« EDUCATION POUR LA CYBERSECURITE EN MILIEU SCOLAIRE A CETTE ERE DU NUMERIQUE AU BENIN : UNE STRATEGIE DE COMMUNICATION POUR LE DEVELOPPEMENT ».

Dr Valentin MONNOU
(Université d'Abomey-Calavi, Bénin)
movalino1@gmail.com
Dr Sammuel DJENGUE
(Maître de Conférences à l'UAC)
Ayajemu M. E. Judith DJENGUE
(Doctorante à l'UAC)

RESUME :

Le passage de l'analogie au numérique, a profondément changé la physiologie de la société traditionnelle qui s'est très vite transformée en une société des TIC. Ces outils indispensables au développement économique, sont aujourd'hui utilisés à des fins de criminalité qui constituent des menaces pour la sécurité des citoyens dans le monde. Ces menaces n'épargnent guère le bénin au regard des actualités qui ne cessent de faire quotidiennement cas des comportements cybercriminels. Mais ces comportements ne sont pas des actions spontanées. Ils sont des fruits d'un certain nombre de facteurs regroupés en deux grandes catégories: les facteurs prédisposants et les facteurs facilitants.

Dans le combat, la stratégie de la police républicaine menée par l'OCRC (Office Centrale de Répression de la Cybercriminalité), mérite l'accompagnement par la prévention à travers l'école. Cette institution peut valablement accompagner la lutte à travers l'insertion de l'EPC (Education Pour la Cybersécurité) dans les curricula de formation.
Mots clés : *Cybersécurité- Education- Communication.*

SUMMARY

The transition from analog to digital has profoundly transformed the structure of traditional society, which rapidly evolved into an ICT-based society. These tools, essential for economic development, are now being misused for criminal purposes, posing serious threats to the security of citizens worldwide. Benin is not spared from these threats, as daily reports

continue to highlight various forms of cybercriminal behavior. However, such behaviors are not spontaneous; they result from a number of factors, which can be classified into two main categories: predisposing factors and facilitating factors.
In addressing this issue, the strategy of the Republican Police, implemented by the Central Office for the Repression of Cybercrime (OCRC), deserves to be complemented by preventive measures within the educational system. Schools can effectively support this fight through the integration of Cybersecurity Education (CSE) into training curricula.
Keywords: *Cybersecurity – Education – Communication*

0. INTRODUCTION

Dans un monde de plus en plus interconnecté et dépendant de la technologie, la cybersécurité est devenue un enjeu crucial pour la stabilité et la durabilité de nos sociétés. Les avancées rapides dans le domaine de la technologie ont ouvert de nouvelles opportunités, mais ont également créé de nouveaux risques et menaces, notamment ceux liés à la cybercriminalité. Face à ces défis croissants, l'éducation pour la cybersécurité émerge comme une réponse essentielle pour protéger les individus, les entreprises et les gouvernements contre les attaques cybernétiques. L'intégration de la cybersécurité dans les programmes d'enseignement et la sensibilisation du public aux risques en ligne sont devenus des impératifs pour assurer un développement numérique durable. La présente étude intitulée « Education pour la cybersécurité en milieu scolaire à cette ère du numérique au Bénin : une stratégie de communication pour un développement durable » s'inscrit dans cette approche préventive et s'articule autour de deux grands chapitres : le premier concerne le cadre théorique et méthodologique ; le second quant à lui est lié au cadre empirique de la recherche

CHAPITRE 1 : CADRE THEORIQUE ET METHODOLOGIQUE

1.1. Cadre théorique

1.1.1. Problématique

Instruments majeurs de la mondialisation, les technologies de l'information et de la communication (TIC) ont profondément transformé les modes de vie, d'apprentissage et de travail à travers le monde. Leur intégration croissante dans les systèmes éducatifs devrait, en principe, favoriser la créativité, l'innovation et le développement socio-économique. Cependant, l'essor du numérique s'accompagne d'une recrudescence de la cybercriminalité, notamment en Afrique de l'Ouest, où le Bénin n'est pas épargné.

Selon les rapports récents de l'Agence nationale de la sécurité des systèmes d'information (ANSSI-Bénin) et de la Plateforme de lutte contre la cybercriminalité (PLCC), le pays enregistre chaque année une augmentation notable des cas d'escroqueries en ligne, d'usurpations d'identité, de piratages de comptes bancaires et de diffusion de fausses informations. Cette situation touche particulièrement les jeunes, souvent auteurs ou victimes, en raison d'une faible éducation numérique et d'un manque de sensibilisation aux risques cybernétiques.

