48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée

Novembre 2026

Résolution sur l'intelligence artificielle dans le secteur de l'éducation

La présente résolution est soumise par l'équipe de rédaction du Groupe de travail sur l'éducation numérique au sujet de l'intelligence artificielle dans le domaine de l'éducation.

PARRAINEURS :

- Autorité catalane de protection des données, Catalogne
- Commission de protection des données personnelles, Bulgarie
- Commission nationale de l'informatique et des libertés, France
- Bureau d'inspection de la protection des données de l'Estonie
- Commissariat à l'information, Royaume-Uni
- Commissariat à l'information et à la protection de la vie privée de l'Ontario, Canada
- Commissariat à la protection de la vie privée pour les données personnelles, Hong Kong, Chine

COPARRAINEURS :

- Commissariat à la protection de la vie privée du Canada
- Agence d'accès à l'information publique, Argentine
- Commissaire à la protection des données et à la liberté d'information de Rhénanie-Palatinat, Allemagne
- Autorité de protection de la vie privée, Israël
- Commissariat à l'information et à la protection des données, Albanie
- Autorité de protection des données, Belgique
- Agence pour la protection des données, Croatie
- Commission nationale pour le contrôle et la protection des données personnelles, Maroc

À l'occasion de la 48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée qui a eu lieu en 2026 :

Reconnaissant le caractère transformateur de l'intelligence artificielle (IA) pour l'éducation, ainsi que la rapidité avec laquelle son adoption progresse chez les enseignants et éducateurs et les élèves[1] partout dans le monde;

Rappelant que les lois sur la protection des données et les principes de protection de la vie privée demeurent applicables aux technologies d'IA, tandis que diverses juridictions poursuivent l'élaboration de lois et de politiques propres à l'IA;

Reconnaissant qu'un des rôles essentiels des autorités de protection des données consiste à protéger les données et la vie privée des enfants, ceux-ci étant vulnérables et leurs données personnelles étant par nature sensibles;

Reconnaissant que les outils d'IA reposant sur la collecte, l'utilisation et la communication à grande échelle de données personnelles tout au long du cycle de vie de l'IA devraient être sûrs et robustes, depuis leur développement et leur entraînement jusqu'à leur déploiement ultérieur;

Reconnaissant que le contenu des interactions avec un système d'IA[2] reflète le niveau de connaissances et de compétence des enfants dans un domaine donné, ainsi que, le cas échéant, leurs processus de réflexion, leur jugement et leur esprit critique, et que ces éléments constituent des données personnelles, ce qui exige que les outils d'IA utilisés en éducation[3] soient transparents quant aux renseignements qu'ils recueillent et utilisent;

Reconnaissant que les enfants peuvent tirer des avantages des outils d'IA créés à des fins d'éducation (« IA en éducation[4] »), notamment sous les formes suivantes :

- apprentissage à distance;
- tutorat adaptatif axé sur des compétences particulières;
- soutien adapté aux difficultés d'apprentissage individuelles;
- accès accru à l'information et à la traduction;
- rétroaction en temps réel.

Reconnaissant que les enfants peuvent également être exposés à d'importants risques d'atteinte à la protection des données et à la vie privée découlant de l'utilisation de l'IA en éducation, notamment :

---

[1] Dans la présente résolution, les enfants s'entendent des individus âgés de moins de 18 ans inscrits aux deux premiers niveaux de l'éducation formelle.

[2] « Système d'IA » s'entend d'un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels – Recommandation du Conseil de l'OCDE sur l'intelligence artificielle .

[3] Dans la présente résolution, l'expression « outil d'IA » est utilisée dans un sens large pour désigner les applications de l'IA et de l'IA générative utilisées dans les contextes éducatifs, notamment les plateformes, les applications, les services et les technologies.

[4] « IA en éducation » s'entend de l'intégration de l'IA et de technologies avancées dans les environnements d'apprentissage.

- collecte et conservation inutiles et disproportionnées de données personnelles, y compris à des fins commerciales sans mesures de sécurité appropriées;
- choix limité quant aux utilisations secondaires de ces renseignements, notamment pour l'entraînement ou l'amélioration de l'IA, leur communication à des tiers ou d'autres utilisations commerciales;
- profilage, inférences et catégorisations susceptibles d'influer sur leur parcours éducatif, voire de le façonner de manière anticipée;
- conception favorisant la manipulation, y compris des fonctionnalités visant à maximiser l'engagement ou la collecte de renseignements permettant d'influencer plus efficacement les enfants en tant que public cible;
- informations inexactes, hallucinations de l'IA, contenu standardisé ou générique et recyclage de données;
- lacunes réglementaires concernant les mesures de protection juridique nécessaires pour que l'intérêt supérieur de l'enfant demeure au cœur des technologies éducatives;
- atteintes à la protection des données, lesquelles présentent des risques importants dans la mesure où les données personnelles peuvent être utilisées à des fins malveillantes (par exemple la cybercriminalité).

Reconnaissant que l'utilisation de l'IA peut avoir des répercussions sur l'écosystème de l'éducation dans son ensemble en :

- favorisant une approche excessivement normalisée de l'enseignement et de l'évaluation;
- normalisant l'utilisation par les enfants de technologies numériques commerciales ainsi que la communication, à l'extérieur du milieu éducatif, de données personnelles liées aux méthodes d'enseignement et aux résultats scolaires;
- exacerbant les inégalités en matière d'accès à un système d'IA et de son utilisation; les élèves ne bénéficient pas tous du même accès aux connaissances ni aux mêmes outils numériques à la maison.

