المندوبية الوزارية المكلفة بحقوق الإنسان

المملكة المغربية
Royaume du Maroc

Délégation Interministérielle aux Droits de l'Homme
Interministerial Delegation for Human Rights

Eléments de réponse au questionnaire émanant du Haut-Commissariat des Nations Unies aux Droits de l'Homme sur la promotion de l'éducation numérique des jeunes

Question 1 : Quels sont Les principaux défis auxquels les jeunes de votre pays sont confrontés pour accéder à l'éducation numérique ? Veuillez prendre en compte la situation spécifique des jeunes marginalisés et de ceux en situation de vulnérabilité dans votre réponse.

L'éducation numérique au Maroc offre de nombreuses opportunités pour les jeunes, mais elle est également confrontée à de nombreux défis. Parmi les plus importants, on peut citer :

- **La fracture numérique** : une partie des jeunes marocains, en particulier ceux vivant dans les zones rurales ou reculées, n'a pas accès à internet ou aux équipements digitaux. De plus, le coût de ces technologies pourrait être hors de portée pour certaines familles.
- **Les inégalités sociales** : les jeunes marginalisés, en situation de pauvreté ou de handicap, ainsi que les filles et les femmes rurales, sont les plus susceptibles de ne pas bénéficier d'une éducation numérique.
- **La qualité du contenu pédagogique** : les ressources éducatives numériques de qualité et adaptées au contexte Marocain gagneraient à être développées davantage. De plus, les enseignants ne sont pas toujours formés à l'utilisation des technologies dans l'enseignement.

Question 2 : Quelles mesures le gouvernement prends-t-il pour s'assurer que l'éducation numérique est accessible et promue parmi les jeunes ? veuillez fournir des exemples de loi et de réglementation, de mesures, de politiques et de programmes spécifiques visant à garantir l'accès universel des jeunes à l'éducation numérique.

En ce qui concerne les mesures mises en place pour s'assurer que l'éducation numérique est accessible et promue parmi les jeunes, on peut citer le chantier

prioritaire de la feuille de route de l'Agence de Développement du Digital[1] portant plan national de formation dans le digital « génération digitale ». Le chantier consiste à mettre en place un programme national de formation au digital pour inclure les nouveaux métiers du digital dans l'enseignement supérieur, la formation continue, la formation professionnelle et la recherche scientifique ainsi que promouvoir la culture digitale auprès des jeunes et des citoyens. Il vise à :

- Former les jeunes aux compétences et aux nouveaux métiers du digital ;
- Aider les employés du privé et du public à mettre à jour leurs compétences digitales ;
- Développer les compétences des citoyens dans le domaine du digital et promouvoir l'usage des outils digitaux et la culture digitale
- Faire émerger un pool de talents capables de répondre à la demande du marché.

Aussi, parmi les principales initiatives prises dans le cadre de ce projet, on peut citer :

- La plateforme d'E-Learning Nationale « Academia Raqmya » proposant une offre de formation diversifiée, ciblant trois catégories d'apprenants : les collaborateurs des Administrations Publiques, des Entreprises (PME, TPE et Startups) et le grand public (y compris les jeunes).
  Des contenus spécialisés sur les dernières technologies digitales applicables dans plusieurs domaines d'activités au niveau du public et du privé, sont mis à disposition des bénéficiaires.
  La plateforme offre les parcours de formation suivants :
  - « Perfectionnement Digital » pour la formation continue dans le domaine du digital en faveur des collaborateurs des Administrations Publiques et Entreprises (TPE, PME et Startup).
  - « Acculturation Digitale » pour la sensibilisation et l'initiation du grand public au digital et l'obtention du passeport digital disponible en arabe dialectal (Darija).
  - « Partenaires technologiques » des formations e-learning de qualité sont disponibles à tous les visiteurs de la plateforme en partenariat avec les grands acteurs technologiques internationaux.

  Depuis son lancement en Mai 2022, la plateforme compte plus de 1 200 heures de formation en ligne, 177 cours et 11 parcours de formations spécialisés dans le numérique et disponibles en plusieurs langues et compte une des plus importantes communautés d'apprentissage en ligne au niveau national, avec plus de 27 000 bénéficiaires inscrits, dont une grande partie sont des jeunes.

---

[1] L'Agence de Développement du Digital (ADD), créée en vertu de la loi N°61.16 publiée au bulletin officiel n°6604 du 14 septembre 2017, est un établissement public stratégique doté de la personnalité morale et de l'autonomie financière. L'ADD est chargée de mettre en œuvre la stratégie de l'Etat en matière de développement du digital et de promouvoir la diffusion des outils numériques et le développement de leur usage auprès des citoyens.

