

Ensemble de principes communs aux membres du G7 définissant un espace numérique plus sûr et plus protecteur pour les mineurs

1. Nous, ministres du G7 chargés du Numérique et des Technologies, nous engageons à œuvrer en faveur d'un espace numérique plus sûr et plus protecteur pour les mineurs – les enfants et les adolescents. Afin de préserver leur bien-être physique, mental et cognitif ainsi que leur développement, des principes pérennes sont nécessaire pour orienter nos efforts continus pour protéger les mineurs contre un large éventail de risques, l'engagement des fournisseurs de services numériques en faveur de la sécurité en ligne, et nos objectifs communs de protection de la sécurité, la vie privée, la liberté d'expression en ligne, des droits de l'homme et des libertés fondamentales. Ces principes contribueront à donner les moyens nécessaires aux parents, aux familles, aux tuteurs, aux professionnels de santé et aux enseignants pour que les mineurs puissent bénéficier pleinement des nouvelles technologies et vivre des expériences en ligne en toute sécurité.

2. Les services numériques peuvent constituer un puissant outil d'apprentissage, de découvertes et d'échanges. En outre, le fait que les mineurs, les tuteurs et les enseignants disposent de compétences numériques et d'une éducation à l'IA peut aider les mineurs à aborder en confiance le monde numérique et à en tirer profit. Toutefois, des inquiétudes ont été exprimées, notamment par la communauté scientifique, concernant les risques pour les mineurs liés aux temps d'écran excessifs et à l'utilisation de certains services numériques intégrant des fonctionnalités conçues pour capter l'attention et maximiser l'engagement, qui menacent la santé physique et mentale des mineurs, ainsi que leur vie privée, leur sécurité, leur bien-être et leur développement cognitif et social. Cela peut conduire à des pratiques et des comportements problématiques, notamment compulsifs et addictogènes, susceptibles d'affecter leur estime de soi et compromettre encore davantage leur santé.

En l'absence d'actions communes et d'approches globales incitant les fournisseurs de services numériques, les gouvernements et les tuteurs à renforcer la sécurité en ligne, les mineurs peuvent également être exposés à des contenus ou à des interactions illégaux ou inappropriés à leur âge sur les services numériques, qui portent atteinte à leur santé mentale et à leur bien-être. Cela inclut notamment l'exposition au cyberharcèlement, au pédopiéage (*grooming*), à l'automutilation, au recrutement par des groupes criminels organisés, aux activités criminelles, aux sollicitations à des fins sexuelles illicites ou non consenties, à l'exploitation et aux abus sexuels et aux activités criminelles liées à la diffusion non consentie d'images intimes.

Les nouvelles technologies telles que l'IA générative, notamment les agents conversationnels (*chatbots*), bien que présentant des avantages, peuvent reproduire ou exacerber, sous de nouvelles formes, les risques existants auxquels sont exposés les mineurs. La diffusion non consentie d'images intimes, les contenus à caractère pédopornographique générés par IA, les contenus d'exploitation sexuelle ou pornographiques et les contenus ou interactions trompeurs, violents ou coercitifs, tels que les hypertrucages (*deepfake*) et les interactions simulées à des fins de manipulation suscitent des préoccupations particulières. Ces risques, qui portent atteinte à la santé et la sécurité des mineurs, renforcent la nécessité pour les mineurs d'être en mesure de reconnaître les contenus synthétiques, d'identifier la provenance des contenus et de développer leurs compétences numériques essentielles pour s'engager de manière responsable dans les espaces numériques. Dans la mesure où ces technologies ne cessent de se développer et de se diffuser, un soutien doit être apporté aux citoyens pour accroître leurs culture et compétences numériques afin de pouvoir évoluer et interagir dans les espaces numériques de manière critique et responsable. Des principes doivent également être définis pour orienter la réponse des pouvoirs publics afin de mieux protéger les mineurs en situation de vulnérabilité contre les risques susmentionnés et de renforcer la collaboration continue entre les parties prenantes.

3. Nous, ministres du G7 chargés du Numérique et des Technologies, nous engageons à réaffirmer les principes suivants définissant un espace numérique plus sûr et plus protecteur pour les mineurs.

Principe 1 : Un contrôle effectif de l'âge est indispensable pour garantir aux mineurs une expérience plus sûre, sécurisée et adaptée à leur âge. La mise en œuvre de ce principe repose sur des solutions de vérification de l'âge robustes, fiables, fondées sur les risques, appropriées, respectueuses des droits et de la vie privée et interopérables, et devrait constituer une mesure visant à faciliter une expérience en ligne adaptée à l'âge des mineurs et à prévenir leur exposition à des services ou produits en ligne qui leur sont interdits, tels que la pornographie, l'alcool ou le tabac, et à des services en ligne qui présentent des risques pour les mineurs, conformément aux lois nationales en vigueur. La protection de la liberté d'expression et de la vie privée étant un élément central de la protection des mineurs en ligne ainsi qu'un droit et une liberté fondamentale, le contrôle de l'âge devrait être mis en œuvre de manière à permettre, lorsque nécessaire, le consentement parental, et le respect des obligations légales au moyen de systèmes les moins intrusifs possibles, appropriés, respectueux de la vie privée, équitables et techniquement réalisables.

