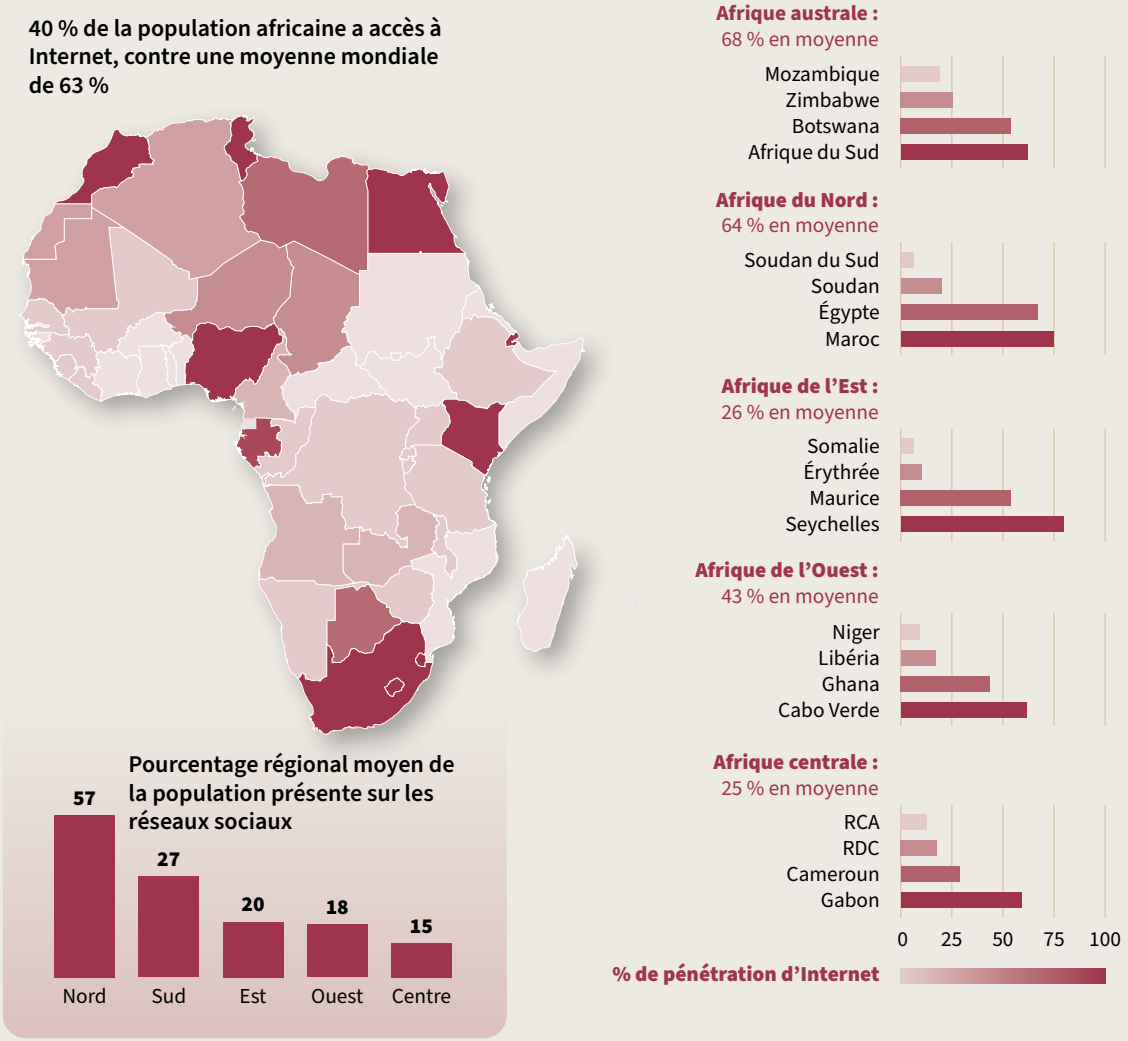

FIGURE 1 Taux de pénétration d'Internet en Afrique.

SOURCE : Adapté de CRE Venture Capital, Internet penetration, https://www.cre.vc/news-slider/internet-penetration-in-africa-infographic

Si la connectivité à Internet est devenue essentielle à l'innovation à l'échelle mondiale, l'Afrique demeure en retrait par rapport à la plupart des autres régions : seuls environ 40 % de sa population utilisent Internet, contre près de 63 % à l'échelle mondiale. Cette proportion a toutefois fortement progressé, passant de seulement 9 % en 2012 à 21 % en 2017, puis à près de 40 % aujourd'hui, ce qui signifie que le taux de pénétration a quadruplé au cours de la dernière décennie et doublé au cours des cinq dernières années. L'Afrique australe et l'Afrique du Nord affichent les taux de pénétration les plus élevés (environ 68 % et 64 %, respectivement), tandis que l'Afrique centrale et l'Afrique de l'Est restent en retrait, avec des taux d'environ 26 % et 25 % (voir la figure 1).

Les principaux obstacles à l'accès à Internet sont le coût des appareils et des services de données, le faible niveau de culture numérique et l'insuffisance des infrastructures, en particulier dans les zones rurales. L'extension du haut débit, des réseaux mobiles et des centres de données nécessitera des investissements considérables, que la Banque mondiale estime à environ 100 milliards de dollars des États-Unis. Des projets d'infrastructure en cours — tels que le câble sous-marin 2Africa, le câble Equiano de Google et les investissements majeurs réalisés par des consortiums de télécommunications — visent à réduire les coûts et à élargir l'accès à Internet. Ils étayent les projections selon lesquelles l'économie numérique de l'Afrique pourrait atteindre 180 milliards de dollars des États-Unis d'ici à 2025, puis 712 milliards de dollars des États-Unis d'ici à 2050, à mesure que l'amélioration de la connectivité ouvre de nouvelles perspectives de développement économique et social[6].

L’essor de la connectivité numérique et les vulnérabilités qui en découlent en Afrique centrale

Au cours des deux dernières décennies, les technologies numériques ont profondément transformé la vie en Afrique centrale. La généralisation des téléphones mobiles, des réseaux sociaux et de l’accès à Internet est devenue un élément central des communications et des échanges commerciaux. Au Cameroun, par exemple, un secteur des télécommunications relativement développé et la position stratégique du pays ont favorisé un essor important du numérique[7]. Pour des millions de jeunes au Cameroun, un smartphone constitue souvent une véritable bouée de sauvetage et un vecteur de mobilité sociale.

Au Tchad, si le taux de pénétration du numérique est plus faible, cette évolution n’en est pas moins significative. L’utilisation des téléphones mobiles est désormais largement répandue, et des plateformes comme Facebook et WhatsApp sont solidement implantées, y compris dans les communautés les plus isolées. Cette intégration numérique, bien que plus lente, permet aux Tchadiens d’accéder à des informations et à des opportunités qui leur étaient auparavant hors de portée. C’est dans ce contexte de croissance rapide, mais inégale, du numérique que l’exploitation criminelle de cette nouvelle connectivité a pris racine.

Cette expansion du numérique au Cameroun et au Tchad s’inscrit dans une tendance plus large observée en Afrique subsaharienne, où les technologies mobiles ont profondément transformé la connectivité, malgré la persistance d’obstacles structurels.

Au Cameroun, la connectivité à Internet et aux réseaux mobiles s’est considérablement développée au cours de la dernière décennie. À la fin de l’année 2025, le Cameroun comptait environ 11 millions d’utilisateurs d’Internet, soit près de 41,9 % de sa population. Les connexions mobiles étaient presque universelles, avec 29 millions d’abonnements à la téléphonie mobile, soit l’équivalent de 96,4 % de la

population. Parmi ces abonnements, 87,5 % correspondaient à des connexions à haut débit (3G/4G), ce qui témoigne d'un accès largement répandu aux réseaux mobiles modernes[8]. Malgré ces progrès, plus de 58 % de la population n'utilise toujours pas Internet, ce qui met en évidence le décalage persistant entre la couverture des réseaux et leur utilisation effective. Selon les estimations de l'Union internationale des télécommunications, jusqu'à 75 % de la population aurait accès aux services 3G ou 4G, un niveau nettement supérieur à celui de nombreux autres pays de la Communauté économique des États de l'Afrique centrale (CEEAC)[9]. L'essor des smartphones et du haut débit mobile a élargi l'accès aux réseaux sociaux, aux services bancaires numériques et aux services en ligne, en particulier chez les jeunes des zones urbaines et périurbaines.

À l'inverse, la transformation numérique du Tchad a été plus lente et plus limitée. À la fin de l'année 2025, le Tchad comptait environ 2,79 millions d'utilisateurs d'Internet, soit un taux de pénétration de 13,2 % de la population, l'un des plus faibles du continent africain. Bien que le Tchad ait enregistré une augmentation du nombre de connexions mobiles (le taux de pénétration de la téléphonie mobile ayant dépassé les 60 % au cours des dernières années), le décalage entre la disponibilité des réseaux et l'utilisation effective d'Internet demeure important[10]. Les infrastructures limitées, le coût élevé de l'accès à Internet ainsi que le caractère sporadique ou la faible qualité des services à haut débit continuent de freiner leur adoption à grande échelle.

Des partenaires du développement, tels que la Banque mondiale, ont récemment lancé des initiatives visant à étendre le haut débit et à renforcer les compétences numériques afin d'élargir l'accès aux zones rurales et périurbaines et de développer les capacités numériques, en particulier chez les jeunes et les femmes[11].

Dans les deux pays, le profil des utilisateurs du numérique est généralement celui de jeunes citadins ambitieux. Au Cameroun, les jeunes, en particulier les 18–34 ans, sont de plus en plus nombreux parmi

L'essor rapide des smartphones et de l'Internet mobile transforme le quotidien au Cameroun, en donnant à un nombre croissant de personnes accès à l'information et à de nouvelles possibilités, tout en les exposant davantage aux arnaques. *© AFP via Getty Images*

les utilisateurs d'Internet, tandis que l'adoption des réseaux sociaux continue de progresser. Toutefois, les compétences numériques demeurent inégales, de nombreux internautes ne possédant pas les compétences nécessaires pour évoluer dans les espaces numériques de manière sûre et efficace. Au Cameroun, le décalage entre une couverture élevée du haut débit mobile et un taux d'adoption d'Internet relativement plus faible laisse penser que le coût d'accès, les compétences numériques et la pertinence des services en ligne constituent les principaux freins. De même, au Tchad, la couverture limitée du haut débit ainsi que le coût élevé des appareils et des forfaits de données touchent de manière disproportionnée les jeunes et les personnes sans emploi, ce qui accroît leur vulnérabilité dans les environnements numériques.

Cette population croissante de jeunes internautes se trouve dans une situation paradoxale : elle aspire à de meilleures perspectives économiques grâce au numérique, tout en restant exposée aux risques en ligne en raison des difficultés d'accès à l'emploi et de compétences numériques insuffisantes. Ces conditions offrent un terrain propice aux cybercriminels, qui exploitent à la fois l'augmentation de la présence en ligne et le faible niveau de compétences numériques pour mener des escroqueries et des fraudes de plus en plus sophistiquées.

Cette croissance rapide, mais inégale, du numérique a favorisé l'émergence des escroqueries à l'emploi en ligne en tant que menace particulière, les cybercriminels exploitant les vulnérabilités créées par cette transformation. Parmi les nombreuses menaces liées à la cybercriminalité, les escroqueries à l'emploi en ligne sont particulièrement préoccupantes pour plusieurs raisons, notamment les suivantes :

- **Pauvreté et chômage généralisés.** Le taux de chômage des jeunes, qui dépasse souvent les 13 %, crée un contexte de précarité et de vulnérabilité dont les criminels tirent parti. La promesse d'un emploi à l'étranger peut apparaître comme la seule issue, poussant certaines personnes à investir toutes leurs économies dans des offres d'emploi frauduleuses.
- **Pression démographique et migration.** Du fait de leur importante population de jeunes, les deux pays sont confrontés à des pressions migratoires. Pour de nombreux jeunes, la migration apparaît comme la seule voie vers un avenir meilleur. Les escrocs exploitent cette situation en proposant de fausses offres d'emploi en Europe ou dans d'autres régions du monde, ce qui peut parfois conduire à des situations de traite des êtres humains ou de travail forcé.
- **Conflits généralisés.** Les conflits persistants dans le bassin du lac Tchad ont entraîné le déplacement de millions de personnes, créant une importante population de personnes vulnérables. Les escroqueries exploitent cette vulnérabilité en proposant de fausses offres d'emploi, qui peuvent parfois servir de moyen de recrutement pour des groupes armés ou des réseaux de traite des êtres humains.
- **Expansion du numérique et faibles compétences numériques.** L'adoption rapide des réseaux sociaux et des applications de messagerie a été plus rapide que le développement des compétences numériques. Ce décalage crée une population d'utilisateurs vulnérables, désireux de profiter des possibilités offertes par le numérique, mais insuffisamment préparés aux risques de désinformation, d'hameçonnage et de faux profils.

Si l'essor du numérique en Afrique centrale est porteur de profondes transformations, il offre également un terrain propice aux cybercriminels. Ils exploitent la convergence entre la généralisation de la connectivité, la vulnérabilité socio-économique et le faible niveau de compétences numériques pour mettre en œuvre des escroqueries sophistiquées, dont les escroqueries à l'emploi en ligne constituent un exemple particulièrement préjudiciable.

Mode opératoire des auteurs d'escroqueries à l'emploi en ligne au Cameroun et au Tchad

En Afrique centrale, les escroqueries à l'emploi en ligne reposent principalement sur des techniques de manipulation plutôt que sur le piratage informatique. La présente section examine les principales méthodes employées dans les escroqueries à l'emploi en ligne au Cameroun et au Tchad.

