



RÉPUBLIQUE TOGOLAISE

Travail-Liberté-Patrie

MANUEL D'ÉDUCATION À LA CITOYENNETÉ NUMÉRIQUE



Elaboré par
LA DIRECTION DE LA FORMATION CIVIQUE

Août 2022

 Editions
Awoudy

***MANUEL D'ÉDUCATION
À LA CITOYENNETÉ NUMÉRIQUE***

**ÉLABORÉ PAR LA DIRECTION
DE LA FORMATION CIVIQUE**

**MANUEL D'ÉDUCATION À LA
CITOYENNETÉ NUMÉRIQUE**

Août 2022

Editions Awoudy

ISBN 978-2-37316-412-1

© 2022 Direction de la Formation Civique

© Editions Awoudy, Lomé, 2022

04 B.P. 969 Lomé-Togo

Tel : (+228) 22502327 - 90062327

edit.awoudy@hotmail.fr

www.editionsawoudy.com

Octobre 2022

*Tous droits de reproduction, d'émission
ou d'adaptation réservés pour tout pays.*

SOMMAIRE

Préface.....	7
Remerciements.....	10
Sigles et abréviations.....	11
Introduction.....	13
1. HISTORIQUE ET CONCEPTS FONDAMENTAUX DU NUMERIQUE.....	15
2. ENVIRONNEMENT DU NUMERIQUE AU TOGO.....	41
3. QUELQUES CONSEILS PRATIQUES.....	61
Bibliographie.....	81

PRÉFACE

La révolution du numérique a favorisé une nouvelle façon de communiquer, de travailler, d'apprendre, de faire les affaires, de se divertir. Son impact positif sur le mode de vie de l'homme et sur le développement de nos pays n'est plus à démontrer.

Cependant, le cyberspace est fortement miné par des comportements inacceptables tels que : la dépravation des mœurs, la prolifération des fake news, l'escroquerie, la diffamation, l'intimidation, des propos suscitant la haine, la violence, l'intolérance, les attaques de tout genre.

Les pouvoirs publics, dans leur rôle d'éducateur et de protecteur des droits humains, ont lancé des programmes de sensibilisation et de formation de la population en général et des jeunes en particulier, à l'utilisation responsable et judicieuse des services et technologies numériques, dont les réseaux sociaux.

Le présent document, intitulé « Manuel d'éducation à la citoyenneté numérique », est une contribution du Ministère des droits de l'homme, de la formation à la citoyenneté et des relations avec les institutions de la République avec l'appui

technique des ministères chargés de la sécurité, de l'économie numérique et de l'enseignement supérieur à cette œuvre d'information et de formation du public.

Il est un outil didactique à la disposition des formateurs et des organisations de la société civile pour mieux aider à comprendre et à diffuser les règles et principes de la citoyenneté numérique et à maîtriser les compétences indispensables en la matière.

Il doit être utilisé avec pédagogie pour favoriser un meilleur apprentissage commun des technologies du numérique. Il est accessible à tout public.

J'exprime mes remerciements à tous les pédagogues et autres contributeurs à son élaboration et souhaite à tous un bon usage de ce manuel.

Le Ministre des droits de l'homme, de la formation à la citoyenneté et des relations avec les institutions de la République

Dr Christian Eninam TRIMUA

REMERCIEMENTS

Le Ministère des droits de l'homme, de la formation à la citoyenneté et des relations avec les institutions de la République (MDHFCRIR) remercie le Ministère de l'économie numérique et de la transformation digitale (MENTD), le Ministère de l'enseignement supérieur et de la recherche (MESR), le Ministère de la sécurité et de la protection civile (MSPC), les Organisations de la société civile (OSC) et les personnes ressources dont les apports ont été déterminants dans la rédaction, la validation et la finalisation de ce manuel.

Ces remerciements sont également adressés à tous ceux qui ont contribué, de près ou de loin, à l'élaboration de ce précieux document. A tous ces acteurs, le MDHFCRIR exprime sa gratitude et sa reconnaissance, au nom de l'idéal de promotion des valeurs civiques et citoyennes.

Ce document a été élaboré grâce à la participation de :

- TCHENDO Kpatcha, commissaire divisionnaire de police, conseiller en communication au ministère de la sécurité et de la protection civile ;
- ETIM Messanvi, directeur juridique au ministère de l'économie numérique et de la transformation digitale ;
- TCHANGAI Bassa Ezzo, Maître Assistant en Histoire contemporaine et Formateur à l'Ecole normale supérieure (ENS) d'Atakpamé ;
- TALIM Asksno Anathère, juriste, conseiller d'action culturelle, directeur de la formation civique ;
- TCHAKPALA Alfa, conseiller d'action culturelle, chef de division chargé des conférences et séminaires à la direction de la formation civique (DFC) ;
- SOBO Doh-Kossi, conseiller d'action culturelle à la DFC ;
- KOKOVENA Yawo Dzigbodi, conseiller d'action culturelle adjoint à la DFC.

SIGLES ET ABREVIATIONS

- ANCy : Agence Nationale de Cybersécurité
- ANID : Agence Nationale d'Identification
- ANSR : Agence Nationale du Spectre des Radiofréquences
- ARCEP : Autorité de Régulation des Communication Electronique et des Postes
- ATD : Agence Togo Digital
- CDA : Cyber Défense Africa
- CERT : Computer Emergency Response Team
- COE : Conseil de l'Europe
- DFC : Direction de la Formation Civique
- ECN : Education Citoyenneté Numérique
- ENS : Ecole Normale Supérieure
- FSN : Fond de Souveraineté Numérique
- IRM : Imagerie par Résonance Magnétique
- ISBN : International Standard Book Number / Numéro International Normalisé du Livre
- LCE : Loi N° 2012-018 sur la Communication Electronique modifiée par la loi N° 2013-003
- LOSITO : Loi N° 2017-006 d'Orientation sur la Société de l'Information au TOGO
- LTE : loi N° 2017-07 relative aux Transactions Electroniques
- MDHFCRIR : Ministère des Droits de l'Homme, de la Formation à la Citoyenneté, des Relations avec les Institutions de la République
- MENTD : Ministère de l'Economie Numérique et de la Transformation Digitale
- MESR : Ministère de l'Enseignement Supérieur et de la Recherche
- MOOC : Massive Online Open Courses
- MSPC : Ministère de la Sécurité et de la Formation Civile

- NIU : Numéro d'Identification Unique
- NTIC : Nouvelle Technologie de l'Information et de la Communication
- ODD : Objectif de Développement Durable
- ONU : Organisation des Nations Unies
- OPT : Office Postal du TOGO
- OPTT : Office des Postes et Télécommunication du TOGO
- OSC : Organisation de la Société Civile
- PND : Plan National de Développement
- PNFC-EC : Politique Nationale de Formation Civique et d'Education à la Citoyenneté
- PTT : Poste Télégraphe et Téléphone
- SMS : Short Message Service
- SPT : Service des Postes et Télécommunication
- SOFIE
- TIC : Technologie de l'Information et de la Communication
- UNESCO : Organisation des Nations Unies pour l'Education, la Science et la Culture
- UNICEF : Fonds des Nations Unies pour l'Enfance
- URL : Uniform Resource Locator
- USB : bus informatique plug and play
- USM : Université Sans les Murs
- VPN : Réseau Privé Virtuel
- WARCIP : Programme Ouest-Africain de Développement des Infrastructures de Communication

INTRODUCTION

L'apparition du numérique, dans le monde en général et au Togo en particulier, a profondément révolutionné la façon dont les individus communiquent, travaillent, apprennent, commercent et se divertissent. Son impact positif sur le développement n'est plus à démontrer. Le gouvernement, s'inscrivant dans cette dynamique, a prévu, dans le plan national de développement (PND) 2018-2022, en son axe stratégique 1, encadré 1, effet attendu 5, de faire du numérique un véritable levier de modernisation de l'économie et de la société togolaise en rendant les services des technologies de l'information et de la communication (TIC) accessibles au plus grand nombre de citoyens estimé à 90% de la population à l'horizon 2022. C'est, également, à juste titre que la feuille de route 2021-2025 du gouvernement lui consacre une bonne place dans les priorités en l'inscrivant à l'axe 3 qui place le digital au cœur de la modernisation de l'Etat. Cette ambition affichée par les plus hautes autorités de notre pays ne peut être effective sans une réelle prise de conscience, par les utilisateurs, des enjeux des services numériques, particulièrement des réseaux sociaux.

En effet, ces dernières années, notre pays fait face à une montée de l'incivisme dans le cyberspace caractérisé par la dépravation des mœurs, la prolifération des fake news, des intimidations, des attaques de tout genre, de l'escroquerie, de la diffamation, des propos suscitant la haine, la violence, l'intolérance, etc. Malgré l'existence de plusieurs lois, notamment celles sur la cybersécurité,

la protection des données à caractère personnel, la communication électronique et sur la société de l'information, la situation reste préoccupante. On note une persistance de la diffusion de scènes perverses touchant toutes les tranches d'âges et qui achoppent aux bonnes mœurs.

Il est donc important de conscientiser la population à l'utilisation responsable des services numériques, notamment des réseaux sociaux.

A cet effet, il importe de disposer d'outils de référence permettant d'assurer l'éducation des populations en la matière en vue de contribuer à l'atteinte du but visé par la Politique nationale de formation civique et d'éducation à la citoyenneté (PNFC-EC), à savoir : amener le citoyen à s'approprier et à vivre les valeurs républicaines à travers une citoyenneté active en vue de sa pleine participation au développement humain durable conformément à la vision de faire du Togo une nation moderne, forte, unie et prospère.

C'est pour y parvenir que le MDHFCRIR, à travers la DFC, a élaboré le présent manuel destiné aux acteurs de l'éducation à la citoyenneté numérique (ECN) et aux usagers du numérique. Il se donne pour vocation de compiler les concepts fondamentaux en éducation à la citoyenneté numérique, l'environnement du numérique au Togo et quelques conseils pratiques.

1. HISTORIQUE ET CONCEPTS FONDAMENTAUX DU NUMERIQUE

1.1. Historique du numérique

L'une des conséquences jugée positive de la deuxième guerre mondiale est la révélation, dans les années 1940, de l'ordinateur, l'élément déclencheur de la « révolution numérique ».

Selon G. Berry (2008), « Le numérique est un langage, un code constitué de suites de nombres représentés en système binaire par des groupes de 0 et de 1. Ce langage est utilisé par différents équipements conçus pour le comprendre, comme les ordinateurs, les tablettes, les appareils photo, les caméscopes, les écrans de télévision (...).

L'usage des techniques numériques présente d'innombrables avantages : elles facilitent les opérations délicates telles que la comptabilité, la statistique, la diffusion des informations, la sécurisation des données, la reproduction facile et rapide des documents, etc.

La prise de conscience qu'avec l'usage des Techniques numériques tout devient facile, on dépense peu, on va vite, on peut tout faire sans forcément se déplacer, etc., a poussé progressivement les hommes du XXe siècle à se tourner vers le numérique. Alan Turing, l'un des initiateurs de l'intelligence artificielle, a prédit en 1950 que le numérique sera dans quelques années à la base de profonds bouleversements dans le monde.