Rappelant que le droit fondamental à la protection des données personnelles et à la vie privée suppose un degré élevé de choix, de contrôle et d'autonomie de la part de l'individu à l'égard de la collecte, de l'utilisation et de la communication de ses données personnelles;

Reconnaissant que les enfants sont titulaires de droits et que leur droit à l'autodétermination informationnelle doit être respecté, notamment au moyen de véritables possibilités de remettre en question les technologies éducatives qu'ils utilisent et la façon dont celles-ci font usage de leurs données personnelles, d'une manière adaptée à leur stade de développement et conforme à leurs droits à l'autonomie et à la dignité;

Soulignant que les recherches menées auprès des enfants démontrent clairement que ceux-ci expriment diverses préoccupations quant aux répercussions de l'IA sur leurs données personnelles, leur éducation, notamment la perte d'esprit critique attribuable au délestage cognitif, et leur vie en général, et qu'il importe non seulement de prêter attention à ce que disent les enfants, mais aussi de tenir compte de leurs points de vue, conformément à l'article 12 de la Convention des Nations Unies relative aux droits de l'enfant;

Rappelant la reconnaissance croissante et répandue à l'échelle internationale des risques importants auxquels sont exposées les jeunes générations qui grandissent dans un environnement numérique où l'IA est de plus en plus intégrée, ainsi que la nécessité de mettre en place des mesures de sécurité rigoureuses et adaptées à l'âge en matière de protection de la vie privée afin de protéger les enfants et les jeunes dans les milieux de l'éducation, comme en témoignent les sources internationales pertinentes ainsi que les résolutions et documents de l'Assemblée mondiale pour la protection de la vie privée énumérés à l'annexe 1;

Reconnaissant que les outils d'IA à usage général et, plus largement, les technologies utilisées en éducation évoluent dans un contexte où les partenariats public-privé et les processus de passation de marchés constituent la norme, ce qui peut faire en sorte que les objectifs commerciaux liés aux données ne concordent pas toujours avec ceux de l'enseignement public;

Affirmant qu'il incombe aux gouvernements de veiller à ce que l'intérêt supérieur de l'enfant, y compris la protection de ses données et de sa vie privée, soit pris en considération lors de l'évaluation et de l'autorisation de l'IA en éducation;

Insistant sur le fait que les enfants méritent une protection particulière dans les contextes éducatifs et sur le rôle essentiel que jouent les établissements d'enseignement dans leur vie, compte tenu notamment :

- de leur statut de titulaires de droits distincts en vertu de la Convention relative aux droits de l'enfant;
- du caractère obligatoire de la fréquentation d'un établissement d'enseignement pendant de nombreuses années pour la plupart des enfants;
- du rôle particulier des établissements d'enseignement comme milieux de confiance favorisant l'apprentissage, l'épanouissement affectif et le développement des enfants, notamment en leur offrant la possibilité de faire des erreurs, d'explorer des idées et d'évoluer au fil du temps;
- des répercussions que la collecte, l'utilisation ou la communication inappropriée de données peuvent avoir, dans le milieu scolaire, sur le bien-être social et affectif des enfants ainsi que sur leur avenir;
- du rôle important de l'éducation dans le développement de la littératie numérique en tant que composante fondamentale de la vie contemporaine, ce qui suppose que les générations futures acquièrent des connaissances en matière d'IA et de données et soient préparées à comprendre les limites et les risques des outils d'IA, à les utiliser de façon responsable et critique et à se protéger contre les préjudices susceptibles de découler de leur utilisation.

Reconnaissant que les besoins et les capacités des enfants évoluent rapidement et de façon marquée tout au long de leur parcours d'éducation formelle, et que cette évolution devrait être prise en compte dans les décisions visant à déterminer si, quand et comment des outils et technologies d'IA sont introduits dans leurs environnements d'apprentissage, de manière à ce que ces décisions soient toujours fondées sur l'intérêt supérieur de l'enfant;

Affirmant qu'une bonne gouvernance des données à l'égard des technologies et des outils d'IA dans les contextes éducatifs constitue un fondement essentiel de la protection des données personnelles et de la vie privée, de la sécurité, de l'égalité, de l'autonomie et de la dignité des enfants;

Affirmant que tous les outils d'IA approuvés pour une utilisation dans les contextes éducatifs doivent être valides et fiables, sûrs, respectueux de la vie privée, respectueux des droits de la personne, transparents et responsables. Les outils d'IA devraient être évalués afin de déterminer s'ils conviennent aux contextes éducatifs et il devrait être démontré qu'ils contribuent à l'atteinte d'objectifs pédagogiques tout en réduisant au minimum les risques pour la protection es données et la vie privée et la sécurité des enfants;

Affirmant que toute décision d'acquérir ou d'utiliser l'IA dans les contextes éducatifs devrait tenir compte de la protection des données et de la vie privée et de la sécurité, et que les principes de nécessité et de proportionnalité doivent être respectés chaque fois qu'un système d'IA traite des données personnelles;

Reconnaissant l'importance cruciale de protéger les données personnelles sensibles des enfants vulnérables et de ne pas conserver leurs informations plus longtemps que nécessaire, afin d'atténuer le risque d'atteintes à la protection des données susceptibles d'avoir des conséquences durables sur la vie privée et de compromettre de façon permanente leur sécurité, aujourd'hui et à l'avenir;

Reconnaissant que les enfants, en tant que principaux titulaires de droits impactés par l'utilisation de l'IA en éducation, ainsi que leurs tuteurs légaux, devraient recevoir de l'information, de la formation et des orientations adaptées à leur situation afin de développer leur esprit critique à l'égard de l'utilisation de l'IA. Les élèves devraient également avoir accès à un soutien et à des mécanismes leur permettant de poser des questions, de contester des décisions, de demander une intervention humaine et d'exercer leurs droits. Dans la mesure du possible, les enfants devraient avoir la possibilité de prendre part de façon significative aux discussions et aux décisions concernant l'utilisation des outils d'IA en éducation qui les concernent;