Malgré l'adoption du Code du numérique (2017) et de plusieurs programmes de cybersécurité, les mesures essentiellement répressives semblent insuffisantes face à la complexité et à la dynamique du phénomène. D'où la nécessité de repenser la lutte contre la cybercriminalité non plus seulement sous l'angle policier et juridique, mais aussi comme un enjeu éducatif et communicationnel.

Dès lors, plusieurs interrogations s'imposent :

Les stratégies de sensibilisation actuelles mises en œuvre par l'État sont-elles réellement efficaces ?

Quels sont les facteurs socioculturels, économiques et communicationnels qui favorisent l'implication des jeunes dans les actes cybercriminels ?
L'éducation en milieu scolaire peut-elle constituer un levier stratégique de prévention durable?
Comment une stratégie de communication pour le développement, intégrant l'éducation numérique et la sensibilisation citoyenne, peut-elle contribuer à réduire la cybercriminalité et à promouvoir un usage responsable du numérique au Bénin ?

1.1.2. Hypothèses de l'étude

1.1.2.1. Hypothèse générale

Dans ce contexte de répressions contre des comportements cybercriminels, la contribution de l'éducation s'avère importante.

1.1.2.2. Hypothèses spécifiques

- L'état des lieux sur les types de cybercrimes et les répressions menées par l'Etat béninois est fait ;
- Les facteurs psychosociaux sont responsables des comportements cybercriminels ;
- La contribution de l'Education pour la Cybersécurité(EPC) dans la lutte contre les comportements cybercriminels en vue d'une perspective pour le développement durable est importante.

1.1.3. Objectifs de l'étude

Si cette étude est réalisée, c'est pour essentiellement atteindre les objectifs suivants :

1.1.3.1. Objectif général

Promouvoir dans les écoles, une éducation pour la cybersécurité dans la lutte contre les comportements cybercriminels au bénin.

1.1.3.2. Objectifs spécifiques

- Faire l'état des lieux sur les types de cybercrimes et les répressions menées par l'Etat béninois dans ce sens ;
- Identifier les facteurs psychosociaux liés aux comportements des cybercriminels ;
- montrer la contribution de l'Education pour la Cybersécurité(EPC) dans la lutte contre ces pratiques en vue d'une perspective pour le développement durable.

1.1.4. Théories mobilisées

La plupart des approches criminologiques classiques ont pour objectif principal de dissuader les délinquants en recourant à la répression (Hirschi, 1969). Toutefois, lorsqu'il s'agit d'obtenir un changement de comportement durable, la dissuasion seule s'avère insuffisante.

Dans le cadre de la lutte contre la cybercriminalité, il est plus judicieux d'adopter une approche préventive et éducative, fondée sur la communication pour le développement. C'est pourquoi les modèles théoriques mobilisés dans cette étude s'inspirent en grande partie des théories de la prévention comportementale issues des sciences sociales et de la santé publique, mais applicables au domaine de la cybersécurité éducative.

Ces modèles permettent de comprendre comment les représentations, les croyances et l'environnement social influencent l'adoption de comportements sécuritaires face aux menaces numériques. Ils visent non seulement à prévenir les actes délictueux, mais aussi à protéger les élèves contre les risques de victimisation en ligne.

1.1.4.1. Le Health Belief Model (HBM)

Le Health Belief Model (HBM) a été élaboré dans les années 1950 par Rosenstock.

C'est une théorie des croyances relatives à la santé qui s'avère particulièrement utile pour prédire les comportements préventifs.
Selon Godin (1984), « le HBM pose comme prémisse que tout individu est susceptible d'entreprendre une action pour prévenir une maladie ou une situation désagréable, s'il possède des connaissances minimales sur la question et s'il considère cette dimension comme importante pour sa vie ».
Transposé au domaine de la cybersécurité, cela signifie que tout individu est capable d'agir pour prévenir une menace cybernétique s'il dispose des connaissances nécessaires et perçoit le risque comme réel. Deux déterminants essentiels guident cette action préventive : la perception de la menace, liée à la vulnérabilité ressentie face aux cyberattaques ; la croyance en l'efficacité des actions préventives, fondée sur les avantages perçus des comportements sécuritaires (Becker, 1963).
Ainsi, l'éducation numérique en milieu scolaire doit viser à accroître la conscience du risque et à renforcer la confiance des apprenants dans leur capacité à adopter des comportements protecteurs (mots de passe forts, vigilance face aux arnaques, etc.).

