المجلس الاقتصادي والاجتماعي والبيئي

المملكة المغربية
Royaume du Maroc

ⵓⵔⵔⵣⵔ ⵓⵏⵎⵓⵍ ⵏ ⵜⵓⵎⵙⵜ ⵏ ⵜⵎⵎⵓⵔⵜ

Conseil Economique, Social et Environnemental

Avis

du Conseil Economique, Social et Environnemental

Pour un environnement numérique inclusif et protecteur des enfants

Auto-saisine n° 75/2024

المجلس الاقتصادي والاجتماعي والبيئي

المملكة المغربية
Royaume du Maroc

ⵓⵔⵔⵣⵛ ⵓⵏⵛⵓⵏ ⵏ ⵖⵓⵛⵖⵓⵖ ⵏ ⵖⵍⵛⵓⵉ

Conseil Economique, Social et Environnemental

Avis

du Conseil Economique, Social et Environnemental

Pour un environnement numérique inclusif et protecteur des enfants

Président de la Commission et rapporteur de la thématique : M. Jaouad Chouaib

Experts internes du CESE : Nadia Sebti et Mohamed El Khamlichi

Auto-saisine n° 75/2024

Conformément à l'article 6 de la loi organique N°128-12, le Conseil Economique, Social et Environnemental (CESE) s'est autosaisi, aux fins de préparer un avis sur l'enfance et les réseaux sociaux.

Dans ce cadre, le Bureau du Conseil a confié à la commission permanente chargée des affaires sociales et de la solidarité[1] l'élaboration d'un avis sur le sujet.

Lors de sa 156ème session ordinaire, tenue le 28 mars 2024, l'Assemblée Générale du Conseil Economique, Social et Environnemental a adopté, à l'unanimité, l'avis intitulé « Pour un environnement numérique inclusif et protecteur des enfants ».

Elaboré sur la base d'une approche participative, cet avis est le résultat d'un large débat entre les différentes catégories qui composent le Conseil et des auditions organisées avec les principaux acteurs concernés[2]. Il s'est également enrichi des contributions citoyen(ne)s sur la base d'une consultation lancée sur la plateforme digitale de participation citoyenne « ouchariko.ma »[3].

1 - Annexe 1 : Liste des membres de la commission permanente chargée des affaires sociales et de la solidarité

2 - Annexe 2 : Liste des acteurs auditionnés

3 - Annexe 3 : Résultats de la consultation lancée sur la plateforme de participation citoyenne du CESE sur l'utilisation des réseaux sociaux par les enfants

Acronymes

ADD : Agence de développement du digital

ANRT : Agence Nationale de Réglementation des Télécommunications

CESE : Conseil Economique, Social et Environnemental

CMRPI : Centre marocain de recherches polytechniques et d'innovation

CNDP : Commission nationale de contrôle de la protection des données à caractère personnel

CNIL : Commission nationale de l'informatique et des libertés (France)

CPASS : Commission permanente chargée des affaires sociales et de la solidarité

DGSN : Direction Générale de la Sûreté Nationale

DGSSI : Direction Générale de la Sécurité des Systèmes d'Information

EMC : Espace Maroc Confiance

GR : Gendarmerie Royale

HACA : Haute Autorité de la Communication Audiovisuelle

IAM : Maroc Telecom

IFOP : Institut français d'opinion publique

IWF : *Internet* Watch Foundation

MENPS : Ministère de l'Éducation Nationale, du Préscolaire et des Sports

MJ : Ministère de la Justice

MSISF : Ministère de la Solidarité, de l'Insertion Sociale et de la Famille

MTNRA : Ministère de la Transition Numérique et de la Réforme de l'Administration

NEET : Not in Education, Employment or Training

ONDE : Observatoire National des Droits de l'Enfant

ITU : International Telecommunication Union (Agence des Nations Unies spécialisée dans les technologies de l'information et des télécommunications)

TIC : Technologies de l'information et de la communication

Synthèse

Le présent avis du CESE, élaboré dans le cadre d'une auto-saisine, s'inscrit dans un contexte marqué par l'utilisation massive, aux niveaux mondial et national, des réseaux sociaux par les enfants. Si ces plateformes numériques offrent certains avantages tangibles, elles exposent également les enfants à des risques importants pour leur santé physique et mentale ainsi que pour leur développement social et scolaire. Des pistes d'action sont proposées pour concilier les bénéfices du numérique avec l'impératif de protéger les enfants contre ses dangers potentiels, tout en les éduquant à une utilisation éclairée et responsable des réseaux sociaux. ». Le CESE a adopté à l'unanimité cet avis lors de la 156ème session ordinaire de son Assemblée Générale tenue le 28 mars 2024.

Les réseaux sociaux, utilisés de manière appropriée, peuvent stimuler la créativité, encourager l'expression personnelle et faciliter l'accès au savoir. Ils offrent aux enfants l'opportunité de rester en contact avec leurs pairs, de s'engager dans des communautés en ligne et d'accéder à une multitude de ressources éducatives et récréatives. En 2023, des plateformes comme *Facebook, WhatsApp et Instagram* comptaient des milliards d'abonnés à travers le monde. Au Maroc, 23 millions de personnes (66% de la population) les utilisent, y compris les enfants de 5 à 18 ans.

Il demeure, néanmoins, que l'utilisation excessive et inappropriée du numérique, en particulier des réseaux sociaux chez les enfants, constitue une menace sérieuse pour leur santé mentale et physique. Des recherches approfondies et documentées ont révélé une série de troubles psychologiques et comportementaux préoccupants, allant des troubles du sommeil et de la concentration aux comportements violents, addictions, troubles anxieux, isolement social, dépressions, voire des tentatives de suicide.

Bien que le Maroc ait ratifié la convention internationale des droits de l'enfant des Nations Unies et qu'il dispose d'un cadre légal dédié à la protection des enfants, les dispositifs actuels s'avèrent insuffisants face aux défis spécifiques posés par les plateformes en ligne. L'absence de réglementations précises encadrant l'utilisation des réseaux sociaux par les mineurs obère la capacité à garantir une protection efficace et durable dans l'espace numérique.

De plus, et malgré l'engagement de nombreux acteurs nationaux et internationaux, les initiatives en faveur de la protection des enfants en ligne restent fragmentées et souffrent d'un manque patent de coordination et de convergence des parties prenantes concernées autour d'une vision stratégique nationale partagée.

Aux facteurs précités s'ajoutent, selon les acteurs auditionnés et les enquêtes réalisées, une prise de conscience insuffisante des parents concernant les risques associés aux réseaux sociaux, ainsi qu'une connaissance limitée des outils de contrôle parental, exacerbant de ce fait la vulnérabilité des enfants face aux effets délétères potentiels des réseaux sociaux.

Sur la base de ce diagnostic partagé, le CESE appelle à la mise en place d'un environnement numérique inclusif et sécurisé pour les enfants. Pour y parvenir, il est essentiel que tous les acteurs impliqués dans la protection de l'enfance intensifient leur collaboration, coordonnent

leurs actions et mutualisent leurs efforts afin de relever les différents défis associés à la protection des enfants contre les dangers des réseaux sociaux. A cette fin, il est nécessaire de renforcer la politique intégrée de protection de l'enfance (PIPE) en intégrant explicitement, parmi ses objectifs stratégiques, la sécurité numérique des enfants, notamment la protection contre les risques liés aux réseaux sociaux. Dans ce sens, un ensemble de recommandations ont été émises par le CESE, parmi lesquelles :

- Adapter le cadre légal aux développements du numérique en harmonisant les lois nationales avec les normes internationales pour protéger les enfants des dangers des réseaux sociaux. Cela inclut la caractérisation des crimes en ligne, la clarification des responsabilités des entreprises technologiques et des opérateurs de télécommunications, ainsi que l'établissement de règles spécifiques pour encadrer l'utilisation, par les enfants, des réseaux sociaux.
- Fixer un âge minimum pour l'accès aux réseaux sociaux, accompagné de mesures contraignantes pour les plateformes, telles que l'obligation de refuser l'inscription des mineurs sans consentement parental.
- Intensifier la collaboration entre les autorités gouvernementales et les plateformes numériques afin d'assurer une meilleure sécurisation de l'espace numérique, notamment en définissant des protocoles clairs et rapides pour signaler et traiter les contenus inappropriés ou dangereux (cyberharcèlement, contenus violents, *etc.*).
- Déployer les outils de l'intelligence artificielle pour détecter proactivement les contenus inappropriés, analyser les comportements à risque, adapter les contrôles parentaux de manière personnalisée et automatiser la modération des contenus dangereux, afin d'assurer une réponse rapide et efficace face aux menaces présentes sur les réseaux sociaux.
- Intégrer, dès le plus jeune âge, l'éducation numérique dans les programmes scolaires, en mettant l'accent sur le développement de l'esprit critique et la vérification des informations. Parallèlement, sensibiliser les producteurs d'information à leurs responsabilités dans la lutte contre les fausses informations, et mener des campagnes de sensibilisation ciblées à l'attention des parents et des utilisateurs sur les risques liés aux réseaux sociaux, tout en promouvant l'adoption de contrôles parentaux.
- Elaborer un rapport annuel sur la situation de la protection des enfants en ligne, à soumettre aux commissions compétentes du Parlement pour évaluation et suivi.

Introduction

L'univers numérique offre de nombreuses opportunités pour le développement des enfants, en stimulant leur créativité, en favorisant leur libre expression, en enrichissant leur acquisition de connaissances et en leur offrant la possibilité de s'engager dans des échanges et activités ludiques variées. Les réseaux sociaux, largement adoptés à travers le monde, constituent une composante essentielle de cet univers. En 2023, des plateformes telles que *Facebook, WhatsApp* et *Instagram* regroupent des milliards d'utilisateurs, avec une présence marquée au Maroc où 21 millions de personnes, soit plus de 56%[4] de la population, utilisent ces réseaux sociaux. Une enquête de L'Agence Nationale de Réglementation des Télécommunications (ANRT) de 2023 montre que cette utilisation est très répandue parmi les internautes marocains, y compris chez les enfants de 5 à 18 ans[5].

Il existe plusieurs définitions des réseaux sociaux, mais celle énoncée par la loi française du 7 Juillet 2023[6] recouvre tous les aspects de ces médias sociaux. Il est entendu par réseau social « *toute plateforme permettant aux utilisateurs finaux de se connecter et de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils, en particulier au moyen de conversations en ligne, de publications, de vidéos et de recommandations* » (article 1er). Il est à souligner que cette définition était déjà inscrite dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Les réseaux sociaux incluent ainsi les applications et jeux en ligne qui permettent l'interaction directe entre utilisateurs, via un Chat. L'utilisation de ces plateformes par les enfants pose un risque particulier en raison de ces interactions possibles, pouvant les exposer à des actes criminels tels que la prédation, le harcèlement et la manipulation. L'étude « *Enfants et jeunes marocains en ligne* » du CMRPI (2021) a en effet révélé que 29% des enfants et des jeunes utilisent *Internet* pour communiquer avec d'autres personnes et 49% l'utilisent pour se connecter aux réseaux sociaux. Si 49% utilisent souvent *Internet* pour parler à des membres de leurs familles, 51% utilisent la messagerie instantanée (WhatsApp et Viber) et 21% pour accéder à des groupes de rencontre et discussion.

Cependant, malgré les avantages indéniables que les réseaux sociaux peuvent offrir, ils exposent également les enfants à des risques significatifs. Ces risques incluent la propagation de *fake news*, la manipulation de l'opinion publique, le chantage, l'extorsion, le cyberharcèlement, ainsi que l'incitation à la haine, à la violence et même au suicide. Des menaces telles que le recrutement par des réseaux terroristes, l'exploitation sexuelle et le développement de comportements addictifs sont également présentes, avec des répercussions profondes sur le bien-être physique et psychique des jeunes, ainsi que sur leurs relations sociales, leurs valeurs, leurs droits et engagement civique.

4 - Source : We are social/Meltwater

5 - ANRT, Enquête de collecte des indicateurs TIC auprès des ménages et des individus, 2023.

6 - la loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne.

Une enquête assez récente[7] portant sur 1.293 enfants et jeunes marocains âgés de 8 à 28 ans révèle que 80% d'entre eux utilisent régulièrement *Internet* et que 70% fréquentent les réseaux sociaux. Parmi eux, 43% souffrent de troubles du sommeil, 35,6% rapportent des conflits avec la famille ou des amis, et 41,5% observent une baisse dans leurs performances scolaires. De manière encore plus alarmante, un tiers de ces jeunes sont confrontés au cyberharcèlement, 40% partagent des données personnelles avec des inconnus et 40% ne maîtrisent pas les paramètres de confidentialité de leurs profils en ligne.

Un rapport de 2023[8] sur la violence en milieu scolaire au Maroc vient corroborer ces résultats, en mettant en lumière une augmentation de la cyberviolence. Ce rapport confirme que la forme d'intimidation psychologique ou sexuelle en ligne s'intensifie et atteint des proportions alarmantes dans certains milieux. Il note que près de 10% des élèves de primaire ont reçu « des messages désagréables, méchants ou insultants sur *Internet* », et un nombre significatif d'entre eux ont été victimes de publications non désirées ou d'exclusion de groupes en ligne.