Dans les années 2000, Nicolas Aguila (2008) a distingué trois grandes phases ou tournants dans l'histoire du numérique :

- la généralisation de l'ordinateur personnel et la naissance d'Internet dans les années 1980. Pour mémoire, le premier téléphone mobile (une DynaTac 8000¹) a été vendu par la firme Motorola en 1983 ;
- l'explosion du phénomène Internet, surnommé « le réseau des réseaux » dans les années 1990² ;
- l'apparition, dans les années 2000, du smartphone ou ordinateur dans la main pouvant être utilisé pratiquement partout sur la planète.

Les importantes innovations observées sont : les échanges par voie électronique et la disparition des barrières géographiques et culturelles. Ces mutations bouleversent l'ensemble des règles géopolitiques mondiales. L'économie devient planétaire, rendant ainsi caduques les mesures protectionnistes classiques. La perception du monde par les individus et leurs comportements avec autrui changent. Le monde devient un village planétaire sous la houlette du numérique.

La culture numérique se caractérise ainsi par de nouveaux produits très variés, notamment les microordinateurs, les portatifs, les téléphones portables, les clés USB, etc.

Les techniques numériques sont aujourd'hui indispensables. L'exemple le plus plausible est l'usage des téléphones portables à partir desquels les activités sont organisées dans tous les secteurs :

¹ Nicolas Aguila, 2008 : « Il était une fois, le téléphone portable », Tom's Guide, 7 mai 2008.

² Dico info : <http://dictionnaire.phpmyvisites.net/definition-Reseau-des-Re-seaux-9504.htm>]

primaire, secondaire, tertiaire et surtout quaternaire : c'est "**l'ère du numérique**", "**la révolution numérique**".

La révolution numérique est aussi connue sous les appellations : révolution technologique, révolution Internet, ou révolution digitale.

La tendance au numérique qui a commencé en Occident, a gagné en si peu de temps le monde asiatique puis l'Afrique. Contrairement aux modèles classiques de la technique occidentale qui ont mis des décennies pour parvenir à l'Afrique, les innovations technologiques, grâce à la magie de la diffusion, parviennent, de façon instantanée, à tous les coins du globe.

De 1980 à ce jour, l'adaptation des Africains aux TIC a connu plusieurs phases. Qu'en est-il de l'histoire du numérique au Togo ?

Historique du numérique au Togo

Si l'ordinateur est l'élément déclencheur du numérique et de son évolution, on peut alors situer les prémices du numérique dans les années 1980 à travers les premières initiations à l'informatique qui ont révolutionné la bureautique et l'administration. L'apparition et l'usage de nouveaux matériels tels que l'ordinateur, l'imprimante, la photocopieuse, ont commencé par s'inviter dans le quotidien des Togolais. Les éléments les plus visibles sont à l'actif des services de téléphonies créés et les prestations rendues possibles par ceux-ci.

L'héritage colonial en matière de téléphonie au Togo mérite d'être souligné. Les principales réalisations sont :

- la mise en place de communications postales, téléphoniques et télégraphiques en 1888 ;
- l'installation d'une station émettrice à Kamina (Atakpamé) en

1913. Par ce poste, Lomé fut reliée le 3 janvier 1913 au câble sous-marin qui joignait l'Allemagne ;

– la création des Postes, Télégraphes et Téléphones (PTT) le 13 octobre 1920 ;

– la transformation des PTT en Office Postal du Togo (OPT) en 1934 ;

– la création des Services des Postes et Télécommunications (SPT) en 1947 (N. Gayibor, 1987).

Au lendemain des indépendances (1960), les services de la téléphonie s'inscrivent progressivement dans l'environnement numérique.

En 1986, les télécommunications voient le jour à travers l'Office des Postes et Télécommunication du Togo (OPTT)³.

Pour être en phase avec les TIC, le Togo crée en 1996 la Société des Télécommunications du Togo (Togo Télécom) indépendamment de la Société des Postes du Togo (SPT)⁴.

Le 18 février 1998, en moins de deux ans, au regard de la flambée de la téléphonie mobile, le groupe Togo Télécom se dote d'une filiale mobile, Togo Cellulaire, une société d'Etat à caractère commercial de droit privé.

En 1999, le secteur togolais des télécommunications accueille un nouvel opérateur : Télécel, qui, en 2007, devient Atlantique Télécom Togo, filiale du groupe Etisalat, puis aujourd'hui Moov Africa.

La politique sectorielle élaborée par le Ministère des Postes et Télécommunication en 2011, renouvelée en 2018 encourage l'utilisation des TIC dans les services de l'Etat et dans l'éducation.

³ Décret PR/ N°86-190 du 17 septembre 1986.

⁴ Décret PR/ N°96-22 du 28 février 1996.

Le changement de dénomination du ministère pour intégrer le terme d'« économie numérique » traduit la volonté de l'Etat togolais de placer les TIC au cœur du développement.

Le 30 juin 2014, le Ministère des postes et de l'économie numérique a procédé au lancement d'un avis d'appel d'offres portant attribution d'une troisième licence d'établissement et d'exploitation de réseaux et services de télécommunications 2G, 3G et 4G dans le but de relever le niveau de la concurrence pour des services de qualité. Aujourd'hui, le pays est passé à la phase expérimentale de la 5G.

La transformation du groupe Togo Télécom en Togocom a été réalisée pour permettre à cet acteur historique de mieux répondre aux défis du futur.

L'histoire des télécommunications au Togo est loin d'être achevée. De nombreux chantiers dans le domaine sont en cours afin de permettre au pays de ne pas rester en marge de la révolution du numérique qui, d'ailleurs, s'impose au monde entier.

1.2. Clarification des concepts

Les concepts clés indispensables à la compréhension de l'ECN sont : l'éducation, la citoyenneté, le numérique et la citoyenneté numérique.

- L'éducation

Selon le Petit Larousse (2018), l'éducation est l'action de former l'esprit de quelqu'un, de développer ses aptitudes intellectuelles, physiques, son sens moral.

Elle est, pour E. Durkheim (2013), « l'action exercée par les

générations adultes sur celles qui ne sont pas encore mûres pour la vie sociale. Elle a pour objet de susciter et de développer chez l'enfant un certain nombre d'états physiques, intellectuels et moraux que réclament de lui et la société politique dans son ensemble et le milieu spécial auquel il est particulièrement destiné ».

Les objectifs assignés à l'éducation sont dynamiques et fonction de l'environnement des apprenants et des enjeux mondiaux.

A travers cette nouvelle vision de l'école, le gouvernement togolais recherchait un profil de citoyen : « (...), des individus sains, équilibrés et épanouis dans toutes les dimensions ». La nouvelle école devrait permettre la formation de l'esprit critique, base de toute culture moderne.

Le citoyen ainsi formé devra être capable de s'adapter aisément à toutes les situations nouvelles, plein d'initiatives et apte à agir sur le milieu pour le transformer.

- La citoyenneté

La Politique Nationale de Formation Civique et d'Education à la Citoyenneté (PNFC-EC) définit la citoyenneté comme la qualité par laquelle une personne est reconnue comme membre d'une société ou d'un Etat. Elle est synonyme de nationalité qui est la reconnaissance d'appartenance à un Etat. C'est le lien social entre une personne et l'Etat en vertu duquel cette personne est jugée apte à exercer l'ensemble des droits politiques attachés à cette qualité. Elle se définit aujourd'hui comme une participation active à la vie de la cité.

Pour A. Bergougnieux (2005)⁵, «l'éducation à la citoyenneté est un ensemble de valeurs, de principes, de savoirs, de pratiques, estimés indispensables à un moment donné pour préparer les jeunes à participer le mieux possible à la vie démocratique, en assumant et en exerçant leurs droits et leurs devoirs citoyens ».

- Le numérique

L'adjectif « numérique » vient du latin « *numerus* » (« nombre », « multitude ») et signifie « représentation par nombres ». Devenu substantif, « numérique » désigne actuellement les technologies de l'information et de la communication (TIC). Cet usage est spécifique au français, la plupart des autres langues, notamment l'anglais, utilisent le mot « digital », du latin « *digitus* » qui signifie « doigt ». *Digital*, en anglais, est spécifique au traitement informatique en rapport avec l'usage du doigt.

En lien avec la citoyenneté, on parle de citoyenneté numérique.

- La citoyenneté numérique

Elle désigne le maniement efficace et positif, par le citoyen, des technologies numériques pour créer, communiquer, apprendre, rechercher, travailler, partager, établir des relations sociales, jouer, etc. C'est la participation active et responsable du citoyen à tous les niveaux de la vie de sa communauté à travers le numérique.

L'Organisation des nations unies pour l'éducation, la science et la culture (UNESCO) définit la citoyenneté numérique comme le fait de « posséder des équipements et des compétences TIC qui

⁵ Bergougnieux Alain, 2005 : « L'École et l'éducation civique », pp54-60. Il est Inspecteur général de l'Éducation nationale en France

permettent de participer à la société numérique, par exemple d'accéder à des informations gouvernementales en ligne, d'utiliser des sites de réseaux sociaux et de faire usage d'un téléphone mobile ».

Ainsi, **le citoyen numérique** fait référence à une personne en mesure d'utiliser les TIC pour s'engager dans la société⁶. C'est une personne qui est capable, parce qu'elle a acquis un large éventail de compétences, de participer de façon active, positive et responsable aux communautés en ligne et hors ligne, au niveau local ou mondial.

La citoyenneté numérique implique une « littératie numérique— », c'est-à-dire une compréhension des limites entre les blagues, les taquineries, les actions inoffensives et les comportements criminels. Étant donné que les gouvernements sanctionnent de plus en plus sévèrement la cyberintimidation, il est nécessaire que les jeunes, leurs parents et les écoles soient conscients des risques légaux que suscitent leurs actions. D'où l'importance d'une éducation à la citoyenneté numérique.

- **L'éducation à la citoyenneté numérique**

L'éducation à la citoyenneté numérique est un ensemble de pratiques et d'activités développées pour permettre aux enfants, jeunes et adultes de participer de façon active et responsable à la société numérique.

Il s'agit des connaissances, des compétences et de la compréhension nécessaires aux utilisateurs pour exercer et défendre leurs droits et responsabilités démocratiques en ligne, et pour promou-

⁶ Mossberger, Tolbert et Mc Neal dans leur livre *Digital citizenship : The Internet, society, and participation*.

voir et protéger les droits de l'homme, la démocratie et l'Etat de droit dans le cyberspace.

À son niveau le plus simple, il vise à faire en sorte que ceux qui ne sont pas des « natifs du numérique » ou qui n'ont pas la possibilité de devenir des « citoyens numériques » ou des « digizens », ne soient pas marginalisés dans la société future. Avec le développement d'une technologie relativement peu coûteuse, le « fossé numérique » est plus susceptible d'être un déficit de compétences requises pour faire un usage avancé de la technologie que l'accès à la technologie en soi.

Dans certains pays, les écoles introduisent une « éducation à la citoyenneté numérique » pour encourager les jeunes à développer leurs compétences, leur engagement et leur créativité en ligne, ainsi qu'à prendre conscience des implications juridiques de leur activité en ligne.

Le Conseil de l'Europe entend par ECN :

- un *engagement compétent et positif avec les technologies numériques* (créer, travailler, partager, socialiser, enquêter, jouer, communiquer et apprendre) ;
- une participation *active et de manière responsable* (valeurs, compétences, attitudes, connaissances) aux communautés (locales, *nationales, mondiales*) à tous les *niveaux* (politique, économique, social, culturel et inter-culturel) ;
- une implication *dans un double processus d'apprentissage tout au long de la vie* (dans des contextes formels, informels et non formels) et défendre *continuellement la dignité humaine* ». (COE, 2016, p 2).