1.1.4.2. La théorie sociale cognitive (TSC)

Proposée par Albert Bandura (1977), la théorie sociale cognitive met l'accent sur l'influence de l'environnement social, de l'apprentissage par observation et du sentiment d'efficacité personnelle sur les comportements.
Elle complète le HBM en insistant sur le rôle de la croyance en sa propre capacité à agir (auto-efficacité).
Selon Bandura, les différences individuelles dans l'adoption d'un comportement donné s'expliquent par deux croyances fondamentales : la croyance en l'efficacité du comportement (le comportement est perçu comme utile pour prévenir la menace) ;

la croyance en l'efficacité personnelle (l'individu se croit capable de mettre en œuvre ce comportement).
Dans le cadre de l'éducation à la cybersécurité, cela implique que les apprenants doivent être outillés, encouragés et soutenus afin de se sentir capables d'appliquer les mesures de protection numérique enseignées. L'environnement éducatif — enseignants, pairs, encadrants — joue un rôle déterminant dans la consolidation de cette auto-efficacité.

1.1.4.3. La théorie de l'action raisonnée (TAR)

Élaborée par Fishbein et Ajzen (1975), la théorie de l'action raisonnée vise à prédire les comportements sociaux en fonction de l'intention d'agir.
Selon ce modèle, l'intention d'adopter un comportement dépend de deux composantes :
-l'attitude à l'égard du comportement, c'est-à-dire l'évaluation positive ou négative des conséquences de l'action envisagée ;
-la norme subjective, soit l'importance accordée à l'opinion des personnes significatives dans l'entourage.
Appliquée à la prévention de la cybercriminalité, la TAR permet de comprendre que l'élève choisira d'adopter des pratiques sécuritaires en ligne s'il :
-perçoit les avantages de ces comportements (par exemple : éviter le vol de données, préserver sa réputation numérique) ;
- ressent une pression sociale positive provenant de ses pairs, enseignants ou parents, qui valorisent la prudence numérique.

Ainsi, l'éducation pour la cybersécurité doit non seulement renforcer les attitudes favorables à la prévention, mais aussi créer un environnement normatif positif, où les comportements responsables en ligne sont encouragés et valorisés.

1.1.5. Clarification conceptuelle

1.1.5.1. La communication

Étymologiquement, l'expression « communication » veut dire mettre en commun ce qui ne doit pas rester privé. Selon Paul ROBERT (1912 ; p.139), elle signifie aussi « établir une relation avec quelqu'un ou quelque chose ». La communication est le fait de transmettre à quelqu'un tout ce qui est nécessaire pour l'informer. Elle peut être une information, une annonce, un avis, un message, une note, une nouvelle ou un renseignement.

1.1.5.1.1. La communication pour le développement (C4D)

La C4D est une approche stratégique qui utilise les techniques et outils de communication pour faciliter le changement social, améliorer la participation des communautés et promouvoir le développement durable. C'est:

« *l'utilisation de façon planifiée et organisée des techniques et des moyens de communication (médiatiques et non médiatiques) pour promouvoir le développement, à travers un changement d'attitude et/ou de comportement, en diffusant l'information nécessaire et en suscitant la participation active et consciente de tous les acteurs, y compris des bénéficiaires au processus* » (DJENGUE, 2015 p.27).

Elle comprend essentiellement trois axes stratégiques à savoir l'éducation ou la sensibilisation (pour le changement de comportements, de connaissances, d'attitudes et de pratiques); la mobilisation sociale(pour la construction de partenariat plus large acquis à une cause donnée) et le plaidoyer(pour susciter l'engagement des décideurs politiques). La présente étude s'intéresse beaucoup plus à l'une de ces stratégies qui est l'éducation.

1.1.5.2. L'éducation

Selon Emile DURKHEIM(1922), l'éducation est 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 chez un enfant un certain nombre d'états physiques intellectuels et moraux que réclame de lui la société politique dans son

ensemble et le milieu spécial auquel il est particulièrement destiné.
Pour ROUSSEAU (1762), elle est l'art de former les hommes et consiste moins à enseigner des connaissances qu'à cultiver la capacité à bien vivre.

1.1.5.3. Le développement

Globalement, le développement est l'ensemble des transformations techniques, sociales et culturelles qui permettent l'apparition et la prolongation de la croissance économique ainsi que l'élévation des niveaux de vie. Il est également « un long processus de changement d'ordre quantitatif et qualitatif intervenant dans une société aux plans politique, économique, social, culturel et scientifique et menant vers un bien-être individuel et collectif »(MONNOU 2022 P.35).
Le concept développement durable quant à lui, est « tout développement qui permet de satisfaire les besoins des générations actuelles sans compromettre la satisfaction de ceux des générations futures et qui est centré sur l'homme ; développement de l'homme par l'homme et pour l'homme, de tout l'homme et de tous les hommes»(MONNOU 2022 P.38).