Le CESE s'est ainsi attaché à traiter le sujet de la protection dans l'environnement numérique, en se focalisant particulièrement sur le cas des enfants. L'objectif principal est de dresser un état des lieux des risques ainsi que des mesures mises en place par les divers acteurs pour les prévenir et les maîtriser en proposant des recommandations en vue de renforcer la sécurité des enfants dans l'espace numérique.

7 - « Enfants et jeunes marocains en ligne - Comportements et risques du numérique » - Centre marocain de recherches polytechniques et d'innovation - 2021

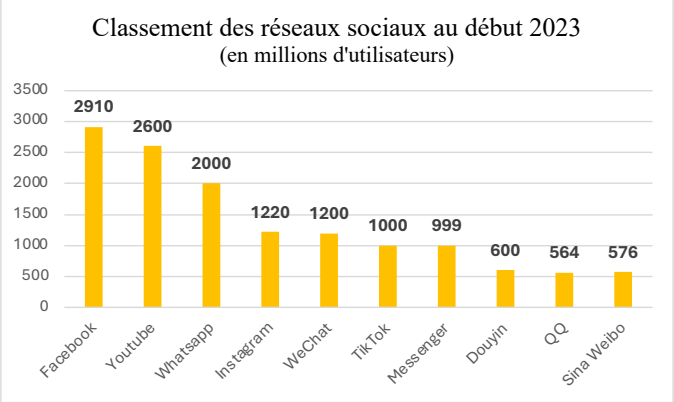
8 - Rapport thématique « La violence en milieu scolaire » - Conseil supérieur de l'éducation de la formation et de la recherche scientifique, Instance nationale d'évaluation du système d'éducation, de formation et de recherche scientifique en partenariat avec l'UNICEF (2023)

I. L'engouement pour les réseaux sociaux est un phénomène global et porteur d'opportunités et de risques pour les enfants

Au début de l'année 2023[9], le nombre d'utilisateurs de téléphones mobiles dans le monde a atteint 5,44 milliards, soit 68 % de la population mondiale totale, enregistrant une augmentation de 3% par rapport à 2022. Une écrasante majorité de cette population utilise aussi *Internet*, soit 5,16 milliards de personnes, ce qui signifie que 64,4 % de la population mondiale totale est « connectée ». Chez les hommes, la proportion des utilisateurs d'*Internet* atteint 67,2%, tandis que chez les femmes le pourcentage est de 61,6%.

Les réseaux sociaux rassemblent aujourd'hui 4,76 milliards d'utilisateurs, soit 92% des internautes, ce qui représente presque 60 % de la population mondiale, en croissance de 3 % par rapport à 2022. Il est toutefois important de noter que l'adoption du numérique présente des disparités significatives entre les pays.

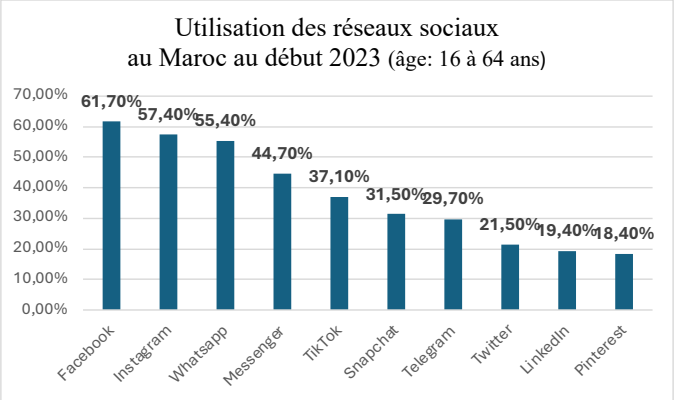
Graphique 1 : classement des réseaux sociaux au début 2023 (en millions d'utilisateurs)



Source : Statista 2023

Au Maroc, selon l'ANRT[10], le taux d'utilisation des réseaux sociaux parmi les internautes frôle les 100%.

Graphique 2 : utilisation des réseaux sociaux au Maroc au début 2023 (âge : 16 à 64 ans)



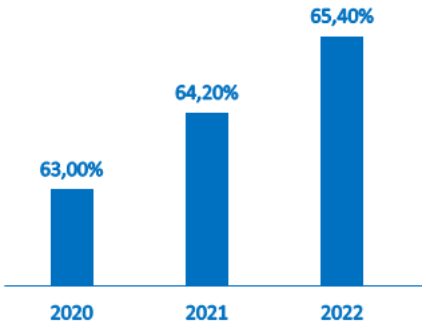
Source : We are Social, Meltwater

9 - Source : Digital 2023 Global Overview - We Are Social et Meltwater

10 - ANRT, Enquête de collecte des indicateurs TIC auprès des ménages et des individus, 2023.

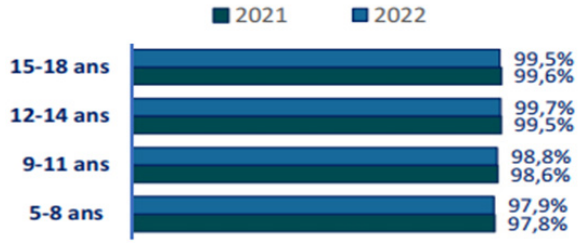
L'activité numérique est bien plus ancrée chez les enfants et les jeunes. À l'exception des enfants en bas âge, dont le stade de développement ne leur permet pas encore d'utiliser des dispositifs numériques, la grande majorité des enfants montre un vif intérêt pour la manipulation de smartphones, tablettes et autre matériel digital, et parmi ceux qui sont en âge d'utiliser *Internet*, presque tous utilisent fréquemment les réseaux sociaux (voir graphes 3 et 4).

Graphique 3 : utilisation d'*Internet* par les enfants au Maroc



Source : ANRT

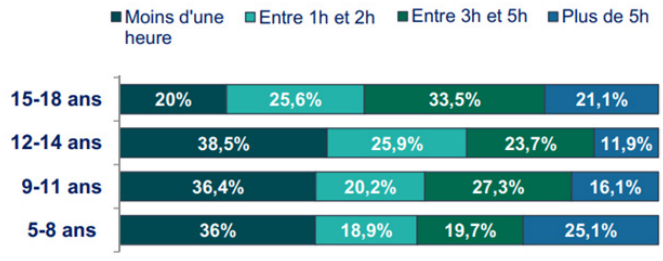
Graphique 4 : Utilisation des réseaux sociaux chez les enfants internautes



Source : ANRT

Selon des données de l'ANRT, plus d'une personne sur cinq appartenant à la génération «Z» (nées entre 1997 et 2010) passe plus de 5 heures par jour sur *Internet*. Le graphique 6 fournit des données détaillées sur le temps que les enfants marocains passent en ligne.

Graphique 5 : Volume horaire d'utilisation d'*Internet* chez les enfants au cours des trois derniers mois de 2022



Source : ANRT

En dépit des niveaux d'utilisation élevés d'*Internet* et des réseaux sociaux par les enfants, la fracture numérique persiste encore en raison de plusieurs facteurs :

- des contraintes financières ou techniques limitant l'accès au réseau *Internet* et aux dispositifs tels que les smartphones, les tablettes et les ordinateurs ;
- l'insuffisance ou l'absence de formation au numérique chez les enfants et/ou leurs parents ou tuteurs. Il est à préciser que l'éducation numérique englobe la maîtrise des outils informatiques, l'éducation aux médias, à l'information et les compétences en informatique[11].

Sur le premier aspect, et malgré les retards enregistrés dans la transformation digitale soulignés par le CESE[12], le Maroc progresse avec détermination. Des efforts considérables sont constamment réalisés pour améliorer la couverture territoriale du réseau *Internet* et rendre les technologies numériques plus accessibles à tous. Selon une enquête de l'ANRT, en l'espace de 5 ans (2018-2022), le taux d'équipement en téléphonie mobile a notablement augmenté, passant de 92,4% à 96,5%. L'équipement en téléphonie mobile chez les enfants varie, selon l'âge, entre 80% et 94%, tandis que chez les adolescents ce taux frôle les 99%. En milieu rural, ces chiffres sont légèrement inférieurs, accusant un écart de 4 points par rapport aux zones urbaines.

Le second aspect, relatif à l'éducation numérique, présente des défis plus complexes, nécessitant une action de grande ampleur à long terme. En raison notamment du déficit en nombre et en compétences des ressources humaines, et de contraintes liées au *curricula* scolaire. L'inclusion numérique de nombreux enfants demeure ainsi un défi majeur à surmonter.

Consultation citoyenne sur la plateforme du CESE « ouchariko.ma »

Les participants au sondage lancé sur la plateforme de participation citoyenne du CESE ouchariko.ma ont souligné l'importance d'inclure l'éducation numérique dans les programmes scolaires. Ils ont été plus de 88% à soutenir cette mesure.

1.1. De grandes opportunités d'apprentissage, de socialisation et d'émancipation

Le numérique offre incontestablement aux enfants de précieuses opportunités de développer un large éventail de compétences indispensables pour leur avenir :

- L'apprentissage en ligne : la pandémie de la covid-19 a provoqué un bouleversement des méthodes d'apprentissage des enfants. Le système éducatif s'est vu obligé d'instaurer l'enseignement à distance pour permettre aux enfants de poursuivre leur scolarité. Désormais, l'apprentissage en ligne est une pratique courante dans l'ensemble de l'écosystème éducatif, y compris à l'université et dans la formation continue. Toujours en rapport avec l'école, le numérique facilite la recherche de l'information, ainsi que le renforcement des connaissances sur un large éventail de sujets. Les enfants apprennent ainsi à découvrir l'environnement qui les entoure et à bâtir progressivement leur propre vision du monde.

11 - Persch Magali et Soulairol Mélody, Métiers de l'enseignement, de l'éducation et de la formation, Mémoire de 2ème année, MASTER MEEF mention 1er degré, Faculté de l'Education, Université de Montpellier 2018 – 2019.

12 - « Vers une transformation digitale responsable et inclusive » - Avis du CESE – 2021

- En matière de socialisation : les réseaux sociaux font désormais partie de la vie quotidienne, et les enfants sont amenés de fait à en faire un moyen pour construire et entretenir des relations sociales. Sous réserve d'un accompagnement par des adultes avertis, les réseaux sociaux peuvent contribuer à une socialisation harmonieuse des enfants et à leur développement psychologique, d'où l'intérêt de leur apprendre à communiquer et interagir en ligne.
- Une préparation indispensable pour l'avenir : la mutation numérique transforme divers aspects de la vie quotidienne. Désormais, pour bénéficier des services publics et d'une multitude de services utiles, le citoyen doit disposer d'un minimum de compétences dans le domaine du digital. Il en est de même pour divers aspects pratiques de la vie de tous les jours ; essentiels pour réussir une intégration socio-économique dans un environnement dominé par le numérique (opportunités de formation, d'emploi, de réalisation de projets, *etc.*). Une bonne maîtrise des outils numériques par les enfants contribue substantiellement à une bonne préparation pour l'avenir.

L'enquête du centre marocain de recherches polytechniques et d'innovation (CMRPI)[13] révèle que 37% utilisent *Internet* souvent pour faire leurs devoirs et 28% le font au moins une fois par semaine ; 19% l'utilisent au moins une fois par mois pour la recherche des ressources et événements de leur quartier. 32% de l'échantillon l'utilisent souvent pour la recherche de nouvelles et informations, 21% l'utilisent souvent pour la recherche d'informations sur leur santé et 56% l'utilisent pour la recherche et l'utilisation d'applications qui leur sont utiles[14].

La même enquête fait état d'autres utilisations assez fréquentes chez les enfants et les jeunes, telles la création de vidéos ou de blogs, la musique, le visionnage d'émissions ou de films, les achats ou les ventes en ligne, *etc.*

1.2. Des risques significatifs affectant la santé, la sécurité et l'éducation des enfants

Les risques d'impact délétère sur le développement cognitif et sensoriel des enfants et sur leur santé mentale liés à l'utilisation des écrans

L'utilisation excessive et inappropriée du numérique chez les jeunes est désormais reconnue comme une menace sérieuse pour leur santé mentale et physique. Des recherches dans ce domaine ont révélé une série de troubles psychologiques et comportementaux alarmants, notamment le développement de comportements addictifs[15], de comportements violents, de troubles anxieux, le repli sur soi et l'isolement social, des automutilations, des troubles du sommeil, des troubles de la concentration, de la dépression, ainsi que des tentatives de suicide et des suicides.

