المرصد الوطني للإجرام
ⵜⴰⵙⴷⴰⵡⵜ ⵏⵜⵎⴰⵡⴰⵙⵜ
Observatoire National de la Criminalité

المَمْلَكة المَغْربيّة
وزَارة العَدْل
ⵜⴰⴳⵍⴷⵉⵜ ⵏ ⵍⵎⵖⵔⵉⴱ
ⵜⴰⵎⴰⵡⴰⵙⵜ ⵏ ⵜⵣⵔⴼⵜ
مديرية الشؤون الجنائية والعفو ورصد الجريمة

POLICY PAPER

(Synthèse)

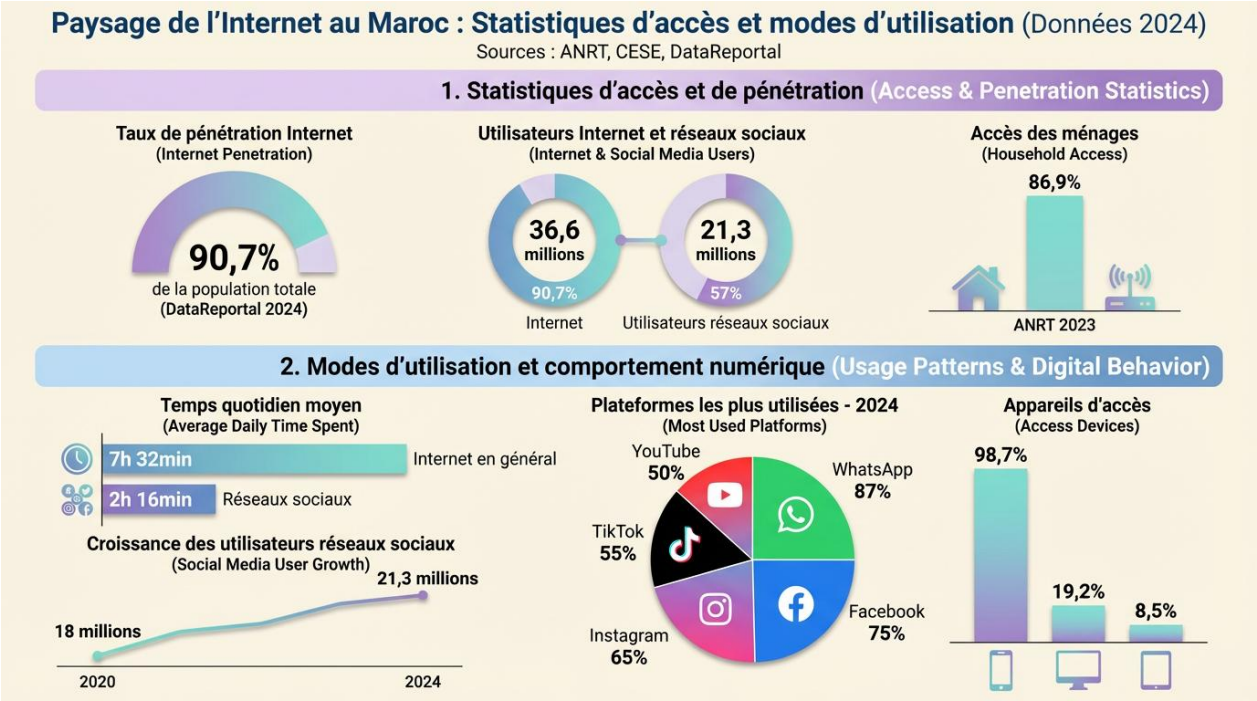
MÉTAVERS SOCIAUX ET PROTECTION DES MINEURS AU MAROC

SYNTHÈSE EXÉCUTIVE

L'émergence des métavers sociaux et des plateformes de jeu en ligne massivement multijoueurs crée un environnement numérique inédit où les frontières entre divertissement, socialisation et exposition aux risques criminels s'estompent. L'analyse conduite révèle une convergence entre vulnérabilités structurelles nationales et menaces internationales documentées, justifiant une réflexion approfondie sur l'adaptation du cadre réglementaire marocain.