Reconnaissant que de nombreux acteurs interviennent dans la conception, le développement, la fourniture, le déploiement, la surveillance et l'utilisation des outils d'IA en éducation tout au long du cycle de vie de l'IA, et qu'ils ont des responsabilités distinctes en ce qui concerne le respect des droits fondamentaux des enfants, la protection de leurs données personnelles et le maintien d'environnements d'apprentissage sûrs, équitables et adaptés à leur développement. Les acteurs suivants ont des responsabilités particulières à cet égard :

- **Les fournisseurs de technologies éducatives et les développeurs d'IA**, y compris les sous-traitants et les sous-traitants ultérieurs, devraient veiller à ce que les outils d'IA en éducation soient conçus et déployés dans le respect des droits de l'enfant, des lois et exigences applicables en matière de protection des données et de la vie privée dans les juridictions concernées, ainsi que des cadres mondiaux ou régionaux applicables. Cela comprend la transparence concernant les catégories de données personnelles traitées et les finalités de leur traitement, notamment lorsque ces données sont utilisées pour entraîner ou améliorer des systèmes d'IA, ainsi que la mise en place de mesures de sécurité appropriées à l'appui du caractère licite et équitable du traitement, de l'exactitude et de la minimisation des données, de la limitation des finalités, de la sécurité et du respect des droits des personnes concernées.
- **Les législateurs, les ministères de l'Éducation, les autorités locales et les autres organismes publics** responsables de l'adoption des lois, de l'élaboration des politiques en matière d'éducation ou de l'imposition d'outils d'IA devraient veiller à ce que leurs instruments et

leurs décisions soient conformes aux pratiques exemplaires internationales ainsi qu'aux exigences applicables en matière de protection des données et de la vie privée.

- **Les responsables des établissements d'enseignement**, y compris les écoles et les organismes responsables de l'éducation de la petite enfance, qui acquièrent, approuvent ou utilisent des outils d'IA en éducation et qui déterminent les finalités et les moyens du traitement des données personnelles, devraient respecter les obligations qui leur incombent au titre de responsables de traitement, notamment en ce qui concerne le caractère licite du traitement, la transparence, la minimisation des données, la sécurité, la responsabilité et les droits de l'enfant. Ils devraient également évaluer si chaque outil d'IA en éducation convient à l'usage auquel il est destiné et, lorsqu'il n'est pas possible d'atténuer les risques de façon adéquate ou les problèmes de conformité recensés, s'abstenir de l'utiliser.

- **Les enseignants et les autres professionnels de l'éducation** devraient utiliser les outils d'IA en éducation conformément aux exigences applicables en matière de protection des données et de la vie privée. Lorsqu'ils ne disposent pas des connaissances techniques nécessaires pour comprendre les risques que de tels outils présentent pour la protection des données et de la vie privée, y compris les outils d'IA gratuits ou non approuvés, les enseignants et les autres professionnels de l'éducation devraient recevoir un soutien et des lignes directrices appropriées, notamment sous forme de formation et d'information ciblées.

- **Les autorités de protection des données et de la vie privée** devraient, conformément à leur mandat respectif, fournir des lignes directrices aux parties prenantes concernées, promouvoir le respect des lois sur la protection des données et de la vie privée, et soutenir les activités d'éducation et de sensibilisation du public concernant les mesures de sécurité et les risques associés à l'IA en éducation. Elles devraient également veiller au respect des normes en matière de protection des données au moyen d'audits réguliers et de sanctions, lorsque cela s'avère nécessaire.

Reconnaissant que les droits à la protection des données et à la vie privée sont fondamentaux, mais que de nombreuses technologies d'IA sont conçues, entraînées, mises en œuvre et maintenues d'une manière qui peut entrer en conflit avec ces droits. Nous affirmons l'importance des principes fondamentaux suivants en matière de protection des données, qui devraient être respectés par tous les acteurs tout au long du cycle de vie de l'IA (y compris lors de la conception, du développement, de la sélection, de la fourniture, du déploiement, de la surveillance et de l'utilisation d'outils d'IA en éducation), conformément aux lois applicables sur la protection des données et de la vie privée :

1. L'intérêt supérieur de l'enfant en tant que préoccupation primordiale

- L'intérêt supérieur de l'enfant doit être une préoccupation primordiale pour tous les acteurs tout au long du cycle de vie de tout outil d'IA utilisé dans les contextes éducatifs. Aucun intérêt commercial, impératif opérationnel ou gain d'efficacité ne peut l'emporter sur ce principe. Une approche fondée sur les droits de l'enfant est nécessaire afin de protéger les enfants contre les préjudices potentiels associés à l'IA.

- Lorsque l'utilisation d'un outil d'IA est imposée par l'établissement d'enseignement et qu'elle est obligatoire pour les élèves, tous les acteurs concernés doivent veiller à ce que cet outil soit sûr et respecte les droits de l'enfant.

- Lorsqu'ils évaluent l'intérêt supérieur de l'enfant, les acteurs responsables devraient déployer tous les efforts raisonnables pour concilier le droit de l'enfant à la protection de la vie privée et les autres droits et intérêts susceptibles d'être impactés par le traitement de ses données personnelles, notamment le droit à la non-discrimination, le droit à l'éducation et le droit à être entendu.

2. Rôles et responsabilités

- Tous les acteurs qui interviennent à une étape ou une autre du cycle de vie d'un outil d'IA en éducation doivent définir leurs responsabilités ainsi que, s'il y a lieu, celles des autres parties participant au traitement des données personnelles des enfants (responsable de traitement, responsables conjoints du traitement, sous-traitants, sous-traitants ultérieurs ou autres fournisseurs de services). Le respect de ses obligations par un acteur ne dégage aucun autre acteur de ses propres responsabilités.
- Tous les acteurs qui conçoivent et développent des outils d'IA à des fins éducatives doivent se conformer aux exigences en matière de protection des données.
- Afin de faciliter le respect des obligations en matière de protection des données et de la vie privée, la personne à qui sont confiées des responsabilités en la matière (par exemple le délégué à la protection des données) devrait être consultée dès les premières étapes de toute décision visant à développer ou à utiliser un outil d'IA.