L'enquête réalisée par le CMRPI adresse plusieurs répercussions significatives de l'utilisation du numérique sur :

13 - Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI), Ausim, Conseil de l'Europe, Université Ibn Tofail et Association Ibny – « Enfants et jeunes marocains en ligne : Comportements et risques du numérique », 2021 - https://ausimaroc.com/wp-content/uploads/2021/12/RAPPORT-DETUDE-ANALYTIQUE-CMRPI-2021-21-2-1.pdf

14 - Source : ENFANTS ET JEUNES MAROCAINS EN LIGNE COMPORTEMENTS ET RISQUES DU NUMERIQUE - RAPPORT D'ÉTUDE ANALYTIQUE - CMRPI 2021

15 - Rapport CESE « Faire face aux conduites addictives : état des lieux et recommandations »

- **La santé :** près de 43 % des jeunes interrogés négligent leurs besoins fondamentaux tels que l'alimentation et le sommeil en raison de leur usage excessif du numérique.
- **La vie sociale :** environ 36 % des participants ont rapporté des conflits avec leur famille ou leurs amis, illustrant l'impact perturbateur de l'usage intensif des technologies sur les relations personnelles.
- **L'éducation et l'apprentissage :** 42 % des jeunes ont subi une baisse de leurs performances scolaires, soulignant les effets délétères d'une consommation excessive d'écrans sur les résultats scolaires.

Les répercussions sociales de ces troubles peuvent être profondes, plongeant les jeunes dans une spirale de conséquences désastreuses telles que le décrochage et l'abandon scolaire, diverses addictions, les fugues, le développement de troubles mentaux, l'exclusion sociale, les cas de vie marginale dans la rue, ou encore le statut de « NEET » (ni en emploi, ni en éducation, ni en formation).

Encadré 1 : impact des Réseaux Sociaux sur la santé mentale des jeunes américains

Des recherches substantielles aux États-Unis[16], réalisées sur de grandes cohortes, ont identifié une corrélation significative entre le temps passé par les enfants sur les réseaux sociaux et l'atteinte à leur santé mentale. Une étude majeure a ainsi examiné la relation entre l'intériorisation des problèmes et le temps d'engagement sur les réseaux sociaux. Portant sur 6 595 enfants de 12 à 15 ans, elle a révélé que ceux passant plus de trois heures par jour sur les réseaux sociaux sont susceptibles de présenter un risque doublé de rencontrer des problèmes de santé mentale, y compris des symptômes d'anxiété et de dépression, et surtout des problèmes liés à l'intériorisation de leurs difficultés. Des études futures devraient explorer dans quelle mesure la mise en place de limites d'utilisation quotidienne, l'amélioration de l'éducation aux médias, et la refonte des plateformes sociales pourraient réduire efficacement ces problèmes de santé mentale chez les jeunes.

Par ailleurs, une enquête nationale américaine plus récente[17] réalisée auprès de 1 480 enfants de 13 à 17 ans a révélé que, bien que ces jeunes voient de nombreux avantages à l'utilisation des réseaux sociaux et soient ouverts aux restrictions, 46 % d'entre eux estiment que les réseaux sociaux détériorent leur image corporelle. Ainsi, pour près de la moitié de ces adolescents, l'interaction avec les réseaux sociaux contribue négativement à leur perception de leur propre image, engendrant des répercussions psychologiques notables.

Les risques d'impact sur l'intégrité psychique et la santé mentale des enfants liés spécifiquement au « mésusage » des réseaux sociaux

Le rapport annuel de la représentante spéciale du secrétaire général des Nations Unies[18] pour la violence contre les enfants dédie un chapitre entier à la violence envers les enfants dans l'environnement numérique. Plusieurs études menées par divers organismes (UNICEF, IWF, ITU, ANRT, *etc.*) ont clairement identifié les risques associés à l'utilisation des réseaux sociaux par les enfants. Ces risques peuvent être résumés comme suit :

16 - U.S Surgeon General Advisory, About effects social media use has on youth mental health, 2023.

17 - Social Media and Youth Mental Health - The U.S. Surgeon General's Advisory - 2023

18 - Assemblée générale des Nations unies - Février 2023 A/HRC/52/61

1. L'exposition à des contenus inappropriés :

- contenus extrémistes, violents, sanglants, racistes… ;
- jeux d'argent en ligne ;
- contenus à caractère sexuel et pornographique ;
- fausses informations ;
- contenus filtrés par des algorithmes à des fins de manipulation.

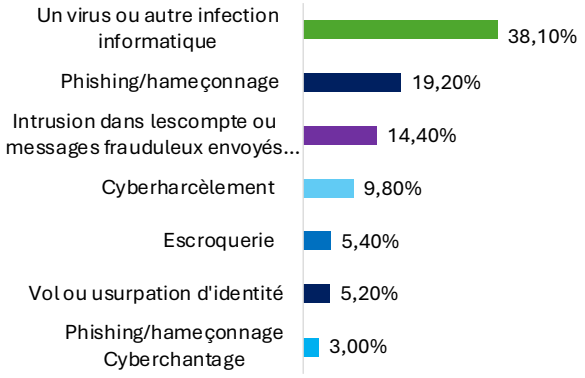
En 2019, la Fondation *Internet* Watch (IWF) a recensé plus de 132 000 pages web dont il a été confirmé qu'elles comportaient des images et des vidéos montrant des abus sexuels sur des enfants. Chaque page web pouvait contenir jusqu'à des milliers d'images de ce type d'abus.

2. La cyberviolence et le cyberharcèlement

La cyberviolence est une forme d'intimidation psychologique ou sexuelle qui se produit en ligne. Cela comprend l'affichage ou l'envoi de courriels, comprenant des textes, photos ou vidéos, dans le but de harceler, menacer ou cibler une personne au moyen de médias sociaux. La cyberviolence comprend également la diffusion de rumeurs, de fausses informations, de messages malveillants, de photos ou de commentaires embarrassants, ou l'exclusion d'une personne sur les médias sociaux ou d'autres moyens de communication[19].

Le cyberharcèlement, quant à lui, désigne un comportement répétitif visant à provoquer peur, irritation ou honte chez les individus ciblés[20]. Parmi les méthodes employées figure notamment la diffusion non consentie de photos intimes dans le but d'humilier, de faire chanter ou d'intimider. Ce type de harcèlement peut être perpétré par des adultes ou des pairs et touche plus fréquemment les enfants vulnérables. A date du 20 octobre 2023, le portail « Espace Maroc Cyberconfiance » avait comptabilisé 1745 signalements. Parmi ceux-ci, 1647 concernaient des contenus publiés sur les réseaux sociaux, tandis que 98 signalements étaient relatifs à des photos et vidéos d'abus sexuels impliquant des enfants en ligne[21].

Graphique 6: victimes de risques ou menaces liées à l'utilisation d'Internet



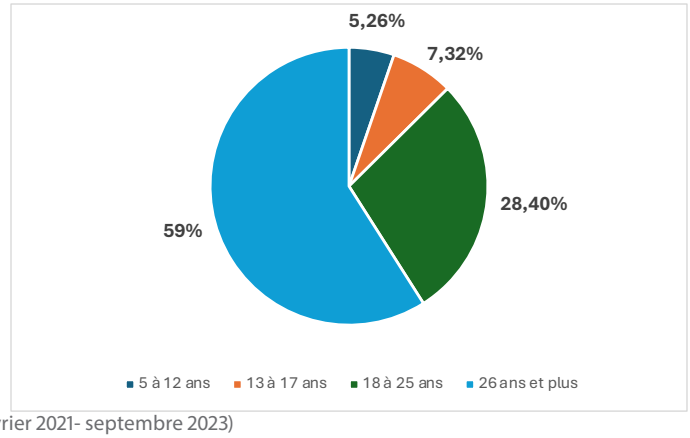
Source : ANRT – Enquête de collecte des indicateurs TIC auprès des ménages et des individus

19 - Conseil supérieur de l'éducation, de la formation et de la recherche scientifique : la violence en milieu scolaire. Rapport thématique - 2023

20 - Audition de l'UNICEF le 27 septembre 2023

21 - Source : CMRPI

Selon les données de la plateforme EMC, les jeunes adultes de 18 à 25 ans sont les plus touchés par la cyberviolence et le cyberharcèlement, représentant 59% des signalements. Les adultes de 26 ans et plus suivent avec 28,40%, tandis que les adolescents de 13 à 17 ans et les enfants de 5 à 12 ans sont également affectés, bien que dans une moindre mesure.



Source : Plateforme EMC (février 2021- septembre 2023)

3. L'abus et l'exploitation

L'abus désigne l'implication d'un enfant (toute personne âgée de moins de 18 ans) dans une activité sexuelle, commerciale ou financière, qu'il ne comprend pas totalement, à laquelle il ne peut consentir de façon éclairée, ou pour laquelle il n'est pas prêt sur le plan du développement et ne peut pas donner son consentement.

Quant à l'exploitation, elle désigne les abus réels ou les tentatives d'abus résultant d'une position de vulnérabilité, d'un déséquilibre des pouvoirs ou de confiance dans le but d'en tirer des bénéfices monétaires, sociaux, politiques ou sexuels. L'abus et l'exploitation relèvent de la manipulation psychologique des enfants.

4. L'incitation à l'automutilation et au suicide

Les médias internationaux relatent fréquemment des incidents tragiques d'automutilation ou de suicide commis par des enfants ou adolescents dépendants aux réseaux sociaux. Dans certains cas, les tribunaux reconnaissent la responsabilité des plateformes numériques dans ces drames. Par ailleurs, des recherches montrent que les réseaux sociaux peuvent exposer les jeunes à de nombreux contenus liés à la dépression. Cette exposition constante peut significativement augmenter le risque de comportements autodestructeurs, tels que l'automutilation ou le suicide, chez les enfants et adolescents.

5. L'incitation à la haine, au racisme, à la discrimination et à la radicalisation

Les réseaux sociaux peuvent favoriser la désinhibition en raison de l'absence de confrontation directe, ce qui peut entraîner une diffusion accrue de contenus haineux, extrémistes et autres messages inappropriés. Dans ce contexte, l'enfant se trouve doublement vulnérable : il peut être victime de ces contenus, mais il peut aussi, potentiellement, en devenir l'auteur, portant ainsi préjudice à ses pairs.

6. L'utilisation des données personnelles à des fins criminelles : la fraude, l'escroquerie, le vol le piratage, l'usurpation d'identité

L'essor des réseaux sociaux expose les utilisateurs à divers risques liés à l'exploitation criminelle des données personnelles. La fraude, l'escroquerie, le vol, le piratage et l'usurpation d'identité sont des menaces potentielles. Le piratage de comptes peut entraîner le vol d'informations personnelles, tandis que l'usurpation d'identité peut causer des préjudices significatifs, tant sur le plan financier que psychologique. Il est, de ce fait, essentiel de sensibiliser les enfants dès leur plus jeune âge à la sécurité en ligne et à la protection de leurs données personnelles. En plus de les inciter à la prudence quant aux informations qu'ils partagent, il est crucial de leur enseigner les bonnes pratiques pour sécuriser leurs comptes sur les réseaux sociaux.

L'étude « *Enfants et jeunes marocains en ligne* » du CMRPI[22] révèle que 40 % des enfants et des jeunes ne savent pas modifier les paramètres de confidentialité, 58 % se retrouvent sur des sites Web sans savoir comment ils y sont arrivés, 30 % ne savent pas différencier entre ce qui peut être partagé et ce qui ne peut l'être. Ils sont 31% à être exposés au cyberharcèlement, 40% à accepter des gens comme amis sans les connaître, et seulement 25% à informer leurs parents en cas d'un évènement bouleversant en ligne.

1.3. Les difficultés relatives au contrôle parental sur l'utilisation des réseaux sociaux par les enfants

Selon l'enquête de l'ANRT, la majorité des parents ne sont pas opposés à ce que leurs enfants utilisent *Internet*, espérant qu'ils bénéficient des avantages offerts par la technologie. Près de 60% des parents ont une perception plutôt positive de l'usage d'*Internet* par leurs enfants. Toutefois, des préoccupations subsistent : 79% des parents expriment une inquiétude quant au temps que leurs enfants passent en ligne et à l'impact potentiel sur leur santé physique et mentale.

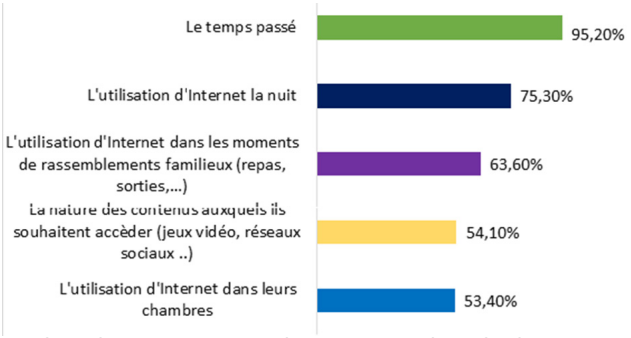
Selon l'enquête de collecte des indicateurs TIC auprès des ménages et des individus réalisée par l'ANRT, les parents/tuteurs expriment cinq principales préoccupations quant à l'utilisation d'*Internet* par leurs enfants :

- 79 % sont préoccupés par la proportion du temps passé en ligne par rapport à d'autres activités ;
- 78 % s'inquiètent de l'impact sur la santé, notamment le sommeil et la concentration ;
- 45 % craignent l'accès à des contenus inappropriés ;
- 44 % sont préoccupés par le manque de connaissance sur les activités en ligne de leurs enfants ;
- 42 % sont préoccupés de ne pas savoir avec qui leurs enfants interagissent en ligne.