Anatomie d'une escroquerie à l'emploi en ligne : une approche en plusieurs étapes

Une approche par étapes permet d'analyser le déroulement d'une escroquerie à l'emploi en ligne en plusieurs phases distinctes, chacune conçue pour manipuler la victime. Plutôt que de se dérouler de manière aléatoire ou opportuniste, ces escroqueries suivent un processus structuré en plusieurs étapes, au cours duquel les escrocs établissent progressivement leur crédibilité, obtiennent des informations personnelles et financières et, dans certains cas, en viennent à exploiter physiquement leurs victimes. Les escroqueries à l'emploi en ligne reposent sur la manipulation psychologique et l'ingénierie sociale, les escrocs exploitant tout au long du processus la confiance des victimes, le sentiment d'urgence, l'autorité perçue et leur vulnérabilité économique[12].

L'escroquerie débute généralement par une phase d'appâtage, au cours de laquelle une offre est conçue pour paraître particulièrement attrayante, voire « trop belle pour être vraie ». Ces offres ciblent généralement les personnes sans emploi ou confrontées à de graves difficultés économiques. Afin de rendre ces offres plus attrayantes, les escrocs promettent des salaires exceptionnellement élevés pour des emplois peu ou non qualifiés à l'étranger, n'exigent que peu de qualifications et mettent en avant des avantages tels que la prise en charge du logement, du transport ou des frais de voyage. Les auteurs de ces escroqueries se font fréquemment passer pour des institutions de confiance ou prétendent agir en leur nom, notamment des ministères chargés de l'emploi ou des services publics, des entreprises multinationales de renom ou des organisations internationales reconnues. La présentation de faux documents officiels, ou la promesse de leur délivrance, notamment de contrats de travail, de permis de travail ou d'autorisations administratives, renforce l'apparence de légalité et de légitimité de l'offre et persuade les victimes de son authenticité.

Une fois l'intérêt de la victime suscité, l'escroquerie entre dans une phase de prise de contact et d'instauration de la confiance. Les offres d'emploi sont largement diffusées sur des plateformes à forte fréquentation afin de renforcer leur crédibilité. Il s'agit souvent des réseaux sociaux, où des faux profils et des pages frauduleuses sur des plateformes telles que Facebook ou WhatsApp permettent de cibler des groupes démographiques spécifiques. Les escrocs utilisent également des sites web et des courriels frauduleux imitant ceux d'agences de recrutement professionnelles, en recourant souvent à des noms de domaine identiques ou très similaires aux domaines légitimes. Dans certains cas, de faux communiqués de presse ou de fausses annonces sont diffusés sur des stations de radio locales, exploitant le haut niveau de confiance dont jouissent ces médias, en particulier dans les communautés rurales.

L'étape suivante repose sur une fraude aux frais anticipés associée à une collecte systématique de données personnelles. Les victimes sont convaincues de verser une série de frais, d'abord modestes puis progressivement plus élevés, au titre notamment du traitement des demandes de visa, des formalités administratives ou du matériel de formation. Les paiements sont généralement demandés par l'intermédiaire de services de paiement mobile, dont les transactions sont difficiles à retracer. Parallèlement, sous couvert de procédures de recrutement officielles, les victimes sont incitées à communiquer des informations personnelles sensibles, notamment des pièces d'identité, des coordonnées bancaires et d'autres données confidentielles. Ces informations peuvent ensuite servir à l'usurpation d'identité ou être revendues sur des marchés illicites.

Pour les victimes les plus vulnérables, l'escroquerie peut évoluer vers une phase plus grave, dans laquelle la fraude financière cède la place à une exploitation physique. Dans ces cas, la prétendue offre d'emploi sert d'appât à des fins de traite des êtres humains. Les victimes peuvent être acheminées vers des destinations telles que les États du Golfe, où elles sont soumises au travail forcé ou à l'exploitation sexuelle. Le contrôle exercé sur les victimes repose souvent sur la confiscation de leur passeport et d'autres documents d'identité ou de voyage, ce qui les rend dépendantes de ceux qui les exploitent. À ce stade, les victimes peuvent être privées de leur liberté et rester sous le contrôle de ceux qui les exploitent.

Le cas du Cameroun : une approche numérique bien rodée

Le taux relativement élevé de pénétration d'Internet au Cameroun, associé à une population jeune nombreuse en quête de meilleures perspectives économiques, a façonné l'économie de l'escroquerie dans le pays. Dans ce contexte, plusieurs formes d'escroqueries à l'emploi en ligne sont particulièrement répandues.

Un exemple courant est l'escroquerie dite du « *Plan d'urgence spécial pour la jeunesse* ». Dans ce stratagème, les auteurs montent de toutes pièces de prétendues initiatives gouvernementales, présentées comme des programmes officiels d'emploi ou de soutien à la jeunesse. Ils s'appuient sur des sites web contrefaits, des communications falsifiées et des systèmes de paiement mobile pour escroquer un grand nombre de jeunes.

Un autre mode opératoire courant est celui des escroqueries dites « Dubai Dream » ou « Canada Job », qui ciblent de jeunes Camerounais à la recherche de perspectives à l'étranger. Ces stratagèmes sont généralement mis en œuvre par l'intermédiaire de fausses agences de recrutement et reposent sur une mise en confiance progressive des victimes, structurée en plusieurs étapes et souvent menée au sein de groupes WhatsApp. Les escrocs font miroiter de fausses possibilités d'emploi ou de migration et gagnent progressivement la confiance des participants. Les communications comportent souvent des erreurs grammaticales, des incohérences linguistiques et des passages du français à l'anglais et inversement, autant de signes qui peuvent éveiller les soupçons. Les groupes WhatsApp contribuent à créer un sentiment d'appartenance et à renforcer la crédibilité du stratagème, notamment grâce à de faux témoignages de personnes présentées comme ayant bénéficié du programme.

Le cas du Tchad : le désespoir comme levier

Au Tchad, le niveau relativement faible de connectivité à Internet, conjugué à une pauvreté généralisée, a influencé les tactiques employées par les escrocs, donnant lieu à des méthodes plus directes et davantage axées sur l'exploitation des victimes. Dans ce contexte, les escroqueries reposent moins sur des plateformes numériques sophistiquées que sur des moyens de communication largement accessibles permettant de cibler des populations économiquement vulnérables[13].

L'une des principales stratégies consiste à recourir à l'hameçonnage par SMS et par téléphone, des pratiques communément appelées respectivement « smishing » et « vishing ». Ces méthodes sont privilégiées car elles ne nécessitent ni smartphone ni forfait Internet coûteux, mais reposent sur l'utilisation de téléphones mobiles classiques ainsi que sur l'envoi de SMS et les appels téléphoniques à faible coût. Les escrocs envoient des SMS qui semblent provenir d'institutions de confiance, telles que des banques, des opérateurs de paiement mobile, des organismes publics ou des agences de recrutement. Ces messages créent un sentiment d'urgence en affirmant qu'un compte a été suspendu, qu'un paiement est en attente ou qu'une vérification immédiate est nécessaire, incitant ainsi les destinataires à répondre par SMS ou à appeler le numéro de téléphone indiqué. Cette méthode est particulièrement efficace auprès des utilisateurs qui se servent de téléphones mobiles classiques ou qui limitent leur consommation de données mobiles en raison de leur coût.

L'hameçonnage vocal (« vishing ») vient compléter cette méthode par des appels téléphoniques directs ou des appels de suivi. Les escrocs exploitent la confiance qu'inspirent les échanges de vive voix en se faisant passer pour des agents de service à la clientèle, des représentants des pouvoirs publics ou des recruteurs. Par un discours persuasif, ils font pression sur les victimes pour les amener à divulguer des informations personnelles, des mots de passe à usage unique ou les codes PIN de leurs comptes de paiement mobile. Les appels téléphoniques permettent également aux fraudeurs d'adapter leur discours en temps réel, de dissiper les doutes et de passer du français à l'anglais ou aux langues locales afin de renforcer leur crédibilité. En privilégiant les SMS et les communications vocales plutôt que les plateformes en ligne, ces escroqueries permettent de contourner les obstacles liés à la connectivité et à l'accès aux équipements, et ainsi de toucher une population plus large et souvent plus vulnérable.

Une autre tactique courante consiste à exploiter la précarité économique au moyen d'offres axées sur les besoins essentiels. Ces escroqueries proposent des offres axées sur des besoins de subsistance immédiats — « argent facile », « tout emploi disponible » ou « recrutement urgent » — qui ciblent des personnes en situation de vulnérabilité socio-économique. Les exigences en matière de qualifications, de documents et d'expérience sont délibérément minimisées afin d'attirer les personnes qui disposent de peu d'options, en particulier les réfugiés et les personnes déplacées à l'intérieur de leur propre pays. Les escrocs se font fréquemment passer pour des organisations humanitaires, des organismes publics ou de grands employeurs afin de renforcer leur crédibilité. Des messages annonçant des offres de recrutement fictives sont diffusés par SMS, WhatsApp ou appels téléphoniques et proposent des emplois de courte durée auprès de compagnies pétrolières, des programmes de travail contre rémunération ou un recrutement accéléré dans l'armée ou les services de sécurité. Les victimes sont ensuite invitées à payer des frais de traitement ou à fournir des informations personnelles et financières sous prétexte de procéder à leur inscription ou à

Une publicité d'un opérateur de téléphonie à N'Djamena, au Tchad. Les escrocs exploitent la précarité économique au moyen de SMS, d'appels téléphoniques et de fausses offres d'emploi qui ciblent les personnes confrontées à des besoins urgents et à des perspectives limitées. *© Xaume Olleros/Bloomberg via Getty Images*

des vérifications. En faisant correspondre leurs offres frauduleuses à des besoins urgents et en les associant à des institutions jouissant de la confiance du public, ces stratagèmes dissipent les soupçons et incitent davantage les victimes à répondre aux demandes des escrocs.

Les différences entre les arnaques en ligne au Cameroun et au Tchad

Cette analyse comparative des pratiques cybercriminelles au Cameroun et au Tchad repose sur des entretiens menés auprès de 80 répondants issus des forces de l'ordre, du secteur de la cybersécurité, des services financiers, de la société civile et du monde universitaire, ainsi qu'auprès de victimes. Elle met en évidence un paysage de la cybercriminalité dominé par des infractions motivées par des considérations économiques, avec des variations notables d'un pays à l'autre (voir la figure 2).

Au Cameroun, la forme de cybercriminalité la plus fréquemment signalée concerne les offres d'emploi frauduleuses à l'étranger (42 %), suivies des fraudes liées au paiement mobile (38 %) et des escroqueries sentimentales (20 %), ce qui reflète le taux élevé de chômage des jeunes et leurs aspirations à migrer, soutenues par une diaspora active. Au Tchad, les fraudes liées au paiement mobile constituent la forme de cybercriminalité la plus fréquemment signalée (47 %), suivies de l'usurpation d'identité (33 %) et, dans une moindre mesure, des offres d'emploi frauduleuses (20 %), ce qui reflète l'adoption croissante des services financiers mobiles dans une économie largement informelle.

Dans les deux pays, WhatsApp apparaît comme le principal vecteur d'attaque, représentant environ 58 à 60 % des cas, en grande partie en raison de la confidentialité et de la crédibilité qui lui sont prêtées. Des différences apparaissent également dans l'organisation des activités criminelles : au Cameroun, 82 % des répondants font état de liens structurés avec des réseaux nigérians de cybercriminalité, contre un modèle plus opportuniste et localisé au Tchad, signalé par 70 % des répondants.

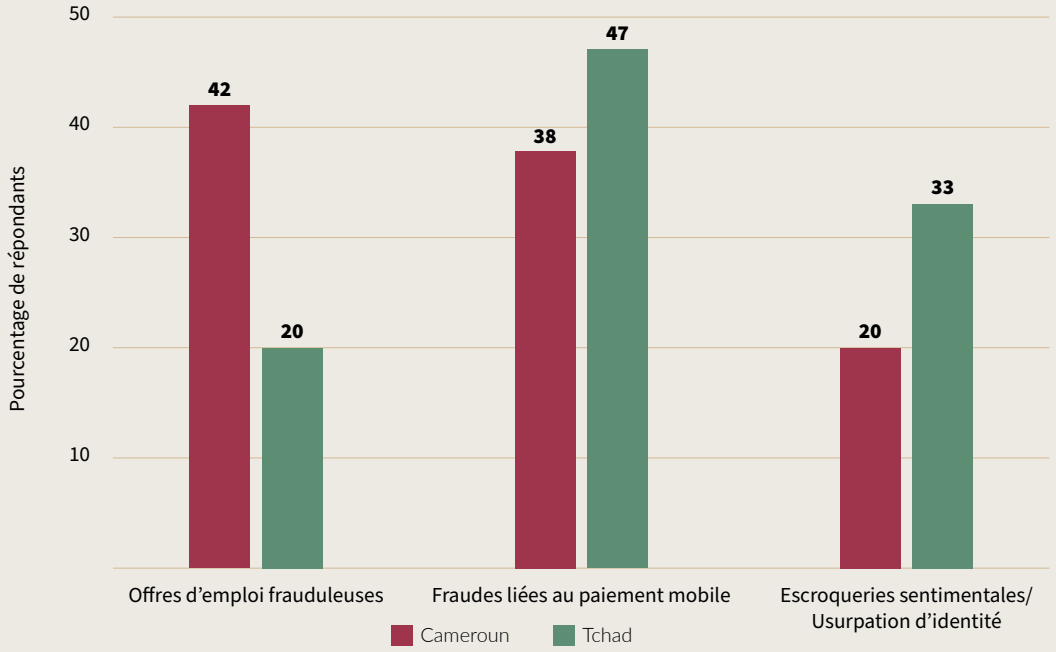

FIGURE 2 Répartition des trois types de cybercriminalité les plus fréquemment signalés au Cameroun et au Tchad.