Ampleur de l'exposition nationale

Sur une population de **11,4 millions d'enfants et jeunes de 5 à 24 ans au Maroc**, le croisement des données démographiques (HCP), des taux d'équipement technologique (ANRT : 89,2% des ménages connectés), et des comportements d'usage (CESE : 97% des mineurs sur réseaux sociaux) établit qu'approximativement 2,1 millions d'enfants et jeunes marocains utilisent potentiellement des plateformes comme Roblox, Fortnite, ou Free Fire[1]. Parmi cette population, l'étude Kaspersky documentant que 88% des parents n'utilisent jamais d'outils de contrôle parental suggère qu'environ 1,85 million de mineurs marocains évoluent dans ces environnements sans supervision effective.

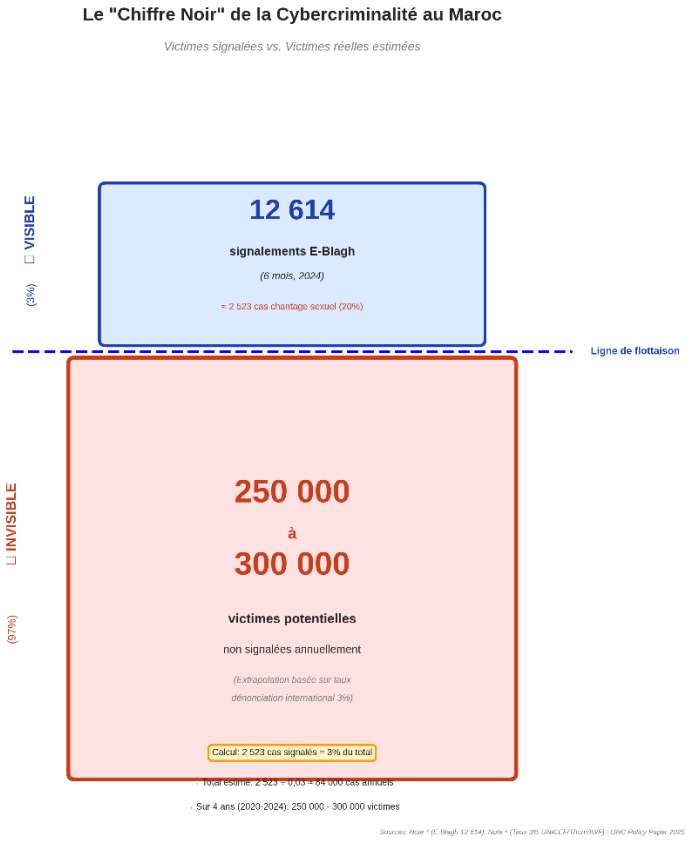


L'implantation économique de Roblox au Maroc se manifeste par une contribution estimée à 15 millions USD au PIB de cinq pays MENA incluant explicitement le Maroc (2023-T3 2024), avec une croissance de 30% des équivalents temps plein soutenus. Six boutiques spécialisées nationales distribuent des cartes prépayées Robux sur l'ensemble du territoire (140 à 1 090 MAD), avec livraison instantanée supprimant les barrières traditionnelles aux dépenses impulsives. Les communautés marocaines organisées

totalisent plus de 11 000 membres identifiés (Morocco Hangout : 4 673 membres Roblox + 6 499 Discord)[2].

Données criminelles et "chiffre noir"

Les données de la Direction Générale de la Sûreté Nationale (DGSN) et de l'Observatoire National de la Criminalité (ONC) documentent une évolution significative de la cybercriminalité au Maroc sur la période 2017-2024. Le volume global d'affaires cybercriminelles a connu une progression : 765 affaires en 2017, 1 091 en 2018 (+43%), 908 en 2019 (-17%), environ 863 en 2020 (-5%), suivies d'une expansion à partir de 2021 avec 5 275 affaires (+7%), 5 623 en 2022 (+7%), 5 969 en 2023 (+6%), et 8 333 en 2024 (+40%), représentant une multiplication par 10,9 en sept ans (+989%)[3].