Par ailleurs, le temps passé sur *Internet* est la principale source de tension entre les parents et leurs enfants. De plus, les parents expriment leur mécontentement face à d'autres comportements qu'ils jugent inappropriés (graphique 7).

22 - Ibid

Graphique 7 : comportements associés à l'utilisation d'Internet par les enfants



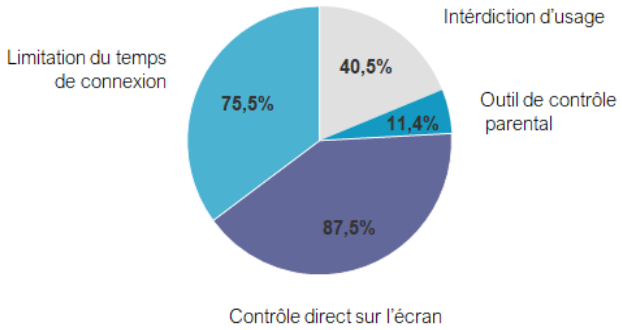
Source : ANRT – Enquête de collecte des indicateurs TIC auprès des ménages et des individus

Consultation citoyenne sur la plateforme du CESE « ouchariko.ma »

La consultation citoyenne révèle une large conscience des parents quant aux risques liés à l'utilisation des réseaux sociaux par les enfants. Ils sont près de 60% à déclarer avoir vécu, dans leur entourage, des cas où l'intégrité psychique ou physique d'un enfant a été compromise par les réseaux sociaux. Ce sont les messages et les contenus auxquels les enfants sont exposés qui sont mis en cause, notamment les contenus à caractère sexuel ou pornographique (67 %) et ceux incitant à la haine et à la violence (55 %), ainsi que des cas de cyberharcèlement (46%), tandis qu'un tiers mentionnent des expériences de piratage de comptes. Plus des 3/4 des incidents rapportés ont eu un impact négatif sur le comportement de l'enfant (78 %).

Face aux dangers que représentent les réseaux sociaux pour les enfants, les parents adoptent des attitudes diverses, allant du contrôle direct de l'écran, pratiqué par presque 90% d'entre eux, à l'usage sporadique d'outils de contrôle parental. L'utilisation de ces dispositifs de surveillance numérique reste marginale[23]. Le coût annuel de 100 dirhams, ou 10 dirhams par mois, ne semble pas être un frein majeur à leur adoption. D'après les témoignages recueillis auprès de certains acteurs auditionnés, il semble que les parents n'ont ni pleine conscience des risques liés à l'utilisation d'*Internet* par leurs enfants, ni une compréhension complète des bénéfices que peuvent apporter les outils de contrôle parental.

Graphique 8 : techniques de contrôle parental



Source : ANRT – Enquête de collecte des indicateurs TIC auprès des ménages et des individus

23 - L'opérateur Ittissalat Al Maghrib annonce que moins de 1% de ses abonnés *Internet* ont souscrit à un service de contrôle parental - audition du 15 novembre

Consultation citoyenne sur la plateforme du CESE « ouchariko.ma »

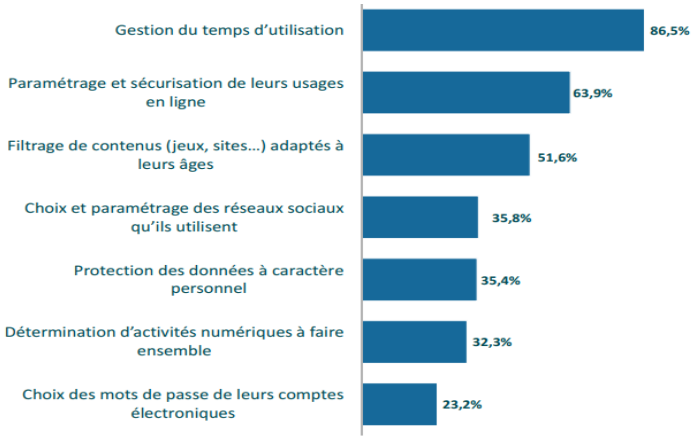
Les résultats de la consultation citoyenne a révélé que le contrôle parental reste modéré dans 47% des cas, et qu'il se concrétise principalement par la limitation du temps de connexion (64%) ou la surveillance directe de l'écran de l'enfant (42%).

Les tuteurs sont généralement conscients de l'importance d'améliorer leurs compétences numériques afin de mieux accompagner et encadrer leurs enfants dans leur utilisation d'*Internet* et des réseaux sociaux. Ils manifestent clairement un besoin d'assistance dans ce domaine.

Le graphique 9 basé sur l'enquête de l'ANRT révèle clairement que les parents ont des besoins diversifiés et différenciés en termes d'assistance pour encadrer l'utilisation numérique de leurs enfants. Une attention particulière est accordée à la gestion du temps d'écran, révélant une préoccupation majeure quant au temps consacré par les enfants aux activités en ligne. Le besoin important d'aide pour sécuriser et configurer les paramètres d'utilisation en ligne a été également mis en avant.

De plus, un nombre considérable de parents sont en recherche de conseil pour le filtrage de contenus, soulignant une préoccupation quant à l'exposition à des contenus inappropriés. Les résultats indiquent parallèlement un vif intérêt pour la gestion des réseaux sociaux et la protection des données personnelles, reflétant une prise de conscience des risques liés à la vie privée en ligne.

Graphique 9 : besoins exprimés par les parents pour encadrer l'utilisation des réseaux sociaux par leurs enfants



Source : ANRT – Enquête de collecte des indicateurs TIC auprès des ménages et des individus

II. Protection de l'enfance des risques numériques : des programmes et des initiatives volontaristes nécessitant la convergence et une approche intégrée

Au Maroc, la protection des enfants en ligne repose sur diverses initiatives impliquant un ensemble d'acteurs publics, la société civile et le secteur privé (opérateurs des télécommunications et médias audiovisuels). Ces initiatives, encadrées par un arsenal juridique, s'articulent autour de deux axes principaux : la prévention et la répression de la cybercriminalité.

2.1. Cadre juridique de la protection numérique

L'arsenal juridique et conventionnel encadrant la protection de l'enfance regroupe un ensemble de textes juridiques et de conventions internationales qui traitent des risques liés à *Internet* de manière explicite ou implicite.

Encadré 2 : Arsenal et instruments juridiques de protection de l'enfance

La Constitution de 2011

Les lois nationales :

- Loi n° 70-03 portant Code de la famille
- Code pénal
- Loi n° 22.01 relative à la procédure pénale
- Loi n° 27-14 relative à la lutte contre la traite des êtres humains
- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel
- Loi n°11-15 portant réorganisation de la Haute Autorité de Communication Audiovisuelle
- Loi n°77-03 relative à la communication audiovisuelle
- Loi n° 07-03 sur les atteintes aux systèmes de traitement automatisé des données
- Loi 83-13 complétant la loi 77-03 relative à la communication audiovisuelle
- Loi n°31-13 relative au droit d'accès à l'information
- Loi n° 103.13 relative à la lutte contre la violence à l'égard des femmes

Les conventions internationales :

- La Convention internationale des droits de l'enfant ratifiée par le Maroc en 1993
- La Convention de Budapest sur la cybercriminalité du Conseil de l'Europe et son protocole additionnel
- La Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels[24]
- La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et ses protocoles additionnels[25]

24 - Le Maroc a émis la demande d'adhérer à la convention du Conseil de l'Europe en 2013 et a publié au bulletin officiel la promulgation de la loi portant approbation de la Convention de Lanzarote en 2014. Toutefois, à ce jour, le processus de ratification n'a pas encore abouti.

25 - Le Maroc a adhéré à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 du Conseil de l'Europe) et à son Protocole additionnel le 28 mai 2019.

Les études réalisées, notamment celle du CMRPI, ainsi que les témoignages recueillis lors des auditions, révèlent que le cadre juridique actuel n'est pas suffisamment adapté aux spécificités de l'environnement numérique. L'absence de qualification précise des délits sur *Internet*, engendre, entre autres conséquences, un vide juridique autour de la responsabilité des entreprises technologiques. Il en est de même s'agissant de règles claires régissant l'aspect « utilisation » des réseaux sociaux par les mineurs, ce qui est de nature à rendre d'autant plus faible la protection de cette catégorie de la population dans l'espace numérique.

D'autres aspects législatifs méritent d'être renforcés pour une protection efficace des enfants sur les plateformes numériques, particulièrement en ce qui concerne la justice des mineurs et les droits des victimes à l'accompagnement et à la réparation, en s'inspirant en cela des législations d'autres pays concernant l'âge de la majorité numérique», la lutte contre la haine en ligne et la mise en place de règles strictes pour la gestion des comptes des mineurs.

Encadré 3 : Extrait de la loi française n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (cas de la République Française)

Art. 6-7.-I.-Les fournisseurs de services de réseaux sociaux en ligne exerçant leur activité en France refusent l'inscription à leurs services des mineurs de quinze ans, sauf si l'autorisation de cette inscription est donnée par l'un des titulaires de l'autorité parentale sur le mineur. Ils recueillent également, dans les mêmes conditions et dans les meilleurs délais, l'autorisation expresse de l'un des titulaires de l'autorité parentale relative aux comptes déjà créés et détenus par des mineurs de quinze ans. Lors de l'inscription, ces entreprises délivrent une information à l'utilisateur de moins de quinze ans et aux titulaires de l'autorité parentale sur les risques liés aux usages numériques et les moyens de prévention. Elles délivrent également à l'utilisateur de moins de quinze ans **une information claire et adaptée** sur les conditions d'utilisation de ses données et de ses droits garantis par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« L'un des titulaires de l'autorité parentale peut demander aux fournisseurs de services de réseaux sociaux en ligne la **suspension du compte du mineur** de quinze ans.

« Lors de l'inscription d'un mineur, les fournisseurs de services de réseaux sociaux en ligne activent un dispositif permettant de contrôler le temps d'utilisation de leur service et informent régulièrement l'usager de cette durée par des notifications.

« Afin de **vérifier l'âge des utilisateurs finaux** et l'autorisation de l'un des titulaires de l'autorité parentale, les fournisseurs de services de réseaux sociaux en ligne utilisent des solutions techniques conformes à un référentiel élaboré par l'Autorité de régulation de la communication audiovisuelle et numérique, après consultation de la Commission nationale de l'informatique et des libertés.

« II.-Lorsqu'il constate qu'un fournisseur de services de réseaux sociaux en ligne n'a pas mis en œuvre de solution technique certifiée pour vérifier l'âge des utilisateurs finaux et l'autorisation de l'un des titulaires de l'autorité parentale de l'inscription des mineurs de quinze ans, le président de l'Autorité de régulation de la communication audiovisuelle et numérique adresse à ce fournisseur, par tout moyen propre à en établir la date de réception, une mise

en demeure de prendre toutes les mesures requises pour satisfaire aux obligations prévues au I. Le fournisseur dispose d'un délai de quinze jours à compter de la mise en demeure pour présenter ses observations.

« A l'expiration de ce délai, en cas d'inexécution de la mise en demeure, le président de l'Autorité de régulation de la communication audiovisuelle et numérique peut saisir le président du tribunal judiciaire de Paris aux fins d'ordonner au fournisseur de mettre en œuvre une solution technique conforme.

« Le fait pour un fournisseur de services de réseaux sociaux en ligne de ne pas satisfaire aux obligations prévues au même I est puni d'une amende ne pouvant excéder 1 % de son chiffre d'affaires mondial pour l'exercice précédent.

« III.-Les obligations prévues au I ne s'appliquent ni aux encyclopédies en ligne à but non lucratif ni aux répertoires éducatifs ou scientifiques à but non lucratif.

« IV.-Les modalités d'application du présent article sont fixées par un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés. »

2.2. Répression de la cybercriminalité[26]

La Direction générale de la sûreté nationale (DGSN) joue un rôle-clé dans la prévention et la répression de la cybercriminalité, notamment les infractions ciblant les enfants. Elle est structurée pour répondre efficacement à ces défis grâce à ses compétences techniques et humaines spécialisées.

Elle organise ainsi ses opérations via plusieurs unités :

- un service central de lutte contre la criminalité liée aux nouvelles technologies à la Direction centrale de la police judiciaire, équipé d'un laboratoire d'analyse des supports numériques ;

- un office national spécialisé au niveau de la brigade nationale de la police judiciaire (BNPJ) ;

- cinq laboratoires d'analyse situés à Casablanca, Fès, Marrakech, Laayoune et Tétouan, ainsi que 32 brigades dédiées à la cybercriminalité réparties sur le territoire nationale.