- Le Centre Interactif Digital « IDC Morocco » est un Centre de transfert technologique dans les domaines des technologies immersives (réalité virtuelle, réalité augmentée et réalité mixte). L'IDC Morocco est le fruit d'une collaboration rassemblant l'Agence de Développement du Digital (ADD), l'Agence des États Unis pour le développement international (USAID), La société EON Reality (USA), l'Université Mohammed VI Polytechnique de Benguerir (UM6P), avec le soutien du Ministère de l'Industrie et du Commerce, le Ministère de l'Enseignement supérieur, de la Recherche scientifique et de l'Innovation, ainsi que l'Université Mohammed V de Rabat.
  Depuis son inauguration en Février 2020, L'IDC Morocco a permis de former/sensibiliser plus de 2000 bénéficiaires, majoritairement des jeunes sur les technologies immersives avec plus de 11 cohortes de développeurs spécialisés dans les domaines des technologies immersives formé au niveau de la « Virtual Reality innovation Academy » sur une à travers un Bootcamp professionnalisant alliant formation de base technique et projets de développement pratiques sur 6 mois au sein du campus de l'UM6P.
- Le programme AL KHAWARIZMI qui vise à encourager et promouvoir la recherche scientifique appliquée auprès d'équipes de recherche nationales dans les domaines de l'intelligence artificielle et du big data. Le programme finance et accompagne 45 projets de recherche relevant de 15 universités et structures marocaines de recherche. Ces projets couvrent un large spectre de domaines : santé, agriculture, industrie, énergie, logistique, environnement, éducation, justice...).
  Ce programme a pu promouvoir la production scientifique et technique auprès des jeunes chercheurs comptant une communauté de plus de 130 Doctorants et 140 Chercheurs.

Question n°3 : quelles mesures le gouvernement prend-il pour veiller à ce que les jeunes puissent exercer leurs droits fondamentaux en ligne en toute sécurité, de manière inclusive et qui renforce l'autonomie des jeunes ?

Pour veiller à ce que les jeunes puissent exercer leurs droits fondamentaux en ligne relatifs à l'accès et l'usage des technologies et outils numériques en sécurité et pour les protéger des éventuelles menaces en ligne, l'initiative « Culture digitale/protection des enfants en ligne » a été initié afin de mettre en place, en partenariat avec les acteurs concernés, des actions de sensibilisation et de communication pour promouvoir la culture d'usage approprié du digital et protéger les enfants des risques y afférents.

L'initiative a pour objectifs :

- D'inculquer les bonnes pratiques et les techniques d'usage sécurisé du digital auprès des enfants ;

- D'informer, sensibiliser et proposer aux parents/tuteurs et éducateurs des solutions, recommandations et outils pour éduquer et protéger les enfants en ligne ;
- De développer une vigilance d'autoprotection en ligne pour les enfants ;
- De limiter les risques en ligne pour les enfants.

Pour la gouvernance de l'initiative « Culture digitale/protection des enfants en ligne », un comité de coordination national chargé du pilotage et suivi de mise en œuvre du plan d'actions a été créé en novembre 2020. Ce Comité se réunit pour statuer sur l'état d'avancement des projets du plan d'actions de l'initiative. Le comité est composé des départements et institutions suivants :

- Le Ministère de la Justice ;
- Le Ministère de l'Education Nationale, du Préscolaire et des Sports ;
- Le Ministère de la Solidarité, de l'Insertion Sociale et de la Famille ;
- Le Ministère de la Transition Numérique et de la Réforme de l'Administration ;
- Bank Al Maghrib ;
- La Haute Autorité de la Communication Audiovisuelle ;
- La Direction Générale de la Sécurité des Systèmes d'Information ;
- La Gendarmerie Royale ;
- La Direction Générale de la Sûreté Nationale ;
- L'Agence Nationale de Réglementation des Télécommunications ;
- L'Agence de Développement du Digital ;
- L'Observatoire National des Droits de l'Enfant.