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

La lutte contre la cybercriminalité se heurte à des difficultés systémiques, notamment le manque de formation spécialisée des enquêteurs (86 %) et la faible coopération avec les entreprises technologiques (78 %). Ces difficultés sont aggravées par le faible niveau de sensibilisation du public, 92 % des répondants estimant que la compréhension des cyberrisques au sein de la société est « faible » ou « très faible ».

La plupart des répondants font état d'une nette évolution des pratiques cybercriminelles dans les deux pays, 94 % des participants au Cameroun et 87 % au Tchad ayant observé des changements importants au fil du temps (voir la figure 3). Ces évolutions se traduisent notamment par une professionnalisation accrue, les messages frauduleux devenant plus sophistiqués et comportant moins d'erreurs, ce qui laisse penser que des outils automatisés ou l'intelligence artificielle pourraient être utilisés. Les répondants soulignent également le passage de l'envoi massif de messages à des techniques d'ingénierie sociale plus ciblées, les attaquants utilisant les profils sur les réseaux sociaux pour personnaliser leur approche. En outre, la cybercriminalité repose de plus en plus

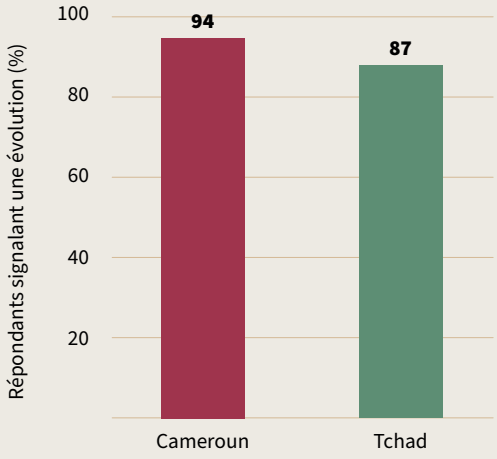

FIGURE 3 Perception de l'évolution des techniques utilisées par les cybercriminels au Cameroun et au Tchad.

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

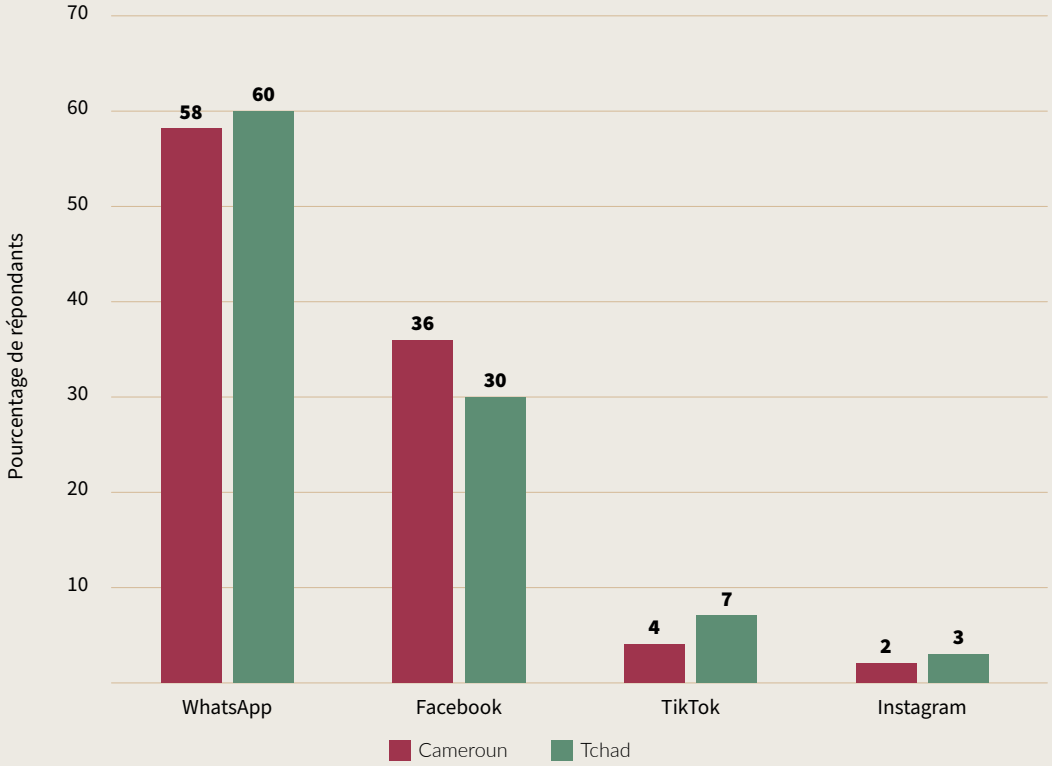

FIGURE 4 Plateformes les plus utilisées par les cybercriminels pour lancer leurs attaques au Cameroun et au Tchad

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

sur des attaques multivecteurs, dans lesquelles le premier contact peut être établi sur des plateformes telles que Facebook, se poursuivre par des échanges privés sur WhatsApp et aboutir à l'extraction de fonds par l'intermédiaire de services de paiement mobile, ce qui complique davantage la détection et l'intervention.

Au Cameroun comme au Tchad, les plateformes de réseaux sociaux constituent les principaux canaux par lesquels les cybercriminels entrent en contact avec leurs victimes. Les répondants ont été invités à indiquer la plateforme la plus couramment utilisée pour lancer les escroqueries (figure 4).

Les données montrent que WhatsApp constitue le principal vecteur d'attaque dans les deux pays, suivi de Facebook, tandis que les autres plateformes, telles que TikTok et Instagram, jouent un rôle nettement plus limité. Cela témoigne du rôle central des plateformes de communication privée largement utilisées, qui facilitent les activités d'escroquerie.

Les répondants ont également été invités à indiquer si les cybercriminels opèrent de manière autonome ou en lien avec des réseaux étrangers. Les réponses font apparaître des différences importantes entre les deux pays (voir la figure 5). Au Cameroun, 82 % des répondants (en particulier les membres des forces de l'ordre) font état de liens entre les réseaux cybercriminels nigérians (tels que les Yahoo Boys) et les réseaux de la diaspora camerounaise impliqués dans des escroqueries à l'emploi en ligne et des escroqueries sentimentales. Au Tchad, 70 % des répondants décrivent une forme de cybercriminalité plus locale et opportuniste, tandis que 30 % (en particulier les experts) font état de liens émergents avec des réseaux soudanais ou nigérians impliqués dans des fraudes liées au paiement mobile. Au Cameroun, 82 % des répondants font état de liens entre des acteurs locaux et des réseaux cybercriminels transnationaux d'Afrique de l'Ouest. Ces résultats mettent en évidence un réseau plus intégré au Cameroun, par rapport à une forme plus « artisanale » de cybercriminalité au Tchad, pays enclavé, même si cette dernière pourrait se professionnaliser au fil du temps.

Afin d'évaluer les difficultés auxquelles les deux pays sont confrontés dans la lutte contre les escroqueries à l'emploi en ligne, les répondants ont été invités à identifier les principales difficultés liées à la détection et à la poursuite des cybercriminels.

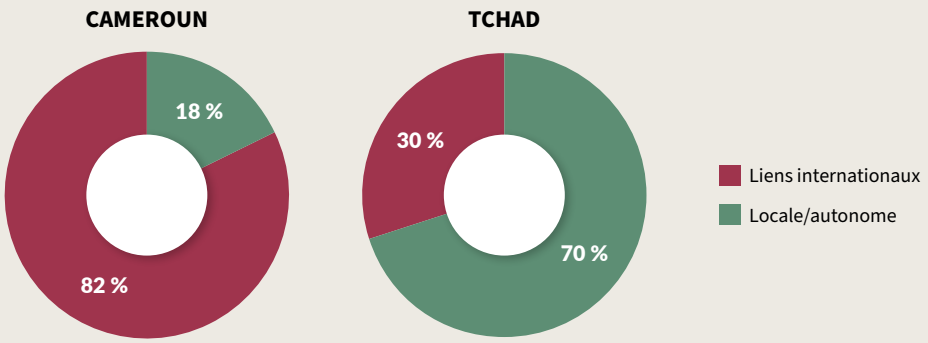

FIGURE 5 Perception de l'organisation des cybercriminels (locale ou internationale) au Cameroun et au Tchad

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

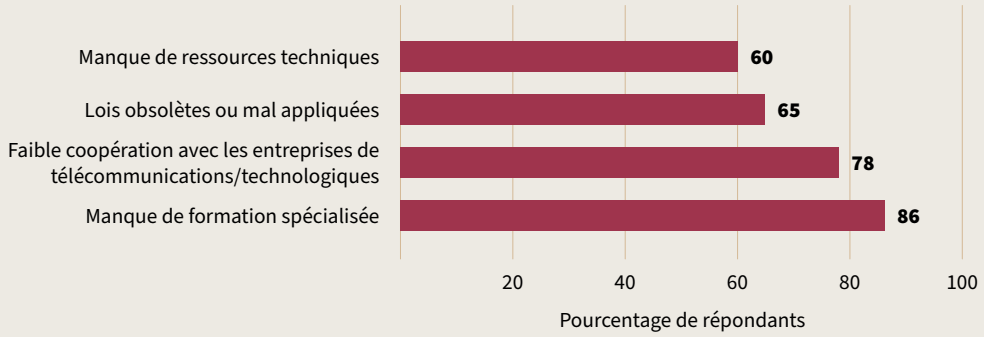

FIGURE 6 Classement des principaux obstacles à la lutte contre la cybercriminalité au Cameroun et au Tchad

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

Les obstacles sont en grande partie structurels et similaires dans les deux pays. Comme le montre la figure 6, 86 % des répondants considèrent le manque de formation spécialisée des enquêteurs et des juges comme l'une des principales difficultés. Environ 78 % des répondants soulignent également le manque de coopération opérationnelle avec les opérateurs de télécommunications et les entreprises technologiques (telles que Facebook et Google) pour l'obtention de preuves. Au moins 65 % des répondants indiquent que les cadres juridiques régionaux sont obsolètes ou appliqués de manière inégale. Les répondants (60 %) soulignent également l'insuffisance des ressources techniques, notamment des logiciels d'analyse forensique.

Dans l'ensemble, ces résultats indiquent que la lutte contre la cybercriminalité est davantage entravée par des lacunes en matière de capacités techniques et juridiques que par un manque de volonté politique. Bien qu'un cadre législatif existe au Cameroun (notamment la loi de 2010 sur la cybersécurité et la cybercriminalité), son application reste limitée. Ces contraintes en matière de capacités sont plus prononcées au Tchad.

Le grand public est considéré comme particulièrement vulnérable. Tous groupes de répondants confondus, 92 % d'entre eux estiment que le niveau de sensibilisation est « très faible » ou « faible ». Une faible minorité (8 %), composée d'experts et d'universitaires, estime que le niveau de sensibilisation est « moyen », tandis qu'aucun répondant ne le considère comme « bon ».

Un agent de services de paiement mobile à N'Djamena a indiqué : « Les gens reçoivent un SMS disant : "Votre compte est bloqué, appelez ce numéro", et ils appellent sans réfléchir. Ils nous donnent leurs codes sans comprendre le danger. »

Si les victimes camerounaises subissent des pertes plus élevées par incident (≈ 132 000 FCFA) que les victimes tchadiennes (≈ 58 000 FCFA), les données de la figure 7 montrent également que l'éventail des pertes est plus large au Cameroun (18 000–738 000 FCFA) qu'au Tchad (6 000–277 000 FCFA). Au Cameroun, les pertes sont généralement liées au paiement de visas, de frais administratifs ou de formations, tandis qu'au Tchad, elles sont plus souvent associées à des retraits effectués via des services de paiement mobile et à des paiements frauduleux liés à l'aide humanitaire. Malgré des pertes moins élevées par incident au Tchad, la fréquence plus importante des fraudes de faible ampleur liées au paiement mobile entraîne des répercussions économiques cumulées considérables à l'échelle nationale.

Les cybercriminels adaptent leurs stratégies aux réalités démographiques. Les jeunes adultes constituent le groupe le plus touché, tandis que le ciblage tend à s'équilibrer entre les hommes et les femmes (voir figure 8).

Les données indiquent également que, si les mécanismes sous-jacents des escroqueries restent les mêmes, leur mise en œuvre est façonnée par les conditions locales. Au Cameroun, cela se traduit par des opérations plus complexes et transnationales, tandis qu'au Tchad, la fraude tend à être plus directe et opportuniste, ciblant les groupes économiquement vulnérables.

Pays	Perte moyenne (FCFA)	Fourchette (FCFA)	Principal type de perte
Cameroun	132 000	18 000–738 000	Paiements de frais de visa, de frais administratifs ou de frais de formation
Tchad	58 000	6 000–277 000	Retraits par paiement mobile et fausses aides humanitaires

FIGURE 7 Estimation de la perte financière moyenne par escroquerie aboutie au Cameroun et au Tchad

SOURCE : Données issues d'entretiens avec des informateurs clés, 2025

Catégorie	Cameroun	Tchad	Observations
18–30 ans	61 %	58 %	Les jeunes restent le principal groupe ciblé en raison du chômage et de leur engouement pour le numérique.
31–50 ans	33 %	37 %	Vulnérabilité croissante liée au paiement mobile et à l'emploi informel.
Plus de 50 ans	6 %	5 %	Exposition limitée, mais risque croissant d'hameçonnage par SMS ou par téléphone.
Répartition par sexe (F/H)	45 % / 55 %	49 % / 51 %	Écart entre les sexes en baisse ; les femmes sont davantage ciblées par les arnaques à l'emploi à l'étranger et les escroqueries sentimentales.