La plateforme E-Blagh (système national de signalement en ligne, lancée le 3 juin 2024) a enregistré 12 614 signalements en six mois. L'analyse des trois premiers mois révèle que 60% des signalements concernent l'escroquerie et la fraude numérique, 20% le chantage sexuel, 10% les injures et diffamation, et 10% d'autres infractions[4].

La sextorsion présente une trajectoire variable sur la période 2021-2024 : 498 affaires en 2021, 417 en 2022 (-16%), 508 en 2023 (+22%), puis 391 en 2024 (-23%). L'année 2024 a conduit à l'interpellation de 163 individus et impliqué 394 victimes, dont 123 ressortissants étrangers. Le nombre d'interpellations a diminué de 40% sur trois ans (270

en 2021 → 163 en 2024), tandis que les victimes étrangères ont augmenté de 29% (95 en 2021 → 123 en 2024)[5].

La Présidence du Ministère Public (PMP) documente pour la période 2020-2023 : **2 915 affaires traitées et 3 646 personnes poursuivies.** La typologie des infractions établit que l'extorsion de fonds par menace de divulgation représente 1 173 poursuivis, les infractions aux systèmes de traitement automatisé de données 809 poursuivis, et le harcèlement sexuel par moyens électroniques 716 poursuivis[6]. Les autres données institutionnelles incluent : le Conseil Supérieur du Pouvoir Judiciaire (CSPJ) documente 269 victimes de traite des êtres humains dont 94 mineurs, l'Entraide Marocaine pour la Protection de l'Enfance (EMC) a enregistré 1 745 signalements dont 98 agressions sexuelles digitales, et le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) signale une augmentation de 35% des cas de cyberviolence ciblant les mineurs en 2024[7].

Toutefois, les études internationales établissent que seuls 3% des mineurs victimes d'abus en ligne dénoncent les faits[8], suggérant que les 12 614 signalements E-Blagh (dont 20% liés au chantage sexuel, soit environ 2 523 cas) pourraient représenter une réalité de 250 000 à 300 000 victimes potentielles non signalées au Maroc. Cette hypothèse repose sur l'application du ratio de dénonciation international au contexte marocain, et mériterait validation par enquêtes de victimation nationales spécifiques.

Positionnement régional préoccupant

L'analyse d'Interpol révèle que **69,24% des cas africains de sextorsion financière sont concentrés au Maroc**[9], configuration qui résulte de la convergence de plusieurs facteurs : le taux de chômage des jeunes de 37,7% favorisant l'économie criminelle numérique[10], le multilinguisme (arabe, français, anglais, darija) facilitant l'exploitation transfrontalière[11], l'infrastructure numérique avancée (12,6 millions de cyberattaques bloquées en 2023) attirant les criminels organisés[12], et le décalage horaire stratégique permettant l'exploitation continue des victimes européennes et nord-américaines[14].

Menaces internationales convergentes

L'Opération Restore Justice du FBI (mai 2025) a abouti à 205 arrestations de prédateurs ciblant des victimes âgées principalement de 11,3 à 12,8 ans dans des environnements immersifs[15]. L'opération Kidflix d'Europol (2024-2025) a identifié 1,8 million de fichiers d'exploitation pédopornographique dans des univers virtuels[16], tandis que l'opération Cumberland (octobre 2024) a démantelé des réseaux utilisant l'intelligence artificielle générative pour créer des contenus d'abus synthétiques[17].

Le Groupe d'Action Financière (GAFI) a documenté en mars 2025 trois vecteurs de monétisation criminelle : l'extorsion de crypto-actifs via menace de divulgation, l'achat de contenus illicites par NFT anonymes, et le blanchiment via économies virtuelles[18]. Le National Center for Missing & Exploited Children (NCMEC) a enregistré 2 847 signalements concernant des plateformes de métavers[19], et le rapport Hindenburg Research identifie 38 groupes criminels organisés opérant sur ces plateformes[20].

Cadre juridique actuel : Acquis législatifs et efforts de modernisation

Le Maroc s'est engagé depuis 2003 dans une démarche continue visant à combler le vide législatif relatif à la cybercriminalité, en construisant un dispositif juridique complet couvrant quatre piliers fondamentaux :

Premièrement - Transactions électroniques : Loi n° 05.53 relative à l'échange électronique de données juridiques (2007), et Loi n° 43-20 relative aux services de confiance concernant les transactions électroniques (2020).