Des brigades des mineurs sont également opérationnelles dans les services de la police judiciaire, spécialisées dans le traitement des affaires impliquant des enfants et équipées de locaux adaptés à l'accueil de jeunes victimes.

En outre, la DGSN maintient une veille continue sur *Internet* et collabore avec des partenaires internationaux, y compris *Interpol* et des réseaux sociaux, pour faciliter l'accès aux données nécessaires aux enquêtes judiciaires.

26 - La cybercriminalité est un terme général qui décrit nombre d'activités criminelles menées à l'aide d'un ordinateur, d'un réseau informatique ou d'un dispositif numérique. Les cybercriminels mènent des activités illégales diverses qui se jouent des frontières géographiques. Il s'agit de crimes tels que le piratage de compte, l'usurpation d'identité, la sextorsion, l'escroquerie, la diffamation, le chantage, *etc.*

2.3. Plusieurs programmes et initiatives portant sur la prévention, la formation et la sensibilisation

En 2020, le comité de coordination nationale[27] pour la « culture digitale/protection des enfants en ligne » a été constitué et activé. Le portail e-himaya.ma a ainsi été lancé afin de promouvoir l'usage approprié du numérique parmi les enfants. Ce portail est complété par la diffusion d'un ensemble de guides thématiques pour divers groupes cibles (enfants, parents/tuteurs, jeunes/étudiants, enseignants) et l'organisation de séminaires et ateliers de formation[28].

Le département ministériel chargé de l'éducation nationale a mis en place un ensemble d'initiatives pour l'intégration des technologies de l'information et de la communication dans le système éducatif, en particulier avec le Programme *GENIE* lancé depuis 2006. Ce programme a contribué à la formation de 300 000 cadres de l'éducation nationale et au développement de ressources numériques pédagogiques. Dans le cadre de sa feuille de route 2022-2026, l'utilisation pédagogique des outils numériques a été renforcée. En outre, à l'occasion du « *Safer Internet Day* », célébrée au mois de février de chaque année, le département organise des campagnes de sensibilisation au cyberharcèlement et au harcèlement en milieu scolaire.

En janvier 2022, un programme pilote[29] a été lancé pour améliorer le climat scolaire et prévenir les situations d'intimidation et de harcèlement dans plusieurs établissements scolaires. Ce programme comprend des ateliers de formation spécifiques pour les enseignants, visant à les outiller pour mieux gérer et prévenir ces situations. Parallèlement, une unité sur la cybersécurité a été introduite dans le programme d'éducation civique pour les élèves de 5ème année, soulignant l'importance de la sécurité en ligne. Enfin, un programme de formation de formateurs a démarré, fin 2023, avec un budget de près de 2 millions de dirhams au titre de l'année scolaire 2023-2024, en vue de renforcer les compétences des éducateurs dans la protection des enfants en ligne.

Il est à signaler que d'autres départements, institutions et instances publiques contribuent également à cette sensibilisation, notamment la HACA[30], l'Agence de Développement du Digital à travers la plateforme «*Academia Raqmya*», le département ministériel en charge de la solidarité, de l'insertion sociale et de la famille qui a édité un guide sur la protection des enfants sur les réseaux sociaux, en collaboration avec l'UNICEF. La CNDP a également mis en place la plateforme «*Koun3labal*»[31], laquelle offre des outils éducatifs de sensibilisation des jeunes et de leurs parents aux dangers liés au partage de données personnelles. Par ailleurs, la DGSN mène régulièrement des campagnes de sensibilisation à la sécurité en ligne dans les écoles[32].

27 - Composition : MJ ; MENPS ; MISF ; MTNRA ; DGSSI ; Bank Al Maghrib ; HACA ; Gendarmerie Royale ; DGSN ; ANRT ; ADD ; ONDE

28 - À fin août 2023, 2940 enfants, 280 enseignants et 320 jeunes avaient été sensibilisés ou formés.

29 - Le projet pilote a démarré en janvier 2022 au niveau de 3 lycées de l'Académie régionale d'éducation et de formation de Rabat-Salé- Kenitra, et dans 61 collèges de la direction provinciale de Tanger relevant de l'Académie de Tanger Tétouan Al Hoceima. A cette occasion des ateliers de formation sont dispensés aux enseignants en collaboration avec des partenaires, tels que l'ADD, le Comité de coordination de l'initiative « Culture digitale/ protection des enfants en ligne », la DGSN et la Gendarmerie Royale.

30 - La Haute Autorité de la Communication Audiovisuelle (HACA) promeut depuis 2016 l'éducation aux médias et à l'information, avec des initiatives telles que le guide « Être connecté en toute sécurité ». Ce guide aide les utilisateurs à développer des réflexes de vérification de l'information, à identifier les contenus inappropriés, à protéger leurs données personnelles et à éviter l'addiction numérique. Il met également en avant l'importance du dialogue entre enfants et parents concernant l'utilisation des réseaux sociaux.

31 - «Koun3labal» est une plateforme qui a pour objectif de sensibiliser les enfants, adolescents, parents et enseignants aux risques de partager leur vie privée en ligne. La plateforme propose des guides, des jeux et des conseils pour protéger les données personnelles.

32 - Concernant en particulier l'utilisation du digital, la DGSN a publié plusieurs brochures d'information qui couvrent divers sujets, dont la protection du courrier électronique et des comptes sur les réseaux sociaux, la protection de l'ordinateur et du téléphone personnels, la sextorsion, la navigation sécurisée sur *Internet, etc.*

La société civile, aussi, joue un rôle important à travers des initiatives telles que le portail « *cyberconfiance.ma* », lancé en 2021 par le centre marocain de recherches polytechniques et d'innovation[33]. Ce portail permet de signaler le cyberharcèlement des enfants et des jeunes et l'éducation à la citoyenneté numérique.

Consultation citoyenne sur la plateforme du CESE « ouchariko.ma »

La consultation citoyenne révèle que les diverses plateformes visant à sensibiliser aux enjeux et défis de l'utilisation des réseaux sociaux par les enfants et les jeunes sont peu connues du public. À peine 14 % des répondants connaissent e-himaya.gov.ma, 9% connaissent cyberconfiance.ma et 7 % connaissent koun3labal.ma.

En conclusion, bien que de nombreuses initiatives soient en place, elles demeurent fragmentées et opèrent souvent de manière isolée, sans une vision stratégique nationale partagée. Une approche intégrée est pourtant essentielle pour une protection effective et durable des enfants dans l'environnement numérique.

3. Recommandations des instances internationales pour le renforcement de la protection des enfants dans l'environnement numérique

Les instances internationales de l'ONU recommandent une approche globale et stratégique pour la protection des enfants dans l'environnement numérique, en mettant l'accent sur l'importance cruciale d'intégrer les droits des enfants dans les politiques nationales. Elles préconisent l'implication de toutes les parties prenantes, en particulier les enfants, en sollicitant leur participation active, et en s'assurant de leur consentement éclairé et adapté à leur niveau de développement. Les points de vue des enfants doivent être dûment pris en compte, avec l'obligation de les tenir informés sur l'impact de leurs contributions sur les décisions finales. Des moyens suffisants devraient être mis à disposition pour garantir une participation réelle des enfants.

A cet égard, **l'Observation générale no 25 (2021) du Comité des droits de l'enfant** insiste sur la nécessité d'adapter les politiques nationales pour protéger les enfants dans l'environnement numérique, d'assurer leur accès sécurisé et de les aider à tirer profit de ces interactions. Les législations doivent être conformes aux normes internationales et les mécanismes de protection des enfants en ligne doivent être renforcés.

Par ailleurs, **l'Union internationale des télécommunications** a énoncé 11 principes pour élaborer une stratégie nationale de protection en ligne des enfants, incluant la collaboration entre secteurs public et privé, le respect des droits fondamentaux des enfants et la participation des enfants dans l'élaboration de ces stratégies.

Pour sa part, la **Représentante spéciale du Secrétaire Général des Nations Unies** recommande une protection proactive des enfants sur les réseaux sociaux, l'alignement des législations avec les normes internationales, et des actions de sensibilisation pour les parents et les entreprises.

33 - Le CMRPI est une association savante à but non lucratif et un acteur socio-universitaire regroupant des chercheurs et des experts dans divers domaines liés aux sciences appliquées et aux nouvelles technologies.

Quant à **l'UNICEF**, cet organisme préconise une action à plusieurs niveaux, incluant politique, justice pénale, soutien aux victimes, engagement sociétal, régulation de l'industrie et sensibilisation par les médias.

De même, **l'U.S Surgeon General's Advisory on social media and youth mental health** appelle à des actions concrètes des décideurs politiques, des entreprises technologiques, des parents, des enfants et des chercheurs pour garantir une interaction sûre et saine avec les médias sociaux.

Enfin, le **Conseil de l'Europe (Recommandation CM/Rec (2018)7)** encourage les États à élaborer des stratégies nationales complètes, à impliquer les enfants dans ces processus, et à évaluer régulièrement les progrès réalisés.

Encadré 4 : forces, faiblesses et messages clés

Sur la base de l'analyse de l'interaction entre l'enfance et les réseaux sociaux, le CESE a dégagé une série de forces et de faiblesses qui façonnent l'environnement numérique national.

Forces Identifiées

1. **Conscience accrue de la protection nécessaire** : reconnaissance généralisée de la nécessité d'agir pour sécuriser l'environnement numérique des enfants, notamment sur les réseaux sociaux.
2. **Mobilisation multisectorielle** : engagement fort de divers acteurs, incluant le gouvernement, la société civile, et le secteur des télécommunications et du digital pour protéger les enfants en ligne.
3. **Cadre juridique existant** : des lois couvrant des aspects cruciaux de la protection de l'enfance sont déjà en place.
4. **Collaborations étendues** : des partenariats nationaux et internationaux renforcent les efforts de protection.
5. **Disponibilité de données** : existence de recherches et d'études nationales de qualité sur le sujet.

Faiblesses Identifiées

1. **Absence d'une vision commune** et clairement définie concernant la protection de l'enfance en ligne partagée par les acteurs impliqués dans la protection des enfants sur *Internet*.
2. **Absence de coordination stratégique** : un manque de synchronisation et d'organisation entre les actions des différents intervenants.
3. **Suivi et évaluation limités** : une faible analyse de l'impact des réseaux sociaux et des initiatives de sensibilisation sur les enfants.

4. **Éducation numérique insuffisante** : un déficit patent dans l'éducation des enfants et des familles pour utiliser de manière sûre et responsable l'environnement numérique, ce qui limite leur capacité à gérer les risques associés à l'utilisation des réseaux sociaux.
5. **Participation limitée des enfants et des jeunes** : un engagement restreint des enfants et des jeunes dans les processus de décision et d'action.
6. **Insuffisances législatives** : des lacunes importantes dans les textes législatifs entravant la prise en charge des spécificités du numérique et des progrès accélérés de la cybercriminalité ciblant les enfants.

Il en découle les messages clés suivants :

- **Potentiel du numérique** : le digital offre des opportunités significatives pour le développement personnel et créatif des enfants.
- **Nécessité de protection** : il est crucial de sécuriser l'utilisation des réseaux sociaux par les enfants pour prévenir des risques notables.
- **Responsabilité collective** : la protection des enfants dans le numérique nécessite une approche coordonnée impliquant tous les acteurs, avec un rôle central pour l'État qui doit mettre en place le cadre de coordination et l'environnement juridique nécessaires à l'effectivité de cette protection.
- **Importance de l'éducation numérique**[34] : former les enfants et les familles à naviguer de manière sécurisée dans l'environnement numérique est essentiel pour réduire les risques.

4. Nécessité d'intégrer la protection des enfants en ligne dans les objectifs de la politique publique intégrée de protection de l'enfance

Sur la base de ce diagnostic partagé et en s'inspirant des orientations des instances internationales, le Conseil Économique, Social et Environnemental exhorte à la mise en place d'un environnement numérique qui soit à la fois inclusif et sécurisé pour les enfants. Cela requiert une mise en œuvre accélérée et un renforcement substantiel de la politique intégrée de protection de l'enfance (PIPE), tout en mettant spécifiquement l'accent sur l'intégration de la protection des enfants en ligne dans ses objectifs stratégiques[35].

Pour y parvenir, il est crucial que tous les acteurs impliqués dans la protection de l'enfance intensifient leur collaboration, coordonnent leurs actions et mutualisent leurs efforts, afin de relever les différents défis associés à la protection des enfants, notamment dans le domaine du numérique.

34 - Magali Persch, Mélody Soulairol. L'éducation au numérique. Education. 2019.
« L'éducation au numérique regroupe la pratique de l'outil informatique en tant que tel, l'éducation aux médias et à l'information et l'informatique. »

35 - Rappel des objectifs stratégiques de la Politique intégrée de protection de l'enfance :
- 1. Renforcement du cadre légal de protection des enfants et de son effectivité ;
- 2. Mise en place de dispositifs territoriaux intégrés de protection de l'enfance ;
- 3. Standardisation des structures, des services et des pratiques ;
- 4. Promotion de normes sociales protectrices des enfants ;
- 5. Mise en place de systèmes d'information fiables et standardisés et de suivi-évaluation et monitoring régulier et effectif.