FIGURE 8 Répartition des victimes de la cybercriminalité par âge et par sexe au Cameroun et au Tchad

SOURCE : Données issues d'entretiens avec des informateurs clés, juin 2025

Acteurs, réseaux et outils de la cybercriminalité

L'écosystème de la fraude en ligne en Afrique centrale, en particulier au Cameroun et au Tchad, n'est ni aléatoire ni isolé. Il s'agit d'un système à plusieurs niveaux, adaptatif et de plus en plus transnational, composé d'acteurs, de réseaux et d'outils numériques. Il est essentiel de comprendre cette structure pour concevoir des interventions et anticiper les tendances futures.

Les acteurs de l'écosystème de la cybercriminalité

Au cœur de l'écosystème de la cybercriminalité se trouvent les cybercriminels agissant à titre individuel, généralement de jeunes hommes âgés de 18 à 35 ans qui ont des perspectives d'emploi limitées, mais possèdent des compétences numériques moyennes. Souvent appelés « Yahoo Boys », ou localement « scammers », ces acteurs opèrent généralement seuls ou au sein de petits groupes informels. Leurs activités reposent davantage sur l'ingénierie sociale et la manipulation psychologique que sur des compétences techniques avancées[14]. Au Cameroun, ces individus se concentrent principalement dans les centres urbains, où l'accès à Internet est plus répandu et où ils se livrent à des escroqueries sentimentales et à des fraudes à l'investissement, ou publient de fausses offres d'emploi. Au Tchad, où la connectivité est plus faible et moins fiable, des acteurs similaires adaptent leurs méthodes en privilégiant les SMS et les appels vocaux. Dans les deux pays, leur principale motivation est la nécessité de subvenir à leurs besoins, la cybercriminalité étant perçue comme un moyen risqué mais accessible de gagner de l'argent.

Au-delà de ces acteurs individuels, on trouve des réseaux criminels organisés, qui constituent un niveau plus sophistiqué et plus dangereux de la cybercriminalité. Ces groupes opèrent souvent par-delà les frontières et sont fréquemment liés à des confréries nigérianes ou à des organisations cybercriminelles ouest-africaines bien établies. Sur le plan structurel, ils s'apparentent à des organisations de type entrepreneurial, dotées de hiérarchies clairement définies comprenant des dirigeants, des coordinateurs, des recruteurs et des « petites mains » chargées des opérations. Certains réseaux gèrent des « hustle academies » informelles, où les nouvelles recrues sont formées à la falsification de documents, à l'ingénierie sociale fondée sur des scénarios préétablis et aux techniques permettant d'échapper aux forces de l'ordre. Leurs activités

dépassent largement le cadre des escroqueries à l'emploi en ligne et englobent également les escroqueries sentimentales, la sextorsion et les stratagèmes liés à la migration. Il convient de souligner que ces réseaux sont souvent liés à d'autres économies illicites, telles que le trafic de stupéfiants, la contrebande et la traite des êtres humains, ce qui témoigne d'une convergence plus large entre la cybercriminalité et la criminalité transnationale organisée.

Les activités cybercriminelles, qu'elles soient le fait d'acteurs individuels ou de réseaux organisés, s'appuient sur une vaste catégorie d'acteurs qui en facilitent ou en permettent la conduite. Il s'agit notamment de recruteurs qui identifient et conditionnent de nouveaux participants ; de mules financières et de blanchisseurs informels qui font circuler les produits illicites par l'intermédiaire de plateformes de paiement mobile, de cryptomonnaies ou de biens de consommation ; et d'acteurs fournissant un appui technique, qui créent de faux sites web, reproduisent des noms de domaine de messagerie électronique ou fournissent une assistance de base en matière de TIC. Dans certains cas, des agents publics corrompus ou des intermédiaires complices jouent également un rôle en fermant les yeux sur des activités suspectes ou en facilitant l'accès à des documents et à des systèmes. Ces acteurs brouillent la frontière entre les auteurs directs et les acteurs fournissant un soutien logistique, ce qui complique considérablement les efforts visant à démanteler les réseaux cybercriminels.

Les dynamiques de genre façonnent également l'écosystème de la cybercriminalité. Si les hommes constituent la majorité des principaux auteurs, les femmes jouent fréquemment des rôles stratégiques en tant que recruteuses ou complices, en particulier dans les escroqueries sentimentales, où la confiance perçue et la crédibilité sur le plan émotionnel sont déterminantes. Dans le même temps, les femmes sont surreprésentées parmi les victimes, en particulier dans les escroqueries liées aux relations sentimentales, aux possibilités de travailler comme mannequin ou à l'emploi à l'étranger. Ces stratagèmes les exposent souvent à des risques accrus d'exploitation sexuelle et de traite des êtres humains, mettant ainsi en évidence la dimension genrée de la criminalité facilitée par le numérique.

Structures des réseaux et liens transnationaux

Les réseaux cybercriminels au Cameroun et au Tchad présentent diverses formes d'organisation, allant de groupes de pairs aux liens relativement informels à des organisations hiérarchisées. De nombreuses escroqueries trouvent leur origine dans de petites cellules informelles, au sein desquelles les individus partagent des scripts, des modèles et des méthodes par l'intermédiaire des réseaux sociaux ou des plateformes de messagerie[15]. Au fil du temps, les groupes qui réussissent développent souvent des structures plus hiérarchisées, ce qui leur permet d'accroître leur capacité à opérer à plus grande échelle, de spécialiser davantage les rôles et de renforcer leur résilience opérationnelle.

Les liens transnationaux jouent un rôle déterminant dans cette évolution. La diaspora africaine joue un rôle essentiel en facilitant l'accès à des comptes bancaires à l'étranger, à des sociétés-écrans et à une connaissance des contextes culturels permettant d'adapter les escroqueries aux victimes établies à l'étranger. Les membres de la diaspora peuvent également agir comme mules financières ou intermédiaires, contribuant ainsi à faire circuler des fonds entre différentes juridictions. Au Cameroun, les membres des forces de l'ordre et les experts interrogés soulignent systématiquement l'existence de liens étroits avec les réseaux cybercriminels nigérians, notamment avec des confréries telles que Black Axe. Le Tchad, bien que moins intégré sur le plan numérique, présente des liens de plus en plus étroits avec des groupes soudanais et nigérians, en particulier dans le domaine de la fraude liée au paiement mobile. Ces liens transforment des escroqueries qui, autrement, pourraient rester localisées en opérations relevant de la criminalité transnationale organisée.

Sur le plan économique, la cybercriminalité prospère dans les environnements caractérisés par des lacunes réglementaires et la faiblesse des mécanismes de contrôle. Les plateformes de paiement mobile sont fréquemment exploitées pour effectuer des transactions de faible montant, rapides et difficiles à retracer, tandis que les cryptomonnaies facilitent le blanchiment transfrontalier dans le cadre d'opérations de plus grande envergure. Les bénéfices sont généralement répartis de manière hiérarchique, de façon à maintenir une incitation financière à chaque niveau de l'organisation. Dans certaines communautés, la circulation des revenus illicites alimente la consommation locale et une redistribution informelle, favorisant ainsi une forme de complicité silencieuse qui contribue à ancrer davantage la cybercriminalité dans le tissu social.

Outils et technologies numériques

L'efficacité des opérations cybercriminelles est étroitement liée à l'utilisation stratégique des outils numériques. Les réseaux sociaux et les plateformes de messagerie, en particulier Facebook et WhatsApp, sont les principaux canaux de recrutement et de communication, offrant des moyens de communication directs et privés qui renforcent la crédibilité et la confiance[16]. Telegram et LinkedIn sont de plus en plus utilisés pour mener des escroqueries plus ciblées ou professionnalisées, tandis qu'Instagram sert à construire des identités en ligne fictives mais attrayantes.

Les techniques bien établies, telles que l'hameçonnage et l'usurpation d'identité, restent au cœur des pratiques cybercriminelles. Les escrocs utilisent couramment des courriels d'hameçonnage, des SMS et des sites web clonés, en se faisant passer pour des banques, des ministères ou des organisations humanitaires afin de créer un sentiment d'urgence et de donner une apparence de légitimité à leurs démarches. Ces méthodes sont particulièrement efficaces dans les contextes où la confiance envers les institutions reste relativement élevée et où les compétences numériques sont limitées.

Le transfert et la dissimulation des fonds reposent sur une combinaison d'outils de paiement et d'anonymisation. Les services de paiement mobile sont privilégiés pour les transactions de faible montant, tandis que les cryptomonnaies, les VPN et les techniques d'anonymisation sont utilisés pour dissimuler les identités et blanchir les produits d'activités illicites dans le cadre d'opérations de plus grande envergure ou plus complexes.

Plus récemment, l'adoption de technologies émergentes a marqué une nette progression dans le degré de sophistication des pratiques. Les outils reposant sur l'IA permettent désormais de produire des messages d'hameçonnage exempts de toute erreur grammaticale, de recourir à des agents conversationnels automatisés capables d'interagir simultanément avec un grand nombre de victimes et, dans certains cas, d'utiliser le clonage vocal ou des contenus hypertruqués (« deepfakes ») afin de renforcer la crédibilité des escroqueries. Ces innovations permettent de mener des escroqueries en ligne à une échelle considérablement plus grande, d'atteindre un public plus large et d'en rendre la détection plus difficile.

En définitive, l'écosystème de la cybercriminalité au Cameroun et au Tchad englobe un continuum d'acteurs, allant d'individus opportunistes à des organisations criminelles transnationales hautement structurées, qui s'appuient sur un réseau dense d'acteurs facilitant leurs activités ou contribuant à les rendre possibles. Sa résilience repose sur des structures organisationnelles adaptatives, des liens transfrontaliers établis par l'intermédiaire de la diaspora et l'exploitation stratégique des outils numériques. Les lacunes réglementaires qui caractérisent les systèmes de paiement mobile et de cryptomonnaies contribuent à ancrer la cybercriminalité dans les économies locales, tandis que les technologies émergentes telles que l'IA marquent une nouvelle phase de professionnalisation. Il est donc indispensable de comprendre les interactions entre les acteurs, les réseaux et les technologies afin d'élaborer des stratégies de lutte efficaces et adaptées au contexte en Afrique centrale.

Victimisation, vulnérabilité et exploitation

Les escroqueries numériques orchestrées par des réseaux criminels organisés en Afrique centrale causent d'importants préjudices financiers, psychologiques et physiques aux individus et aux communautés. Loin de constituer des infractions marginales ou de nature purement économique, les fausses offres d'emploi en ligne et les escroqueries connexes représentent un enjeu majeur sur les plans social et des droits humains. Cette section examine l'ampleur de la victimisation, identifie les populations les plus à risque et analyse le continuum de l'exploitation, en faisant valoir que la fraude facilitée par les technologies numériques est devenue un vecteur de violence structurelle et d'abus.

Ampleur et impact économique de la fraude en ligne

Il reste difficile de mesurer avec précision l'ampleur de la fraude en ligne en Afrique centrale en raison de la sous-déclaration généralisée des cas. De nombreuses victimes ne signalent pas ce qu'elles ont vécu, en raison de la honte et de la stigmatisation, en particulier lorsque l'escroquerie repose sur une tromperie d'ordre sentimental ou intime. La sous-déclaration s'explique également par un manque de confiance généralisé envers les institutions chargées de l'application de la loi, souvent perçues comme inefficaces, corrompues ou insuffisamment équipées pour faire face à ce phénomène. Dans les cas les plus graves, la crainte de représailles de la part de réseaux criminels organisés ou de réseaux de traite contribue encore davantage à dissuader les victimes de signaler les faits[17]. Par conséquent, les chiffres officiels ne rendent compte que d'une faible proportion des incidents, et l'ampleur réelle de la victimisation est presque certainement bien supérieure à ce que laissent penser les données disponibles.

Malgré ces limites, les estimations disponibles font état d'un coût économique considérable. Au Cameroun, l'ANTIC a estimé que la cybercriminalité avait entraîné des pertes d'environ 12,2 milliards de francs CFA pour la seule année 2021. Au Tchad, bien que l'on ne dispose pas de données nationales exhaustives, l'impact reste néanmoins considérable. Les pertes sont réparties entre des milliers de transactions de faible montant, en particulier dans le cadre de fraudes liées au paiement mobile, ce qui contribue à perpétuer les cycles de pauvreté et d'endettement. Pour les victimes, la perte de leur épargne — souvent

constituée en vue d'un projet migratoire, d'études ou pour subvenir aux besoins de leur famille — peut provoquer une véritable crise existentielle et plonger les ménages dans une précarité financière durable.

Les préjudices ne se limitent pas aux pertes financières directes. La prévalence des escroqueries érode la confiance dans les plateformes numériques et les institutions, ce qui freine le recours au commerce électronique et aux services en ligne, ainsi que la participation aux initiatives d'inclusion financière telles que le paiement mobile. Cette érosion de la confiance constitue un risque systémique pour les efforts de transformation numérique, agissant de fait comme une taxe régressive sur la participation au numérique et compromettant le potentiel de développement offert par la connectivité.