Principe 2 : Protéger les mineurs des dangers en ligne grâce à des approches reposant sur le principe de sécurité dès la conception (*safety by design*), tels que des paramètres de protection et par défaut, y compris des outils de contrôle parental, qui permettent de prévenir l'exposition des mineurs à des contenus, interactions et fonctionnalités qui ne sont ni adaptés à leur âge ni sûrs ni sécurisés. La confidentialité et la sécurité des comptes des mineurs devraient être garantis à travers des paramétrages par défaut, ainsi qu'en fournissant aux parents des outils leur permettant de gérer les paramètres par défaut des comptes de leurs enfants en matière de confidentialité et de sécurité, en aidant les mineurs et les parents à limiter le temps passé sur les écrans et en protégeant les mineurs contre des risques spécifiques, comme la géolocalisation ou les sollicitations non consenties, et contre des fonctionnalités entraînant une utilisation compulsive ou addictive. En outre, les gouvernements devraient collaborer avec le secteur privé, la société civile et les chercheurs afin d'alimenter les discussions sur ces paramètres.

En particulier, il est essentiel, s'agissant des mineurs, que les systèmes de recommandation, lorsqu'ils sont utilisés, soient conçus de manière à privilégier des contenus adaptés à leur âge et à limiter leur exposition aux risques. Ces systèmes ne devraient pas être conçus pour capter l'attention et maximiser l'engagement des mineurs en ligne, mais, au contraire, donner aux parents et aux mineurs des outils de paramétrage leur permettant de mieux contrôler leurs expériences et leurs données en ligne.

Principe 3 : La création et la diffusion de contenus pédopornographiques ainsi que les activités criminelles liées aux images intimes non consenties doivent être empêchées, conformément aux obligations légales en vigueur dans les pays du G7. La création, la détention et la diffusion de contenus pédopornographiques sont illégales dans tous les pays du G7 et des mesures urgentes doivent être prises pour empêcher leur circulation à l'échelle mondiale et pour garantir les droits des victimes et des survivants. Cela inclut la lutte contre les contenus pédopornographiques et les images intimes non consenties générés par l'intelligence artificielle. Ce principe s'inscrit dans la continuité des actions prioritaires définies dans le plan d'action du G7 pour lutter contre l'exploitation, la violence et les abus sexuels en ligne (2021), qui encourage le secteur privé à adopter, au minimum, les principes volontaires pour contrer l'exploitation et les abus sexuels en ligne (2020). Ces principes établissent une base de mesures volontaires que les entreprises peuvent mettre en œuvre pour faire face à l'ampleur et à la nature de ces crimes. Le partage et la diffusion continue d'images intimes non consenties, notamment celles générées par l'IA, renforcent l'urgence de prendre des mesures de prévention concrètes. Étant donné que ces violences peuvent entraîner des traumatismes prolongés, il est essentiel d'offrir un accompagnement et un soutien adaptés aux victimes et survivants, et de doter des moyens nécessaires à leurs enquêtes les autorités chargées de l'application de la loi.

Principe 4 : Les parents, tuteurs et autres personnes en charge de mineurs devraient disposer d'outils de contrôle parental simples d'utilisation, efficaces, respectueux de la vie privée, interopérables lorsque cela est techniquement possible, afin de les aider dans l'accompagnement et l'autonomisation des mineurs en ligne. Des outils performants aident les parents et les tuteurs à gérer les paramètres de confidentialité et de contrôle des comptes de leurs enfants, leur temps d'écran et leur exposition aux contenus. Les fournisseurs de services numériques et les gouvernements devraient proposer des campagnes de sensibilisation et d'éducation pour promouvoir les compétences numériques et les outils numériques, ainsi qu'aider les familles à mieux naviguer dans les environnements numériques pour en tirer pleinement parti. Ces outils complémentaires devraient être efficaces, conformes aux cadres juridiques applicables et respectueux des droits. Ils peuvent être développés en coopération avec des professionnels de santé, les communautés éducatives et tout autre acteur concerné.