3. Fondement juridique et limitation stricte des finalités

- Chaque acteur qui traite des données personnelles doit déterminer le fondement juridique applicable à chaque activité de traitement et s'y conformer, conformément aux lois applicables dans la juridiction concernée.
- Dans les contextes éducatifs, le consentement peut souvent ne pas être applicable, soit en raison d'un déséquilibre de pouvoir entre les parties concernées, soit en raison de restrictions prévues par les lois applicables, par exemple lorsque le fondement juridique du traitement est l'exécution d'une mission d'intérêt public ou l'exercice de l'autorité publique dont est investi le responsable du traitement.
- Lorsque le consentement constitue le fondement juridique du traitement des données, il doit être donné librement, pour des finalités précises, de façon éclairée et sans équivoque. Les informations fournies aux enfants ou à leurs tuteurs légaux devraient être clairs et faciles à comprendre, d'une manière adaptée à l'âge et au degré de maturité de l'enfant. Lorsque le consentement du tuteur légal est requis ou approprié conformément au cadre juridique applicable, il convient de tenir compte de l'âge de l'enfant, de son stade de développement et de l'évolution de ses capacités dans la façon dont ce consentement est obtenu et exercé, et celui-ci ne devrait pas supplanter les droits de l'enfant ni sa participation dans la mesure prévue par les lois applicables.
- Les enfants ou leurs tuteurs légaux ne devraient subir aucune conséquence négative s'ils refusent de donner leur consentement. Si un refus de consentement risque d'entraîner des

conséquences négatives, d'autres options susceptibles d'offrir des effets et des conséquences comparables doivent être proposées aux enfants et à leurs tuteurs légaux.

- Lorsque les intérêts légitimes constituent le fondement juridique du traitement des données, les intérêts commerciaux de l'entité qui fournit le service d'IA doivent être conciliés avec l'intérêt supérieur de l'enfant ainsi qu'avec ses droits et libertés, et le traitement ne devrait avoir lieu que lorsque cette conciliation favorise l'intérêt supérieur de l'enfant. Dans ce contexte, le traitement ne devrait avoir lieu que lorsque les intérêts légitimes poursuivis par le responsable du traitement ne l'emportent pas sur l'intérêt supérieur de l'enfant ni sur ses droits et libertés fondamentaux, compte tenu tout particulièrement du fait que la personne concernée est un enfant. Dans le cas contraire, ce traitement ne devrait pas être effectué.

- Les données des enfants recueillies ou déduites au moyen d'outils d'IA en éducation ne doivent pas être utilisées pour des finalités commerciales ou publicitaires. Lorsqu'il existe, conformément aux lois applicables, un fondement juridique approprié et une finalité éducative définie, l'amélioration d'un produit ou l'entraînement d'un modèle d'IA ne devraient avoir lieu que lorsqu'ils sont réalisés au bénéfice des enfants et dans leur intérêt supérieur.

- Les fonctionnalités d'IA supplémentaires ou facultatives qui ne sont pas directement liées à la fonction éducative, ou dont il n'a pas été démontré qu'elles sont sûres, respectueuses de la protection des données et de la vie privée et bénéfiques sur le plan pédagogique, ne devraient pas être activées dans les contextes éducatifs.

4. Évaluation d'impact relative à la protection des données et aux risques pour la vie privée

- Les évaluations d'impact relatives à la protection des données et aux risques pour la vie privée peuvent être obligatoires et constituent, dans tous les cas, une pratique exemplaire pour tous les outils d'IA en éducation, avant leur déploiement et lors de leur mise à jour.
- Les évaluations ainsi que, le cas échéant, les mesures d'atténuation mises en œuvre devraient être documentées et mises à la disposition des autorités de contrôle sur demande. Au besoin, certaines parties de l'évaluation devraient être mises à la disposition des enseignants et éducateurs et des autres personnes concernées.

- Les évaluations exigent que tous les acteurs participant à la conception et au développement de l'outil d'IA fournissent tous les renseignements nécessaires (par exemple les caractéristiques, les capacités et les limites de rendement de l'outil d'IA). Cette exigence s'applique à l'ensemble de la chaîne d'approvisionnement de l'IA, y compris à l'utilisation, à l'adaptation, à l'intégration, à la mise à jour et à la surveillance des systèmes d'IA.

- Les évaluations des outils d'IA devraient faire l'objet d'un examen périodique à mesure que les circonstances évoluent et être fondées sur une approche tenant compte non seulement des risques pour le droit la protection des données et à la vie privée, mais également des incidences sur d'autres droits et intérêts fondamentaux pouvant découler du traitement des données et entraîner un préjudice réel ou potentiel, qu'il soit physique, matériel ou moral.

Ces préjudices peuvent notamment prendre la forme de discrimination, d'une atteinte à la confidentialité des données personnelles, de la réidentification non autorisée de personnes à partir de données pseudonymisées ou anonymisées, ou de tout autre préjudice important. Cela comprend également les situations où les enfants risquent d'être privés de leurs droits et libertés ou de se voir privés du contrôle de leurs données personnelles.