Profil des victimes et conséquences sociales

La victimisation n'est pas aléatoire. Les escrocs ciblent délibérément les populations que leur situation socio-économique et leur degré d'exposition aux technologies numériques rendent particulièrement vulnérables. Les jeunes et les personnes à la recherche d'un emploi constituent des cibles privilégiées, en particulier dans les contextes caractérisés par un chômage élevé et des possibilités d'emploi formel limitées[18]. Les fausses offres d'emploi et de recrutement exploitent les aspirations à l'ascension sociale, tant dans le pays qu'à l'étranger. Les migrants, les réfugiés et les personnes déplacées à l'intérieur de leur propre pays sont tout aussi vulnérables, car ils cherchent souvent à échapper à la pauvreté ou aux conflits et peuvent ne pas avoir accès à des informations fiables ou à des institutions susceptibles de les protéger. Les personnes âgées et celles dont les compétences numériques sont limitées sont également exposées à un risque accru, car elles sont moins à même de détecter les tromperies en ligne ou d'en reconnaître les signes avant-coureurs.

La fraude en ligne a des répercussions fortement différenciées selon le genre. Les femmes sont ciblées de manière disproportionnée par les escroqueries sentimentales, les fausses offres dans le mannequinat et les escroqueries liées aux emplois dans le secteur des soins à la personne, qui débouchent fréquemment sur de la sextorsion, de l'exploitation sexuelle ou de la traite des êtres humains. Ces expériences s'accompagnent d'une forte stigmatisation sociale, qui réduit souvent les victimes au silence et aggrave les préjudices psychologiques. Les hommes, en revanche, sont plus souvent ciblés par des escroqueries à l'emploi avec paiement anticipé, en particulier celles liées à des emplois à l'étranger ou dans le secteur de la sécurité.

Un piéton téléphone dans une rue de Douala, au Cameroun. Au-delà des pertes financières, les arnaques numériques laissent souvent aux victimes des séquelles émotionnelles et sociales durables. *© Daniel Beloumou Olomo/AFP via Getty Images*

Au-delà des pertes financières, les victimes subissent des traumatismes psychologiques durables. Les sentiments de honte et de culpabilité, la dépression et l'anxiété sont fréquents et s'accompagnent souvent d'une perte de confiance envers autrui et les systèmes numériques. L'ostracisme social et les atteintes à la réputation contribuent à isoler davantage les victimes, entravant leur rétablissement et les dissuadant de recourir aux mécanismes de soutien. En ce sens, la fraude en ligne engendre non seulement des souffrances individuelles, mais aussi une fragmentation sociale plus large.

De la fraude à l'exploitation : un continuum de l'exploitation

Si l'exploitation financière constitue la conséquence la plus visible des escroqueries en ligne, elle ne représente souvent que la première étape d'un continuum plus large d'abus. Le principal mécanisme est la fraude aux frais anticipés, qui consiste à amener les victimes à effectuer une série de paiements de montants croissants pour des visas, des formations, des démarches administratives ou des services fictifs. Parallèlement, de nombreuses escroqueries impliquent une usurpation d'identité, les documents personnels et les données recueillis sous couvert de « procédures officielles » étant réutilisés dans le cadre d'autres activités criminelles ou revendus sur des marchés illicites.

Plus préoccupant encore, un nombre croissant de cas témoignent d'un passage de la fraude en ligne à des formes d'exploitation physique et coercitive. Les offres d'emploi frauduleuses sont de plus en plus utilisées comme outils de recrutement par les réseaux de traite des êtres humains. Les victimes sont acheminées vers des destinations telles que les États du Golfe ou certaines régions d'Asie, où elles sont soumises au travail forcé ou à l'exploitation sexuelle dans des conditions s'apparentant à des formes modernes d'esclavage. Le contrôle est maintenu par la confiscation des documents, la servitude pour dettes et les menaces de violence, ce qui maintient les victimes dans une situation de dépendance vis-à-vis de leurs exploiteurs.

Les évolutions observées en Asie du Sud-Est constituent un avertissement sans équivoque pour l'Afrique centrale. Ces dernières années, des dizaines de milliers de personnes ont été victimes de traite vers des « centres d'escroquerie », où elles sont détenues et contraintes de se livrer à des activités de fraude en ligne sous la menace de torture. Les mécanismes qui sous-tendent ces opérations — recrutement en ligne, confiscation des documents, coercition et criminalité forcée — sont déjà présents en Afrique centrale. Ce parallèle met en évidence le risque que la région devienne à l'avenir une plaque tournante ou une zone d'approvisionnement pour des entreprises criminelles similaires si les tendances actuelles ne sont pas endiguées.

Enfin, la fraude en ligne en Afrique centrale ne constitue pas simplement un enjeu de cybersécurité, mais une menace multidimensionnelle qui reflète et accentue les inégalités structurelles existantes. Elle engendre des pertes économiques considérables, cause des préjudices psychologiques durables et facilite de plus en plus la traite des êtres humains et l'exploitation. La lutte contre ce phénomène exige donc une réponse globale, qui considère la fraude en ligne comme un enjeu de politique publique, de protection sociale et de droits humains, plutôt que comme un problème strictement technique. Sans une telle approche, le coût humain de la criminalité numérique continuera d'augmenter à mesure que la connectivité elle-même se développe.

Liens entre la cybercriminalité, les conflits régionaux et les migrations irrégulières

La fraude en ligne en Afrique centrale ne peut être appréhendée de manière isolée. Elle résulte plutôt de facteurs structurels, au premier rang desquels figurent les conflits armés prolongés, l'effondrement économique et la migration irrégulière. La cybercriminalité, l'insécurité et la migration irrégulière forment un triangle dans lequel ces trois phénomènes se renforcent mutuellement. Les conflits et l'instabilité créent les conditions sociales et économiques qui rendent les escroqueries en ligne à la fois attractives et efficaces ; ces escroqueries facilitent à leur tour la traite des êtres humains et la migration irrégulière ; et les produits de ces activités illicites peuvent être réinvestis dans de nouvelles violences. Dans ce cycle, la fraude en ligne apparaît non seulement comme une entreprise criminelle, mais aussi comme une menace pour la sécurité humaine et la stabilité régionale.

Les conflits et l'instabilité, facteurs favorisant la cybercriminalité

Les conflits armés ont un effet multiplicateur sur la cybercriminalité en désorganisant les économies formelles, en affaiblissant les institutions étatiques et en érodant la confiance sociale. Dans les régions touchées par la violence, les moyens de subsistance sont détruits, l'éducation est perturbée et les jeunes — souvent dotés de compétences numériques mais privés de perspectives économiques — sont poussés vers des stratégies de survie informelles et illicites. La cybercriminalité prospère dans ce vide, tirant parti des capacités limitées des services répressifs et de la banalisation des comportements à risque[19].

La crise anglophone au Cameroun illustre clairement cette dynamique. En effet, le conflit prolongé dans les régions du Nord-Ouest et du Sud-Ouest a déplacé plus d'un demi-million de personnes, dévasté les économies locales et réduit les possibilités d'emploi pour les jeunes diplômés. De nombreux anglophones, qui étaient auparavant en mesure de se lancer dans l'entrepreneuriat numérique licite, se trouvent désormais exclus du marché du travail formel[20]. Dans ce contexte où les possibilités sont limitées, la fraude

en ligne est ainsi perçue par certains comme une activité économique rationnelle plutôt que comme une activité purement criminelle. Les compétences numériques qui pourraient autrement être mises au service de l'innovation et du développement sont réorientées vers des activités d'escroquerie, inscrivant ainsi la cybercriminalité dans un contexte plus large d'effondrement économique provoqué par le conflit.

Une dynamique similaire s'observe dans le bassin du lac Tchad, où l'insurrection de Boko Haram a provoqué l'une des crises humanitaires les plus graves de la région. Des millions de personnes dans le nord du Cameroun et au Tchad sont déplacées à l'intérieur de leur propre pays ou dépendent de l'aide humanitaire. Les réseaux criminels exploitent cette vulnérabilité en se faisant passer pour des organisations internationales telles que le Haut-Commissariat des Nations Unies pour les réfugiés ou des ONG bien connues, et en proposant des programmes fictifs de réinstallation, des bourses d'études ou des possibilités d'emploi à l'étranger. Pour les personnes qui n'ont guère de perspectives d'avenir et ne bénéficient que d'une protection institutionnelle limitée, ces offres frauduleuses représentent une planche de salut, ce qui les rend plus enclines à payer des frais à l'avance ou à communiquer des informations personnelles malgré les risques.

Déplacements forcés, désespoir et cycles d'exploitation

Les personnes déplacées à l'intérieur de leur propre pays et les réfugiés occupent une position particulièrement précaire au sein de cet écosystème. Le déplacement fragilise les réseaux sociaux, érode les formes traditionnelles de protection communautaire et place les personnes concernées dans une situation de grave insécurité financière. Dans le même temps, les populations déplacées ressentent souvent un besoin urgent de reconstruire leur vie, ce qui les rend particulièrement vulnérables aux promesses d'emploi, de mobilité ou de statut juridique.

Les escroqueries ciblant les personnes déplacées imitent fréquemment les procédures d'aide humanitaire et exigent le paiement de « frais de traitement » pour de faux programmes d'aide, des visas ou des possibilités de formation. Les répercussions psychologiques de telles tromperies sont profondes, aggravant les traumatismes existants et renforçant la méfiance à l'égard des institutions. Plus préoccupant encore, les mêmes situations de détresse qui rendent les jeunes déplacés vulnérables aux escroqueries en font également des recrues potentielles pour les réseaux cybercriminels. Le déplacement alimente ainsi une dynamique cyclique dans laquelle la vulnérabilité conduit à l'exploitation, laquelle favorise à son tour une participation accrue aux activités criminelles.

Des personnes déplacées par Boko Haram vivent dans des abris de fortune à Hile Alifa, au Cameroun. Les déplacements forcés peuvent accroître le risque d'arnaques et d'exploitation pour les communautés vulnérables.
© Saabi Jeakespier/Anadolu via Getty Images

Cybercriminalité, migrations irrégulières et traite des êtres humains

Les escroqueries numériques constituent désormais le principal mécanisme de recrutement reliant la cybercriminalité à la migration irrégulière et à la traite des êtres humains. La fraude aux frais anticipés est particulièrement efficace, car elle permet de sélectionner des victimes qui se sont déjà engagées financièrement, se montrent coopératives et sont fortement investies psychologiquement dans la possibilité qui leur a été promise. Lorsque des offres d'emploi frauduleuses servent de façade à des opérations de traite des êtres humains, elles n'aboutissent pas à une migration irrégulière, mais à une forme d'esclavage moderne.

Les victimes recrutées en ligne sont acheminées vers des destinations telles que les États du Golfe ou de grandes villes africaines, où leurs passeports sont confisqués et où elles sont contraintes à la servitude domestique, à l'exploitation sexuelle ou au travail forcé. Les éléments constitutifs de la traite des êtres humains — tromperie, coercition et exploitation — sont tous présents, l'escroquerie numérique constituant le mécanisme initial de tromperie. En ce sens, la fraude en ligne n'est pas simplement connexe à la traite des êtres humains : elle fait partie intégrante de son mode opératoire[21].

Une autre dimension de cette convergence réside dans le risque que les revenus issus des escroqueries soient détournés pour financer les conflits armés. La fraude en ligne génère des revenus considérables et difficiles à retracer, en particulier dans les régions où le contrôle financier est faible. Ces fonds peuvent être blanchis par l'intermédiaire de réseaux transnationaux et, dans les contextes où la gouvernance est fragile, servir à acheter des armes ou à financer des groupes armés. Il en résulte un cercle vicieux dans lequel les conflits favorisent la cybercriminalité, la cybercriminalité finance l'instabilité et l'instabilité contribue à son tour à l'enracinement des économies criminelles.

Pris dans leur ensemble, les liens entre la cybercriminalité, les conflits et la migration irrégulière en Afrique centrale constituent une menace complexe et croissante. La violence armée et les déplacements engendrent des situations de détresse ; les escrocs exploitent cette détresse au moyen de tromperies numériques ; le recrutement frauduleux facilite la traite des êtres humains et les migrations forcées ; et les profits tirés de ces activités criminelles peuvent contribuer à financer les conflits qui les ont rendues possibles. La lutte contre la fraude en ligne exige donc davantage que de simples mesures techniques de cybersécurité. Elle nécessite une approche globale qui intègre la prévention de la cybercriminalité dans les politiques humanitaires, la gestion des migrations et les stratégies de sécurité régionale, tout en s'attaquant aux vulnérabilités sous-jacentes qui permettent à l'exploitation numérique de prospérer.

Vulnérabilités systémiques et réponses à la cybercriminalité

Les escroqueries à l'emploi en ligne au Cameroun et au Tchad perdurent dans un contexte marqué par un ensemble de facteurs structurels étroitement liés. Il s'agit notamment des lacunes en matière de culture numérique, des limites des cadres juridiques et institutionnels, des capacités restreintes des services répressifs et d'une coopération régionale et internationale inégale. Bien qu'il existe tout un éventail de mesures aux niveaux national, régional et international, leur mise en œuvre demeure inégale et leur efficacité reste limitée dans la pratique. La section suivante examine ces vulnérabilités parallèlement aux mesures actuellement mises en œuvre et met en évidence les principales lacunes qui continuent de favoriser la fraude en ligne.