1.1.5.4. La cybersécurité:

Qui dit Cybersécurité, dit mesure de sécurité qui est, selon le code du numérique en République du Bénin (2018: p.28), « toute utilisation des procédures, des dispositifs ou des programmes informatiques spécialisés à l'aide desquels l'accès à un système informatique est limité ou interdit pour certaines catégories d'utilisateurs ». Plus précisément, c'est l'ensemble des mesures et des actions destinées à protéger le cyberespace des menaces associées à ses réseaux et à son infrastructure informatique ou susceptibles de leur porter atteinte. La cybersécurité vise à préserver la disponibilité et l'intégrité des

réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues.

Ce concept fait appel à d'autres comme la Cybercriminalité, les cyberattaques qui urgent d'être clarifiés dans cette étude.

1.1.5.4.1. La cybercriminalité

Maras (2021) définit la cybercriminalité comme la commission d'un crime, c'est-a-dire un acte qui viole une ou des lois existantes, par l'entremise de la technologie (avec l'utilisation d'internet, d'un ordinateur).

Selon H. ALTERMAN et A. BLOCH (1988), la cybercriminalité se définit comme « tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données »

Pour Samuel DJENGUE(2015), «c'est une infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau».

1.1.5.4.2. Les types de cyberattaques

Les cas les plus fréquents sont les suivants :

• Rançongiciel/ransomware : virus informatique qui rend indisponible un système et des données tant qu'une rançon n'a pas été payée. C'est un logiciel malveillant qui chiffre les données personnelles puis exige au propriétaire d'envoyer de l'argent en échange de la clé de déchiffrement. Par exemple, un entrepreneur constate un jour que toute la comptabilité de l'entreprise a disparu parce que quelqu'un aurait cliqué sur un lien piégé ou sur une pièce jointe infectée un ''cheval de Troie'' s'est introduit, rendant le système inutilisable. Peu de temps après, il reçoit un e-mail lui demandant une rançon, associée à une minuterie qui décompte le temps qui reste.

• L'hameçonnage/phishing : il se définit comme une « cyberattaque consistant à appâter (hameçonner) une personne pour lui faire exécuer une action nuisible, comme l'ouverture d'une pièce jointe corrompue ou d'un lien pointant vers un site malveillant » (H. ALTERMAN et A. BLOCH : La Fraude: 1988).

C'est une technique de fraude visant à obtenir des informations confidentielles, telles que les mots de passe ou des numéros de carte de crédit au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales. Il désigne les différentes techniques utilisées pour soustraire des informations sensibles. Le principe consiste non pas à utiliser une faille informatique mais une ‘’faille humaine’’ en dupant les internautes par le biais d'un courriel (phishing), d'un appel (vishing) ou d'un sms (smishing) apparemment sûr. Il emprunte le plus souvent l'identité d'une entreprise de confiance et demande à l'internaute de mettre à jour des informations le concernant via un formulaire factice. Les pirates réussissent à obtenir identifiants, mots de passe ou encore données personnelles ou bancaires (numéros de client ou numéro de compte en banque). Conséquence : les hackers peuvent transférer directement de l'argent sur un autre compte.

• L'escroquerie: c'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. Ainsi, un individu se faisant passer pour le dirigeant (avec usurpation du n° d'appelant et modification de la voix, aujourd'hui techniquement possible), demandant à une assistante de faire un virement ‘’urgent et confidentiel’’. Mise en oeuvre de techniques d'intimidation, de flatterie (‘’vous étiez très en beauté lors de la cérémonie à Paris

avec votre robe rouge'' (l'assistante portait effectivement une robe rouge photo publiée sur FB), de menace aussi si la personne ne s'exécute pas.

1.2. Méthodologie de recherche

La présente étude qui est une contribution théorique et fondamentale propose une approche pédagogique et élémentaire adaptée à l'enseignement de l'éthique en milieu scolaire en vue de lutter contre les comportements cybercriminels. Nous n'avons nullement l'intention d'aborder les aspects purement répressifs du phénomène.

Notre analyse s'appesantira plutôt sur la nécessité de changer de paradigme de lutte en pensant à l'intégration de l'EPC (Education pour la Cybercrimnalité) dans le dispositif des programmes scolaires. C'est une étude qui se veut qualitative et quantitative en ce sens:

- qu'elle s'évertuera à mettre en évidence les facteurs qui favorisent et renforcent les comportements cybercriminels;
- qu'elle est surtout focalisée sur le milieu scolaire, une occasion d'impacter une plus grande majorité de la population béninoise.