5. Protection de la vie privée dès la conception et par défaut

- Tous les développeurs et fournisseurs d'outils d'IA destinés à être utilisés à des fins éducatives ou susceptibles d'être utilisés dans des contextes éducatifs doivent intégrer les droits de l'enfant comme exigence fondamentale de conception et de gouvernance dès les premières étapes du processus de conception, afin de servir l'intérêt supérieur de l'enfant. Ils doivent notamment :

  a) appliquer les principes de protection de la vie privée dès la conception, y compris ceux de sécurité dès la conception ou de conception adaptée à l'âge, en veillant à ce que les paramètres par défaut ne permettent la collecte ou la déduction du strict minimum de données nécessaires à la fonction éducative, prévoient un mécanisme permettant de supprimer toute donnée inutile et désactivent par défaut toutes les fonctionnalités non éducatives ainsi que celles conçues pour prolonger l'engagement ou accroître la communication de données;

  b) définir avec précision les contrôles d'accès. Il devrait être clairement établi qui peut avoir accès aux données ou aux résultats produits par un système d'IA donné. Cela comprend des précisions concernant l'accès accordé aux enseignants et éducateurs, à l'administration, aux développeurs et aux autres parties;

  c) exclure l'utilisation des données des élèves à des fins de profilage commercial, de publicité, d'amélioration de produits sans lien avec le service éducatif faisant l'objet du contrat ou d'entraînement de modèles commerciaux d'IA à usage général;

  d) faire preuve de diligence raisonnable à l'égard des droits de l'enfant et procéder à des évaluations des biais tout au long du cycle de développement et d'exploitation, y compris avant le déploiement, et mettre en œuvre, au besoin, des mesures d'atténuation pour remédier aux risques recensés;

  e) mettre en place une architecture de surveillance humaine garantissant que les fonctions qui ont des conséquences importantes présentent les résultats produits par l'IA comme des recommandations soumises à un examen par un humain, et non comme des décisions automatisées;

f) exclure dès la conception toute fonctionnalité incompatible avec les droits de l'enfant, notamment l'anthropomorphisation[5], l'obséquiosité, la manipulation subliminale, la notation sociale, la surveillance biométrique et la reconnaissance des émotions;

g) assurer une transparence complète concernant les flux de données, le recours à des sous-traitants ultérieurs, les limites relatives à l'exactitude, les résultats des essais de détection des biais et les risques connus, et communiquer ces renseignements aux organisations qui déploieront l'outil avant la signature du contrat.

- Sauf lorsqu'une exception juridique précise s'applique et que des mesures de sécurité supplémentaires sont en place, les outils d'IA ne devraient pas traiter de catégories particulières de données, telles que les données biométriques, les données relatives à l'origine ethnique déduites à partir de noms ou de la langue, ou les données de santé, y compris celles concernant les difficultés d'apprentissage ou l'état émotionnel d'un élève.

- Tous les acteurs qui utilisent des outils d'IA en éducation devraient recenser les mesures de protection des données et de la vie privée dès la conception et par défaut qui ont été intégrées à ces outils et veiller à ce qu'elles soient appliquées et mises en œuvre de manière appropriée et, au besoin, mettre en place des mesures de sécurité additionnelles adaptées au contexte particulier d'utilisation.

6. Exactitude des données et limitation de la durée de conservation

- Les données des enfants traitées par des systèmes d'IA devraient être exactes. Les erreurs découlant de données inexactes dans les évaluations produites par l'IA ou les profils d'élèves doivent pouvoir être corrigées.

- Les données des enfants ne devraient pas être conservées au-delà de la période strictement nécessaire à la réalisation de chaque finalité éducative déterminée. Des périodes de conservation clairement définies doivent être établies pour chaque catégorie de données d'élèves traitées par des outils d'IA, en tenant compte de l'intérêt supérieur de l'enfant.

- Les responsables de traitement devraient veiller à ce qu'à la fin du contrat ou de l'accord, les données des élèves soient retournées à l'établissement d'enseignement ou supprimées de façon définitive par le fournisseur ou le sous-traitant.

7. Prise de décisions automatisée

- Les décisions susceptibles d'avoir une incidence sur les enfants ne devraient pas reposer exclusivement sur des résultats générés par des systèmes de prise de décision automatisée

[5] « [L]es systèmes d'IA sont conçus pour interagir d'une manière anthropomorphique, ce qui peut conduire les utilisateurs à leur accorder une confiance excessive et à développer une dépendance psychologique, mais ces systèmes ne possèdent ni la compréhension, ni l'expérience, ni la capacité d'agir socialement, propres à l'être humain ». Conseil de l'Europe, Recommandation CM/Rec(2026)12 du Comité des Ministres aux États membres sur la littératie en intelligence artificielle (partie III, section A, paragraphe 14).

et devraient être soumises à un examen par un humain, particulièrement lorsqu'elles sont susceptibles d'entraîner des conséquences négatives.

- Lorsque la prise de décision automatisée fondée sur l'IA est utilisée dans des conditions licites, les organisations doivent faire de l'intérêt supérieur des enfants dont les données personnelles sont traitées une préoccupation primordiale et ne recourir à la prise de décision automatisée que lorsqu'elle est nécessaire, proportionnée à la finalité éducative poursuivie et qu'elle ne porte pas atteinte aux droits de l'enfant, notamment à ses droits à l'autonomie, à la liberté de pensée et d'expression, à l'accès à une diversité d'informations et au développement.
- La prise de décision automatisée fondée sur l'IA doit être transparente et explicable pour les enfants et leurs tuteurs légaux, notamment par la communication d'informations utiles sur la logique sous-jacente au traitement ainsi que sur son importance et ses conséquences prévues pour les personnes.
- Les enfants ou leurs tuteurs légaux doivent disposer d'un moyen clair et efficace d'exprimer leur point de vue et de contester la prise de décision automatisée.
- Des informations adaptées à l'âge de l'enfant concernant la nature de la décision, les systèmes utilisés, la logique sous-jacente ainsi que l'importance et les conséquences prévues de ce traitement (c'est-à-dire le résultat obtenu) pour l'enfant devraient être fournis.
- Lorsqu'une prise de décision automatisée est utilisée, il faut veiller à ce que les personnes chargées de superviser l'utilisation des outils d'IA qui y ont recours, reçoivent une formation adéquate. Les personnes chargées de la supervision de la prise de décision automatisée doivent être en mesure de comprendre les limites et les risques du système, y compris les biais qu'il peut comporter, les résultats qu'il produit et la façon dont ces résultats ont été obtenus. Elles doivent également être capables de déceler les erreurs et, au besoin, de modifier ou de rejeter les décisions du système d'IA.
- En tout état de cause, l'IA devrait soutenir, et non remplacer, la prise de décisions et la surveillance humaines; les professionnels responsables doivent conserver l'autorité, les compétences et la capacité concrète nécessaires pour remettre en question, modifier ou rejeter les résultats générés par l'IA.
- La littératie en matière d'IA doit être considérée comme une condition préalable pour garantir que les systèmes d'IA respectent les droits humains, la démocratie et l'état de droit.