Aussi, et depuis le lancement de l'initiative en 2020, plusieurs actions ont été réalisées dont notamment :

- L'élaboration des guides thématiques de sensibilisation sur la culture d'usage sécurisée du digital pour les cibles de l'initiative (enfants, parents/tuteurs, jeunes/étudiants et enseignants) ;
- La mise en place de la plateforme nationale e-himaya de sensibilisation aux dangers du digital et à la protection des enfants en ligne (https://www.ehimaya.gov.ma);
- La promotion de l'usage des outils de contrôle parental ;
- L'organisation des séminaires et ateliers de formation et de sensibilisation pour les cibles de l'initiative ainsi que les acteurs de l'écosystème protection des enfants en ligne.

Question 4 : Quelles sont les principales lacunes et les principaux défis en matière de protection des jeunes contre les menaces en ligne dans la législation, la politique et la pratique de votre pays et quels sont les impacts sur les droits de l'homme des jeunes ? Veuillez prendre en compte la situation de vulnérabilité dans votre réponse.

Les principales lacunes et défis en matière de protection des jeunes contre les menaces en ligne sont :

- L'évolution des menaces et l'apparition des nouvelles attaques en ligne sophistiquées basées sur les nouvelles technologies émergentes telles que l'intelligence artificielle malveillante, les deepfakes et les stratégies de manipulation psychologique basées sur les données personnelles des utilisateurs ;
- L'accès facile non restreint à des contenus inappropriés par rapport à l'âge et aux mœurs ;
- La difficulté de suppression des contenus en ligne préjudiciables ;
- La montée des discours de haine et de xénophobie en ligne qui incitent à la discrimination, à l'hostilité et à la violence

Question n°5 : Quelles mesures le gouvernement prend-il pour s'assurer que les jeunes sont protégés contre les menaces en ligne ? veuillez fournir des exemples de lois et de règlementions, de mesures, de politiques et de programmes spécifiques ?

❖ **Cadre juridique national**

La constitution marocaine a accordé une place importante à la participation des jeunes au développement social, économique, culturel et politique du pays, en stipulant, dans son article 33, qu'il incombe aux pouvoirs publics de de faciliter l'accès des jeunes à la culture, à la science, à la technologie, à l'art, au sport et aux loisirs, tout en créant les conditions propices au plein déploiement de leur potentiel créatif et innovant dans tous ces domaines.

Aussi, la législation nationale consacre une grande importance à la promotion et à la protection des jeunes en ligne contre les menaces en ligne qui peuvent constituer des violations de leurs droits, ainsi que la protection de leurs données personnelles.

A cet égard, le code pénal marocain consacre des dispositions répressives à la protection effective contre les infractions relatives aux systèmes de traitement automatisé des données, notamment les articles 607-3, 607-4, 607-5, 607-6, 607-7, 607-8, 607-9, 607-10. Quant aux infractions relatives à l'utilisation des systèmes d'information pour commettre des infractions de droit commun contre des individus, le code pénal marocain stipule dans son article 447-1 que « *Est puni d'un emprisonnement de six mois à trois ans d'une amende de 2.000 à 20.000 dirhams, quiconque procède, sciemment et par tout moyen, y compris les systèmes informatiques, à l'interception, à l'enregistrement, à la diffusion ou à la distribution de*

paroles ou d'informations émises dans un cadre privé ou confidentiel, sans le consentement de leurs auteurs.

Est passible de la même peine, quiconque procède, sciemment et par tout moyen, à la capture, à l'enregistrement, à la diffusion ou à la distribution de la photographie d'une personne se trouvant dans un lieu privé, sans son consentement ».

L'article 447-2 du code pénal prévoit aussi une peine d'emprisonnement *d'un an à trois ans et d'une amende de 2.000 à 20.000 dirhams, quiconque procède, par tout moyen, y compris les systèmes informatiques, à la diffusion ou à la distribution d'un montage composé de paroles ou de photographie d'une personne, sans son consentement, ou procède à la diffusion ou à la distribution de fausses allégations ou de faits mensongers, en vue de porter atteinte à la vie privée des personnes ou de les diffamer* ».

Les infractions à caractère numérique commises en état de récidive ou par un époux, un conjoint divorcé, un fiancé, un ascendant, un descendant, un kafil, un tuteur ou une personne ayant autorité sur la victime ou ayant sa charge ou contre une femme en raison de son sexe ou contre un mineur, sont punies d'un an à cinq ans d'emprisonnement et d'une amande de 5.000 à 50.000 dirhams (article 447-3).