Deuxièmement - Protection des données personnelles : Loi n° 09.08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (18 février 2009).

Troisièmement - Cybersécurité : Loi n° 05-20 relative à la cybersécurité (2021), avec criminalisation des atteintes aux systèmes de traitement automatisé des données par la Loi n° 03-07 complétant le Code pénal (11 novembre 2003).

Quatrièmement - Protection des consommateurs en ligne : Loi n° 08.31 édictant des mesures de protection du consommateur (2011).

Ce dispositif juridique a été renforcé par la Loi n° 88.13 relative à la presse et à l'édition qui criminalise les comportements délictueux commis par le biais de moyens audiovisuels ou électroniques, et par la Loi n° 103.13 relative à la lutte contre les violences faites aux femmes qui contient des dispositions répressives concernant la violence numérique (2018).

Sur le plan international, le Royaume du Maroc a ratifié la Convention de Budapest sur la cybercriminalité (29 juin 2018), son Protocole additionnel premier relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (daté du 28 janvier 2003, ratifié en 2014), et a signé le Protocole additionnel second (12 mai 2022) qui établit des mécanismes simplifiés pour émettre des injonctions directes aux fournisseurs de services relevant d'autres États, des mécanismes de divulgation accélérée des données de trafic, et l'obtention de preuves électroniques lors d'enquêtes pénales conjointes.

En continuité de cet engagement international, le Maroc a participé activement à l'élaboration de la Convention des Nations Unies contre la cybercriminalité dans le cadre des travaux du Comité spécial à composition non limitée (2019-2024) conformément à la résolution de l'Assemblée générale n° 74/247. Monsieur le Ministre de la Justice, Abdellatif Ouahbi, a signé la Convention à Hanoï le 25 octobre 2025, après son adoption par consensus par l'Assemblée générale des Nations Unies lors de sa soixante-dix-neuvième session (décembre 2024).

Le **positionnement international du Maroc** témoigne de cette maturité institutionnelle : **50ème rang mondial** sur 194 pays dans l'**Indice mondial de cybersécurité de l'Union internationale des télécommunications 2020** (Niveau 1 Tier 1/Role Modelling avec **97,5 points**), **52ème rang** dans l'**Indice d'inclusivité d'Internet 2022**, et **88ème rang mondial (6ème rang africain)** dans l'**Indice Oxford Insights de préparation gouvernementale à l'IA 2023** sur 193 pays.

Sur le plan procédural, le nouveau Code de procédure pénale (Loi n° 03-23, septembre 2025) a introduit des évolutions importantes adaptées à la réalité de la cybercriminalité : les **enquêtes numériques transfrontalières** autorisant la perquisition de systèmes d'information situés hors du territoire national, la **saisie accélérée de preuves électroniques volatiles** dans un délai de 48 heures sans autorisation préalable en cas de danger imminent, et la **coopération judiciaire renforcée** permettant l'échange de données en 72 heures avec les États parties à la Convention de Budapest. Ce code a également prévu la procédure de perquisition numérique des appareils informatiques et outils électroniques, la saisie des données, preuves électroniques et traces numériques, la procédure d'analyse des traces numériques pour extraire les données et preuves liées aux infractions, la détermination de la procédure d'interception des communications réalisées via des formes de communication électronique ou moyens technologiques modernes, et la détermination de la procédure d'interception, diffusion et enregistrement des sons, images et données électroniques, ainsi que la localisation.