1.3. Le vaste champ du numérique

Le numérique recouvre à la fois les sciences et technologies de l'information et de la communication (informatique, électronique, télécommunications). Son champ comprend des équipements, des applications, des logiciels, des produits et services, etc.

Comme équipements, on peut citer : les ordinateurs, les photocopieurs, les postes récepteurs radios et télévisions, les caméras, les smartphones, les tablettes, les clés USB, les disques compacts, les cartes mémoires, les GPS, les vidéoprojecteurs, le kit de visioconférence, le microphone, les casques avec ou sans fil, les fibres optiques, le kit de connexion wifi, le pack de sonorisation, le décodeur, etc.

Les applications usuelles sont les jeux vidéos, les réseaux sociaux (facebook, WhatsApp, Instagram, Twitter, Viber, Badoo, Tik tok, LinkedIn, etc.), les applications de traitement de texte (word, excel, power point), le tableur, etc.

Les produits se présentent sous forme de fichiers informatiques comme les articles et les ouvrages en ligne, les logiciels, les vidéos, les photos, les audio, la musique, etc.

Les services numériques comprennent les solutions informatiques (le conseil, l'ingénierie, la conception, le développement, la maintenance, la formation, etc.), la vente en ligne, les transferts monétaires, la formation à distance, le télé travail, la télé médecine, le vote électronique, etc.

1.4. Domaines de l'ECN

Le programme d'ECN du Conseil de l'Europe définit clairement les compétences que les enfants devront acquérir pour de-

venir des citoyens numériques actifs et responsables. Selon ce programme, l'ECN est déclinée en dix (10) piliers fondamentaux regroupés en trois (03) domaines, à savoir : être en ligne, bien-être en ligne et droits en ligne.

Que fait-on pour être en ligne et une fois en ligne, que peut-on faire ? Que doit-on éviter de faire ?

1.4.1. Être en ligne (Being on line)

Trois critères sont à mobiliser pour être en ligne : l'accès et l'intégration, l'apprentissage et la créativité, la maîtrise des médias et de l'information.

- Accès et intégration ou inclusion

Le numérique ouvre de précieuses possibilités d'apprentissage aux enfants, c'est pourquoi il faut leur permettre d'y accéder et de l'intégrer. A cet effet, les conditions suivantes doivent être réunies : l'accès effectif aux technologies numériques, l'acquisition des aptitudes fonctionnelles et numériques de base ainsi que l'existence d'infrastructures techniques sûres. L'Etat, l'école et la famille doivent y jouer un rôle important.

- Apprentissage et créativité

Internet permet aux citoyens d'apprendre à tout moment de leur vie, mais il a aussi accéléré le renouvellement des connaissances. Afin de préparer les jeunes à un monde de plus en plus numérique, Jacques Delors, ancien président de la Commission européenne, proposait, dès les années 1990, de restructurer l'éducation autour de quatre piliers essentiels à savoir : apprendre à connaître, à faire,

à être et à vivre ensemble.

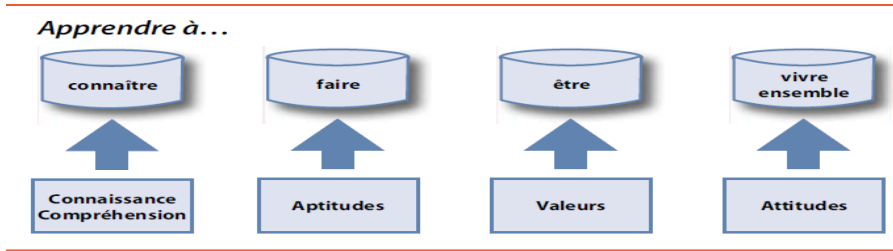


Figure 1 : Quatre piliers de l'éducation et compétences nécessaires à la citoyenneté numérique

S'il est impossible de tout apprendre à l'école, il l'est grâce aux technologies numériques. L'apprentissage mobile, les réseaux sociaux et les jeux en ligne font basculer la transmission du savoir et de certaines aptitudes des enseignants vers les apprenants. Les formations à distance comme les Massive Online Open Courses (MOOC) permettent aux citoyens d'acquérir de nouvelles qualifications professionnelles par-delà les anciennes barrières. Les doués peuvent suivre au même moment plusieurs formations.

Au-delà des connaissances universelles à assimiler, les apprenants par leur imagination peuvent créer ou innover. A. Einstein souligne à cet effet que « le véritable signe de l'intelligence n'est pas le savoir, mais l'imagination ». Un citoyen actif doit être capable de formuler dans tous les débats des points de vue originaux, des idées et des opinions. Il faut pour cela maîtriser une série d'aptitudes cognitives complexes, allant de l'analyse des sources au tri et à l'interprétation des informations.

La créativité et l'innovation étant aujourd'hui des caractéristiques du développement et de la richesse, il est judicieux que les Etats accordent une priorité aux TIC. L'apprentissage par le

jeu et l'auto-apprentissage fondé sur les technologies répondent généralement à ces critères, et peuvent donc aboutir à des résultats créatifs. Atteindre des buts immédiats encourage les apprenants à se fixer des buts plus ambitieux, et donc à définir leur propre programme d'apprentissage. Cette approche novatrice est qualifiée « d'apprendre à apprendre ». Elle consiste à « persister dans l'apprentissage et s'organiser soi-même, notamment à travers une bonne gestion du temps et des informations, à la fois seul et en groupe ». Aujourd'hui, les éducateurs comme les décideurs estiment qu'il s'agit d'une aptitude de base pour réussir dans la société de l'information.

- Maîtrise des médias et de l'information

Les polémiques autour de l'éducation aux médias et à l'information sont nombreuses et liées aux terminologies. Les termes souvent employés pour désigner maîtrise des médias sont entre autres : littératie numérique, compétence médiatique ou d'éducation aux médias. En somme, la maîtrise des médias est le fait de savoir manier correctement les médias et les sources d'information. Pour ce faire, les écoles doivent former les futurs citoyens à la compréhension, à la critique et à la création d'informations. C'est à l'école que les citoyens doivent développer et conserver un esprit critique leur permettant de participer réellement à leur communauté. Les apprenants doivent maîtriser non seulement les médias traditionnels et les images qu'ils véhiculent, mais aussi le foisonnement de technologies et d'applications nouvelles qui bouleversent le mode de transmission des informations.

Acteurs	Accès et intégration	Apprentissage et créativité	Maîtrise des médias et de l'information
Etat	<p>Rend disponibles et accessibles les TIC :</p> <ul style="list-style-type: none"> -Mise sur pied des infrastructures adéquates d'accès continu à l'Internet (Fibre sous-marine, implantation d'antennes, de câbles, etc. - Création de sociétés de téléphonie pour satisfaire les besoins de la population (services, écoles, institutions, ménages) en réseaux, supports et autres appareils de communication. -Subvention du coût d'accès aux TIC⁷ 	<p>Repenser les programmes, actualiser les pédagogies</p> <ul style="list-style-type: none"> -Intégrer les TIC dans les programmes d'enseignement -Introduire l'ECN dans les programmes d'enseignement 	

⁷ L'accessibilité prenant en compte les principes de l'équité et de la démocratie, l'Etat doit s'assurer que toute l'étendue du territoire est couverte en réseaux Internet à moindre frais

<p>Familles</p>	<ul style="list-style-type: none"> -Equiper leurs enfants en supports technologiques : ordinateurs, tablettes smartphones, clés USB, etc., -se connecter et s'abonner à l'internet -se former et former les enfants à l'usage des outils technologiques, -suivre et réguler les activités en mode virtuel 	<ul style="list-style-type: none"> -aider les enfants à acquérir les savoirs et les moyens dont ils ont besoin pour demander de l'aide et développer leur résilience. -les encourager à créer 	<ul style="list-style-type: none"> -Permettre aux enfants de se familiariser aux TIC, - encourager les enfants à aller à l'information
<p>Ecoles/ Enseignants</p>	<ul style="list-style-type: none"> - Doter les établissements de centres informatiques bien équipés, de plateformes médiatiques et multi médiatiques en supports technologiques ; -connexion au réseau internet - se former et former les enfants à l'usage des outils technologiques, 	<ul style="list-style-type: none"> -transmettre aux enfants et aux jeunes les savoirs et les moyens dont ils ont besoin pour demander de l'aide et développer leur résilience. -les initier aux techniques d'apprendre à apprendre -suivre, réguler et évaluer les activités en mode virtuel 	<ul style="list-style-type: none"> -Former les futurs citoyens à la compréhension, à la critique et à la création d'informations. C'est à l'école que les citoyens doivent développer et conserver un esprit critique leur permettant de participer réellement à leur communauté

Apprenants	<ul style="list-style-type: none"> - se connecter, créer leurs comptes, intégrer les plateformes -s'approprier un environnement informatique de travail ; adopter une attitude responsable ; 	<ul style="list-style-type: none"> - créer, produire, traiter, exploiter les données ; -s'informer, se documenter ; -communiquer, échanger ; -étudier le respect de l'intégrité des personnes et l'interdiction des atteintes à autrui y compris liés à l'usage d'Internet. 	<ul style="list-style-type: none"> -développer des réflexes, - se comporter en citoyen actif, -maîtriser les médias traditionnels -maîtrise de technologies et d'applications nouvelles qui bouleversent le mode de transmission des informations.
-------------------	--	---	--

NB : Concernant les aptitudes numériques, une bonne partie des enfants ne peut jouir pleinement des enseignements de base du fait de leur pauvreté, de leur genre ou de l'endroit où ils vivent.

Les obstacles sociaux ne dépendent pas toujours directement de la situation socio-économique, mais aussi des pesanteurs culturelles. On constate aujourd'hui une nouvelle fracture numérique : certains enfants sont mis en danger par un manque de surveillance et/ou par un accès excessif aux technologies, souvent dès la petite enfance, au détriment des activités sociales et physiques adaptées à leur âge. Ils peuvent ainsi sauter des étapes importantes de leur développement, avec des répercussions durables sur leurs facultés d'apprentissage.

1.4.2. Bien-être en ligne

Le bien-être dépend de notre capacité à :

- exploiter tout notre potentiel ;
- faire face aux contraintes habituelles de notre environnement ;
- travailler et communiquer de façon productive et fructueuse ;
- nous sentir utiles à la communauté.

Le bien-être en ligne répond à la satisfaction de trois critères érigés en thèmes : éthique et empathie, santé et bien-être, présence et communications en ligne.

- **Éthique et empathie**

L'éthique est l'ensemble des principes moraux qui régissent le comportement des personnes. Elle repose en théorie sur ce qui est généralement considéré comme bien ou mal dans une société ou un groupe donné. En ligne, des comportements acceptés s'écartent souvent de l'éthique et semblent parfois même rencontrer une approbation tacite. En outre, l'absence de frontières du monde numérique permet de passer, sans effort, d'un cadre social ou d'un groupe à l'autre. De ce fait, ce qui est vu comme moral dans un cadre peut s'avérer choquant dans un autre.