8. Sécurité de l'information

- Les systèmes d'IA qui soutiennent l'apprentissage des enfants doivent offrir des garanties solides en matière de sécurité et de sûreté. Ils nécessitent des mesures de cybersécurité robustes, à condition que toute surveillance exercée à cette fin demeure proportionnée et ne porte pas inutilement atteinte à la protection des données et à vie privée des enfants, des élèves et du personnel enseignant.
- Il faut intégrer les principes de sûreté et de sécurité dès la conception afin d'anticiper, de repérer et d'éliminer de façon proactive les préjudices en ligne avant qu'ils n'aient des répercussions sur les enfants.

- Tous les acteurs qui interviennent à une étape ou une autre du cycle de vie d'un outil d'IA en éducation doivent appliquer des mesures de sécurité techniques et organisationnelles appropriées, proportionnelles aux risques et tenant compte de la vulnérabilité des enfants en tant que personnes concernées.

9. Transparence et obligation de rendre compte

- Les responsables du traitement sont tenus de veiller à ce que les outils d'IA respectent les principes et les obligations en matière de protection des données et de la vie privée.
- La transparence et la capacité d'expliquer les résultats produits par l'IA sont essentielles. Les systèmes d'IA utilisés en éducation devraient être suffisamment transparents pour permettre de comprendre leur fonctionnement, de retracer l'utilisation des données et d'expliquer les résultats qu'ils génèrent. Ils devraient également fournir des renseignements clairs sur l'utilisation des données et la surveillance humaine, dans un langage adapté aux enfants et aux jeunes.

- Les responsables du traitement devraient informer les enfants ou leurs tuteurs légaux, dans un langage adapté à l'âge de l'enfant, des éléments exigés par les lois applicables en matière de protection des données et de la vie privée, notamment :

  a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, celles du délégué à la protection des données;

  b) les finalités du traitement auquel les données personnelles sont destinées ainsi que le fondement juridique de ce traitement;

  c) les destinataires ou les catégories de destinataires des données personnelles, le cas échéant;

  d) le cas échéant, le fait que le responsable de traitement, les sous-traitants ou les sous-traitants ultérieurs ont l'intention de transférer des données personnelles vers un autre pays ou à une organisation internationale, ainsi que le fondement juridique et le mécanisme de transfert applicable à ce transfert, y compris les mesures de sécurité qui doivent être mises en place;

  e) la période pendant laquelle les données personnelles seront conservées ou stockées ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette période;

  f) l'existence du droit, lorsqu'il est prévu par les lois nationales applicables, de demander au responsable du traitement l'accès aux données personnelles, leur rectification, leur suppression ou leur transfert, ainsi que la limitation du traitement des données personnelles d'un enfant ou le droit de s'y opposer;

  g) la manière dont les droits relatifs aux données personnelles peuvent être exercés et les mécanismes de contrôle mis à la disposition des enfants et de leurs tuteurs légaux;

  h) si ce droit existe dans la juridiction concernée, le droit de déposer une plainte auprès de l'autorité de contrôle compétente;

i) un résumé des mesures de sécurité mises en œuvre (par exemple les mesures visant à garantir une expérience adaptée à l'âge de l'enfant).

- Les enfants et leurs tuteurs légaux devraient également être informés de la manière dont l'IA est utilisée dans l'outil et de son mode de fonctionnement. Cela devrait inclure toutes les informations pertinentes leur permettant de comprendre de quelle manière l'utilisation d'un outil d'IA pourrait avoir une incidence sur leurs droits, particulièrement dans le contexte éducatif, y compris les risques d'hallucinations, de biais ainsi que d'effets manipulateurs ou addictifs.
- Les enfants, leurs tuteurs légaux et les éducateurs devraient être clairement informés lorsque du contenu éducatif, de la rétroaction, des évaluations ou d'autres résultats pertinents sont générés par l'IA ou ont fait l'objet d'un apport important de celle-ci, au moyen d'un affichage clair ou de toute autre forme appropriée de communication de cette information.
- Les renseignements fournis aux enfants ou à leurs tuteurs légaux devraient être faciles d'accès, concis et formulés dans un langage clair et facile à comprendre, adapté à l'âge et au degré de maturité de l'enfant, et communiqués au moment opportun par rapport au traitement des données (des informations « fournies en temps réel »).
- Lorsqu'il y a lieu, les enfants devraient être informés de l'utilisation ou du traitement de leurs données aux fins de l'entraînement d'un modèle d'IA, du développement de produits ou d'autres finalités secondaires, conformément aux lois ou aux lignes directrices applicables, dans le respect de l'intérêt supérieur de l'enfant et de son degré de maturité.
- Si l'outil d'IA comprend un agent conversationnel ou un assistant d'IA, la personne qui l'utilise devrait être informée qu'elle communique avec une machine et non avec un être humain.
- Les enfants et leurs tuteurs légaux devraient être clairement informés des interactions avec un système d'IA qui pourront être consultées par leurs pairs, leurs enseignants et éducateurs ou d'autres personnes.
- Les enseignants devraient être en mesure d'évaluer la pertinence des systèmes d'apprentissage adaptatif pour chaque enfant et de comprendre les raisons ayant conduit aux résultats obtenus, particulièrement lorsque ceux-ci ont une incidence importante sur le parcours scolaire de l'enfant.
- L'utilisation d'outils d'IA en éducation, particulièrement par les enfants ayant des besoins particuliers en matière d'apprentissage et relatif à des handicaps, doit être mise en œuvre de manière transparente et adaptée au contexte éducatif. De plus, le traitement des données de ces enfants ne devrait pas aller à l'encontre des engagements pris en matière de protection des données et de la vie privée.
- L'utilisation, par les enseignants et éducateurs, de certains types d'outils de détection du plagiat fondés sur l'IA peut miner la relation de confiance entre les élèves et les enseignants et éducateurs et porter atteinte aux droits de l'enfant. La transparence est essentielle, compte tenu des risques d'inexactitude et des préjudices que ces outils pourraient causer aux enfants, et des mesures doivent être mises en place afin d'offrir des mécanismes de protection ou de recours adaptés aux enfants et à leurs tuteurs légaux.