Au niveau des réformes en cours, et consciente de l'importance de la transformation numérique et des risques qui en découlent, le Ministère de la Justice s'est attelé à poser les bases d'un ensemble de réformes législatives relatives à la lutte contre les formes émergentes de cybercriminalité, dans le but de surmonter les contraintes pratiques résultant de la multiplicité et de la dispersion des textes juridiques ou de leurs chevauchements. Le **projet de Code pénal** vise à criminaliser les agressions sexuelles numériques, l'usurpation d'identité électronique (utilisation de données personnelles dans le but de porter atteinte à l'honneur ou à la considération des personnes en publiant leurs photos et identifiants personnels et en diffusant des contenus offensants), la diffusion de contenus intimes sans consentement—ce qui est internationalement connu sous le terme de **"revenge porn" (pornographie de vengeance)**—ainsi que la lutte contre le phénomène du **deepfake (hypertrucage)**. Le projet offre également une protection pénale renforcée pour les enregistrements, propos ou informations captés dans un lieu privé, avec doublement de la peine s'il s'agit d'images ou d'informations de nature sexuelle (articles 447-1, 447-2 et 447-3), criminalise la capture, transmission ou diffusion de la localisation d'une personne sans son consentement, criminalise l'ouverture, suppression, retard ou détournement d'appels ou de correspondances électroniques de mauvaise foi, l'interception, détournement ou divulgation de correspondances, et l'installation de dispositifs permettant ces interceptions. Plus important encore, le projet **criminalise la vente, fourniture ou importation d'outils techniques** utilisés pour

commettre ces infractions ou même leur publicité—ce qui cible directement le modèle du **"Cybercrime-as-a-Service" (Cybercriminalité en tant que service)**.

Néanmoins, **malgré ces avancées substantielles et les réformes en cours, le cadre actuel présente des limites** face aux défis spécifiques posés par les métavers sociaux :

Premièrement - Proportionnalité des sanctions : Les sanctions pénales demeurent disproportionnées par rapport à l'ampleur des violations et aux capacités des multinationales. **L'amende maximale de 200 000 dirhams (environ 20 000 dollars américains) prévue par l'article 607-4 du Code pénal représente à peine 0,0001% des revenus annuels d'une plateforme comme Roblox (15 milliards de dollars en 2024),** soit l'équivalent d'une heure seulement de chiffre d'affaires, alors que le Digital Services Act européen prévoit des sanctions pouvant atteindre 6% du chiffre d'affaires mondial (soit 900 millions de dollars potentiels pour une entreprise comme Roblox).

Deuxièmement - Champ d'application territorial : La Loi n° 05-20 relative à la cybersécurité ne mentionne pas explicitement les systèmes d'information des entités privées dans son champ d'application.

Troisièmement - Concepts spécifiques aux environnements immersifs : Bien que le projet de Code pénal prévoie la criminalisation des agressions sexuelles numériques, de l'usurpation d'identité, de la diffusion de contenus intimes et du deepfake, les concepts juridiques fondamentaux **spécifiques aux environnements immersifs** demeurent absents du droit positif marocain : le **"grooming"** (approche prédatrice progressive des mineurs dans les espaces virtuels), la **"manipulation algorithmique"** (exploitation des biais cognitifs des enfants par l'intelligence artificielle), et la **"facilitation des violations"** (responsabilité des plateformes pour les dommages systémiques résultant de choix de conception).