L'empathie est la capacité à comprendre ou à ressentir ce que vit une autre personne au sein de son propre cadre de référence. Elle consiste à comprendre la réalité de l'autre et à se mettre à sa place. Parce qu'elle nous amène à comprendre les intérêts, les besoins et les points de vue d'autrui, l'empathie est un important

déterminant du comportement moral et un élément nécessaire à la construction de communautés morales inclusives. En cela, l'empathie « colore » le cadre éthique transmis par la famille et la société et permet à chacun de créer, peu à peu, son propre filtre, à travers lequel il analyse ce qu'il reçoit, entreprend des actions « bonnes » ou utiles ou prend certaines décisions.

L'éthique et l'empathie s'apprennent habituellement auprès des parents. Cependant, quand les enfants entrent à l'école, les échanges avec les autres de milieux divers les confrontent rapidement à d'autres réalités. C'est là une part importante du rôle de socialisation de l'école : la diversité et l'intégration de tous deviennent des atouts pour les enfants dans leur cheminement vers une citoyenneté numérique active.

L'éthique et l'empathie ne sont pas figées, elles évoluent à mesure que les enfants cherchent à comprendre leurs camarades et, à travers ces interactions, modifient réciproquement leurs manières de voir.

L'empathie et l'éthique sont au cœur du modèle de compétences puisqu'elles reposent sur la valorisation de la dignité humaine et des droits de l'homme, le respect des autres, le sens des responsabilités collectives et une saine connaissance de soi. Ces compétences, associées à l'écoute, l'observation et la coopération, permettent d'envisager la réalité sous plusieurs angles et d'aborder les autres dans toute leur diversité (D. Goleman, 2011)⁸.

Lorsque les apprenants sont sensibilisés au rôle de l'éthique et

⁸ D. Goleman, 2011, *The Brain and Emotional Intelligence: New Insights, More Than Sound*, États-Unis, 2011.

ont suffisamment d'empathie, ils envisagent des choses sous plusieurs angles, tolèrent mieux l'ambiguïté et sont moins facilement influencés par leurs pairs, par les médias et par les tendances. Ils sont capables d'accepter, sans ressentir le besoin de convaincre ou de convertir les autres, que la coexistence de points de vue multiples peut être un élément enrichissant et moteur. L'éthique et l'empathie sont en cela des atouts précieux pour le développement de l'imagination, la résolution des problèmes et l'apprentissage en autonomie.

- Santé et bien-être

Contexte et impacts

Les technologies en ligne ont considérablement modifié nos façons d'interagir. Tout en bombardant notre cerveau de sons et d'images, ces technologies rendent plus difficile la lecture « entre les lignes ». Les messages non verbaux (expression du visage, langage corporel...) sont essentiels à la communication car ils facilitent la compréhension et réduisent le risque de malentendu. Exception faite des outils de transmission de la voix (VoIP),⁹ une bonne part des échanges d'aujourd'hui, en particulier entre adolescents, se réduit à des sonneries, des icônes et un langage abrégé.

Les émoticônes, par exemple, n'offrent qu'une palette limitée pour préciser le sens d'un message ou le type de communication, possibilités si importantes pour développer des compétences de citoyenneté numérique comme l'écoute, l'observation et l'empathie.

Le régime saturé en sons et en images qui nous est servi au-

⁹ VoIP est utilisée dans les applications vidéo comme Skype ou WhatsApp

jourd'hui a aussi d'autres effets sur le bien-être des enfants et des jeunes, et notamment sur leur capacité à traiter les informations. Non seulement les sources d'informations sont souvent douteuses, mais les internautes sont constamment profilés par les moteurs de recherche, qui évacuent les informations « non conformes » à leur profil.

De ce fait, les jeunes sont souvent privés des moyens d'étudier un sujet sous plusieurs angles et tombent rapidement dans les extrêmes comme le montre la montée du discours de haine, de radicalisation et de positions aussi excessives que mal informées.

Des chercheurs, en s'appuyant sur des Imageries par Résonance Magnétique (IRM) ont montré que même un usage modéré des technologies en ligne pouvait entraîner une hypertrophie de certaines parties du cerveau au détriment d'autres.

Des enseignants de maternelle et des pédopsychologues alertent aussi sur l'impact considérable des technologies en ligne sur les phases de développement des très jeunes enfants, avec, en particulier, une capacité de concentration réduite et un retard dans l'acquisition de certaines fonctions motrices.

Education

La santé et le bien-être soutiennent le développement personnel tout au long de la vie. Comme le montre la pyramide des besoins de Maslow, adoptée par la plupart des éducateurs dans le monde, les enfants dont les besoins de base ne sont pas satisfaits seront incapables de se réaliser pleinement et de devenir des citoyens actifs, en ligne ou ailleurs. La santé et le bien-être sont à la fois les conditions et les conséquences de l'écoute, de l'observation, de

la coopération et de l'empathie. Ces compétences indispensables à des aptitudes cognitives contribuent à leur tour à ce que la personne comprenne et pratique les droits fondamentaux, l'équité et l'ouverture à la diversité des cultures, des pratiques et des visions du monde, pierres angulaires de la justice et de la démocratie. Les citoyens ayant une vision du monde négative ou limitée, engendrée par un manque de bien-être, contribuent moins activement à la vie sociale.

- Présence et communication en ligne

La présence en ligne désigne notre façon d'être présents sur le web et s'étend aux qualités personnelles et interpersonnelles qui aident à entretenir notre réputation et notre identité en ligne.

On peut vérifier l'étendue et la qualité de sa présence en ligne en tapant son nom ou d'autres informations personnelles dans un moteur de recherche. En fonction de ce qu'on communique, la présence en ligne peut être positive ou négative ; elle peut aussi être influencée, en bien ou en mal, par les aptitudes sociales et cognitives avec lesquelles on entretient sa réputation en ligne.

Les méthodes de communication sont variées et peuvent comprendre :

- les chats (terme informel désignant des communications interactives sur un espace de discussion prévu à cet effet);
- la messagerie instantanée (type de chat en ligne avec envoi de textes en temps réel);
- les textos;
- le courrier électronique;
- la téléphonie en ligne;

- les réseaux sociaux;
- les podcasts;
- la réalité virtuelle et augmentée;
- les environnements de jeux.

On a vu apparaître, entre autres, des communications simultanées via plusieurs de ces méthodes et médias. Par exemple, on peut chatter tout en jouant à un jeu vidéo, ou utiliser un réseau social pour échanger avec d'autres sur son score pendant qu'on joue.

1.4.3. Droits en ligne

Qui rend compte de quoi sur internet ? Ce chapitre aborde quatre derniers thèmes: participation active, droits et responsabilités, vie privée et sécurité, sensibilisation des consommateurs.

- Participation active

La participation active est une manière de contribuer à une communauté en ligne et d'en tirer des bénéfices. Les étudiants et les esprits curieux devaient auparavant fréquenter les bibliothèques ou se lancer dans de longues recherches pour comprendre les débats ou les enjeux philosophiques ; aujourd'hui, ils peuvent prendre part à d'intéressantes discussions en ligne.

La participation active en ligne peut s'avérer difficile pour certains : dire tout haut ce qu'on pense et mettre son avis sur la place publique a des avantages et des inconvénients. Néanmoins, les internautes ont le droit d'exprimer librement leurs opinions à partir du moment où ils ne portent pas atteinte aux droits et aux libertés d'autrui.

La participation en ligne suit d'assez près les droits et les libertés fondamentales soulignés dans le Guide des droits de l'homme pour les utilisateurs d'internet (Conseil de l'Europe) à savoir :

- accès et non-discrimination ;
- liberté d'expression et d'information ;
- réunion, association et participation ;
- protection de la vie privée et des données personnelles ;
- éducation et connaissances générales ;
- informations et contenus adaptés aux enfants et aux jeunes ;
- voies de recours.

- **Droits et responsabilités**

Comme les citoyens dans le monde physique, les citoyens numériques ont des droits et des responsabilités dans le monde en ligne. Ils ont droit au respect de leur vie privée, à la sécurité, à l'accès et à l'inclusion, à la liberté d'expression, etc. Cependant, ces droits s'accompagnent de certaines responsabilités, comme le respect de l'éthique, l'empathie, etc., afin d'assurer à tous un environnement numérique sûr et responsable.

Internet peut être un puissant outil de promotion des idées et des communautés, mais aussi une arme destructrice lorsqu'il entrave les droits des internautes ou ne leur donne aucune chance de les exercer. Les internautes, les gouvernements, les industriels et les institutions publiques sont tenus de préserver l'intégrité de la communauté internet, que ce soit au niveau local ou au niveau international.

- **Vie privée et sécurité**

Préserver sa vie privée consiste à protéger ses propres informations en ligne et celles des autres, à assurer sa sécurité et à avoir conscience de ses actions et de ses comportements en ligne.

La vie privée et la sécurité constituent une part importante de l'éducation à la citoyenneté numérique, à laquelle doivent veiller les gouvernements, les autorités éducatives, les familles et les enfants eux-mêmes. Il faut, pour cela, apprendre à gérer ses informations et sa sécurité sur le Net (notamment en utilisant des filtres de navigation, des mots de passe, des antivirus et un pare-feu) pour éviter les situations dangereuses ou déplaisantes et pour savoir réagir.

- **Sensibilisation des consommateurs**

La sensibilisation des consommateurs revêt deux aspects : premièrement, connaître leurs droits; deuxièmement, savoir les appliquer et connaître également leurs responsabilités lorsque des produits ou services portent atteinte aux droits d'autrui.

On ne saurait nier les avantages du commerce en ligne, qui a rendu les achats plus simples et plus commodes ; mais les transactions en ligne ne sont pas sans danger.

Sur internet et ses multiples espaces, tels que les réseaux sociaux et autres lieux d'échanges virtuels, on est rarement un citoyen numérique sans être aussi consommateur. Comprendre la réalité commerciale propre aux espaces en ligne et ses implications fait partie des compétences à acquérir pour conserver son autonomie en tant que citoyen numérique.

1.5. Quelques avantages et inconvénients du numérique

1.5.1. Avantages

Depuis son apparition, le numérique a contribué à révolutionner beaucoup de domaines. Il se présente de nos jours comme :

❖ *un outil de développement et de renforcement du lien social*

– Sur le plan éducatif, le numérique contribue significativement à l'amélioration de la qualité de l'enseignement (les méthodes de cours, d'apprentissage, de recherche), à l'apparition des bibliothèques numériques (accès instantané à une plus grande quantité d'informations), etc.

– Sur le plan sanitaire, on note l'amélioration des prestations avec l'accès à des outils et techniques de soins de plus en plus pointus (le scanner, l'échographie, la radiographie, etc.). La mise en place de la télémédecine est une véritable révolution.

– Sur le plan économique et commercial, le numérique facilite et sécurise la transaction monétaire (Tmoney, flooz, western union, money gram, etc.). Il permet aussi aux entreprises de faire la visibilité de leurs biens et services, de pratiquer le commerce en ligne, etc.

– Sur le plan agricole, le numérique contribue à l'amélioration des méthodes et techniques de production, de transformation et de commercialisation des produits.

– Sur le plan social, le numérique facilite la communication, les échanges et le partage d'informations à moindre coût et de façon instantanée. Il constitue également un moyen de distraction.

❖ *Le numérique, outil de liberté d'expression et de promotion des droits humains et de la démocratie*

Le numérique donne la parole à tout le monde et permet la libre expression des pensées, des idées et des opinions (exemple des réseaux sociaux comme WhatsApp, Facebook, Twitter, Instagram, Tik Tok, etc.).