10. Accord sur le traitement des données et passation de marchés

- Les relations entre le responsable du traitement et le sous-traitant devraient être régies par un contrat ou un accord dans lesquels les parties établissent leurs obligations respectives ainsi que les instructions nécessaires au traitement des données personnelles conformément aux lois applicables.
- Les éléments suivants devraient notamment être pris en considération :

  a) les obligations en matière de protection des données ainsi que les instructions applicables aux sous-traitants ultérieurs;

  b) des informations sur le lieu de stockage des données, les personnes qui y ont accès, leur durée de conservation ainsi que les mesures de protection applicables aux interactions des enfants avec l'outil;

  c) l'interdiction ou l'autorisation de transferts internationaux de données et, le cas échéant, les conditions d'autorisation ainsi que les exigences et les mesures de sécurité applicables à l'hébergement à l'étranger, à l'accès à distance et aux transferts subséquents effectués par des sous-traitants ultérieurs;

  d) l'interdiction d'utiliser les entrées, les résultats, l'historique des conversations, les données analytiques sur l'apprentissage ou d'autres données d'interaction des enfants pour entraîner ou améliorer le modèle d'IA du fournisseur, sauf lorsqu'un fondement juridique existe, qu'une justification claire est fournie, que cette utilisation fait l'objet d'une communication transparente et que des mesures de sécurité rigoureuses sont en place dans l'intérêt supérieur de l'enfant;

  e) les obligations imposées au sous-traitant fournissant les services, notamment l'obligation d'obtenir une autorisation écrite et de réaliser une évaluation d'impact en matière de protection des données ou une évaluation des risques pour la vie privée pour l'utilisation d'outils d'IA;

  f) des mesures de sécurité et des contrôles d'accès appropriés.

11. Garanties relatives aux droits des personnes (enfants, tuteurs légaux et professionnels de l'éducation)

- Les acteurs responsables doivent mettre en place un mécanisme clair et souple permettant l'exercice effectif des droits en matière de protection des données et de la vie privée dans le contexte des outils d'IA. De tels mécanismes devraient également faciliter, lorsqu'il y a lieu, l'exercice effectif des autres droits fondamentaux impactés par l'utilisation de l'IA en éducation, notamment le droit d'obtenir une explication concernant les décisions individuelles, le droit à la non-discrimination et à l'égalité, le droit à l'autonomie et le droit à l'éducation.
- Les enfants, leurs tuteurs légaux et les professionnels de l'éducation doivent pouvoir signaler et contester les utilisations ou les résultats problématiques de l'IA au moyen de mécanismes accessibles et efficaces donnant accès à un examen par un humain, à la correction des erreurs

et à des recours appropriés. Par conséquent, la littératie en matière d'IA devrait faire partie intégrante du processus éducatif.

- Les enfants et leurs tuteurs légaux devraient disposer de mécanismes accessibles, en temps utile et efficaces leur permettant de contester les décisions ou les pratiques reposant sur l'IA qui impactent l'enfant, ainsi que d'obtenir une intervention humaine effective, la correction des erreurs, des mesures de réparation et tout autre recours approprié en cas de préjudice ou d'atteinte à leurs droits.

Dans le cadre de la 48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée, il est donc convenu ce qui suit :

1. Informer et sensibiliser les personnes sur les risques et les responsabilités en matière de protection des données et de la vie privée associés à l'utilisation de l'IA dans les contextes éducatifs, notamment en ce qui concerne les préoccupations énoncées dans la présente résolution.

2. Encourager les membres à s'appuyer sur la présente résolution pour élaborer des lignes directrices complémentaires visant à aider les autorités en charge de l'éducation ainsi que les fournisseurs et les développeurs de systèmes d'IA, à s'acquitter de leurs obligations en matière de protection des données et de la vie privée, en tenant compte de la nature sensible des données personnelles des enfants.

3. Diffuser la présente résolution et ses recommandations auprès des parties prenantes et décideurs politiques dans leurs juridictions et leurs réseaux.

4. Assurer la liaison avec les organisations internationales compétentes, les organisations non gouvernementales traitant des droits de l'enfant et les autres groupes de la société civile afin de promouvoir la présente résolution et d'en assurer le suivi, notamment en favorisant une participation significative des enfants et, lorsqu'il y a lieu, en représentant leurs intérêts ou en contribuant à les faire valoir.