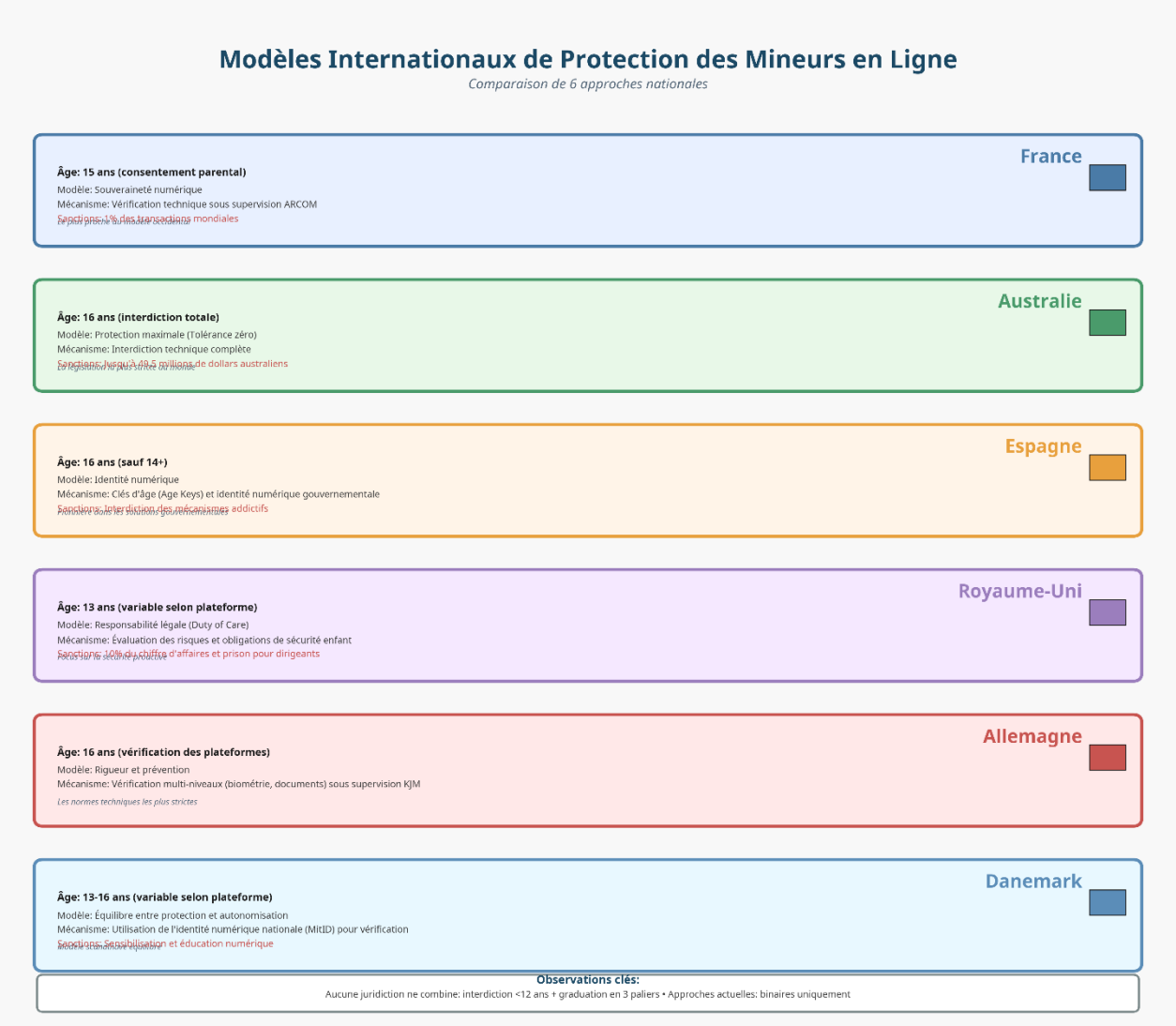
Quatrièmement - Obligations préventives imposées aux plateformes : L'absence d'obligations préventives imposées aux plateformes opérant hors du territoire national concernant l'**évaluation des risques systémiques** menaçant les mineurs, la **modération proactive par intelligence artificielle** des contenus et interactions, le **signalement obligatoire** des contenus criminels aux autorités nationales, et la **responsabilité pour les choix de conception** (dark patterns, algorithmes addictifs, économies de microtransactions impulsives, jeux d'argent déguisés) figure parmi les points essentiels à aborder en cohérence avec les normes internationales (Digital Services Act européen, UK Online Safety Act britannique) qui imposent un **"duty of care" (devoir de diligence)** mesurable envers les utilisateurs vulnérables, avec sanctions dissuasives en cas de manquement.

Hiérarchie d'efficacité des interventions

L'analyse comparative de seize juridictions établit une hiérarchie d'efficacité des interventions[26] : la supervision parentale active pourrait réduire les risques de 67% (contrôles techniques, dialogue régulier, co-utilisation), la protection "by design" de 45% (vérification d'âge robuste, séparation des espaces, modération proactive IA), les sanctions financières dissuasives de 23% (amendes proportionnées aux revenus), et l'autorégulation industrielle de 8% (codes de conduite volontaires, certification autodéclarée).

Le Digital Services Act (DSA) européen impose six obligations aux très grandes plateformes[27] : évaluation annuelle des risques systémiques, atténuation mesurable, audits indépendants, interfaces enfants "by design", transparence algorithmique, et coopération avec autorités. Roblox UK, après mise en conformité DSA, a enregistré une réduction de 34% des signalements d'abus entre 2023 et 2024[28]. Le UK Online Safety Act (2023) introduit un "duty of care" envers les utilisateurs mineurs[29], avec obligation de résultats mesurables. Les premières évaluations (décembre 2024) montrent une réduction de 28% des contenus préjudiciables signalés.