❖ *Le numérique, un domaine pourvoyeur d'emplois*

Le numérique s'impose comme un secteur à la croissance rapide et pourvoyeur massif d'emplois. Exemple : De nombreux jeunes s'adonnent de nos jours aux activités génératrices de revenus comme la vente, la réparation, le décodage d'outils numériques, la photographie, les prestations de services numériques (consultation, traitement de textes, photocopie, impression, etc.).

Outre ses nombreux avantages, le numérique présente également des inconvénients.

1.5.2. Inconvénients

Les inconvénients du numérique, essentiellement liés à son mauvais usage, sont multiples :

- prolifération de fake news, d'escroquerie en ligne, de chantage, d'intimidation, de raillerie, d'atteinte aux bonnes mœurs, de radicalisation, de terrorisme, etc. ;
- cyberattaque par rançongiciels ;
- baisse de facultés de concentration et de mémorisation ;
- fracture numérique ;
- isolement et coupure des interactions classiques de la vie en société ;
- pollution de l'environnement. Exemple : les ordinateurs sont difficilement recyclables.

2. L'ENVIRONNEMENT DU NUMERIQUE AU TOGO

L'environnement du numérique au Togo est caractérisé par un incivisme grandissant. Pour venir à bout de cet incivisme et rentabiliser le domaine, l'Etat togolais a institué un cadre juridique et institutionnel y répondant. Par ailleurs de grands projets ont été initiés.

2.1. L'état des lieux de l'incivisme numérique au Togo

Le cyberspace togolais, comme dans la plupart des pays africains, est marqué par diverses infractions qui font l'objet de poursuites.

2.1.1. Les infractions

L'internet et les technologies numériques ont facilité la réalisation d'activités délinquantes. La forte augmentation des actes commis et le préjudice moral et financier qu'ils causent, témoignent de l'intérêt particulier que suscite le réseau numérique auprès des délinquants. On note des infractions contre les biens, contre les personnes et des atteintes aux systèmes informatiques.

2.1.1.1. Les infractions contre les biens

Il s'agit notamment de l'escroquerie (arnaque) et de la tromperie.

- L'escroquerie (ou l'arnaque)

Aux termes de l'article 448 du nouveau code pénal togolais, l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Les cyber escrocs redoublent d'imagination et de créativité et adaptent leurs modus operandi aux situations existantes.

Par exemple, à l'occasion d'un concours, des individus se cachant derrière de faux profils appâtent et détournent de potentiels candidats, les amenant ainsi à verser des sommes d'argent sur des comptes de mobile money prétendant pouvoir les faire réussir.

- La tromperie

Aux termes de l'article 455 du nouveau code pénal togolais, la tromperie est le fait pour un commerçant ou fabricant de mettre en vente, de livrer ou de proposer de mauvaise foi des marchandises, objets ou substances n'ayant pas la qualité loyale et marchande ou n'ayant pas le poids ou la mesure indiqués.

L'exemple de l'arnaqueur qui met en ligne un produit à l'image très attrayante, exige le paiement complet du prix mais livre un produit ne correspondant en rien à celui affiché.

Il existe des infractions assimilées telles que la publicité men-

songère, la filouterie, l'extorsion, etc.

2.1.1.2. Les infractions contre les personnes

Certaines infractions existaient avant l'expansion des TIC et ont pris une autre tournure à cause d'elles. D'autres, par contre, ne doivent leur existence qu'à celle des TIC.

Pêle-mêle, on distingue :

- La menace

Selon l'article 245 du nouveau code pénal togolais, on entend par menace l'acte d'intimidation consistant pour une personne à inspirer, par quelque moyen que ce soit, à une autre la crainte de violences physiques ou morales contre sa personne, sa famille, ses biens ou ses intérêts.

A titre d'exemple, il apparaît de plus en plus aisé de se cacher derrière un numéro, un compte ou un profil, pour proférer des menaces à l'endroit de sa cible.

- Le chantage

L'article 466 du nouveau code pénal togolais définit le chantage comme le fait d'obtenir une signature, un engagement, une révélation, une remise de fonds, un avantage, etc., en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération.

Le cyber délinquant arrive à obtenir de sa victime, par un faux appel vidéo ou un échange de photographies, des photos ou vidéos montrant son intimité. Il s'en sert par la suite pour la faire chanter.

- **L'injure et la diffamation**

Aux termes de l'article 297 du nouveau code pénal togolais, une injure constitue toute expression outrageante, tout terme de mépris ou toute invective ne renfermant l'imputation d'aucun fait.

Le dictionnaire Le Petit Larousse illustré 2018 définit la diffamation comme une imputation d'un fait précis qui est de nature à porter atteinte à l'honneur ou à la considération d'une personne ou d'un corps constitué.

- **Les violations de l'intimité de la personne**

Aux termes de l'article 368 du nouveau code pénal, constitue une violation de l'intimité de la personne, le fait :

- de publier ou de diffuser des papiers ou enregistrements privés, un dessin, une photographie, un film ou tout autre support reproduisant l'image de cette personne sans son accord ou celui de ses ayants droit
- d'organiser, par quelque procédé que ce soit, l'interception, l'écoute ou l'enregistrement de communications privées, orales, optiques, magnétiques ou autres échanges reçus dans un lieu privé, à l'insu ou sans l'accord des personnes en communication ou du maître des lieux.

Exemple des porn revenge ou vengeances pornographiques consistant pour un ex-conjoint à publier des contenus à caractère sexuel de son ancien partenaire.

- **Le cyber harcèlement**

Le cyber harcèlement est une forme de violence intentionnelle, perpétrée, même à une seule occasion, par un individu ou un groupe d'individus au moyen de formes de communication à savoir : sms (Short message service), réseaux sociaux, jeux en ligne, etc. dans le but réel ou apparent d'obtenir de lui un acte quelconque.

- **L'exploitation de l'image pédopornographique**

L'exploitation de l'image pédopornographique est le fait de posséder sciemment, de diffuser, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique.

Elle englobe aussi le fait de consulter habituellement un service de communication en ligne mettant à disposition une telle image ou représentation.

2.1.1.3. Atteinte à la propriété

Les infractions les plus courantes en la matière sont l'accès et le maintien frauduleux dans un système de traitement automatisé de données, les entraves à ce système, le faux en informatique, le sabotage, la reproduction non autorisée d'un programme informatique protégé, l'espionnage, l'altération des données et des programmes informatiques, les dommages affectant des données et des programmes.

2.1.2. La poursuite des infractions

Les infractions commises par le biais du numérique font l'objet de poursuite. Les forces de la poursuite restent les services et unités

traditionnellement investis du pouvoir de police judiciaire, notamment ceux relevant de la police et de la gendarmerie.

2.2. Les enjeux et défis du numérique pour le Togo

Les enjeux et défis du numérique pour le pays sont multiples.

2.2.1. Les enjeux

Entre autres enjeux, figure la nécessité de :

- mettre en œuvre l'aménagement numérique du territoire : assurer le déploiement des infrastructures et améliorer la qualité de service ;
- redéfinir le service universel ;
- inclure l'ensemble des populations et notamment les catégories les plus vulnérables ;
- dynamiser le marché des services aux entreprises ;
- intégrer pleinement les TIC dans l'éducation ;
- concilier concurrence, investissement et innovation ;
- optimiser l'utilisation des TIC dans les services de l'État ;
- assurer la cybersécurité et la protection des citoyens.

2.2.2. Les défis

Parmi les défis à relever, on peut noter :

- la mise en place d'un système de digitalisation de l'administration ;
- la sensibilisation de la population à l'utilisation des TIC ;
- l'amélioration du réseau existant par l'expansion de câbles sous-marins ;
- la démocratisation de la connexion au haut débit ;
- la mise en place d'une politique plus ambitieuse sur le cloud.

2.3. L'ambition du gouvernement togolais en matière d'éducation à la citoyenneté numérique

2.3.1. Domaine de l'éducation

Les objectifs assignés à l'éducation sont dynamiques et fonction de l'environnement des apprenants et des enjeux mondiaux.

Le Togo, dans l'optique de donner aux citoyens une éducation à même de favoriser l'éclosion d'un esprit plus enclin à contribuer efficacement à la vie du pays et à son développement harmonieux, s'est défini avec la réforme de 1975, un profil de citoyen à réaliser, à savoir : « former des individus sains, équilibrés et épanouis dans toutes les dimensions ; permettre la formation de l'esprit critique, base de toute culture moderne ».

Cette préoccupation a été prise en compte par la constitution togolaise de la IV République¹⁰ qui dispose, en son article 35, que : « L'Etat reconnaît le droit à l'éducation des enfants et crée les conditions favorables à cette fin. L'école est obligatoire pour les enfants des deux sexes jusqu'à l'âge de 15 ans. L'Etat assure progressivement la gratuité de l'enseignement public ».

L'ambition 2 de l'axe stratégique 1 de la feuille de route 2020-2025 du gouvernement met l'accent sur le caractère inclusif de l'éducation en envisageant de la rendre accessible au plus grand nombre.

Pour atteindre cette ambition, le Togo a adhéré à plusieurs initiatives sous-régionales et internationales en vue de prendre en compte les nouvelles orientations de l'éducation déclinées par l'ONU à travers les ODD dans sa vision 2030.

¹⁰ La constitution de la IV^e République promulguée le 14 octobre 1992.

2.3.2. Domaine de la citoyenneté

L'avènement de la démocratie au Togo, à l'instar de nombreux pays en développement, a conduit à des situations de conflits entraînant non seulement la fragilisation de la vie économique et politique, mais aussi le déchirement du tissu social caractérisé par des comportements inciviques, notamment la destruction des biens publics et privés, des agressions physiques et verbales, l'instrumentalisation des particularismes ethniques, les violations des droits humains et des libertés publiques, la désobéissance à l'autorité, etc.

De même, notre pays fait face ces dernières années, à une montée de l'incivisme dans le cyberspace caractérisé par la dépravation des mœurs, la prolifération des fake news, des intimidations, des attaques de tout genre, l'escroquerie, la diffamation, des propos suscitant la haine, la violence, l'intolérance, etc.

Pour anticiper sur cette situation, le gouvernement, à travers le ministère chargé de la formation civique, a adopté en 2014 la politique nationale de formation civique et d'éducation à la citoyenneté. Cette politique vise à « (...) Amener le citoyen à s'approprier et à vivre les valeurs républicaines à travers une citoyenneté active en vue de sa pleine participation au développement humain durable ».

De façon spécifique, il s'agit, entre autres de :

- promouvoir des comportements civiques ;
- promouvoir les valeurs patriotiques ;
- promouvoir une éducation formelle et non formelle qui prépare le citoyen à être respectueux de la dignité humaine, des droits de l'Homme et des valeurs démocratiques ;
- encourager et soutenir la participation citoyenne aux affaires publiques.

L'avènement du numérique a profondément révolutionné la façon dont les individus communiquent, travaillent, apprennent, commercent et se divertissent. Son impact positif sur le développement n'est plus à démontrer. Le gouvernement, s'inscrivant dans cette dynamique, s'est défini une ambition à atteindre.