Aussi, le législateur a mis en place un ensemble de lois spécifiques qui condamnent les comportements illicites en ligne et garantissent la protection des utilisateurs d'internet contre les risques et menaces en ligne, notamment la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[2], qui prévoit, dans son article 59, une peine d'emprisonnement de trois mois à un an et d'une amende de 20.000 à 200.000 DH ou de l'une de ces deux peines seulement quiconque procède à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des motifs légitimes ou lorsque ce traitement répond à des fins de prospection, notamment commerciale.

La loi 09-08 prévoit une peine d'emprisonnement de trois mois à un an et d'une amende de 20.000 à 200.000 DH ou de l'une de ces deux peines seulement pour tout transfert de données à caractère personnel vers un Etat étranger, en violation des articles 43 et 44 de la loi[3], (article 60), et une peine d'emprisonnement de trois mois à

---

[2] Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[3] - L'article 43 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel stipule que « *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat étranger que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie notamment en fonction des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. La Commission nationale établit la liste des Etats répondant aux critères définis aux alinéas 1 et 2 ci-dessus* ».

un an et d'une amende de 20.000 à 200.000 DH ou de l'une de ces deux peines seulement pour tout responsable de traitement, tout sous-traitant et toute personne qui, en raison de ses fonctions, est chargé (e) de traiter des données à caractère personnel et qui, même par négligence, cause ou facilite l'usage abusif ou frauduleux des données traitées ou reçues ou les communique à des tiers non habilités (article 61).

D'autres lois sont adoptées en vue de garantir la protection des individus contre les infractions à caractère numérique, notamment :

- La loi 02-00 relative aux droits d'auteur et droits voisins[4] ;
- La loi n° 53-05 relative à l'échange électronique de données juridiques[5] ;
- La loi n° 31-08 édictant des mesures de protection des consommateurs[6] ;
- La loi 93-12 modifiant et complétant la loi 24-96 relative à la poste et télécommunications, en ce qui concerne la cryptographie et la certification électronique[7] ;

- L'article 44 de la loi susmentionnée édicte « *Par dérogation aux dispositions de l'article 43 ci-dessus, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article ci-dessus, si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou :*

1- Si le transfert est nécessaire :
a) à la sauvegarde de la vie de cette personne ;
b) à la préservation de l'intérêt public ;
c) au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
d) à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;
e) à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;
f) à l'exécution d'une mesure d'entraide judiciaire internationale ;
g) à la prévention, le diagnostic ou le traitement d'affections médicales.
2- Si le transfert s'effectue en application d'un accord bilatéral ou multilatéral auquel le Royaume du Maroc est partie ;
3- Sur autorisation expresse et motivée de la Commission nationale lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

[4]- La loi n° 02-00 relative aux droits d'auteur et droits voisins a été promulguée le 15 février 2000, et publiée au bulletin officiel n° 4810.

[5] - La loi n° 53-05 relative à l'échange électronique de données juridiques a été promulguée le 30 novembre 2007 et publiée au bulletin officiel n°5584.

[6] - La loi n° 31-08 édictant des mesures de protection des consommateurs a été promulguée le 18 février 2011 et publiée au bulletin officiel n° 5932.

[7] - La loi 93-12 modifiant et complétant la loi 24-96 relative à la poste et télécommunications, en ce qui concerne la cryptographie et la certification électronique a été promulguée le 17 juin 2013, et publiée au bulletin officiel n°6166.

- La loi n° 43-20 relative aux services de confiance pour les transactions électroniques[8] ;
- La loi n° 05-20 du 25 juillet 2020 relative à la cybersécurité[9].

❖ Mesures de sensibilisation

Concernant les mesures de sensibilisation des acteurs de la société à la sécurité des systèmes d'information, plusieurs initiatives ont étés entreprises, notamment :