L'essor du numérique sans préparation adéquate

L'une des principales faiblesses réside dans l'expansion rapide de l'accès à Internet, qui ne s'est pas accompagnée d'investissements correspondants dans la culture numérique. Au Cameroun et au Tchad, des millions de nouveaux utilisateurs ont accédé aux espaces numériques sans être suffisamment préparés aux risques liés aux usages du numérique. Cette lacune est particulièrement marquée dans les zones rurales et parmi les premières générations d'internautes, qui ont souvent tendance à considérer les contenus en ligne comme intrinsèquement crédibles. Les escrocs exploitent cette confiance en recourant à des sites web d'apparence professionnelle, à des logos officiels, à un langage administratif et, de plus en plus, aux langues locales afin de donner une fausse impression de familiarité et de légitimité.

La précarité économique accentue encore cette vulnérabilité. Dans les contextes marqués par un chômage élevé des jeunes et une mobilité sociale limitée, les offres d'emploi, de bourses d'études ou de possibilités de migration ne sont pas évaluées uniquement en fonction de leur plausibilité, mais aussi de la nécessité d'y recourir. De nombreuses victimes constatent des incohérences, mais donnent malgré tout suite à ces offres, faute d'autre perspective que de rester en situation d'exclusion. En ce sens, les escroqueries réussissent non pas parce que les individus manquent de discernement, mais parce que les privations structurelles les poussent à faire passer l'espoir avant la prudence.

Les initiatives de sensibilisation du public n'ont guère contribué à inverser cette tendance[22]. Les campagnes sont souvent axées sur les zones urbaines, de courte durée et formulées dans un langage technique ou juridique qui ne trouve guère d'écho auprès des personnes les plus exposées. Les populations rurales, les personnes déplacées, les femmes et les jeunes sans emploi sont souvent laissés de côté, alors même qu'ils constituent des cibles privilégiées des escroqueries. En outre, la coordination entre les ministères, les services répressifs, les établissements d'enseignement et les organisations de la société civile demeure insuffisante, et les efforts de prévention sont insuffisamment financés. Par conséquent, la ligne de défense présentant le meilleur rapport coût-efficacité — la sensibilisation du public — reste la moins développée.

Des réponses juridiques et institutionnelles fragiles

Les cadres institutionnels et juridiques du Cameroun et du Tchad sont mal adaptés à la lutte contre la criminalité facilitée par le numérique[23]. Au Cameroun, la loi de 2010 sur la cybersécurité et la cybercriminalité fournit un cadre juridique général, mais son application demeure inégale et fait souvent l'objet de critiques pour privilégier les préoccupations liées à la sécurité de l'État au détriment de la protection des victimes et de leur accès à des voies de recours. Au Tchad, l'absence de législation spécifiquement consacrée à la cybercriminalité contraint les procureurs à s'appuyer sur des dispositions obsolètes relatives à la fraude, mal adaptées aux infractions numériques, ce qui se traduit par de faibles taux de condamnation et un climat d'impunité.

Ces limites juridiques sont aggravées par des faiblesses institutionnelles. Les services répressifs manquent de formation spécialisée, de capacités en matière de criminalistique numérique et de ressources suffisantes pour enquêter sur des escroqueries en ligne complexes. Même lorsqu'il existe des unités spécialisées dans la cybercriminalité, celles-ci ont tendance à manquer de financements, à fonctionner de manière isolée et à être submergées par le nombre d'affaires à traiter. La corruption et les dysfonctionnements bureaucratiques érodent davantage la confiance du public, ce qui dissuade les victimes de signaler les infractions et contribue à perpétuer le sous-signalement.

La nature transnationale de la cybercriminalité pose un défi supplémentaire. Les escroqueries s'étendent fréquemment sur plusieurs juridictions, tandis que l'action des services répressifs reste limitée par les frontières nationales. Les procédures d'entraide judiciaire sont lentes et lourdes, tandis que les cadres de coopération régionale sont insuffisamment développés ou mal mis en œuvre. Les réseaux criminels exploitent ces failles juridictionnelles et opèrent par-delà les frontières sans guère craindre de faire l'objet de poursuites coordonnées.

Lacunes technologiques et déficit de données

Un fossé technologique croissant sépare les cybercriminels des institutions chargées de les combattre. Les enquêteurs ne disposent souvent pas des outils et de l'expertise nécessaires pour analyser les appareils saisis, retracer les transactions numériques ou surveiller les communications chiffrées[24]. Les preuves numériques sont fréquemment mal traitées ou déclarées irrecevables, ce qui compromet les poursuites et renforce la perception d'une incapacité de l'État à agir.

L'absence de données fiables est tout aussi problématique. Le sous-signalement chronique, conjugué à l'absence de mécanismes centralisés de signalement ou de dispositifs d'aide aux victimes, crée un angle mort statistique. Les autorités ne sont pas en mesure de dégager des tendances, de cartographier les

zones sensibles ou d'établir des liens entre des affaires connexes dans différentes régions. Les décideurs sont ainsi contraints d'agir sans disposer de données empiriques sur lesquelles s'appuyer, tandis que les victimes restent isolées et privées de soutien. Ce déficit de données affaiblit non seulement l'action des services répressifs, mais masque également l'ampleur réelle des préjudices causés par la fraude en ligne.

Les réseaux sociaux et le déficit de responsabilité

Les plateformes mondiales de réseaux sociaux et de messagerie constituent la principale infrastructure utilisée pour mener ces escroqueries. Des services tels que Facebook, WhatsApp, Instagram et Telegram offrent anonymat, portée et rapidité, tout en conférant une apparence de légitimité aux profils et aux publicités frauduleux. Bien que ces plateformes affirment lutter contre la fraude, leurs systèmes de modération fonctionnent principalement de manière réactive et sont mal adaptés aux langues locales, aux contextes culturels et aux typologies régionales d'escroqueries.

Ces entreprises ayant leur siège en dehors de la région, les autorités locales se heurtent à des obstacles importants pour obtenir des données sur les utilisateurs ou une coopération en temps utile. Il en résulte un déficit de responsabilisation : les plateformes bénéficient économiquement de la croissance du nombre d'utilisateurs, tout en n'assumant qu'une responsabilité minimale à l'égard des préjudices subis par ces derniers en Afrique centrale. Ce déséquilibre accentue encore la vulnérabilité, les criminels continuant d'exploiter les fonctionnalités des plateformes plus rapidement que les mesures de protection ne sont mises en place.

Des réponses nationales divergentes

Les efforts déployés pour lutter contre la fraude en ligne au Cameroun et au Tchad montrent que, malgré un nombre croissant de lois, d'organismes et de stratégies, leur impact concret reste limité.

Le Cameroun a mis en place le dispositif national de lutte le plus élaboré de la sous-région d'Afrique centrale. Sa loi de 2010 sur la cybersécurité et la cybercriminalité fournit une base juridique formelle pour engager des poursuites, tandis que l'ANTIC constitue l'organisme central en matière de gouvernance de la cybersécurité. L'ANTIC gère une équipe nationale d'intervention en cas d'urgence informatique (CERT), diffuse des alertes à l'intention du public, fournit une assistance en matière de criminalistique numérique et dispense des formations aux membres des services répressifs et aux acteurs du système judiciaire. Ces initiatives constituent des avancées importantes vers l'institutionnalisation de la prévention et de la lutte contre la cybercriminalité.

Malgré ces avancées relatives, l'efficacité de l'ANTIC demeure limitée. Les efforts de sensibilisation du public restent largement axés sur les zones urbaines et ne parviennent pas à atteindre les populations rurales ou en situation d'exclusion numérique. Les rivalités institutionnelles limitent le partage d'informations avec les services de police et de gendarmerie, tandis que le manque de financements restreint la capacité de l'agence à investir dans des outils d'enquête avancés ou à mener durablement des campagnes de sensibilisation du public. Par conséquent, bien que le dispositif camerounais soit plus développé que celui des pays voisins, son effet dissuasif reste limité et inégal.

La situation au Tchad apparaît plus fragile. Bien qu'une loi adoptée en 2015 ait créé l'ANSICE, cette agence de cybersécurité fonctionne avec des effectifs et des moyens budgétaires très limités et ne dispose même pas d'un laboratoire de base de criminalistique numérique. Il n'existe aucune unité de police spécialisée dans la cybercriminalité et les enquêtes sont généralement menées par des agents

généralistes peu formés au traitement des preuves numériques, au chiffrement ou aux demandes de données entre différents pays. Le cadre juridique lui-même est général et insuffisamment adapté aux formes contemporaines de fraude en ligne, si bien que les poursuites aboutissent rarement, voire jamais. Ce vide institutionnel favorise un sentiment d'impunité, qui enhardit les acteurs criminels.

Coopération régionale et sous-régionale : des ambitions sans mise en œuvre

Compte tenu de la dimension transfrontalière de la fraude en ligne, la coopération régionale est indispensable. Pourtant, dans la pratique, cette coopération reste faible et inégale. Aux niveaux continental et sous-régional, des cadres tels que la Convention de Malabo de l'Union africaine et les initiatives menées au sein de la CEEAC visent à harmoniser les législations relatives à la cybercriminalité et à favoriser le partage d'informations. Toutefois, la mise en œuvre a été lente et inégale, plusieurs États, dont le Tchad, n'ayant pas encore ratifié certains instruments essentiels[25]. L'instabilité politique, les priorités concurrentes en matière de sécurité et les ressources financières limitées ont relégué la cybercriminalité au second plan dans les programmes régionaux.

Dans ce contexte, les acteurs non étatiques, en particulier les organisations de la société civile et les ONG, apportent un soutien aux victimes, mènent des campagnes de sensibilisation au niveau local et plaident en faveur de réformes des politiques publiques. Bien qu'utiles, ces efforts restent fragmentés et dépendent de financements à court terme de la part des bailleurs de fonds, ce qui limite leur pérennité et leur portée.

Coopération internationale et contraintes structurelles persistantes

À l'échelle internationale, le Cameroun et le Tchad sont confrontés à des contraintes structurelles qui limitent leur capacité à lutter contre la criminalité facilitée par le numérique. L'une des principales contraintes tient au fait que le Tchad n'est pas partie à la Convention de Budapest sur la cybercriminalité, qui constitue le principal cadre multilatéral de lutte contre la cybercriminalité au moyen d'enquêtes transfrontalières, de normes juridiques harmonisées et de l'entraide judiciaire. Le Cameroun, en revanche, a adhéré à la Convention en 2022, son adhésion étant officiellement entrée en vigueur en avril 2024. Cette non-adhésion limite la coopération avec les services répressifs étrangers, complique les enquêtes conjointes et peut retarder, voire empêcher, l'accès à des preuves numériques essentielles détenues à l'étranger. Dans le cas des escroqueries transnationales, ces lacunes créent des angles morts juridictionnels susceptibles d'être exploités.

Les organisations internationales jouent un rôle important, quoique limité, pour remédier à ces lacunes. INTERPOL joue un rôle particulièrement important en coordonnant des opérations multinationales, des mécanismes de partage de renseignements et des plateformes de communication sécurisées qui permettent aux forces de police nationales d'échanger des informations plus efficacement. De même, des institutions telles que l'ONUDC et l'UE fournissent une assistance technique, des programmes de renforcement des capacités et des formations spécialisées dans des domaines tels que la criminalistique numérique, les enquêtes sur la cybercriminalité et la protection des victimes. Toutefois, ces initiatives sont souvent mises en œuvre dans le cadre de projets ponctuels plutôt qu'intégrées dans des stratégies institutionnelles à long terme. Par conséquent, leur impact tend à être inégal et difficile à pérenniser.

Ces limites à l'échelle internationale se conjuguent aux difficultés rencontrées au niveau national. Bien que les deux pays disposent de cadres juridiques et d'institutions spécialisées, leur mise en œuvre est entravée par un sous-financement chronique, la faible priorité accordée à la cybercriminalité et le manque de personnel qualifié. La forte rotation du personnel au sein des administrations publiques affaiblit encore les capacités, les agents formés étant fréquemment réaffectés à des services sans rapport avec leurs compétences ou quittant la fonction publique, ce qui entraîne une perte de mémoire institutionnelle. Dans le même temps, les réseaux organisés de cybercriminalité disposent de ressources financières plus importantes, d'outils technologiques plus avancés et de structures transnationales souples qui leur permettent de s'adapter rapidement.

Par conséquent, les mesures prises par les États restent largement réactives. Les services répressifs interviennent après que les infractions ont été commises, plutôt que de mener des actions proactives de prévention ou de perturbation des activités criminelles. Le décalage entre l'ampleur, la rapidité et le degré de sophistication des opérations cybercriminelles, d'une part, et les ressources limitées dont disposent les autorités nationales, d'autre part, contribue à la persistance de cette vulnérabilité. Sans des engagements juridiques internationaux plus solides, des investissements durables dans les capacités institutionnelles et une intégration plus étroite des mécanismes de coopération internationale dans les stratégies nationales, ces contraintes structurelles risquent de perdurer.

Défis techniques et réglementaires liés au traçage des téléphones utilisés par les escrocs

Un obstacle technique majeur à la lutte contre les escroqueries à l'emploi en ligne au Cameroun et au Tchad réside dans la difficulté à retracer les téléphones portables utilisés par les auteurs. Cette difficulté résulte d'une combinaison de solutions technologiques improvisées, de lacunes réglementaires et de mesures délibérées de dissimulation mises en œuvre par les réseaux criminels, ce qui limite l'efficacité du traçage des téléphones portables en tant qu'outil essentiel de criminalistique numérique.