Principe 5 : Les mineurs devraient bénéficier d'une éducation complète axée sur l'acquisition des connaissances et des compétences nécessaires à une meilleure compréhension des systèmes numériques, ainsi qu'à l'exercice d'un esprit critique vis-à-vis des technologies numériques, des médias et de l'information, utiles à la reconnaissance des risques en ligne et à leur épanouissement dans l'environnement numérique. En outre, les fournisseurs de services numériques devraient mettre à la disposition des parents et des enfants des outils, des paramètres et des fonctionnalités accessibles, ainsi que des outils efficaces de gestion du temps d'écran. Ceux-ci devraient améliorer la transparence pour les utilisateurs de la collecte des données, les sensibiliser à la manière dont ces données sont exploitées en vue de personnaliser ou d'orienter leur expérience, et leur fournir des options claires pour modifier leurs paramétrages afin qu'ils puissent prendre des décisions éclairées et autonomes concernant l'utilisation de ces systèmes. Ce principe peut aussi être renforcé en développant les compétences numériques en matière d'IA et en s'assurant que les utilisateurs, en particulier les mineurs, soient capables d'identifier de façon transparente les contenus synthétiques et leur provenance grâce à des moyens techniques.

Bien que des progrès aient été accomplis, les fournisseurs de services numériques devraient continuer à innover pour renforcer la protection des mineurs dans les espaces numériques. Cela implique d'élaborer des conditions générales d'utilisation claires et accessibles aux mineurs, de mener des actions de sensibilisation en recourant à un langage adapté à leur âge pour leur expliquer les risques potentiels liés aux différentes technologies, de mettre à disposition des leviers pour développer les compétences numériques, d'élaborer des stratégies d'atténuation des risques et de faciliter les signalements de contenus ou comportements illicites par les mineurs, parents et tuteurs à travers des mécanismes facilement accessibles.

Principe 6 : La sécurité des mineurs est garantie par la mise en œuvre de mesures de gestion, d'évaluation et d'atténuation des risques, et en se référant au principe de sécurité par la conception. Conformément aux obligations légales en vigueur dans les pays du G7, les services numériques devraient poursuivre des efforts soutenus pour évaluer et atténuer tous les types de risques et adapter leurs cadres de protection, par exemple par des mesures spécifiques d'atténuation des risques, des systèmes d'alerte rapide, notamment en cas d'activités criminelles, des ressources d'aide clairement identifiées et des mécanismes de signalement adaptés aux mineurs. Afin d'éviter que les innovations ne soient éclipsées par les risques, les fournisseurs de services numériques devraient promouvoir une transparence significative sur les pratiques et les mesures de protection prises tout au long de la conception et du développement des produits et services, notamment celles garantissant les droits de l'Homme et les libertés fondamentales des mineurs et de leurs parents, et en veillant qu'ils soient adaptés à l'âge des utilisateurs et préservent la sécurité, l'autonomie et le développement sain des mineurs. Enfin, ils doivent soutenir une approche fondée sur des preuves en matière de sécurité des mineurs.

Principe 7 : L'élaboration d'un espace numérique plus sûr et plus protecteur pour les mineurs est rendue possible par la coopération des fournisseurs de services numériques avec les parties prenantes concernées. Cette étroite coopération et ce dialogue entre les gouvernements et les parties prenantes, comprenant notamment la consultation et la collaboration avec les chercheurs, les parents, les tuteurs, les enseignants, les professionnels de santé, la société civile, les entreprises, les spécialistes du développement des enfants et des adolescents, les universitaires et, le cas échéant, les autorités publiques, sont essentiels pour remédier aux risques rencontrés en ligne susmentionnés et pour améliorer la compréhension des risques concernés. Afin de soutenir une approche fondée sur des preuves, la transparence et la responsabilité sont essentielles, tout comme l'analyse et l'évaluation impartiales des risques. La compréhension de ces risques peut être améliorée en permettant le partage de données avec les parties prenantes et en favorisant les approches fondées sur des preuves. Un socle commun de preuves et de données renforcera la pertinence de la recherche dans ce domaine et renforcera les solutions disponibles pour protéger les mineurs en ligne.

4. Nous, ministres du G7 chargés du Numérique et des Technologies, soutenons ces principes. À cette fin, tout en notant que les différentes juridictions peuvent adopter leurs propres approches pour mettre en œuvre ces principes directeurs :

- Nous appelons les fournisseurs de services numériques à traduire ces principes en actions, et à coopérer étroitement avec toutes les parties prenantes concernées pour établir des modalités concrètes d'application de ces principes.
- Nous affirmons qu'une approche fondée sur des données factuelles suppose de prendre en compte le point de vue des mineurs, des parents et des tuteurs au moment de la conception des politiques publiques qui les concernent et de garantir la protection des droits des mineurs dans l'environnement numérique.
- Nous nous engageons à favoriser les synergies et la coopération internationale entre les partenaires du G7 et les acteurs concernés, ainsi qu'à renforcer plus étroitement la coopération entre nos gouvernements, en vue d'appliquer les mesures nécessaires, respectueuses des droits et conformes à ces principes et de définir des domaines de recherche prioritaires communs afin de mieux caractériser et atténuer les risques susmentionnés.