Axe1 : Intégration de la protection de l'enfance en ligne dans les objectifs de la politique intégrée de protection de l'enfance PIPE qui vise à renforcer le cadre légal de protection des enfants et à accélérer sa mise en œuvre. Cette adaptation est impérative pour répondre aux nouveaux défis posés par l'environnement numérique.

Pour ce faire, le Conseil recommande :

1. **L'harmonisation du cadre juridique national** avec les normes internationales relatives aux droits de l'enfant, tout en étant spécifiquement adapté aux dynamiques de l'environnement numérique. Cela comprend la caractérisation des crimes et délits commis en ligne dans la législation, la clarification des responsabilités des entreprises technologiques et des opérateurs de télécommunications, ainsi que l'établissement de règles dédiées à l'encadrement de l'utilisation des réseaux sociaux par les enfants.
2. **La définition d'une majorité numérique** : Il est crucial de réfléchir à l'instauration d'une majorité numérique qui définirait l'âge à partir duquel un enfant peut accéder aux réseaux sociaux sans le consentement des parents. Cette mesure nécessiterait la mise en place de mécanismes contraignants pour les fournisseurs de services de réseaux sociaux, incluant notamment :
    - L'obligation de refuser l'inscription des mineurs sans consentement parental et d'informer clairement les mineurs et leurs parents ou tuteurs légaux des risques associés à l'usage des réseaux et des moyens de prévention, ainsi que des conditions d'utilisation des données personnelles et des droits des utilisateurs.
    - La possibilité pour les parents ou tuteurs légaux de demander la suspension des comptes de leurs enfants.
    - La mise en place de dispositifs de contrôle du temps passé sur les services, avec des notifications régulières envoyées aux utilisateurs concernant leur durée d'utilisation.
3. Le soutien aux victimes de crimes en ligne : il est essentiel de garantir un accompagnement juridique et psychologique efficace et facilement accessible aux victimes de délits numériques.

Axe 2 : Accélérer le déploiement effectif de dispositifs territoriaux intégrés de protection de l'enfance, conformément à l'objectif stratégique 2 de la PIPE, avec pour mission d'assurer la détection, l'assistance et le suivi continu des enfants victimes de la violence numérique.

Pour ce faire, il est de recommandé de :

- Prendre en compte les risques inhérents aux réseaux sociaux en matière de détection et de prise en charge, ce qui implique de mettre en place des mécanismes de signalement et de recours judiciaires et non judiciaires adaptés, agiles et accessibles aux enfants et à leurs tuteurs.
- Assurer une veille territoriale et nationale de l'évolution des risques et des besoins en protection des enfants, en produisant des données et en réalisant régulièrement des travaux de recherche en collaboration avec les universités.

Axe 3 : Développer, dans le cadre de l'objectif stratégique 4 de la PIPE, un environnement numérique inclusif en renforçant significativement l'éducation numérique destinée non seulement aux enfants, mais également aux parents, tuteurs et enseignants. Cette mesure vise à promouvoir les normes sociales qui protègent efficacement les enfants.

A cette fin, il est recommandé de :

- Intégrer l'éducation au numérique dans les programmes scolaires dès le plus jeune âge, en développant l'esprit critique des élèves et en mettant un accent sur la vérification des informations et le croisement des sources, compétences clés pour naviguer de manière avisée dans l'environnement numérique[36].
- Impliquer les enfants, parents, et enseignants dans l'élaboration, la mise en œuvre, le suivi et l'évaluation des programmes d'éducation numérique.
- Alerter régulièrement la population sur les dangers des fausses informations par le biais de divers canaux de communication, en personnalisant le message pour chaque groupe ou catégorie spécifique (enfants, adolescents, seniors, analphabètes, *etc.*) [37].
- Sensibiliser les producteurs d'information et de contenu numérique, professionnels et non-professionnels (blogueurs, influenceurs, *etc.*), sur leur rôle et leurs responsabilités en matière de lutte contre les fakes news, notamment à travers des actions pointues de formation continue[38].
- Favoriser les outils techniques du contrôle parental sur les contenus numériques en facilitant l'exploitation de ces outils et solutions dans les offres d'abonnement *Internet*, et en les mettant en avant dans les offres publicitaires des fournisseurs de ces services.
- Déployer les outils de l'intelligence artificielle pour détecter proactivement les contenus inappropriés, analyser les comportements à risque, adapter les contrôles parentaux de manière personnalisée et automatiser la modération des contenus dangereux, afin d'assurer une réponse rapide et efficace face aux menaces présentes sur les réseaux sociaux.

Axe 4 : Définir, dans le cadre de l'objectif stratégique 5 de la PIPE, des indicateurs précis pour mesurer la protection en ligne des enfants. Cette mesure est essentielle pour établir des systèmes d'information fiables et standardisés, ainsi que pour assurer un suivi, une évaluation, et un monitoring réguliers et efficaces.

Pour ce faire, il est recommandé de :

- Adopter la méthode du Child Online Safety Index (COSI)[39] qui évalue la performance globale d'un pays en matière de protection en ligne des enfants.
- Mettre en place aux niveaux local et régional, des mécanismes d'information, de suivi et évaluation.

36 - Rapport du CESE : « Les fake news, de la désinformation à l'accès à une information avérée et disponible » - 2022

37 - Idem.

38 - Idem.

39 - Annexe 4 : The child online safety index (COSI) from the DQ Institute

Il est important de souligner que l'atteinte de ces objectifs nécessite une mobilisation accrue de tous les acteurs engagés dans la protection de l'enfance. Cette collaboration doit se traduire par une coordination et une mutualisation des actions. Ainsi, il est recommandé de :

- Veiller à l'élaboration d'un rapport annuel thématique rendant compte de la situation de la protection des enfants dans l'environnement numérique et l'évaluation des réalisations dans ce domaine ; rapport à soumettre aux commissions compétentes au Parlement par l'autorité gouvernementale en charge de l'enfance.
- Veiller à ce que tous les acteurs institutionnels et les entités de la société civile, ainsi que les enfants et les jeunes, soient activement impliqués dans la conception et l'évaluation des programmes de protection de l'enfance.
- Renforcer les interactions entre les autorités publiques compétentes et les plateformes numériques pour améliorer la collaboration et le partage d'informations, dans le but de mieux sécuriser l'espace numérique.

Annexes

Annexe 1 : Liste des membres de la Commission permanente des Affaires Sociales et de la Solidarité

Experts
Benseddik Fouad
Himmich Hakima
Lamrani Amina
Rachdi Abdelmaksoud
Syndicats
Bahanniss Ahmed
Bensaghir Mohamed (vice-rapporteur de la Commission)
Dahmani Mohamed
Essaïdi Mohamed Abdessadek (vice-président de la Commission)
Hansali Lahcen (rapporteur de la Commission)
Khlafa Mustapha
Kandila Abderrahmane
Jamaâ El Moâtassim
Organisations professionnelles
Bensalah Mohamed Hassan
Bessa Abdelhai
Boulahcen Mohamed

Société civile
Berbich Laila
Chouaib Jaouad (Président de la Commission)
Naji Hakima
Zahi Abderrahmane
Zaoui Zahra
Membres de droit
Adnane Abdelaziz
Cheddadi Khalid
Boujendar Lotfi
Gayer Othman

Experts ayant accompagné la Commission

Expert permanent au Conseil	Mohamed El Khamlichi
Traductrice	Nadia Ourhiati

Annexe 2 : Liste des acteurs auditionnés

Départements ministériels	• Ministère de l'Éducation nationale, du Préscolaire et des Sports • Ministère de la Solidarité, de l'Insertion sociale et de la Famille
Organismes publics	• Direction générale de la Sûreté nationale • Agence de développement digital • Agence nationale de réglementation des télécommunications
Organisations internationales	• Dr Najat Maalla M'jid, Représentante spéciale chargée de la question de la violence contre les enfants (Nations Unies) • UNICEF
Société civile	Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI)
Opérateurs des télécommunications	Maroc Telecom
Experts	• Dr Mustapha Chagdali • Pr Hamza Chainabou
Visite de terrain : Académie Régionale d'Éducation et de Formation de Rabat-Salé-Kénitra	

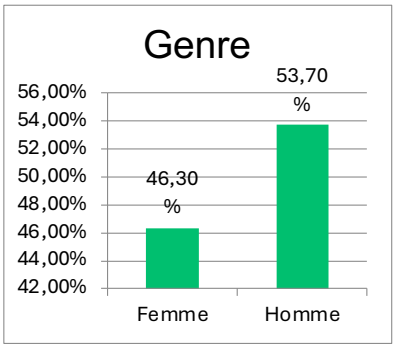
Annexe 3 : Résultats de la consultation lancée sur la plateforme de participation citoyenne du CESE sur l'utilisation des réseaux sociaux par les enfants

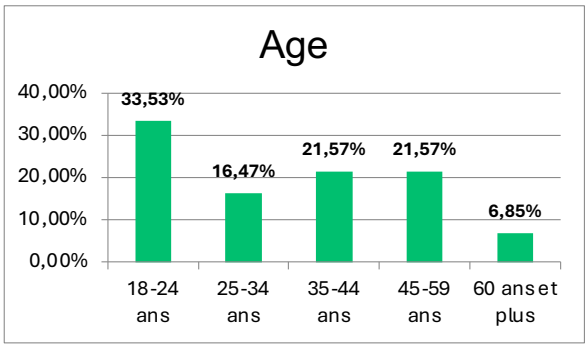
Dans le cadre de l'élaboration de son avis sur l'enfance et les réseaux sociaux, le CESE a lancé, du 19 janvier au 15 mars 2024, une consultation citoyenne à travers sa plateforme « ouchariko.ma », afin de recueillir les opinions et les propositions des citoyennes et des citoyens. Cette consultation a connu la participation de 934 personnes qui ont répondu au questionnaire du sondage. Les résultats de la consultation font ressortir le regard des participants sur la question de l'utilisation des réseaux sociaux par les enfants. Les principaux enseignements tirés de ce sondage ont été pris en compte dans l'élaboration de cet avis.

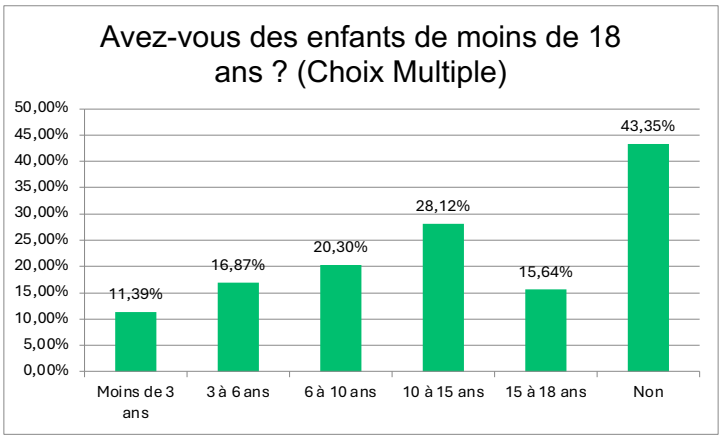
Caractéristiques de l'échantillon

La population des répondants est composée de 54% d'hommes et 46% de femmes. 50% des participants sont âgés de moins de 35 ans (33% entre 18 et 24 ans), plus de 21% sont situés dans la tranche d'âge 35-44 ans, plus de 21% également dans la tranche 45-59 ans et seulement 7% ont plus de 60 ans.

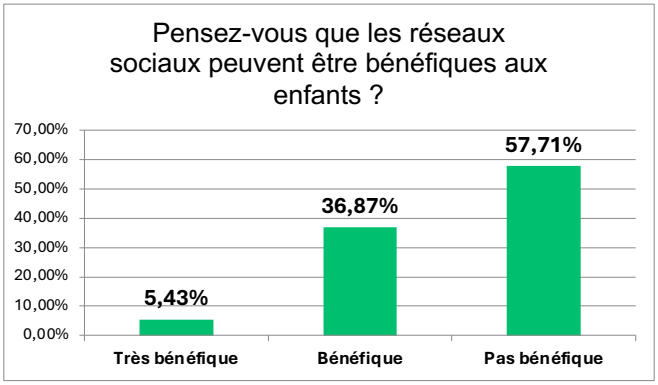
Une écrasante majorité des répondants ont un niveau universitaire (94%), et sont pour près de la moitié (40,78%) des cadres, et pour plus du tiers (35%) des étudiants. Neuf participants sur 10 résidents dans un milieu urbain (92%), et la moitié d'entre eux (50,59%) se concentre dans les régions de Rabat-Salé-Kénitra (32,65%) et Casablanca-Settat (17,94%).