Les principaux facteurs contribuant à cette difficulté sont les suivants :

- **Prévalence des cartes SIM prépayées et non enregistrées.** La plupart des escroqueries sont menées à l'aide de numéros de téléphone mobile associés à des cartes SIM prépayées qui, dans les deux pays, peuvent être achetées anonymement et en grande quantité. Malgré les efforts réglementaires visant à imposer l'enregistrement des cartes SIM, l'application de cette obligation reste inégale. Les escrocs exploitent cette faille en utilisant des cartes SIM enregistrées à l'aide de faux documents d'identité ou de documents d'identité volés, ce qui place les enquêteurs dans une impasse une fois le numéro identifié. Par conséquent, il est difficile de retrouver les preneurs d'otages qui appellent pour négocier et recevoir les rançons, car les cartes SIM sont jetées après utilisation. Les bandits et les preneurs d'otages utilisent les appels téléphoniques classiques depuis les années 1990, en particulier dans les zones rurales et frontalières.
- **Utilisation de téléphones « jetables » et usurpation de numéros de téléphone.** Les escrocs les plus sophistiqués utilisent un modèle fondé sur une « infrastructure éphémère ». Ils utilisent des téléphones et des cartes SIM bon marché pendant de courtes périodes, souvent pour une seule campagne d'escroquerie, avant de s'en débarrasser (« téléphones jetables »). En outre, les services de voix sur IP (VoIP) et les applications d'usurpation de l'identifiant de l'appelant permettent aux escrocs de masquer leurs véritables numéros internationaux en les remplaçant par des numéros camerounais ou tchadiens locaux et apparemment légitimes, ce qui permet de ne pas éveiller les soupçons des victimes et d'induire en erreur les enquêteurs lors des premières tentatives de traçage.

- **Opérations transfrontalières et complexité juridictionnelle.** Les réseaux d'escroquerie sont souvent transnationaux. Un escroc ciblant des victimes à N'Djamena peut opérer depuis une région frontalière du Cameroun en utilisant une carte SIM camerounaise, tandis que le serveur de commande et de contrôle est hébergé dans un pays tiers. Le traçage d'un tel appel nécessite une coopération en temps réel entre plusieurs autorités de régulation des télécommunications et services répressifs de différents pays ; ce processus est entravé par les lenteurs bureaucratiques, l'absence d'accords formels et, souvent, une méfiance mutuelle. Même à l'intérieur d'un même pays, les preneurs d'otages qui négocient le versement d'une rançon se déplacent loin de l'endroit où ils se trouvent réellement avant d'appeler un proche de la victime, orientant ainsi les enquêteurs vers le lieu d'où l'appel a été passé.
- **Capacités techniques limitées des services répressifs.** Même lorsqu'un numéro suspect est identifié, les services répressifs locaux ne disposent souvent pas des unités spécialisées en criminalistique numérique, du matériel et du personnel formé nécessaires pour enquêter efficacement sur les fraudes facilitées par le numérique. Ces capacités comprennent notamment la réalisation d'analyses avancées des réseaux mobiles, l'extraction de données à partir d'appareils saisis et la collaboration avec des opérateurs de télécommunications internationaux afin de retracer des outils plus sophistiqués, tels que les téléphones à double carte SIM et les applications de messagerie chiffrée (par exemple Telegram et WhatsApp), utilisés aux stades ultérieurs des escroqueries.
- **Lacunes dans la collaboration avec les opérateurs de télécommunications.** Un traçage efficace nécessite une coopération rapide des opérateurs de réseaux mobiles, sur décision judiciaire. Dans la pratique, ce processus peut être lent. Les opérateurs de réseaux mobiles peuvent invoquer les lois relatives à la protection de la vie privée ou exiger de nombreuses formalités juridiques, si bien que, lorsque celles-ci sont accomplies, l'escroc a déjà abandonné le numéro. Il n'existe pas non plus de protocoles automatisés permettant le partage de données en temps réel entre les opérateurs de réseaux mobiles et les unités de lutte contre la cybercriminalité concernant les numéros signalés comme étant utilisés à des fins frauduleuses.

Par conséquent, cette difficulté de traçage crée un « bouclier d'impunité » pour les escrocs. Cela reporte la charge de l'enquête sur les témoignages des victimes et les traces numériques (par exemple, captures d'écran et transactions bancaires), éléments souvent insuffisants pour localiser physiquement les auteurs. Cela érode également la confiance du public dans la capacité des autorités à rendre justice, décourage le signalement des infractions et perpétue le cycle de la criminalité.

Conclusions et recommandations

La révolution numérique offre d'importantes perspectives économiques et sociales à l'Afrique centrale, mais fait également émerger de nouveaux risques criminels, notamment des fraudes en ligne liées à de fausses offres d'emploi et à des stratagèmes à caractère socio-économique au Cameroun et au Tchad. Les modes opératoires des auteurs, les conséquences pour les victimes et les liens avec les conflits régionaux et les migrations sont clairement établis. Toutefois, les réponses nationales et régionales révèlent un décalage important entre l'ampleur de la menace et les capacités disponibles pour y faire face. Ces constats mettent en évidence des implications plus larges pour l'Afrique centrale et font ressortir les principales mesures à prendre pour renforcer durablement la cyberrésilience.

La précarité économique, le chômage élevé et la pauvreté persistante créent un terreau fertile tant pour les victimes que pour les auteurs. Les individus, souvent en quête désespérée de débouchés, sont attirés par des promesses d'enrichissement rapide ou de partenariats lucratifs, tandis que les jeunes à l'aise avec les technologies numériques, mais marginalisés sur le plan économique peuvent considérer la cybercriminalité comme un moyen apparemment accessible de sortir de la pauvreté.

L'expansion des infrastructures numériques, conjuguée à leur répartition inégale et à une faible culture numérique, accentue la vulnérabilité. L'argent mobile, les réseaux sociaux et les places de marché en ligne offrent à la fois des outils favorisant l'essor d'activités légitimes et des possibilités d'exploitation. Les escrocs exploitent la confiance, les réseaux de relations et les vulnérabilités émotionnelles pour cibler des individus et des communautés.

Plusieurs thèmes récurrents se dégagent :

- La cybercriminalité s'est développée dans la région sous l'effet des difficultés économiques, du chômage des jeunes, de l'adoption généralisée des technologies numériques et de la faiblesse de la gouvernance. Les escroqueries en ligne liées à l'emploi et à l'intégration ciblent les populations vulnérables et opèrent par-delà les frontières nationales, ce qui accroît leur impact.
- Ces escroqueries ont une double conséquence : des pertes financières et des traumatismes psychologiques pour les victimes, ainsi qu'une érosion de la confiance dans les plateformes numériques, les institutions et les processus publics.

- Les cadres juridiques et institutionnels du Cameroun et du Tchad ont connu des avancées inégales. La loi camerounaise de 2010 sur la cybersécurité et la cybercriminalité ainsi que l'ANTIC ont permis de faire progresser les efforts de sensibilisation, de surveillance et de coordination, mais le sous-financement, le manque de coordination et les lacunes dans la mise en œuvre en limitent l'efficacité. La loi tchadienne de 2015 portant création de l'ANSICE reste largement inappliquée, tandis que la faiblesse des capacités opérationnelles, l'absence d'unités spécialisées et le recours aux méthodes policières traditionnelles compromettent la lutte contre les infractions à caractère technique.
- Les cadres régionaux tels que la Convention de Malabo de l'Union africaine et les initiatives de la CEEAC constituent une base pour l'harmonisation, mais la lenteur des ratifications et la mise en œuvre inégale en limitent les effets. Les organismes axés sur les questions de sécurité n'ont abordé la cybercriminalité que de manière indirecte, tandis que les ONG et les organisations de la société civile mènent des initiatives de sensibilisation du public fragmentées et apportent un soutien aux victimes.
- À l'échelle internationale, l'adhésion à des instruments tels que la Convention de Budapest reste partielle. Les programmes d'INTERPOL, de l'ONUDC et de l'UE contribuent à la formation et aux opérations, mais leur impact à long terme dépend d'une plus grande appropriation au niveau national.

Pris dans leur ensemble, ces constats indiquent que, malgré les progrès accomplis, des difficultés persistantes — notamment la faiblesse des services répressifs, les capacités judiciaires limitées, le manque de ressources techniques, l'insuffisance de la coordination et les facteurs socio-économiques — rendent la réponse de l'Afrique centrale inégale et largement réactive.

Les implications vont au-delà du Cameroun et du Tchad. De fait, la cybercriminalité menace la transformation numérique, le développement économique et la crédibilité des services numériques dans l'ensemble de la région. Les escroqueries érodent la confiance dans les plateformes en ligne, dissuadant ainsi les citoyens et les entreprises de participer à l'économie numérique.

La nature transnationale de la cybercriminalité souligne la nécessité d'une coordination régionale. En effet, les criminels exploitent les lacunes des législations nationales et de leur application, en ciblant le maillon le plus faible de la chaîne régionale. La lenteur de la ratification de la Convention de Malabo et la participation limitée aux instruments internationaux accentuent cette vulnérabilité. La cybercriminalité reflète également des problèmes de gouvernance plus larges : la faiblesse des capacités de l'État, l'application inégale de l'État de droit et le manque de ressources facilitent non seulement la fraude, mais aussi toute une série d'activités illicites, ce qui porte atteinte à la légitimité de l'État.

À ces problèmes de gouvernance s'ajoutent les conditions socio-économiques, qui aggravent encore la menace. Le chômage élevé des jeunes et la pauvreté incitent à participer à des activités de fraude en ligne, contribuant ainsi à banaliser les activités illicites. L'absence de mesures visant à agir sur ces facteurs risque de favoriser l'émergence d'une « culture de la cybercriminalité » dans laquelle la fraude devient un moyen de subsistance. Les conséquences se font sentir à l'échelle mondiale, car la faiblesse des mesures répressives dans une région peut favoriser les activités des réseaux transnationaux, créer des zones de refuge et mettre à rude épreuve les relations internationales. Les réponses nationales et régionales actuelles aux escroqueries à l'emploi en ligne restent fragmentées et nettement insuffisantes. Au niveau national, le Cameroun dispose d'un cadre juridique relativement avancé, qui repose sur la loi de 2010 sur la cybersécurité et la cybercriminalité et sur un organisme spécialisé chargé de son application, l'ANTIC. Toutefois, sa mise en œuvre est fortement entravée par un sous-financement chronique, des capacités techniques limitées et une faible coordination entre les organismes concernés. En revanche, la réponse du Tchad n'en est encore qu'à ses débuts. L'organisme chargé de la mise en œuvre de ce cadre, l'ANSICE, ne dispose ni des ressources financières ni des ressources humaines nécessaires pour lutter efficacement

contre la cybercriminalité, tandis que les instruments juridiques existants sont obsolètes et mal adaptés à la collecte, à la conservation et à l'admissibilité des preuves numériques.

Au niveau régional, des instruments normatifs tels que la Convention de Malabo de l'Union africaine constituent une base solide pour la coopération, mais leur ratification et leur transposition en droit interne restent lentes et inégales en Afrique centrale. La CEEAC, bien que chargée d'assurer la coordination régionale, ne dispose pas de mécanismes opérationnels concrets permettant le partage d'informations en temps réel et la conduite d'enquêtes conjointes, ce qui crée involontairement des failles juridictionnelles et des zones de refuge pour les réseaux cybercriminels.

Sur le plan systémique, les réponses sont affaiblies par le faible niveau de culture numérique de la population, l'obsolescence des cadres juridiques, le manque de ressources et de formation des services répressifs, ainsi que la responsabilisation limitée des plateformes mondiales de réseaux sociaux, qui constituent les principaux vecteurs de recrutement et de diffusion des escroqueries.

Le renforcement de la résilience face à la fraude en ligne nécessite une approche coordonnée et multidimensionnelle intégrant des réponses juridiques, institutionnelles, techniques et socio-économiques, ainsi que des mécanismes de coopération. Le renforcement des cadres juridiques et institutionnels, l'amélioration des capacités techniques et opérationnelles, le renforcement de la prévention et de la sensibilisation du public, l'approfondissement de la coopération régionale et internationale et la prise en compte des facteurs socio-économiques sous-jacents sont autant de composantes essentielles d'une réponse efficace.

Recommandations

Les vulnérabilités au Cameroun et au Tchad sont déterminées à la fois par les méthodes employées par les cybercriminels et par les faiblesses des réponses existantes. Des lois et des institutions formelles existent, mais leur existence ne se traduit pas par une efficacité concrète. La lutte contre la fraude en ligne ne peut se limiter à l'action des services répressifs ; il s'agit d'un enjeu systémique lié aux lacunes en matière de gouvernance, au manque de ressources et aux pressions socio-économiques. Une stratégie coordonnée et multidimensionnelle est donc nécessaire, afin de renforcer les cadres juridiques, de développer les capacités institutionnelles, d'améliorer la sensibilisation du public, de favoriser la coopération, d'assurer un suivi continu des zones exposées aux conflits et d'agir sur les facteurs socio-économiques qui influent à la fois sur la vulnérabilité des victimes et sur les motivations des criminels.

Renforcement des cadres juridiques et institutionnels

Un cadre juridique cohérent est essentiel pour lutter efficacement contre la cybercriminalité. Le Cameroun comme le Tchad sont confrontés à des difficultés liées à l'obsolescence des lois, à la fragmentation des mandats et à la faiblesse de leur application. Une harmonisation avec les normes internationales et une adaptation aux menaces émergentes sont nécessaires. Le Cameroun, qui a ratifié la Convention de Budapest sur la cybercriminalité, doit rendre ses dispositions opérationnelles, notamment en simplifiant le partage de preuves et l'entraide judiciaire. Le Tchad, qui accuse un retard en matière de ratification, devrait accélérer son alignement sur la Convention. À l'échelle continentale, les deux pays devraient accorder la priorité à la mise en œuvre concrète de la Convention de Malabo de l'Union africaine afin d'établir un socle commun pour la coopération transfrontalière entre les services répressifs.