L'Australie a adopté en novembre 2024 une interdiction d'accès aux réseaux sociaux pour les moins de 16 ans[30], avec sanctions pouvant atteindre 50 millions AUD. Les projections gouvernementales anticipent une réduction de 43% de l'exposition aux risques en ligne dans les 24 mois. Le Danemark est devenu en novembre 2025 le premier État membre de l'UE à imposer un âge minimum de 15 ans, avec une exception pour les 13-15 ans sous consentement parental éclairé[31], citant des données nationales : 94% des moins de 13 ans possèdent des profils sur des plateformes interdites, 60% des garçons rapportent un sentiment d'isolation accru, et 15% présentent des diagnostics psychiatriques liés à l'usage des réseaux sociaux.



Le Parlement européen a adopté le 26 novembre 2025 une résolution recommandant 16 ans comme âge minimum harmonisé pour l'accès aux réseaux sociaux dans l'Union européenne[32], avec un seuil absolu de 13 ans. Le vote (483 voix pour, 92 contre, 86 abstentions) reflète un consensus politique. La résolution s'appuie sur un Eurobaromètre 2025 révélant que 90% des parents européens considèrent urgent de réguler l'accès des mineurs, 97% des 13-17 ans utilisent quotidiennement les réseaux sociaux, 78% des parents s'inquiètent du temps d'écran, et 25% des adolescents présentent des signes d'addiction avérée.

Orientations stratégiques recommandées

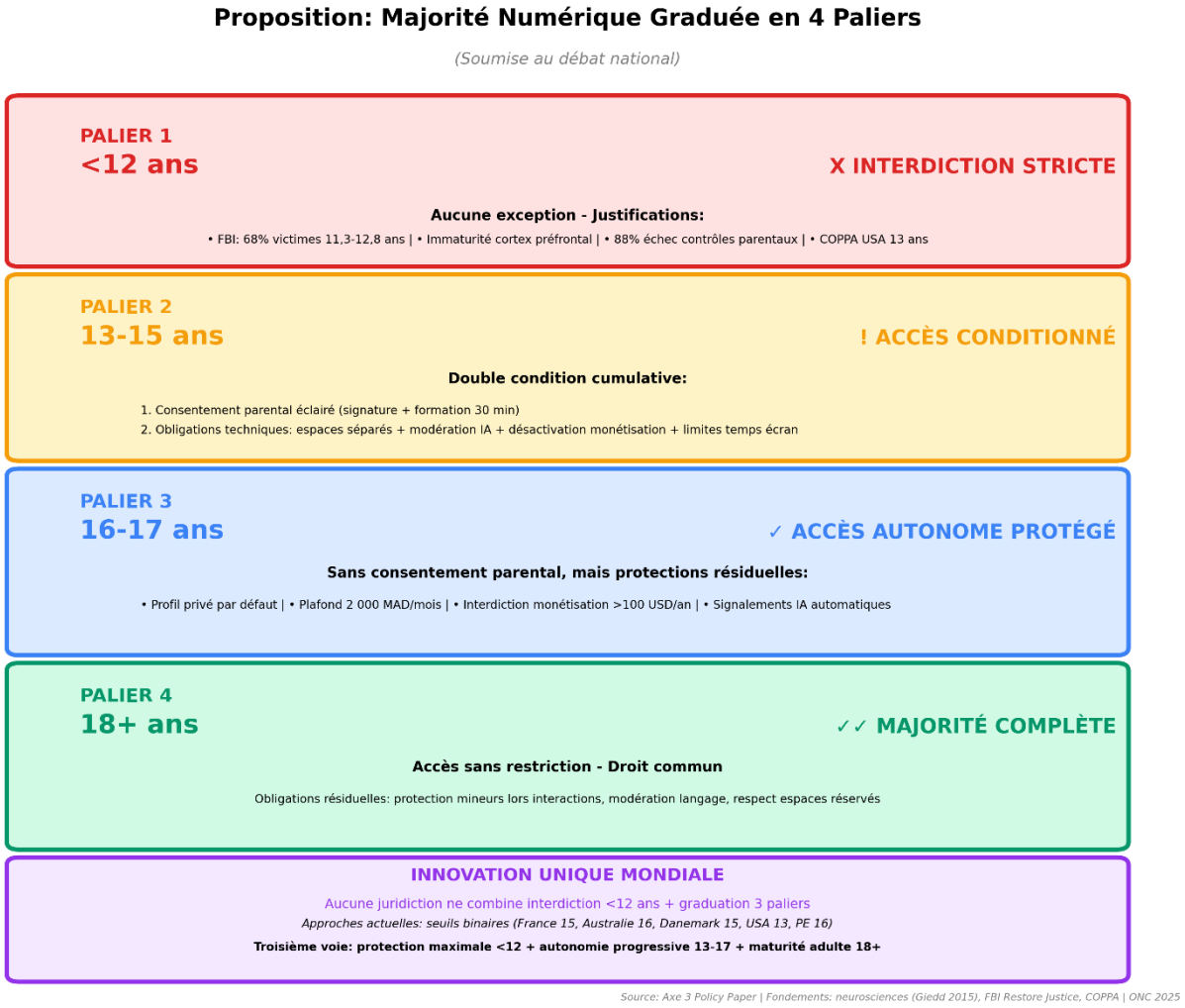
Ces constats orientent cinq axes de réflexion pour le contexte marocain, formulés à titre préliminaire pour éclairer le débat institutionnel et sociétal :