CHAPITRE 2 : CADRE EMPIRIQUE

2.1. Présentation et analyse des résultats

2.1.1. Quelques faits cybercriminels

Un fait très sensible de cybercrime, est l'affaire CAMEO Shell. Que comprendre de cette affaire ? CAMEO Shell est une plateforme d'investissement qui, à l'instar de ICC, propose une variété de gains très intéressants à ses clients. Vis-à-vis de cette structure, il y a plusieurs irrégularités que les utilisateurs ont commencé par dénoncer parce que nombreux n'arrivaient plus à retirer ce qu'ils ont déposé. Le 07 Mars 2023, 365 victimes ont déposé des plaintes contre cette structure pour avoir été spoliés (Béninweb). Après CAMEO Shell, une autre structure du nom de Omega Pro, une plateforme de placement d'argent en ligne,

a disparu avec les sous de ses investisseurs béninois (Libre Express du 04 Aout 2023).

A ce champ qualifié d'escroquerie financière, vient s'ajouter le vol d'identité personnelle. Ainsi, un jeune cybercriminel a été poursuivi par la CRIET pour usurpation de l'identité de Eric Dupond- Moretti, ministre français de la justice. Les faits foisonnent et il urge de passer en revue les différentes luttes de répression qui ont été menée par les autorités béninoises.

2.1.2. Etat des lieux de la lutte contre la cybercriminalité au Bénin

« La cybercriminalité au bénin: le gouvernement s'engage dans une traque permanente ». C'est par ce titre du journal CRYSTAL- NEWS du 04 Mars 2023 que nous allons commencer notre état de lieu de l'engagement ferme du gouvernement à lutter contre ce phénomène. Ainsi, le 09 Mars 2023, dans la commune d'Allada, un marabout a été arrêté par l'OCRC(Office Centrale de Répression de la Cybercriminalité) pour sa complicité de cybercriminalité(in Le potentiel du 09 Mars 2023). Le 1er Mars 2023 à Agoué, dans la commune de Grand-Popo, le commissaire, sur renseignement, y a fait une descente inopinée ; ce qui lui a permis de mettre la main sur 17 présumés gaymens dont 04 femmes (Le triomphe du 06 Mars 2023).

Après leur présentation à la CRIET le vendredi 10 Mars 2023, plusieurs agents de la police républicaine dont un commissaire, ont été déposés en prison de Calavi pour extorsion de fonds chez un cyberciminel (Bénin Web).

A Avrankou, le 11 Mars 2023, un chef d'une bande de gaymen et ses disciples ont été arrêtés (Le Triomphe). De même, à Cotonou dans le quartier Akpakpa, l'OCRC a raisonné une jeune dame présumée redoutable patronne.

Le 19 Mars 2023, les éléments de l'OCRC ont fait l'irruption dans un bar à Godomè lors du match Barça-Réal ; conséquence, une bande de jeunes présumés gaymen ont été appréhendés.

Invité sur une émission spéciale de la télévision nationale le vendredi 21 Avril 2023 , Mario METONOU, le procureur spécial de la CRIET a fait le point des arrestations et condamnations faites dans le cadre de la lutte contre la cybercriminalité au bénin. Ainsi, au cour de l'année judiciaire 2020-2021, il y a 360 condamnations pour des questions de cybercriminalité. L'année judiciaire 2021-2022, 451 cas de condamnations ont été signalés. A la date d'Avril 2023, 1188 cybercriminels sont détenus en prison.

Face à tous ces efforts consentis à la répression de la cybercriminalité, il est primordial de mettre en évidence les facteurs qui sous-tendent ce fléau moderne.

2.1.3. Les facteurs psychosociaux lies aux comportements des cybercriminels

Les comportements cybercriminels doivent être étudiés dans une perspective psychosociale, c'est- à- dire en considérant l'interaction des jeunes avec leurs environnements psychologique et social

Les enquêtes menées auprès de la population ont permis d'identifier quelques facteurs prédisposants et facilitants à la pratique cybercriminelle.

2.1.3.1. Les facteurs prédisposants

Ce sont des facteurs qui fournissent à l'homme, des habiletés intellectuelles et physiques capables de le rendre apte à agir. Ainsi, le premier facteur qui prédispose surtout les jeunes à la cybercriminalité est l'instruction. Ainsi, dans son rôle d'éducation et de formation, l'école produit inconsciemment un effet de boomerang. En effet, les cybercriminels sont pour la plu

part, des jeunes à qui l'école a donné des bases élémentaires qui leur permettent de savoir lire et écrire, d'avoir des passions pour les NTIC qu'ils utilisent conséquemment pour des fins d'escroquerie. Mais elle ne suffit pas à elle seule pour justifier la prédisposition de ces jeunes à la pratique cybercriminelle. La croyance en efficacité des gains que cela procure n'est pas à balayer du revers de la main. Les jeunes qui s'adonnent à ce comportement, pensent fermement que c'est la voie de raccourcis pour vite accéder à la richesse en violation contre la loi sacrosainte de la nature qui est le travail.