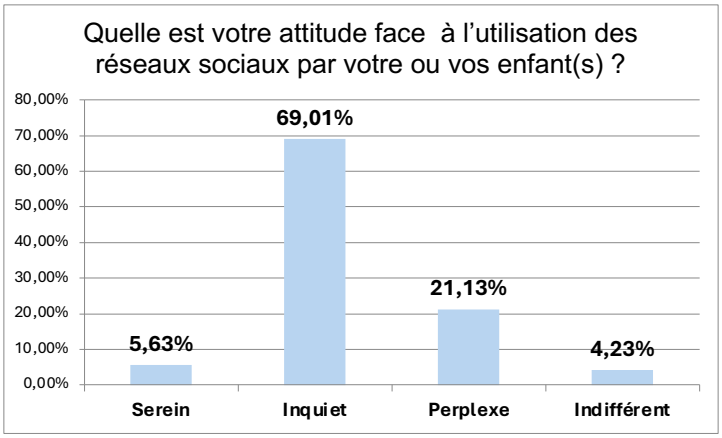




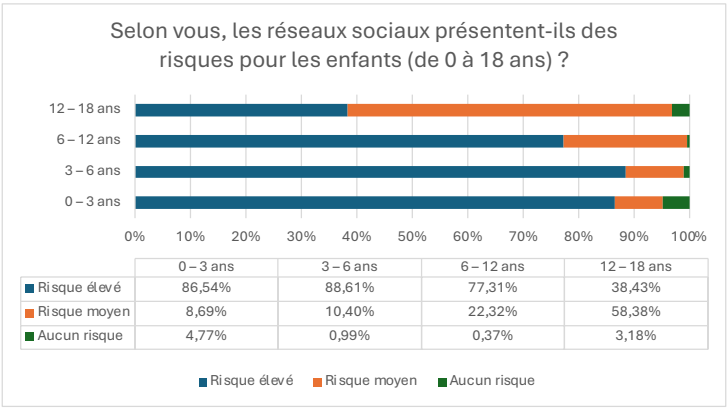
Un peu plus de la moitié des répondants sont parents d'au moins un enfant de moins de 18 ans, dont près de la moitié (47,65%) possèdent un smartphone personnel qu'ils ont obtenu pour la majorité après l'âge de 12 ans. En outre, 36,91% d'entre eux déclarent que leurs enfants sont actifs sur les réseaux sociaux.



Le premier message qui émerge du sondage est une perception plutôt négative des réseaux sociaux, puisque près de 58% des répondants estiment que les réseaux sociaux ne sont pas bénéfiques pour les enfants, et ne considèrent les éventuels effets positifs qu'à partir de l'âge de 15 ans (41,35%). Cette attitude se trouve confirmée par une proportion élevée de répondants qui sont « inquiets » de l'utilisation des réseaux sociaux par les enfants (69%), tandis que 21% sont « perplexes » face à cette utilisation.

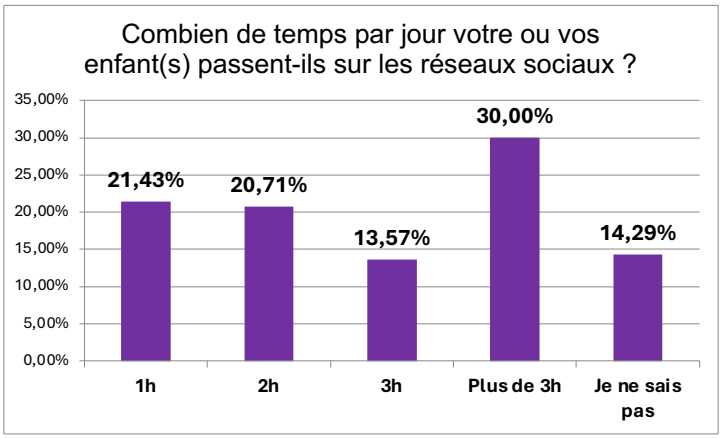


Les répondants s'accordent majoritairement sur le fait que les réseaux sociaux représentent un risque élevé pour les enfants de moins de 12 ans. Ils estiment également, à hauteur de 58,38%, que ce risque continue, bien que de manière plus modérée, au-delà de cet âge.

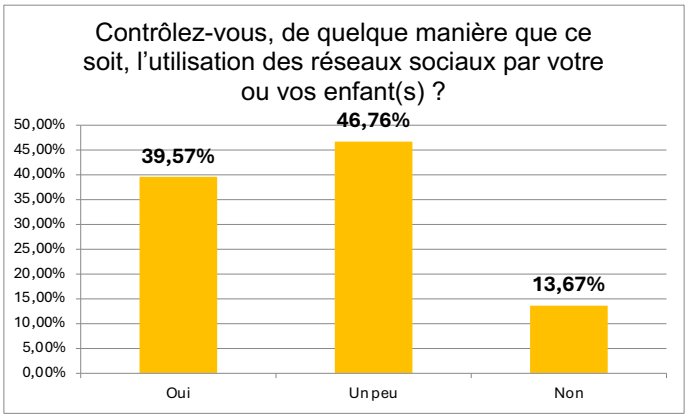


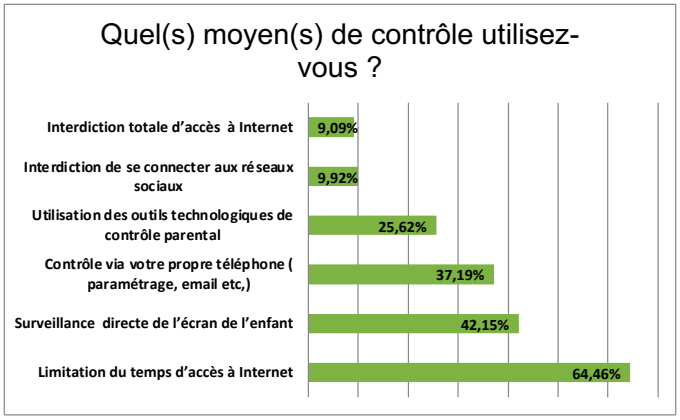
	0 – 3 ans	3 – 6 ans	6 – 12 ans	12 – 18 ans
Risque élevé	86,54%	88,61%	77,31%	38,43%
Risque moyen	8,69%	10,40%	22,32%	58,38%
Aucun risque	4,77%	0,99%	0,37%	3,18%

La durée quotidienne que les enfants passent sur les réseaux sociaux oscille principalement entre une et plus de trois heures. Près de 44% des enfants dédient au moins trois heures chaque jour à ces plateformes. Par ailleurs, plus de 14% des répondants admettent ne pas savoir combien de temps leurs enfants y passent.

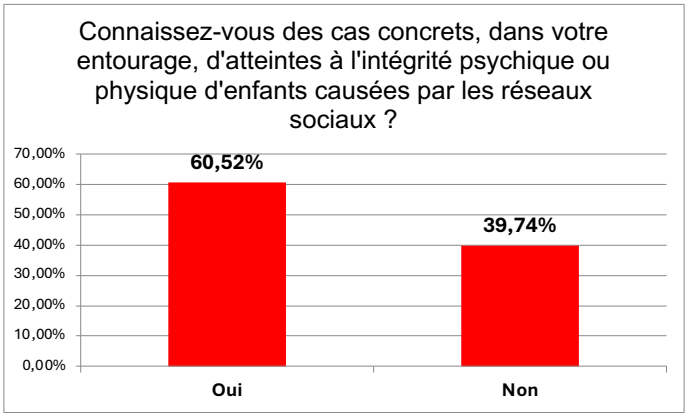


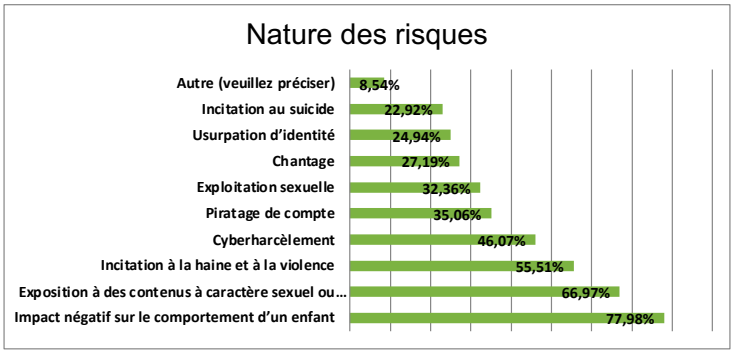
En raison des inquiétudes partagées par de nombreux parents concernant les risques associés aux réseaux sociaux, une grande majorité d'entre eux (près de 87%) surveille l'utilisation que leurs enfants en font. Le contrôle est catégorique pour environ 40% des parents, tandis que 47% utilisent une autre méthode moins directe. Cette surveillance s'effectue principalement par la limitation du temps de connexion, appliquée par 64,46% des parents, ou par la surveillance directe de l'écran de l'enfant, pratiquée par 42,15%.



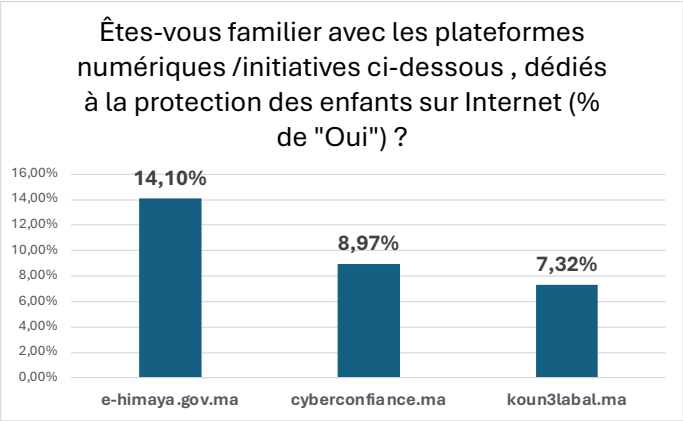


La méfiance générale des parents vis-à-vis des réseaux sociaux découle souvent de leur propre expérience, avec plus de 60% des sondés indiquant connaître au moins un cas d'atteinte à l'intégrité physique ou psychique d'un enfant lié à ces plateformes. Cette inquiétude s'ancre principalement dans la nature des messages et des contenus auxquels les enfants sont exposés, notamment ceux à caractère sexuel ou pornographique (66,97%) et ceux incitant à la haine et à la violence (55,51%). Près de la moitié des participants (46,07%) signalent des incidents de cyberharcèlement, et un tiers mentionnent des cas de piratage de comptes. En outre, plus de trois quarts des incidents rapportés ont un impact négatif sur le comportement de l'enfant (77,98%).

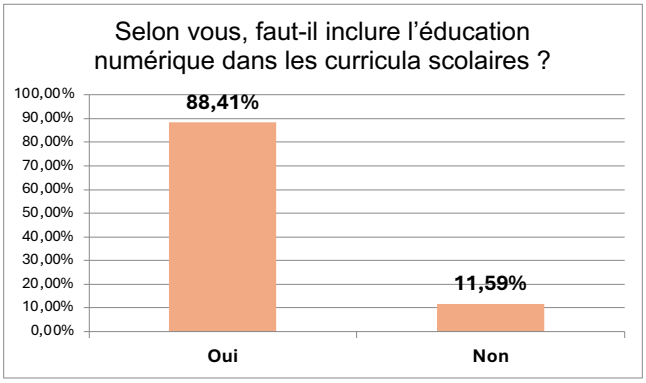




Le sondage révèle que les plateformes destinées à sensibiliser le public sur les dangers des réseaux sociaux pour les enfants et les jeunes demeurent largement méconnues. Seulement 14% des répondants connaissent e-himaya.gov.ma, 9% cyberconfiance.ma et 7% koun3labal.ma.



Enfin, la grande majorité des participants au sondage (88% des répondants), reconnaît l'importance d'intégrer l'éducation numérique dans les programmes scolaires pour faire face aux risques associés aux réseaux sociaux à long terme.



Annexe 4 : La règle «3-6-9-12» pour une gestion saine des écrans chez les enfants

Proposée par le psychiatre et psychologue Serge Tisseron en 2008, la règle «3-6-9-12» offre aux parents un cadre pour réguler l'exposition aux écrans de leurs enfants, tout en sensibilisant à la nécessité de prévenir les abus et les mésusages des écrans.

Avant 3 ans

- éviter les écrans pour favoriser le développement sensoriel des enfants ;
- les parents doivent plutôt jouer et parler avec leurs enfants pour favoriser leur développement.

De 3 à 6 ans

- établir des règles claires sur les temps d'écran ;
- respecter les âges indiqués pour les programmes ;
- éviter de placer la tablette, la télévision et l'ordinateur dans la chambre de l'enfant ;

- interdire les outils numériques pendant le repas et avant le sommeil ;
- ne jamais utiliser les outils numériques pour calmer un enfant.

Afin que l'enfant puisse découvrir ses dons sensoriels et manuels, ses activités principales doivent être des jeux sensorimoteurs et basés sur la stéréotypie motrice.