(1) Réforme du cadre juridique avec introduction de sanctions proportionnées au chiffre d'affaires des plateformes et création de qualifications pénales spécifiques aux

environnements immersifs (grooming, manipulation algorithmique, facilitation d'infractions).

(2) Architecture institutionnelle de supervision relevant du débat national quant à la configuration optimale : élargissement des attributions de régulateurs existants (ANRT, DGSSI), création d'une institution dédiée spécialisée, ou modèle hybride de coordination interministérielle renforcée.

(3) Réflexion sur une majorité numérique graduée en quatre paliers (<12 ans interdiction stricte, 13-15 ans accès conditionné sous supervision parentale, 16-17 ans accès autonome avec protections résiduelles, 18+ majorité complète) — proposition conceptuelle unique au niveau international, soumise au débat national et nécessitant validation par consensus entre acteurs institutionnels, société civile, secteur privé, et experts.



(4) Mécanismes d'application aux plateformes extraterritoriales via obligations de représentation locale, services bancaires nationaux, et procédure d'escalade progressive en cas de non-conformité.

(5) Positionnement régional du Maroc comme potentiel leader africain de la régulation responsable, via organisation d'un sommet annuel, transfert de compétences, et coopération opérationnelle accélérée.

Ces orientations visent à concilier efficacité protectrice, respect des spécificités culturelles marocaines, et maintien de l'attractivité du Maroc comme hub numérique régional.

⚠ Avertissement méthodologique

Une méthodologie multi-sources combinant l'analyse quantitative et qualitative a été adoptée. Toutefois, il convient de signaler trois limites méthodologiques :

Premièrement, compte tenu de la limitation des données statistiques nationales exhaustives et actualisées de manière continue sur l'utilisation du métavers chez les mineurs au Maroc, le recours s'est fait à des indicateurs indirects issus du Conseil Économique, Social et Environnemental (CESE), de la plateforme E-Blagh de la Direction Générale de la Sûreté Nationale, et du Haut-Commissariat au Plan (HCP), avec des projections et un croisement de données provenant de différentes sources d'organisations de la société civile et de certaines plateformes spécialisées nationales et internationales.

Deuxièmement, le recours s'est fait à des données internationales (opérations d'Europol et Interpol, FBI Restore Justice, études en neurosciences) avec une application prudente au contexte marocain.

Troisièmement, les recommandations présentées représentent des orientations générales nécessitant des études complémentaires approfondies.

Ce policy paper vise à ouvrir un débat national éclairé, tout en fournissant un point de départ pour un processus consultatif inclusif.