2.1.3.2. Les facteurs facilitants

Comme leur nom l'indique, ce sont des facteurs capables de faciliter le comportement cybercriminel chez les jeunes et sont tributaires de l'environnement social. D'abord, un regard critique sur l'état de lieu du phénomène ci-dessus présenté nous permet de se rendre compte des complicités des marabouts et de certains agents de la Police Républicaine(PR). Au moment où les cybercriminels se font aider par les fétiches à qui ils offrent des sacrifices humains, certains agents de sécurité, émus par les intérêts personnels, constituent un levier de crime et de son impunité. La Police Républicaine a-t-elle reconnu sa faiblesse à travers certains de ses agents surpris pour extorsion de fonds chez un cybercriminel à Calavi ? Comment, depuis la prison civile de Missérété, un cybercriminel a pu vider les comptes de plusieurs personnes sous le regard impuissant des geôliers ? Voilà autant d'inquiétudes dans le rang de nos forces de sécurité qui justifient la complexité de la lutte contre le fléau.
Ensuite, les parents, harcelés par diverses tâches quotidiennes de la vie, n'ont plus de temps nécessaires pour contrôler les mouvements de leurs enfants qui, par voie de conséquence, finissent par être accueillis par les mauvaises compagnies.

Enfin, l'inégalité sociale axée sur la distribution peu orthodoxe des richesses, a considérablement encouragé le

phénomène. En effet, pendant que la base de l'échelle, c'est-à-dire la jeunesse bardée de diplômes, sont sans emplois, souffrent, une minorité au sommet de l'Etat se taille la part de lion dans la répartition de ces richesses. Il y en a certains qui occupent cumulativement plusieurs postes soi-disant experts qui sont partout et d'ailleurs nulle part. Dans ces conditions, c'est l'espoir de la jeunesse qui s'amenuise, laissant ainsi place à toute forme de crimes.

2. 3. Contribution de l'éducation pour la cybersécurité (EPC) dans la lutte contre la cybercriminalité en vue d'une perspective pour le développement.

Au Bénin, plusieurs actions ont été entreprises pour endiguer la cybercriminalité, notamment à travers des mesures coercitives, des campagnes de sensibilisation ponctuelles et le renforcement du cadre juridique. Cependant, les données recueillies sur le terrain montrent que ces actions, bien que nécessaires, demeurent insuffisantes pour endiguer durablement le phénomène.

Les entretiens réalisés auprès d'enseignants, de chefs d'établissement et d'élèves révèlent que la majorité des apprenants perçoivent encore Internet comme un espace de liberté sans règles, où la transgression est banalisée et parfois même valorisée socialement. Ce constat met en évidence la nécessité de déplacer la lutte contre la cybercriminalité du champ exclusivement répressif vers un champ éducatif et préventif.

En réalité, la lutte contre la cybercriminalité ne saurait être uniquement l'affaire de la Police Républicaine, dont l'arme principale reste la dissuasion. Elle doit s'inscrire dans une approche communicationnelle et intégrée, impliquant l'école comme acteur de socialisation et d'éducation citoyenne. Les observations menées dans plusieurs établissements secondaires du Bénin indiquent que l'absence d'un cadre formel d'éducation

numérique et de cybersécurité laisse les jeunes vulnérables à la désinformation, à la fraude en ligne et aux pratiques d'arnaque électronique. C'est dans ce contexte que l'introduction d'une Éducation pour la Cybersécurité (EPC) apparaît comme une stratégie de communication pour le développement, visant à former un citoyen numérique responsable et éthique.

L'EPC se définit ici comme un dispositif d'acquisition de connaissances, d'attitudes et de comportements responsables relatifs à l'usage des Technologies de l'Information et de la Communication (TIC). Elle s'appuie sur les valeurs morales, la responsabilité individuelle et la compréhension des risques liés à l'environnement numérique. Sur le terrain, plusieurs enseignants interrogés ont souligné que les élèves manquent d'un repère moral face à la tentation des « gains faciles » sur Internet.

Ainsi, une telle éducation contribuerait à développer chez les apprenants le sens critique, la responsabilité numérique et le respect des normes éthiques dans l'utilisation des outils technologiques réputés être des leviers de développement et non des instruments de déviance.