2.3.3. Domaine du numérique

Pour répondre aux enjeux mondiaux, l'Etat, a prévu, dans le plan national de développement (PND) 2018-2022, en son axe stratégique 1, encadré 1, effet attendu 5, de faire du numérique un véritable levier de modernisation de l'économie et de la société togolaise en rendant les services TIC accessibles au plus grand nombre de citoyens estimé à 90% de la population à l'horizon 2022. C'est également à juste titre que la feuille de route 2020-2025 du Gouvernement lui consacre une bonne place dans les priorités en l'inscrivant à l'ambition 7 de l'axe 3 qui place le digital au cœur de la modernisation de l'Etat.

Pour atteindre cette ambition, le Togo s'est défini un cadre juridique et institutionnel conséquent.

2.4. Le cadre juridique et institutionnel

S'inscrire dans la modernité suppose prendre des mesures idoines, notamment un cadre juridique et institutionnel adéquat pour relever les nouveaux défis induits par l'essor fulgurant et ultra rapide des TIC.

2.4.1. Le cadre juridique

Intitulé de la loi	Date d'adoption	Résumé
<p>Loi n° 2020-009 relative à l'identification biométrique des personnes physiques au Togo modifiée par la loi n° 2022- 010 du 24-06-2022.</p>	<p>10 septembre 2020</p>	<p>Cette loi établit un système d'identification et d'authentification des personnes physiques au Togo. Elle institue le Numéro d'identification unique (NIU) et consacre des droits au bénéfice des candidats à l'inscription et à l'authentification. Elle oblige l'administration à utiliser les NIU pour identifier ses usagers et pose l'obligation d'inscription du NIU sur tout document administratif relatif au titulaire du numéro. Elle crée l'Agence nationale d'identification (ANID) qui met en œuvre la procédure d'attribution des NIU aux personnes physiques et assure leur authentification.</p>

<p>Loi n° 2019-014 relative à la protection des données à caractère personnel</p>	<p>04 octobre 2019</p>	<p>La loi relative à la protection des données personnelles assure une protection efficace des libertés et droits fondamentaux des personnes physiques, à l'égard du traitement des données à caractère personnel.</p> <p>A ce titre, elle</p> <ul style="list-style-type: none"> - pose les exigences de conformité légale des traitements de données à caractère personnel, - consacre un ensemble de droits aux personnes dont les données à caractère personnel font l'objet d'un traitement, - met à la charge des responsables du traitement des données une panoplie d'obligations. <p>Elle crée en outre « l'instance de protection des données à caractère personnel » dont la mission principale est de veiller au respect de la vie privée dans le traitement des données à caractère personnel.</p> <p>Elle définit les infractions se rapportant aux traitements de données à caractère personnel ainsi que les sanctions pénales correspondantes.</p>
--	------------------------	--

<p>Loi n° 2018-006 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n° 2022-009 du 24 juin 2022</p>	<p>07 décembre 2018</p>	<p>La loi sur la cybersécurité et la lutte contre la cybercriminalité définit les mécanismes de promotion ainsi que le cadre de gouvernance de la cybersécurité.</p> <p>Elle crée l'Agence Nationale de la Cybersécurité (ANCy) qui prend en charge l'application effective des orientations et mesures stratégiques et juridiques en matière de cybersécurité.</p> <p>Elle crée aussi le Fonds de souveraineté numérique qui participe entre autres, au financement des stratégies nationales de cybersécurité et appuie les actions de l'Agence nationale de la cybersécurité.</p> <p>Elle pose enfin le cadre de la lutte contre la cybercriminalité. Elle réadapte le système pénal national, au moyen d'une modernisation des incriminations du droit pénal classique et d'un réaménagement de quelques instruments procéduraux au regard des exigences de l'environnement numérique.</p>
---	-------------------------	--

<p>Loi n° 2017-07 relative aux transactions électroniques (LTE)</p>	<p>22 juin 2017</p>	<p>La LTE répond au contexte de mutations technologiques mondiales liées à la multiplication exponentielle des échanges au travers des TIC.</p> <p>Elle conforte la liberté de la communication publique en ligne au Togo, offre des niveaux de sécurité appropriée aux usagers, encadre le régime des activités et les obligations des prestataires afin de renforcer le dynamisme de l'économie numérique. Elle offre le cadre juridique permettant de :</p> <ul style="list-style-type: none"> - concrétiser l'écrit électronique comme équivalent du support papier ; - sécuriser les transactions électroniques ; - définir la notion de commerce électronique ; - encadrer le commerce, le contrat et la publicité par voie électronique ; - dématérialiser les formalités et les procédures administratives.
--	---------------------	--

<p>Loi n° 2017-006 d'orientation sur la société de l'information au Togo (LOSITO)</p>	<p>22 juin 2017</p>	<p>La LOSITO définit les objectifs et les grandes orientations de la société de l'information au Togo. Elle consacre les principes directeurs et les valeurs partagées en vue de garantir :</p> <ul style="list-style-type: none"> - le développement d'une société de l'information respectueuse des lois et règlements en vigueur au Togo ; - une liberté responsable de communication, de participation, d'expression et de création de ressources ; - une solidarité numérique à travers l'organisation d'un système d'accès du plus grand nombre aux TIC ; - la sécurité des ressources informationnelles, des personnes et des biens de la société de l'information.
--	---------------------	--

<p>Loi n°2012-018 sur les communications électroniques (LCE) modifiée par la loi n°2013-003</p>	<p>17 décembre 2012 modifiée le 19 février 2013</p>	<p>La LCE propose un cadre juridique applicable aux activités de communications électroniques en vue de la satisfaction de l'intérêt public. A ce titre, elle :</p> <ul style="list-style-type: none"> - réalise progressivement un marché ouvert et concurrentiel pour les réseaux et services de communications électroniques dans l'intérêt des utilisateurs ; - favorise l'accès du plus grand nombre aux services de communications électroniques et l'aménagement numérique (en assurant le service universel par la fourniture d'un service minimal sur tout le territoire national à des prix raisonnables, abordables et accessibles à tous) ; - facilite le développement socio-économique par le développement du secteur des communications électroniques et des technologies de l'information et de la communication. <p>En outre, la LCE crée l'Autorité de régulation des communications électroniques et des Postes (ARCEP) dotée de la personnalité juridique, de l'autonomie financière et de gestion et en a précisé les missions et attributions.</p>
--	---	--

2.4.2. Le cadre institutionnel

Tableau des institutions

Institutions	Textes créateurs	Missions
<p>Autorité de Régulation des Communications Electroniques et des Postes (ARCEP)</p>	<p>Loi n°2012-18 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n°2013-003 du 19 février 2019. (Chapitre 12 section 2 article 63)</p>	<p>La mission de l'ARCEP est de gérer et contrôler les opérateurs autorisés par l'Etat à établir et exploiter des réseaux et services de communications électroniques ouverts au public. Elle se charge aussi de la délivrance des autorisations pour les réseaux indépendants en matière de terminaux et d'installation.</p>
<p>Agence Nationale du Spectre des Radiofréquences (ANSR)</p>	<p>Loi n°2012-18 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n°2013-003 du 19 février 2019. (Chapitre 8 art 43)</p>	<p>Au titre de la coordination du spectre de l'Etat, l'ANSR attribue des fréquences aux différentes administrations et autorités affectataires. Aussi au titre de la gestion des fréquences hertziennes, l'ANSR assigne les fréquences radioélectriques nécessaires aux réseaux de radiodiffusion sonore ou télévisuelle. Les missions de l'Agence nationale du spectre des radiofréquences sont dévolues à l'ARCEP jusqu'à son opérationnalisation.</p>

<p>Autorité de Certification Electronique</p>	<p>Loi n°2017-007 du 22 juin 2017 relative aux transactions électroniques. (Art 84)</p>	<p>L'Autorité de certification est investie des pouvoirs nécessaires et dotée des ressources adéquates pour l'exercice des tâches de contrôle des prestataires de services de confiance. Les fonctions d'accréditation, de contrôle et de médiation sont de la compétence de l'Autorité de certification sous contrôle du ministère chargé des communications électroniques. Les missions et compétences de l'Autorité de certification sont dévolues au ministère chargé des communications électroniques qui les délègue à l'Autorité de régulation des communications électroniques et des postes (ARCEP) sous sa tutelle.</p>
<p>Agence Nationale de la Cybersécurité (ANCy)</p>	<p>Loi n°2018-026 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité. (Chapitre 2 art 6)</p>	<p>L'Agence nationale de la cybersécurité est l'autorité nationale en matière de sécurité des infrastructures essentielles et des systèmes d'information des autorités publiques. Elle concourt de manière significative à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité. Elle apporte son concours aux services de la République togolaise en matière de défense et de sécurité nationale</p>

<p>Fonds de Souveraineté Numérique (FSN)</p>	<p>Loi n°2018-026 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité.</p>	<p>Le Fonds de souveraineté numérique participe à financer toutes les actions menées afin de protéger et garantir la souveraineté numérique du Togo. A ce titre, il participe entre autres au financement des stratégies nationales de cybersécurité et appuie les actions de l'Agence nationale de cybersécurité.</p>
<p>Instance de Protection des Données à Caractère Personnel (IPDCP)</p>	<p>Loi n° 2019-014 relative à la protection des données à caractère personnel. (Chapitre 5 art 55)</p>	<p>L'instance de protection des données à caractère personnel est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi sur la protection des données à caractère personnel. Elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que les TIC ne comportent pas de menace au regard des libertés publiques et de la vie privée.</p>

<p>Cyber Défense Africa (CDA)</p>	<p>Décret n° 2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA)</p>	<p>Cyber Defense Africa (CDA) S.A.S. est la société de service en cybersécurité mandatée par la République Togolaise pour assurer la sécurisation des systèmes d'information au Togo et au-delà de ses frontières. A ce titre, CDA fournit des services de « Security Operations Center » (SOC) et de « Computer Emergency Response Team » (CERT). Elle accompagne aussi les administrations et entreprises privées dans la sécurisation de leurs infrastructures, la protection des applications et la confidentialité de leurs données avec une large gamme de services allant du conseil à la mise en œuvre technique.</p>
<p>Agence Nationale d'Identification (ANID)</p>	<p>Loi n° 2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo. (Chapitre 5 art 19)</p>	<p>L'Agence nationale d'identification a pour objet l'inscription et l'authentification des personnes physiques. Elle est chargée d'organiser le traitement, la gestion, la protection et la sécurisation des données liées à l'identification des personnes physiques.</p>

<p>Agence Togo Digital (ATD)</p>	<p>Décret n°2021-102/PR du 29 septembre 2021 portant création, attributions, organisation et fonctionnement de l'Agence Togo Digital (ATD). (Art 5 du décret)</p>	<p>L'ATD est l'agence chargée d'appuyer la mise en œuvre des projets digitaux, de s'assurer de leur cohérence et de contribuer à l'efficacité dans l'utilisation des moyens de l'Etat. Elle concourt de manière significative à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de digitalisation au Togo.</p>
----------------------------------	---	--

2.5. Quelques projets de l'Etat dans le domaine du numérique

Les projets de l'Etat dans le domaine sont entre autres :

– le projet d'identification nationale biométrique dénommé « e-ID Togo » a pour objectif d'attribuer à toute personne physique de nationalité togolaise ou résidant au Togo un numéro d'identification unique (NIU) sur la base de ses données démographiques et biométriques. Ces données ainsi que les NIU permettront ainsi de mettre en place une base de données centrale, sécurisée et fiable qui servira de référence pour la vérification de l'identité des bénéficiaires de services publics, privés ou sociaux. Ce système, qui s'inspire du modèle d'identification Aadhaar en Inde, permettra de donner à chaque résident togolais une preuve d'identité unique quels que soient son origine ou son lieu de résidence.