Au-delà de l'harmonisation, les législations doivent prendre en compte les innovations technologiques exploitées par les criminels. Des outils tels que les cryptomonnaies, les escroqueries fondées sur l'IA et les

hypertrucages nécessitent des dispositions juridiques ciblées afin de garantir que leurs auteurs répondent de leurs actes. Il est également essentiel d'établir des normes claires en matière de preuves numériques — notamment en ce qui concerne leur admissibilité, leur conservation et la chaîne de possession —, car de nombreuses poursuites échouent en raison d'une mauvaise manipulation des preuves ou de leur rejet. Des lignes directrices procédurales à l'intention des juges, des procureurs et des enquêteurs peuvent contribuer à renforcer le processus judiciaire.

Les capacités institutionnelles sont essentielles à l'application effective de la loi. Des unités spécialisées dans la cybercriminalité devraient être créées au sein des services répressifs, dotées de personnel formé ainsi que de budgets et de ressources techniques dédiés. Les juges et les procureurs doivent bénéficier d'une formation continue sur la cybercriminalité et les preuves numériques. Au Cameroun, l'ANTIC devrait étendre ses activités de sensibilisation dans les zones rurales et renforcer ses capacités en matière de criminalistique numérique, tandis qu'au Tchad, l'ANSICE devrait être développée de manière à devenir une agence pleinement opérationnelle, notamment par la création de CERT chargés de surveiller les menaces, de coordonner la réponse aux incidents et de collaborer aux niveaux régional et international.

Renforcement des capacités opérationnelles et techniques

Les capacités opérationnelles et techniques sont essentielles pour perturber efficacement les activités cybercriminelles. Des investissements dans des laboratoires de criminalistique numérique, du matériel et des logiciels de pointe, ainsi que dans la formation du personnel sont nécessaires. Les gouvernements et les partenaires internationaux devraient accorder la priorité aux outils permettant d'extraire et d'analyser les données provenant des appareils mobiles, du stockage dans le cloud et des transactions en cryptomonnaies. Les systèmes d'IA et d'apprentissage automatique peuvent permettre une détection proactive des menaces en analysant les réseaux sociaux et les places de marché en ligne afin de repérer les schémas d'activités frauduleuses avant qu'ils ne causent des préjudices.

La mise en place d'une base de données centralisée de renseignement sur la cybercriminalité est également essentielle. En compilant les signalements des victimes, des institutions financières et des opérateurs de télécommunications, les autorités peuvent dégager des tendances, établir des liens entre les affaires et suivre les traces numériques. Ces renseignements améliorent l'efficacité des enquêtes et facilitent les poursuites. L'interopérabilité entre les systèmes nationaux et régionaux est essentielle pour permettre un partage rapide des informations et des réponses coordonnées.

Prévention et sensibilisation du public

Une réponse efficace nécessite des actions proactives de sensibilisation du public. Des campagnes nationales de sensibilisation du public devraient être menées sur plusieurs supports, en combinant la radio, la télévision et les réseaux sociaux afin de toucher des publics diversifiés. Les messages devraient être clairs et indiquer les mesures à prendre, en mettant en évidence les signes d'alerte courants, tels que les demandes de paiement anticipé, les promesses qui semblent « trop belles pour être vraies » et les tactiques de manipulation émotionnelle.

La culture numérique et la sensibilisation à la cybersécurité devraient être intégrées dans les programmes scolaires et les programmes de formation des adultes, afin de doter la population des compétences nécessaires pour évoluer en toute sécurité dans l'environnement numérique. Des programmes adaptés aux groupes vulnérables, notamment aux personnes âgées et aux communautés rurales, sont essentiels. Des services d'aide aux victimes accessibles, notamment des lignes d'assistance téléphonique et des

portails en ligne, devraient fournir des conseils, une assistance juridique et un soutien psychologique, en tenant compte des conséquences de la fraude en ligne[26].

Renforcement de la coopération régionale et internationale

La fraude en ligne transcende les frontières et nécessite donc des réponses coordonnées. Les organismes régionaux tels que la CEEAC devraient formaliser des plateformes de partage d'informations en temps réel et d'enquêtes conjointes, et désigner dans chaque État membre des agents de liaison spécialisés dans la cybercriminalité. Des exercices conjoints de formation et des réunions de planification opérationnelle organisés régulièrement peuvent contribuer à harmoniser les procédures et à favoriser des interventions transfrontalières coordonnées.

À l'échelle internationale, il est essentiel de renforcer la coopération avec INTERPOL, l'ONUDC et les programmes d'assistance technique de l'UE. Les pays devraient tirer parti de ces partenariats pour développer des capacités institutionnelles durables, acquérir du matériel de criminalistique numérique, mettre en place des CERT et mener des campagnes de sensibilisation efficaces. L'assistance technique devrait privilégier le transfert de connaissances afin de garantir une appropriation au niveau local et une résilience à long terme.

Prise en compte des facteurs socio-économiques

La cybercriminalité est alimentée non seulement par les lacunes institutionnelles, mais aussi par des conditions socio-économiques structurelles, notamment le chômage élevé des jeunes, la pauvreté et l'exclusion sociale. Pour lutter durablement contre la cybercriminalité, il est nécessaire de mettre en œuvre des mesures économiques offrant des possibilités légitimes de générer des revenus et d'entreprendre. Les gouvernements devraient stimuler une croissance inclusive, soutenir les petites et moyennes entreprises et créer des débouchés dans les secteurs à forte intensité d'emploi, tels que l'agriculture et les services numériques.

Des formations professionnelles axées sur les compétences numériques, notamment la programmation, la conception graphique, l'analyse de données et le marketing numérique, peuvent permettre aux jeunes d'acquérir des compétences recherchées sur le marché du travail. Les programmes devraient cibler les personnes à risque et les anciens cybercriminels, en leur offrant des alternatives aux activités illicites. Les initiatives menées au niveau communautaire, en particulier dans les zones touchées par les conflits et les difficultés économiques, devraient associer des micro-subventions, des programmes de mentorat, un soutien psychosocial et des programmes éducatifs afin d'offrir des moyens de sortir de l'exploitation criminelle.

La lutte contre la fraude en ligne au Cameroun et au Tchad exige de passer de stratégies réactives et étroitement axées sur l'action des services répressifs à une approche proactive, globale et coordonnée. La réforme juridique, le renforcement des capacités institutionnelles, l'innovation technique, la sensibilisation du public, la coopération régionale et internationale et le développement socio-économique doivent aller de pair. La cybercriminalité n'est pas seulement une question de maintien de l'ordre ; elle constitue un enjeu systémique de gouvernance et de développement. Seule une stratégie durable, multidimensionnelle et collaborative permettra de démanteler l'écosystème de la fraude en ligne, de donner aux citoyens les moyens d'agir et de créer des économies numériques inclusives qui réduisent la vulnérabilité. La mise en œuvre de ces recommandations offre l'occasion non seulement de lutter contre la cybercriminalité, mais aussi de renforcer les institutions, de favoriser la cohésion sociale et de garantir à l'ensemble des citoyens un avenir numérique plus prospère.

Notes

1 Les Yahoo Boys désignent, dans le langage courant au Nigeria, de jeunes individus se livrant à la fraude en ligne, notamment au hameçonnage, aux arnaques sentimentales et à la fraude aux frais anticipés. Cette appellation trouve son origine dans l'utilisation initiale de Yahoo! Messenger comme outil pour entrer en contact avec des victimes potentielles.

2 Agence nationale des technologies de l'information et de la communication, citée dans Pouvoirs d'Afrique, « *La cybercriminalité fait perdre des milliards de FCFA au Cameroun* », 8 mars 2022 ; et ITWeb Africa, « Cameroon loses 12.2-bn CFA to cybercrime in 2021 », 18 octobre 2022.

3 Voir : https://data.worldbank.org/indicator/IT.NET.USER.ZS.

4 Union internationale des télécommunications, Statistics : Global and Regional ICT Data, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Chiffres pour 2024 et taux de croissance annuels depuis 2005 calculés à partir de Measuring digital development : Facts and Figures 2024 de l'Union internationale des télécommunications.

5 Ecofin Agency, « Africa's Internet Growth Outpaces World, but Gaps in Access Remain Deep », 5 juin 2025, https://www.ecofinagency.com/news-digital/0506-47164-africa-s-internet-growth-outpaces-world-but-gaps-in-access-remain-deep.

6 Voir CRE VC, Internet Penetration in Africa, https://www.cre.vc/news-slider/internet-penetration-in-africa-infographic.

7 Agence de régulation des télécommunications, Observatoire annuel 2024 du marché des communications électroniques au Cameroun.

8 Simon Kemp, Digital 2026 : Cameroon, DataReportal, 8 novembre 2025, https://datareportal.com/reports/digital-2026-cameroon.

9 Union internationale des télécommunications (UIT), Measuring digital development : Facts and Figures 2025, disponible à l'adresse suivante : https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

10 Simon Kemp, Digital 2026 : Chad, DataReportal, 8 novembre 2025, https://datareportal.com/reports/digital-2026-chad.

11 Banque mondiale, World Bank Increases Access to Broadband Connectivity in Chad, 25 septembre 2024, https://www.worldbank.org/en/news/press-release/2024/09/25/world-bank-increases-access-to-broadband-connectivity-in-chad.

12 Eyong Effi Atem, Assessing the Gaps in Cybersecurity Resilience in Cameroon: Challenges and Opportunities for Strengthening National Cybersecurity Frameworks, *Journal of Computer and Communications*, 13(2) (2025).

13 Alima Nzeket Njoya et al., « Mobile money phishing cybercrimes : Vulnerabilities, taxonomies, and characterization from an investigation in Cameroon », Towards New e-Infrastructure and e-Services for Developing Countries, 14th EAI International Conference, AFRICOMM 2022, Zanzibar, Tanzanie, décembre 2022, https://eudl.eu/proceedings/AFRICOMM/2022.

14 Emmanuel Niyikora, Cybersecurity risk assessment methods for digital financial services in Sub-Saharan Africa, thèse de doctorat, Walden University, 2025, https://scholarworks.waldenu.edu/dissertations/18000/.

15 Yushawu Abubakari, « The reasons, impacts, and limitations of cybercrime policies in Anglophone West Africa: A review », *Przestrzeń Społeczna*, 2021.

16 Victor A. Adewopo et al., Comprehensive analytical review of cybercrime and cyber policy in West Africa, *Journal of Electrical Systems and Information Technology*, 12, 1 (2025).

17 Newman U. Richards et Felix Eboibi, African governments and the influence of corruption on the proliferation

of cybercrime in Africa: wherein lies the rule of law?, *International Review of Law, Computers & Technology,* 35, 2 (2021).

18 O. T. Adisa, The impact of cybercrime and cybersecurity on Nigeria's national security, 2023.

19 Shai Farber, The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications, *Security Journal,* 38, 1 (2025).

20 Fonjock Harris Kunju, Digital warfare: Exploring Cyber criminality amidst armed conflict in the Southwest region of Cameroon, Journal of Research in Social Science and Humanities, 3, 10 (2024).

21 Alex Motshwanetsi Mathole, Coverage of modern slavery and human trafficking in national risk assessments within Sub-Saharan Africa, United Nations University Centre for Policy Research, mars 2023, https://collections.unu.edu/eserv/UNU:9093/National_Risk_Assessments_vFINAL.pdf ; Oluwole Ojewale, Shadow of death: the criminal economy of banditry and kidnapping in northwest Nigeria, *Security Journal*, 37, 4 (2024) ; Freedom C Onuoha, The terrorism-organized crime nexus in the Boko Haram insurgency in Nigeria, in *The Nexus Between Organized Crime and Terrorism.* Cheltenham : Edward Elgar, 2022.

22 Alain Hugues Obame, *L'usage d'Internet comme circonstance aggravante de responsabilité pénale, une introduction*, *ADILAAKU — Droit, politique et société en Afrique*, 2, 1 (2022) ; Tim Hall et Ulrike Ziemer, Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework, *The Commonwealth Cybercrime Journal*, 1, 1 (2023).

23 GN Gasu, Legal responses to combat the menace of cybercrime in sub-Saharan Africa: A comparative analysis, GLR, 4 (2022).

24 Maria Grazia Porcedda et David S Wall, Modelling the cybercrime cascade effect in data crime, dans IEEE European Symposium on Security and Privacy Workshops, 2021.

25 Ugah John Otozi et al., Cybercrime and its negative effects in developing countries, Journal of Mobile Computing and Application, 11, 4 (2024).

26 Tim Hall et Ulrike Ziemer, Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework, *The Commonwealth Cybercrime Journal*, 1, 1 (2023).

ISS | INSTITUT D'ÉTUDES DE SÉCURITÉ

L'Institut d'études de sécurité (ISS) établit des partenariats afin de développer les connaissances et les compétences nécessaires pour assurer l'avenir de l'Afrique. L'ISS est une organisation africaine à but non lucratif disposant de bureaux en Afrique du Sud, au Kenya, en Éthiopie et au Sénégal. Grâce à ses réseaux et à son influence, l'ISS fournit des recherches politiques fiables et opportunes, ainsi que des formations pratiques et une assistance technique aux gouvernements et à la société civile.

issafrica.org

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

The Global Initiative Against Transnational Organized Crime (l'Initiative mondiale contre la criminalité organisée transnationale, GI-TOC) est un réseau international rassemblant plus de 800 experts à travers le monde. La GI-TOC fournit une plateforme destinée à promouvoir un débat plus large et des approches innovantes comme composantes d'une stratégie mondiale inclusive de lutte contre la criminalité organisée.

globalinitiative.net