En tant qu'approche préventive, l'EPC ne vise pas seulement à protéger les usagers potentiels contre les cybercriminels, mais également à favoriser la réinsertion comportementale des jeunes déjà tentés ou engagés dans ces pratiques, en leur permettant de comprendre les conséquences sociales, économiques et juridiques de leurs actes. Plusieurs jeunes interrogés dans les milieux urbains de Cotonou et d'Abomey-Calavi affirment, par exemple, n'avoir jamais reçu de formation formelle sur la cybersécurité, bien qu'ils utilisent quotidiennement les réseaux sociaux et les plateformes de transaction numérique.

Par ailleurs, l'expression « Éducation pour la Cybersécurité » renvoie à une communication organisée autour de la diffusion de savoirs pratiques et citoyens sur les usages numériques responsables. Elle participe du droit à l'information et du devoir

de formation civique reconnus dans tout système démocratique moderne. Elle constitue donc un axe de la communication pour le développement, dans la mesure où elle cherche à produire un changement de comportement collectif en faveur d'une société numérique plus sûre et plus éthique.
Pour sa mise en œuvre dans le système éducatif béninois, deux approches complémentaires peuvent être envisagées :
Premièrement, l'intégration de l'EPC comme une discipline à part entière dans les programmes scolaires, à l'image de l'éducation civique ou de l'éducation aux droits humains ;
Deuxièmement, la mobilisation d'intervenants spécialisés (experts en cybersécurité, communicateurs, acteurs du numérique) pour animer des séances pratiques, des ateliers et des campagnes interactives dans les écoles.
Les données recueillies sur le terrain montrent d'ailleurs une forte adhésion des enseignants et
des parents à une telle initiative, estimant qu'une éducation à la cybersécurité permettrait de réduire significativement le nombre de jeunes attirés par les activités cybercriminelles, tout en favorisant leur insertion sociale et professionnelle dans un environnement numérique plus sécurisé.

2-1-4-1- Quelques règles de protection

Pour se protéger contre les cyberattaques, voici quelques règles de base à appliquer :
- Choisir avec soin ses mots de passe : Il convient de choisir des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou par une tierce personne. Ils doivent être difficiles à trouver mais faciles à retenir et n'ayant aucune référence personnelle (nom, date de naissance, prénom des enfants….).
Les mots figurant dans le dictionnaire sont à proscrire car il existe aussi des « attaques par dictionnaire qui consistent à tester à grande vitesse, via un logiciel spécialisé, tous les mots du

dictionnaire en espérant que l'un d'eux soit utilisé comme mot de passe.
Pour le mémoriser plus facilement, on peut utiliser La méthode phonétique qui tient compte des premières lettres («j'ai un pain que j'ai acheté» devient : g1pqga)
- Ne divulguer à personne les mots de passe;
- Mettre à jour régulièrement ses logiciels: des vulnérabilités existant dans chaque système d'exploitation, les éditeurs proposent régulièrement aux utilisateurs des mises à jour de sécurité ;
- Effectuer des sauvegardes régulières: en procédant à des sauvegardes régulières des données, on évite de s'exposer à une perte trop importante de fichiers si on a été piégé ;
- Etre vigilant avec l'utilisation du Wi-Fi :un Wi-Fi mal sécurisé permet plus facilement à des personnes d'utiliser la connexion dans le but de réaliser des opérations malintentionnées ;
- Installez un code de verrouillage sur l'écran d'accueil et activez la fonction verrouillage automatique ;
- Faire attention au phishing ou l'hameçonnage : le phishing consiste à envoyer un mail d'apparence inoffensif qui redirigera la victime vers une pièce jointe contenant un virus ou vers un faux site où elle devra faire entrer des coordonnées personnelles ;
- Ne jamais ouvrir une pièce jointe ou suivre un lien dont l'expéditeur est soit inconnu, soit d'une confiance relative car un simple clic sur une image ou un lien suffit pour installer un logiciel ou code malveillant (cheval de Troie) sur l'ordinateur ;
- Savoir utiliser l'internet avec précaution: les achats sur internet réclament une grande prudence. Mais dans tous les cas , il faut effectuer les transactions uniquement sur des sites sécurisés reconnus à travers leur adresse internet commençant par « https » et non par « http », le « s » en plus signifiant que la connexion est sécurisée ;

- Etre certain de fermer une session après avoir visité un site qui demande d'entrer de l'information personnelle sensible ;
- Eteindre l'ordinateur après usage.