- L'organisation de la première compagnes nationale de lutte Contre la Cybercriminalité durant la période 2014- 2017 et de la 2ème compagne durant la période 2018-2021. L'objectif étant de sensibiliser et d'éduquer les acteurs de la société sur l'importance de développer la confiance numérique pour pouvoir suivre le rythme du développement des technologies de l'information. Dans ce cadre, plusieurs actions ont été menées, notamment la réalisation d'un plan d'actions pour la mise en œuvre d'une campagne de communication portant sur les enjeux de la sécurité des systèmes d'information sur Internet au profit du grand public (PME, parents, enfants, etc.)
- L'organisation de la caravane nationale de sensibilisation destinée aux enfants dans les écoles, en 2017 afin de sensibiliser les élèves aux dangers que présente l'Internet, aux règles de base et aux mesures et bonnes pratiques nécessaires pour un usage sécurisé des TIC, en particulier de l'Internet. Cette action a été fondamentale et primordiale pour promouvoir la confiance numérique au sein de la société marocaine.
- Le lancement de trois éditions de Campagnes Nationales de prévention contre la cyberviolence et le cyberharcèlement à l'initiative du Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI), en partenariat avec les départements concernés et avec le soutien du Conseil d'Europe.
- La célébration annuelle de la journée mondial Safe Internet Day (SID) depuis 2018. Cet événement, qui est organisé tous les ans, depuis 2004, est une initiative qui a pour objectif de sensibiliser les enfants, les jeunes, les parents et les enseignants aux risques et menaces de l'Internet et d'instaurer une culture d'utilisation sûre, responsable et positive des TIC.
- La constitution, en 2020, d'un Comité national de coordination de la protection des enfants sur Internet composé de différents partenaires concernés. Il a pour objet de mettre en place un plan d'actions annuel et de veiller à sa mise en œuvre.

Dans ce cadre, un ensemble de programmes prioritaires ont été réalisés en partenariat avec les acteurs concernés, parmi lesquels :

---

[8] - La loi n° 43-20 relative aux services de confiance pour les transactions électroniques a été promulgué le 31 décembre 2020, et publiée au bulletin officiel n° 6970

[9] - La loi n° 05-20 du 25 juillet 2020 relative à la cybersécurité a été promulguée le 25 juillet 2020, et publiée au bulletin officiel n° 6906.

- Le lancement de la plateforme nationale de sensibilisation et de protection « Culture numérique », Protection des enfants sur Internet « e-Himaya » : www.e-himaya.gov.ma en décembre 2021 ;
- L'organisation de nombreux ateliers de sensibilisation relatif à la protection des enfants via Internet et la promotion de la plateforme électronique de protection ;
- La publication d'un ensemble de guides pour la sensibilisation et la protection des enfants, des jeunes, des parents/tuteurs et du personnel enseignant.

❖ Mesures techniques

Pour ce qui est des mesures techniques, le Maroc a adopté des normes en lien avec la sécurité de l'information et la protection des données et de la vie privée. Il s'agit de :

- NM ISO/CEI 27000 : 2014 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire
- NM ISO/IEC 27001 : 2022- Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences
- NM ISO/IEC 27002 : 2022 - Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information
- NM ISO/IEC 27701 : 2021 - Techniques de sécurité - Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée - Exigences et lignes directrices ;
- NM ISO/IEC 27003 : 2022 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Lignes directrices
- NM ISO/IEC 27004 : 2022 - Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information - Surveillance, mesurage, analyse et évaluation • NM ISO/IEC 27005 : 2022 - Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information
- NM ISO/IEC 27006 : 2022 - Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information
- NM ISO/IEC TS 27006-2 : 2022 - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité - Partie 2 : Systèmes de management des informations de sécurité
- NM ISO/IEC 27007 : 2022 - Sécurité de l'information, cybersécurité et protection des données privées - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- NM ISO/IEC 27011 : 2022 - Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour les contrôles de la sécurité de

l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications

- NM ISO/CEI TR 27008 : 2013 - Technologies de l'information - Techniques de sécurité - Lignes directrices pour les auditeurs des contrôles de sécurité de l'information
- NM ISO/CEI 27035 : 2013 - Technologies de l'information - Techniques de sécurité - Gestion des incidents de sécurité de l'information
- NM ISO/CEI 27034-1 : 2013 - Technologies de l'information - Techniques de sécurité - Sécurité des applications - Partie 1 : Aperçu général et concepts
- NM ISO/CEI 27033-1 : 2013 - Technologies de l'information - Techniques de sécurité - Sécurité de réseau - Partie 1 : Vue d'ensemble et concepts
- NM ISO/CEI 27033-3 : 2013 - Technologies de l'information - Techniques de sécurité - Sécurité de réseau - Partie 3 : Scénarios de réseautage de référence - Menaces, techniques conceptuelle et questions de contrôle
- NM ISO/CEI 27031 : 2013 - Technologies de l'information - Techniques de sécurité - Lignes directrices pour mise en état des Technologies de la communication et de l'information pour continuité des affaires
- NM ISO/CEI 27010 : 2015 - Technologies de l'information - Techniques de sécurité - Gestion de la sécurité de l'information des communications intersectorielles et inter-organisationnelles
- NM ISO/CEI 27014 : 2015 - Technologies de l'information - Techniques de sécurité - Gouvernance de la sécurité de l'information.