– le projet Université Sans les Murs (USM) est une innovation technologique ayant pour vocation d'appuyer le développement d'un enseignement hybride, adaptatif et bien maîtrisé par ses utilisateurs, assorti d'un accès à une offre pédagogique francophone riche et d'usage libre.

– la digitalisation de la demande du casier judiciaire, du passeport ;

– la campagne de sensibilisation à la citoyenneté numérique.

3. QUELQUES CONSEILS PRATIQUES

Au regard des avantages et des inconvénients liés au numérique, il est important d'éduquer les citoyens à l'utilisation positive de cet outil devenu incontournable. C'est à cet effet que des conseils tirés de plusieurs sources sont proposés pour aider les usagers.

3.1. Recommandations du Conseil de l'Europe

Selon le Conseil de l'Europe, tous les citoyens doivent apprendre à protéger leur identité en ligne et leurs données personnelles et à conserver un minimum de vie privée.

A cet effet :

- sachez que tout ce que vous postez, envoyez ou téléchargez en ligne laisse une trace numérique (un peu comme des empreintes sur le sol) ;
- réfléchissez avant d'envoyer un message, quel qu'en soit le contenu. Quelque chose que vous voyez comme positif peut être mal interprété ;
- gardez toutes les données vous concernant confidentielles, notamment les photos qui peuvent révéler votre identité, votre lieu d'habitation ou votre sexe ;
- respectez le matériel et rappelez-vous que, si vous utilisez les serveurs de votre employeur ou de votre établissement scolaire, vos communications ne seront peut-être pas privées ;

- recherchez les options vous permettant de définir pendant combien de temps vos contributions en ligne resteront visibles.

Par ailleurs, les internautes doivent connaître leurs droits et les procédures à suivre en cas de violation de leurs droits. Ils sont aussi invités à signaler toute violation des droits d'autres utilisateurs en ligne. En cas d'atteintes à leurs droits, les internautes – quel que soit leur âge – devraient avoir à l'esprit trois actions majeures : ignorer le contenu, bloquer la personne qui a adressé la remarque offensante, signaler cette personne.

Pour les citoyens numériques, c'est une responsabilité civique de veiller à la cybersécurité sur l'ensemble de leurs outils connectés à internet, en appliquant les paramètres de vie privée et de sécurité disponibles, et en installant des antivirus (contre les pourriels et logiciels malveillants) et autres logiciels offrant une sécurité optimale. Une sécurité insuffisante facilite la circulation des pourriels, qui sont l'un des premiers moyens de diffusion d'informations fausses ou frauduleuses, ou d'abus de confiance visant à obtenir des informations ou de l'argent.

Il convient de désactiver la géolocalisation et le Bluetooth lorsqu'on ne s'en sert pas, car ils ouvrent la porte aux intrusions et peuvent livrer sur nous beaucoup plus d'informations que nous le souhaiterions.

Avant de fournir des données privées pour effectuer un achat, surveillez l'apparition du symbole « cadenas fermé » dans la barre d'outils. Il montre que la transaction passe par une connexion sécurisée. Avant toute transaction en ligne, assurez-vous que l'URL commence par « https » ; le «s» signifie que le protocole de transfert hypertexte est « sécurisé » et authentifie le site web et le réseau qui lui est associé, ce qui protège contre les attaques par interception.

D'autres conseils se retrouvent également dans le guide d'hygiène numérique de l'Agence nationale de la cybersécurité (ANCy) et le code de bonne conduite élaboré par la Direction de la formation civique.

3.2. Le guide d'hygiène numérique de l'ANCy

Ce guide recommande, en dix (10) points, ce qui suit :

- Utilisez des mots de passe robustes

Un mot de passe robuste permet de sécuriser les accès à vos appareils personnels et professionnels. Il doit être le plus long possible (minimum 8 caractères), n'avoir du sens que pour vous, comporter des chiffres et des caractères spéciaux et avoir une utilisation unique.

Je choisis un bon mot de passe et j'ajoute un second niveau de protection en activant l'authentification à double facteur (2FA) sur tous mes comptes (Facebook, Twitter, Instagram, LinkedIn, Gmail...).

- Méfiez-vous avant de cliquer

Les emails et les messages (WhatsApp, Réseaux Sociaux, etc...) qui vous sont adressés sont les meilleurs vecteurs d'attaque. Je fais donc attention aux correspondances reçues des sources inconnues.

Je ne clique pas sur les pièces jointes d'expéditeurs inconnus. Je ne relaie pas les emails ou messages de type chaînes, canulars, appels à la solidarité, alertes virales, promotion exceptionnelles, etc.

- Mettez à jour vos appareils connectés

La plupart des attaques utilisent des failles des équipements ou des logiciels installés. Les hackers cherchent donc les équipements et

les logiciels qui n'ont pas été mis à jour afin d'utiliser la faille non corrigée pour s'introduire.

Je m'assure en tout temps de disposer des versions à jour de mes systèmes d'exploitations et logiciels sur tous mes équipements connectés.

- Méfiez-vous des réseaux Wi-Fi

Dans les salles de conférences, hôtels, restaurants, aéroports ou ailleurs, le Wi-Fi peut être utilisé pour compromettre vos équipements connectés, voler vos mots de passe, surveiller vos communications, etc.

J'évite de connecter mon téléphone, mon ordinateur portable ou ma tablette au Wi-Fi public ou gratuit. Je privilégie la 3G ou la 4G et dans la mesure du possible, j'active mon Roaming lorsque je voyage. Si je dois absolument me connecter à un réseau Wi-Fi, j'utilise un VPN qui permet de sécuriser la connexion.

- Protégez vos appareils connectés

L'anti-virus est le premier outil de protection contre les menaces cyber.

J'installe sur tous mes appareils connectés (ordinateurs, téléphones, tablettes), un anti-virus de dernière génération et je le maintiens à jour. J'évite au maximum d'utiliser les clés USB proposées lors de conférences, sessions de travail et autres.

- Sauvegardez vos données

J'effectue une sauvegarde de mes données importantes sur des supports sécurisés pour éviter la perte des fichiers en cas de cyberattaque ou de panne de mes équipements.

- Utilisez votre messagerie professionnelle

La messagerie professionnelle limite la fraude et assure à vos inter-

locuteurs de communiquer avec la bonne institution/entreprise et ses représentants et non avec une personne tierce potentiellement malintentionnée. Les messageries professionnelles sont sécurisées et bloquent les messages dangereux avant leur arrivée dans votre boîte de réception. Utiliser une messagerie gratuite de type Gmail, Yahoo, Hotmail, etc., pour vos besoins professionnels, revient à exposer vos données à ces hébergeurs et à leur Etat d'appartenance.

Je m'engage à utiliser mon email professionnel pour les échanges professionnels et à ne communiquer aux tiers que mon adresse email professionnel (sur les cartes de visite et autres supports de communication).

- **Installez des applications et logiciels officiels**

Les logiciels et applications malveillantes sont nombreux et tentent en permanence de s'infiltrer dans vos appareils. Une technique courante utilisée consiste à proposer une version gratuite (crackée) d'un logiciel officiel payant.

Je m'assure d'installer les logiciels légitimes depuis des sources fiables mises à disposition par des magasins d'applications officiels et payer les licences adéquates lorsque le logiciel ou l'application est payant(e).

- **Limitez l'installation d'applications sur vos appareils**

Plus vous installez d'applications sur vos équipements, plus vous augmentez les possibilités offertes aux hackers de pénétrer vos appareils. Il est donc primordial de limiter votre exposition aux attaques.

Je n'installe que les applications et logiciels dont j'ai besoin sur mon téléphone, ma tablette ou mon ordinateur. Je passe régulièrement en revue ces applications et logiciels pour m'assurer de leur utilité.

- **Contactez CERT.tg en cas de doute**

Si je remarque une activité ou un comportement suspect(e) sur mon téléphone, mon ordinateur ou pour toutes questions concernant les mesures décrites dans ce document, **je contacte rapidement le CERT national du Togo sur <https://cert.tg> ou au +228 22 53 59 80.**

3.3. Le code de bonne conduite de la DFC

Il comporte dix points :

- savoir que l'internet est un outil incontournable pour tous ;
- ne pas accepter n'importe qui comme ami sur internet ;
- ne pas exposer son image, elle est sacrée ;
- respecter l'image des autres et ne pas diffamer autrui ;
- ne partager que ce qui est vrai et utile ;
- être courtois et respectueux ;
- ne pas partager les informations confidentielles ;
- éviter toute publication compromettante ;
- être vigilant, faire attention à l'arnaque et aux fake news ;
- éviter les dérapages sur les réseaux sociaux car ils sont punis par la loi.

Ces différents conseils sont ci-dessous illustrés.

1. L'internet est de nos jours un outil de communication incontournable pour tous



L'internet est un outil de communication par excellence, d'éducation, d'information, de formation, de divertissement, de promotion et de vente de produits et de services...

2. Je n'accepte pas n'importe qui comme ami



- N'acceptons pas les invitations des inconnus.
- Pour les personnes connues, assurons-nous qu'il s'agit bien d'elles avant d'accepter ou de répondre.
- Assurons-nous des objectifs des groupes de discussions avant de les intégrer ou d'y rester.

3. Mon image est sacrée. Je ne l'expose pas



- Les photos illustrent notre personnalité. Faisons attention aux postures, aux cadres et aux circonstances dans lesquels nous les prenons.
- Mes publications ne doivent pas porter atteinte aux bonnes mœurs.
- Une fois publiée, mon image peut être utilisée à d'autres fins.

4. Je respecte l'image des autres. Je ne les diffame pas



- J'évite les règlements de comptes à travers les réseaux sociaux.
- Je ne partage pas les images ou publications qui diffament les autres.

5. Je partage seulement ce qui est vrai et utile



- Partageons seulement ce qui présente un intérêt pour tous.
- La publication ou le partage d'une fausse information peut avoir des conséquences

6. Je suis courtois et respectueux



Quelles que soient la situation et mon humeur je m'abstiens de tenir des propos injurieux ou grossiers au cours de mes communications.

7. Je ne partage pas des informations confidentielles sur ma vie privée



- Ne partageons pas nos données personnelles.

8. Toute publication, même supprimée, demeure et peut me rattraper



J'évite de publier des informations compromettantes car il existe des applications qui les enregistrent instantanément et les conservent.

9. L'arnaque et les fake news existent, je reste vigilant



- Faisons attention aux offres alléchantes.
- Vérifions toujours l'authenticité des sites.

10. La loi punit les dérapages sur les réseaux sociaux



Mes postings m'engagent : je réfléchis à mes commentaires et messages avant de les publier.