CONCLUSION

À l'issue de cette étude consacrée à l'« Éducation pour la cybercriminalité en milieu scolaire à cette ère du numérique au Bénin : une stratégie de communication pour le développement », il ressort que la problématique de la cybercriminalité dépasse largement le cadre de la simple délinquance numérique pour devenir une question de société, engageant les dimensions éthiques, éducatives, culturelles et communicationnelles du développement. En effet, les résultats obtenus à partir des observations et entretiens menés sur le terrain montrent que la majorité des apprenants béninois, bien qu'étant des utilisateurs réguliers des outils numériques, disposent d'une connaissance limitée des règles de sécurité et des risques liés à Internet. Cette méconnaissance, combinée à l'attrait des gains rapides et à l'influence des pairs, favorise l'adhésion de nombreux jeunes aux pratiques cybercriminelles.

Face à ce constat, il apparaît clairement que les politiques purement répressives ou coercitives mises en œuvre jusqu'ici ne suffisent pas à éradiquer le phénomène. La lutte contre la cybercriminalité doit s'inscrire dans une approche intégrée, éducative et communicationnelle. C'est dans cette optique que l'introduction d'une Éducation pour la Cybersécurité (EPC) dans le système scolaire béninois s'avère indispensable. En développant chez les élèves une conscience numérique éclairée, une culture de la responsabilité et une éthique de l'usage technologique, l'EPC représente une réponse durable et participative à la criminalité numérique.

De plus, cette démarche s'aligne sur la logique de la communication pour le développement, qui privilégie la

sensibilisation, la participation et le changement de comportement comme leviers de transformation sociale. En formant des citoyens numériques capables d'utiliser les TIC de manière constructive, l'éducation pour la cybersécurité contribue non seulement à la réduction de la cybercriminalité, mais aussi à la consolidation de la paix sociale, à la protection des données et à la promotion d'une économie numérique sûre et inclusive.

Il convient dès lors d'envisager la mise en œuvre de cette éducation selon une approche curriculaire et partenariale : d'une part, en intégrant la cybersécurité comme une discipline transversale au sein des programmes scolaires ; d'autre part, en mobilisant des acteurs spécialisés (enseignants formés, communicateurs, experts en sécurité numérique, associations de jeunesse, médias) dans des campagnes de communication éducative continues.

En somme, l'éducation pour la cybersécurité, envisagée comme une stratégie de communication pour le développement, représente une voie novatrice et durable pour préparer les jeunes à une citoyenneté numérique responsable. Elle permettrait au Bénin de tirer pleinement parti du potentiel des TIC tout en limitant leurs dérives, contribuant ainsi à un développement humain, économique et social harmonieux dans un environnement numérique plus sûr et plus éthique.

BIBLIOGRAPHIE

Ajzen, I., & Fishbein, M. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley, 320 p.

Champy, G. (1990). *La fraude informatique* (Thèse de doctorat, Université d'Aix-Marseille).

Chawki, M. (2006, juillet). *Essai sur la notion de cybercriminalité. Institut des Hautes Études sur la Justice et l'Économie Internationale (IEHEI).*
Djenguè, S. (2015). *Droit des technologies de l'information et de la communication : État des lieux de la législation et de la déontologie au Bénin*. Christo Éditions, Cotonou, 263 p.
Djenguè, S. (2021). *Regard critique sur la trilogie "C4DHD - Territorialité de la TVA - Déséquilibre régional et paupérisation"*. Presses Universitaires de l'UAC, 128 p.
Durkheim, É. (1922). *Éducation et sociologie*. Paris : Presses Universitaires, 143 p.
Frydlender, A. (1985). *La fraude informatique : Étude phénoménologique et typologique appliquée au contexte français* (Thèse de doctorat, Université Paris IX), p. 68.
Godin, G. (1984). *Les fondements psycho-sociaux dans l'étude des comportements reliés à la santé* (Thèse de doctorat en santé communautaire, Université de Toronto), 269 p.
Howard, S. B. (1963). *Studies in the sociology of deviance*. Free Press, 200 p.
Lucas, A. (1987). *Le droit de l'informatique*. Presses Universitaires de France (PUF), n° 413.
Maras, M. H. (2021). *Cybercrime: How to combat cyber threats and secure your business*. CRC Press, 304 p.
Monnou, V. (2022). *Étude du champ sémantique et de la valeur communicationnelle des énoncés anthroponymiques : Une contribution au développement de l'aire culturelle tɔli* (Thèse de doctorat, Université d'Abomey-Calavi, Bénin), 228 p.
Robert, P. (2010). *La communication stratégique*. Éditions Dumod, 240 p.
Rosé, P. (1987). *La criminalité informatique*. Paris : Collection "Que sais-je ?", Presses Universitaires de France (PUF).
Rosé, P. (1996). *Menaces sur les autoroutes de l'information*. Paris : L'Harmattan.

Rousseau, J.-J. (1762). *Émile ou de l'éducation*. Amsterdam, 512 p.