De 6 à 9 ans

- fixer des règles claires sur le temps d'écrans, et parler avec les enfants de ce qu'ils y voient et font ;
- éviter de placer la tablette, la télévision et l'ordinateur dans la chambre de l'enfant ;
- paramétrer la console de jeux ;
- parler du droit à l'intimité, du droit à l'image et des 3 principes d'*Internet* à savoir : tout ce que l'on y met peut tomber dans le domaine public, tout ce que l'on y met y restera éternellement et il ne faut pas croire tout ce que l'on y trouve.

Et ce, afin que les enfants âgés de 6 à 9 ans puissent découvrir les règles du jeu social.

De 9 à 12 ans

- déterminer avec l'enfant l'âge à partir duquel il aura son téléphone mobile ;
- décider s'il a le droit d'aller sur *Internet*, seul ou accompagné ;
- décider avec lui du temps qu'il consacre aux différents écrans ;
- parler avec lui de ce qu'il y voit et fait et lui rappelle les 3 principes d'*Internet* cités précédemment.

Après 12 ans

- laisser l'enfant surfer sur la toile tout en définissant les règles d'usage et en fixant des horaires de navigation à respecter ;
- mettre en place un contrôle parental ;
- parler avec lui du téléchargement, des plagiats, de la pornographie et du harcèlement ;
- couper le Wifi durant la nuit et éteindre les mobiles ;
- refuser d'être son « ami » sur les réseaux sociaux.

Annexe 5 : Observation No 25 du Comité des droits de l'enfant

Rappel de l'Observation générale no 25 (2021) du Comité des droits de l'enfant sur les droits de l'enfant en relation avec l'environnement numérique.

Dans le domaine législatif, le Comité des droits de l'enfant recommande, entre autres, aux Etats membres, les mesures suivantes :

- L'utilisation de l'environnement numérique pour **consulter les enfants sur les mesures législatives**, administratives et autres mesures pertinentes et à veiller à ce que l'opinion des enfants soit prise au sérieux…

- La mise en conformité de **la législation nationale avec les normes internationales** relatives aux droits de l'homme et adopter des textes de loi qui soient conformes à ces normes, pour faire en sorte que l'environnement numérique soit compatible avec les droits énoncés dans la Convention et les Protocoles facultatifs s'y rapportant.
- L'obligation de réalisation d'études d'impact sur les droits de l'enfant, afin d'ancrer les droits de l'enfant dans la législation, les allocations budgétaires et les autres décisions administratives relatives à l'environnement numérique, et promouvoir l'utilisation de ces études auprès des organismes publics et des entreprises en rapport avec l'environnement numérique.
- Les États parties **devraient prendre des mesures législatives,** administratives et autres pour faire en sorte que **la vie privée des enfants soit respectée et protégée** par toutes les organisations et dans tous les environnements qui traitent les données des enfants. La législation devrait prévoir des garanties solides, la transparence, une surveillance indépendante et l'accès à des recours. Les États parties devraient **exiger l'intégration de la protection de la vie privée dès la conception dans les produits et services numériques qui concernent les enfants. Ils devraient revoir régulièrement la législation relative à la vie privée et à la protection des données** et veiller à ce que les procédures et les pratiques permettent de prévenir les atteintes délibérées au droit de l'enfant à la protection de sa vie privée ou les violations accidentelles de ce droit.
- Les États parties **devraient prendre des mesures législatives et administratives pour protéger les enfants contre la violence dans l'environnement numérique,** et notamment examiner régulièrement, actualiser et appliquer des cadres législatifs, réglementaires et institutionnels solides qui protègent les enfants contre les risques, connus et émergents, de toute forme de violence dans l'environnement numérique. Ces risques comprennent la violence physique ou mentale, les blessures ou les sévices, la négligence ou la maltraitance, l'exploitation et les sévices, y compris l'exploitation sexuelle et les abus sexuels, la traite des enfants, la violence fondée sur le genre, les cyberagressions, les cyberattaques et la guerre de l'information.
- Les États parties devraient se doter d'une législation permettant de protéger les enfants contre les infractions commises dans l'environnement numérique, notamment la fraude et l'usurpation d'identité, et allouer des ressources suffisantes pour que ces infractions fassent l'objet d'enquêtes et de poursuites. Les États parties devraient également exiger un niveau élevé de cybersécurité, de protection de la vie privée et de sécurité dès la conception dans les services et produits numériques utilisés par les enfants, afin de minimiser le risque que de telles infractions se produisent.

Annexe 6 : The child online safety index (COSI) from the DQ Institute [40]

The 2022 COSI Assessment Framework

The COSI score represents the overall level of a nation's performance on child online safety measures. The 2022 COSI scoring system is based on 35 indicators related to 12 topics of child online safety across 6 stakeholders—namely, children, families, schools, ICT companies, and soft and hard infrastructures of the government. Each stakeholder score is measured based on the topic scores that belong to each stakeholder, and each topic score is measured based on the indicator scores that belong to each topic, in a hierarchical structure. Stakeholder scores, rigorously defined by the Performance Level Descriptors (PLDs), are designed to give policymakers and national leaders a better understanding of their countries' performance on child online safety. Topic scores are the indicators of performance in different areas of stakeholders' efforts. The indicator scores can be used to develop assessment instruments, learning curriculum, and/or tasks for relevant groups within each stakeholder.

Computation of Scores

The COSI score is calculated by successively combining the scores from each level of the hierarchy. The 6 Stakeholder scores combine the scores of 12 Topics, and the 12 topic scores combine the scores of 35 indicators.

At the lowest level, each score of the 35 Indicators is standardized and measured based on a weighted average of the sub-indicators belonging to each indicator. It is then transformed to a value between 10 and 100, with 10 being the lowest and 100 being the highest possible score.

These indicator scores are combined to create a score for each of the 12 Topics, and eventually a score for each of the 6 Stakeholders. The overall COSI score is then calculated as a weighted average of the 6 Stakeholder scores.

Performance Level Descriptors (PLDs)

Performance level descriptors are a means of describing performance in terms of levels or categories of performance. For the COSI scores, Stakeholder and Topic outcomes are reported in terms of three levels of performance: Level 1, Level 2, and Level 3.

The PLDs for Stakeholder and Topic scores can be considered policy PLDs designed for policymakers. They are general descriptors that articulate the goals and rigor for the final performance standards. These descriptors set the tone for the subsequent descriptors for Indicator scores, which can be considered as range PLDs. They are content-specific descriptors that may be used by corresponding stakeholders to guide assessment or learning development and/or resource enhancement.

40 - dqinstitute.org

Annexe 7 : Lignes directrices d'organisations internationales sur la protection de l'enfance sur Internet

a. L'Union internationale des télécommunications a énoncé 11 principes fondamentaux pour l'élaboration d'une stratégie nationale de protection en ligne des enfants globale et tournée vers l'avenir[41].

Ces principes sont énumérés suivant un lien logique et non par ordre d'importance. Une stratégie de protection en ligne des enfants devrait :

1. reposer sur une vision globale intégrant le secteur public, le secteur privé et la société ;
2. découler d'une compréhension et d'une analyse transversales de l'environnement numérique dans son ensemble, tout en étant adaptée à la situation d'un pays et à ses priorités ;
3. respecter les droits fondamentaux des enfants, tels qu'énoncés dans la Convention des Nations Unies relative aux droits de l'enfant et d'autres conventions et lois internationales essentielles, et être compatible avec ces droits ;
4. respecter les lois et les stratégies nationales existantes, similaires et associées qui sont en vigueur, telles que les lois sur la maltraitance faite aux enfants ou les stratégies sur la sécurité des enfants, et être compatible avec ces lois et ces stratégies ;
5. respecter les droits et les libertés civils des enfants, qui ne doivent pas être sacrifiés au profit de la protection des enfants ;
6. être élaborée moyennant la participation active de toutes les parties prenantes concernées, y compris les enfants, afin de tenir compte de leurs besoins et de leurs responsabilités, et de répondre aux besoins des minorités et des groupes marginalisés ;
7. être conçue de façon à s'aligner sur les programmes plus vastes des gouvernements visant la prospérité économique et sociale, et renforcer autant que possible la contribution des TIC au développement durable et à l'inclusion sociale ;
8. recourir aux instruments politiques les plus adaptés à disposition pour réaliser son objectif, compte tenu des conditions propres au pays concerné ;
9. être établie au plus haut niveau des pouvoirs publics, qui seront chargés d'assigner les rôles et les responsabilités pertinents et d'attribuer des ressources humaines et des ressources financières suffisantes ;
10. contribuer à édifier un environnement numérique digne dans lequel les enfants, les parents/personnes s'occupant d'enfants et les parties prenantes peuvent avoir confiance ;
11. orienter les efforts déployés par les parties prenantes pour autonomiser et doter les enfants des compétences numériques nécessaires pour qu'ils puissent se protéger en ligne.

b. La Représentante spéciale du Secrétaire Général des Nations unies chargée de la question de la violence contre les enfants[42], recommande :

41 - ITU: Guidelines for policy-makers on Child Online Protection (2020), page 2.

42 - Audition du 24 Août 2023 de Dr Najat Maalla M'jid

1. une protection des enfants sur les réseaux sociaux intersectorielle et proactive dans laquelle les enfants sont acteurs à part entière de la solution ;
2. l'alignement des législations nationales sur les normes internationales de droits humains ;
3. l'intégration de la protection des enfants en ligne dans les politiques nationales de protection des enfants ;
4. la garantie de poursuite des responsables de crimes en ligne contre les enfants et la garantie d'une aide et de l'accès à la justice aux victimes ;
5. la mise en place d'actions de sensibilisation et de formation appropriées ;
6. la garantie que les entreprises assument leurs responsabilités en matière de respect des droits des enfants, de prévention et de réparation des violations de leurs droits.

c. L'UNICEF, en matière d'intervention publique, recommande d'agir à 6 niveaux[43].

1. Politique et gouvernance
   - Leadership
   - Législation : un cadre juridique complet et efficace permettant d'enquêter et d'assurer la protection des victimes
2. La justice pénale
   - Application de la loi ; formation de la police ; enquêtes proactives et réactives ; coopération internationale
   - Pouvoir judiciaire : formation des juges, axée sur les victimes
   - Accès aux bases de données
3. Les victimes : services intégrés fournis lors de l'enquête, des poursuites et de la prise en charge
   - Lignes d'assistance téléphonique, soutien aux victimes
4. La société : mécanismes de signalement
5. L'industrie : procédures de retraits de contenus, d'images ; signalement des cas
6. Les médias : reportages, sensibilisation

d. U.S Surgeon General's[44]Advisory on social media and youth mental health [45], recommande un ensemble d'actions que pourraient prendre:

1. les décideurs politiques pour renforcer les protections et garantir une plus grande sécurité aux enfants et aux adolescents qui interagissent avec toutes les plateformes de médias sociaux ;

43 - Audition de l'UNICEF Maroc le 27 Septembre 2023

44 - se référer au rapport du U.S. Surgeon General's Advisory on Social media and youth mental health de 2023.

45 - Annexe 4 : recommandations détaillées extraites du rapport

2. les entreprises technologiques qui jouent un rôle central et ont une responsabilité fondamentale dans la conception d'environnements en ligne sécurisés et dans la prévention, la minimisation et la gestion des risques associés aux médias sociaux ;
3. les parents et les tuteurs pour contribuer à protéger et à soutenir les enfants et les adolescents contre les risques de préjudice ;
4. les enfants et les adolescents pour naviguer sur les réseaux sociaux de manière sûre et saine ;
5. les chercheurs (scientifiques).

e. Le Comité des ministres[46] du Conseil de l'Europe a élaboré des Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique (Recommandation CM/Rec(2018)7).

Ces lignes directrices appellent, entre autres, les États à :

- élaborer une approche stratégique nationale complète et veiller à ce que les politiques et mesures adoptées soient cohérentes et se renforcent mutuellement.
- Impliquer toutes les parties prenantes concernées et veiller en particulier à ce que les enfants soient consultés et à ce qu'ils aient la possibilité de contribuer à ces processus, avec leur consentement éclairé et en fonction du développement de leurs capacités. Leurs points de vue devraient être dûment pris en considération. Les enfants devraient être informés de la manière dont leurs points de vue ont été pris en compte et ont influencé le processus de décision. Des moyens suffisants devraient être mis à disposition pour garantir une participation réelle des enfants.
- Mesurer régulièrement les progrès et évaluer à tous les niveaux les actions de toutes les parties prenantes, prévues par la stratégie ou le plan d'action national.
- Diffuser largement des informations sur les stratégies ou plans d'action adoptés et sur leur mise en œuvre.
- S'assurer que les politiques sectorielles et initiatives sont fondées sur des informations rigoureuses et à jour sur les expériences des enfants dans l'environnement numérique les ressources pour garantir le bien-être des enfants dans l'environnement numérique.

46 - Annexe 5 : extraits du document du Conseil de l'Europe.

Conseil Economique, Social et Environnemental

1, angle rues Al Michmich et Addalbout, Secteur 10, Groupe 5
Hay Riad , 10 100 - Rabat - Maroc
Tél. : +212 (0) 538 01 03 00 Fax +212 (0) 538 01 03 50
Email : contact@cese.ma