Glossaire

- **Antivirus** : logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants.
- **Base de données** : conteneur qui permet de stocker et de retrouver des données structurées, semi structurées ou des données brutes ou de l'information, souvent en rapport avec un thème ou une activité.
- **Cloud** : endroit où sont stockées des ressources informatiques auxquelles on peut accéder à distance via un réseau de communication (bien souvent internet).
- **Consentement** : fait de donner son aval ; c'est une décision libre de ne pas s'opposer à un fait.
- **Cyber criminalité** : ensemble des activités illégales effectuées par l'intermédiaire d'internet.
- **Cybersécurité** : ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un Etat ou d'une entreprise, etc.
- **Donnée à caractère personnel** : information relative à une personne physique identifiée ou pouvant être identifiée directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- **Donnée ou data** : ce qui est connu et qui sert de point de départ à un raisonnement ayant pour objet la détermination d'une solution à un problème en relation avec cette donnée.
- **Internet** : ensemble des réseaux mondiaux interconnectés qui permet à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun.

- **Intranet** : réseau informatique privé utilisé par les employés d'une entreprise ou de toute autre entité organisationnelle utilisant les mêmes protocoles qu'internet.
- **Logiciel malveillant** ou **malicieux** aussi dénommé **programme malveillant** ou **pourriel**: programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté
- **Numérisation** : conversion des informations d'un support ou d'un signal électrique en données numériques que des dispositifs informatiques ou électroniques numériques pourront traiter.
- **Pourriels** : message électronique non sollicité et souvent à caractère publicitaire, envoyé automatiquement et en grand nombre.
- **Télécommunication** : transmission d'informations à distance en utilisant des technologies électroniques, informatiques, de transmission filaire, optique ou électromagnétique.
- **Télétravail** : toute activité professionnelle effectuée en tout ou partie à distance du lieu où le résultat du travail est attendu.
- **TIC** : technologies de l'information et de la communication
- **URL** (uniform resource locator ou localisateur universel de ressources) : adresse qui précise la localisation d'une ressource internet en indiquant le protocole à adopter, le nom de la machine, le chemin d'accès et le nom du fichier.
- **VPN** (virtual private network ou réseau privé virtuel) : outil numérique qui redirige un trafic internet via un tunnel sécurisé.
- **Web** ou **la toile** : système hypermédia permettant d'accéder aux ressources du réseau internet.

Bibliographie

- Aguila Nicolas, 2008 : « Il était une fois, le téléphone portable », *Tom's Guide*, 7 mai 2008.
- AHAT, 2015 : Manuel d'histoire du Togo des origines à 2005, à l'usage des enseignants du secondaire (1er et 2nd cycles) des enseignements général et techniques, les Presses de l'UL, 244p.
- Berry Gérard, 2008, *Pourquoi et comment le monde devient numérique*, Paris, Fayard, 80 p.
- Blaya Catherine, 2015, « Etude du lien entre cyberviolence et climat scolaire : enquête auprès des collégiens d'Ile de France », URL : <http://journals.openedition.org/dse/815> ; DOI : 10.4000/dse.815, p. 69-90.
- Conseil de l'Europe, COE, 2016, 16p.
- Durkheim Emile, 2013 : *Éducation et sociologie*, p.144, ISBN: 978-2-13-056858-2
- Goleman Daniel, 2011, *The Brain and Emotional Intelligence: New Insights, More Than Sound*, États-Unis, ISBN: 1934441155, 79p.
- Feuillard D. (Sd), 1999 : *Education civique 3^e*, Hachette, 110 p.
- Gayibor L. Nicoué (Sd) ,1987 : *Le Togo sous la domination coloniale (1884-1960)*, Les Presses de l'UB, Lomé, 239p.
- Gnane N. Mouncaïla, ANATE Kouméalo, 2017 : « La régulation du secteur des télécommunications au Togo : impacts et défis », Centre d'Etudes et de Recherches sur les Organisations, la Communication et l'Education (CEROCE), No 007, Université

de Lomé, ISSN : 2226-1443, p86-91.

– Freinet Célestin, 1960 : *L'Education Morale et civique*, Paris ICEM¹¹-pédagogie Freinet, 39p.

– Kelsen Hans, 2004 : *La démocratie : sa nature–sa valeur*, Ed. Dalloz, 2^e édit, 122p.

– Kuner Christopher, 2003 : « European data privacy law and online business », Oxford university press, 39p.

– MCCSFC¹²/DFC¹³, 2016 : *Module de didactique de l'ECM à l'usage des enseignants du primaire*, 48p.

MCCSFC/DFC, 2018 : *Module de didactique de l'ECM à l'usage des enseignants du secondaire*, 52p.

– MDHFRCRIR¹⁴ /DFC, 2020 : *Manuel de formation à la citoyenneté à l'usage des organisations de la société civile (OSC)*, Ed. Awoudy (Lomé-Togo), ISBN 978-2-37316-319-3, 108p.

– Peres Eric, 2015 : *Les données numériques : un enjeu d'éducation et de citoyenneté*, les Editions des journaux officiels, 154p.

– Prensky Marc, 2001: « Digital Natives, Digital immigrants », On the Horizon (MCB University Press, Vol. 9 No. 5, 6p.

– République Togolaise, ENI¹⁵, 2015 : *Education civique et morale (ECM)*, résumé des notions fondamentales, 1^{ère} éd, 76p.

¹¹ ICEM : Institut coopératif de l'école moderne.

¹² MCCSFC : Ministère de la communication, de la culture, des sports et de la formation civique.

¹³ DFC : Direction de la formation civique.

¹⁴ Ministère des Droits de l'Homme, de la Formation à la Citoyenneté, des Relations avec les Institutions de la République

¹⁵ ENI : Ecole normale des instituteurs.

- République Togolaise, MEN¹⁶, 1975 : *La réforme de l'enseignement au Togo* (forme abrégée), Lomé, 37p.
- République Togolaise, MEPDD¹⁷, 1983 : *Le précis de législation et de l'administration scolaire*, Paris, Nathan, 126p.
- République Togolaise (MENR), 1997 : *Programme d'Education civique et Morale pour les enseignements du premier, deuxième et troisième degré*, PUB, 53 p.
- République Togolaise, MCCSFC¹⁸, 2014 : *La politique nationale de formation civique et d'éducation à la citoyenneté*, Lomé.
- République Togolaise, UNICEF 2016 : *Le guide d'animation du module d'éducation des adolescents et adolescentes aux compétences de vie courante*.
- République Togolaise, PASCRENA¹⁹, 2014 : *Manuel de formation au civisme et à la citoyenneté*, Lomé, Label Print, 247 p.
- République Togolaise, Coopération Togo-UNESCO, 2012 : *Guide d'Appropriation et d'administration des nouveaux programmes d'éducation civique et morale (ECM)*, Lomé, 121p.
- République Togolaise, UNESCO/CEDEAO, BAD, 2012 : *Les nouveaux programmes d'ECM*, 143p.
- Tchangai B.E., 2017 : *Introduction et Méthodologie de*

¹⁶ MEN : Ministère de l'éducation nationale.

¹⁷ MEPDD : Ministère de l'Enseignement des premier et deuxième degrés.

¹⁸ MCCSFC : Ministère de la communication, de la culture, des sports et de la formation civique.

¹⁹ PASCRENA : Projet d'appui à la société civile et à la réconciliation nationale.

l'enseignement de l'ECM, ENS, Togo, 24p.

– UNICEF, 2015 : *Les objectifs de développement durable (ODD)*, 8p.

– UNESCO, *SansSaeng*, 2018 : *Education à la citoyenneté mondiale dans les contextes locaux*, ISSN, 1599-4880, No 50, 52p.

– UNICEF et Aide et Action 2014 : *Processus de mise en place du gouvernement des enfants*.

– UNICEF/France, 2015 : *Les Objectifs de développement durable (ODD)*, 14p. ISBN 978-2-37316-319-3

– UNICEF, 2018 : *Mon cahier d'exercices aux compétences de vie courante (Like SKILIS) 2013-2017, Rapport final*, 121p.

Table des matières

Sommaire.....	5
Préface.....	7
Remerciements.....	10
Sigles et abréviations.....	11
Introduction.....	13
1. HISTORIQUE ET CONCEPTS FONDAMENTAUX DU NUMERIQUE.....	15
1.1. Historique du numérique.....	15
1.2. Clarification des concepts.....	19
1.3. Le vaste champ du numérique.....	24
1.4. Domaines de l'ECN.....	24
1.4.1. Être en ligne (Being on line).....	25
1.4.2 Bien-être en ligne.....	31
1.4.3 Droits en ligne.....	36
1.5. Quelques avantages et inconvénients du numérique.....	39
1.5.1 Avantages.....	39
1.5.2. Inconvénients du numérique.....	40
2. ENVIRONNEMENT DU NUMERIQUE AU TOGO.....	41
2.1. Etat des lieux de l'incivisme numérique au Togo.....	41
2.1.1 Les infractions.....	41
2.2 Les enjeux et défis du numérique pour le Togo.....	46
2.2.1 Les enjeux.....	46
2.2.2. Les défis.....	46

2.3. L'ambition du gouvernement togolais en matière d'éducation à la citoyenneté numérique.....	47
2.3.1. Domaine de l'éducation.....	47
2.3.2 Domaine de la citoyenneté.....	48
2.3.3 Domaine du numérique.....	49
2.4. Le cadre juridique et institutionnel dans le domaine du numérique.....	49
2.4.1. Le cadre juridique.....	50
2.4.2. Le cadre institutionnel.....	56
2.5. Quelques projets de l'Etat dans le domaine du numérique..	61
3. QUELQUES CONSEILS PRATIQUES.....	61
3.1. Recommandations du Conseil de l'Europe.....	62
3.2. Le guide d'hygiène numérique de l'ANCy.....	63
3.3. Le code de la bonne conduite de la DFC.....	66
Glossaire.....	79
Bibliographie.....	81

**Achévé d'imprimer au Togo
Sur les presses de Gosen Print
pour le compte des éditions Awoudy**

Novembre 2022

Dépôt légal : N° /MATDDT/Novembre 2022

MANUEL D'ÉDUCATION À LA CITOYENNETÉ NUMÉRIQUE

L'apparition du numérique, dans le monde en général et au Togo en particulier, a profondément révolutionné la façon dont les individus communiquent, travaillent, apprennent, commercent et se divertissent. Son impact positif sur le développement n'est plus à démontrer. Le gouvernement, s'inscrivant dans cette dynamique, a prévu, dans le PND 2018-2022, de faire du numérique un véritable levier de modernisation de l'économie et de la société togolaise en rendant les services des TIC accessibles au plus grand nombre de citoyens... Cette ambition affichée par les plus hautes autorités de notre pays ne peut être effective sans une réelle prise de conscience, par les utilisateurs, des enjeux des services numériques, particulièrement des réseaux sociaux.

Ces dernières années, notre pays fait face à une montée de l'incivisme dans le cyberspace caractérisé par la dépravation des mœurs, la prolifération des fake news, des intimidations, des attaques de tout genre, de l'escroquerie, de la diffamation, des propos suscitant la haine, la violence, l'intolérance, etc. Malgré l'existence de plusieurs lois, la situation reste préoccupante.

Pour y remédier, il importe de disposer d'outils de référence permettant d'assurer l'éducation des populations en la matière en vue de contribuer à l'atteinte du but visé par la Politique nationale de formation civique et d'éducation à la citoyenneté (PNFC-EC).

C'est pour y parvenir que le MDHFCRIR, à travers la DFC, a élaboré le présent manuel destiné aux acteurs de l'éducation à la citoyenneté numérique (ECN) et aux usagers du numérique.



9 782373 164121

Illustrations de
Déo Daona