5. Reconnaître la contribution que l'Assemblée mondiale pour la protection de la vie privée peut apporter, dans un contexte international, à l'élaboration de nouveaux instruments d'orientation en matière de gouvernance de l'IA en éducation, et réaffirmer l'importance de sa participation aux initiatives en cours en sollicitant son expertise en matière de protection des données et de la vie privée afin d'éclairer et d'appuyer l'élaboration de politiques mondiales visant à encadrer les systèmes d'IA dans les contextes éducatifs.

6. Coopérer avec les autres membres ainsi qu'avec le Groupe de travail sur l'éducation numérique et le Groupe de travail sur l'IA afin de mettre en commun ressources, connaissances et pratiques exemplaires, notamment par l'établissement d'une liste de ressources et de pratiques exemplaires.

Annexes

La présente annexe contient trois documents visant à favoriser une meilleure harmonisation avec les sources internationales et les références de l'Assemblée mondiale pour la protection de la vie privée. Ces documents fournissent également des éléments de contexte, des explications et des exemples complémentaires relatifs aux recommandations formulées dans la présente résolution :

Document 1 : 1.A Sources internationales; 1.B Sources de l'Assemblée mondiale pour la protection de la vie privée

Boîte à outils stratégique : Aperçu des documents d'orientation 2 et 3

Document 2 : Orientations sur la littératie en matière d'IA à l'intention des élèves et de renforcement des capacités des enseignants et éducateurs

Document 3 : Modèle de charte encadrant l'utilisation de l'IA dans les établissements d'enseignement

Document 1

1.A Sources internationales

- Comité des droits de l'enfant de l'Organisation des Nations Unies (ONU), Déclaration commune sur l'intelligence artificielle et les droits de l'enfant (2026)
- ONU, Pacte numérique mondial (2024)
- ONU, Rapport final de l'ONU sur la gouvernance de l'IA au service de l'humanité (2024)
- Comité des droits de l'enfant de l'ONU, Observation générale no 25 sur les droits de l'enfant en relation avec l'environnement numérique (2021)
- Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), Déclaration ministérielle conjointe sur la préservation de l'éducation comme bien commun à l'ère de l'IA (en anglais seulement) (2026)
- UNESCO, Recommandation sur l'éthique de l'intelligence artificielle (2021)
- UNESCO, Consensus de Beijing sur l'intelligence artificielle et l'éducation (2019)
- Gouvernance des données pour les technologies éducatives : recommandations stratégiques (en anglais seulement) de l'UNICEF (2025)
- Organisation de coopération et de développement économiques (OCDE), Recommandation du Conseil sur les enfants dans l'environnement numérique (2021)
- OCDE, Lignes directrices à l'intention des fournisseurs de services numériques (2021)
- OCDE, Recommandation du Conseil sur l'intelligence artificielle (2019)
- Conseil de l'Europe, Recommandation du Comité des Ministres aux États membres sur la littératie en intelligence artificielle (2026)

- Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (2024)
- Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+) (2018).
- Ministres du Numérique du G20, Principes de haut niveau visant à mieux protéger et outiller les enfants dans l'univers numérique (en anglais seulement), (2021)
- Déclaration dans le cadre de la Table ronde des autorités de protection des données et de la vie privée du G7, Promouvoir l'innovation responsable et protéger les enfants en priorisant la protection de la vie privée (2025)
- Déclaration sur l'intelligence artificielle et les enfants de la Table ronde des autorités de protection des données et de la vie privée du G7 (2024)
- Déclaration sur le rôle des autorités de protection des données dans la promotion d'une IA digne de confiance de la Table ronde des autorités de protection des données et de la vie privée du G7 (2024)
- Déclaration sur l'IA générative de la Table ronde des autorités de protection des données et de la vie privée du G7 (2023)

1.B Sources de l'Assemblée mondiale pour la protection de la vie privée

- Assemblée mondiale pour la protection de la vie privée, Résolution sur la collecte, l'utilisation et la divulgation de données personnelles pour préentraîner, entraîner et mettre au point des modèles d'IA (en anglais seulement) (2025)
- Assemblée mondiale pour la protection de la vie privée, Déclaration commune sur la mise en place de cadres de gouvernance des données fiables pour favoriser une intelligence artificielle innovante et protectrice de la vie privée, adoptée dans le cadre de l'Assemblée mondiale pour la protection de la vie privée (2025)
- Assemblée mondiale pour la protection de la vie privée, Résolution sur les systèmes d'intelligence artificielle générative (en anglais seulement) (2023)
- Assemblée mondiale pour la protection de la vie privée, Résolution sur les droits numériques des enfants (2021)
- Assemblée mondiale pour la protection de la vie privée, Résolution sur les plateformes d'apprentissage en ligne (2018)
- Assemblée mondiale pour la protection de la vie privée, Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle (2018)

Aperçu des documents d'orientation 2 et 3

La présente résolution porte sur l'émergence de nouveaux outils d'IA dans les établissements d'enseignement, tout en demeurant conforme à la Résolution sur les plateformes d'apprentissage

en ligne (2018) de l'Assemblée mondiale pour la protection de la vie privée et à la Résolution sur les droits numériques des enfants (2021) de l'Assemblée mondiale pour la protection de la vie privée. L'objectif est de refléter l'état actuel de la gouvernance des données ainsi que les récentes avancées technologiques dans les contextes éducatifs.

La présente résolution offre à la communauté internationale l'occasion de se pencher de nouveau sur les technologies éducatives en mettant l'accent sur l'IA. Elle s'appuie sur les conclusions de l'enquête menée par le Groupe de travail sur l'éducation numérique de l'Assemblée mondiale pour la protection de la vie privée en 2025-2026, dans le cadre de laquelle les membres de l'Assemblée ont communiqué des modèles de politiques, des documents d'orientation et d'autres renseignements pertinents. Les données recueillies dans le cadre de cette enquête donnent un aperçu des fondements juridiques appropriés et des recommandations relatives au traitement des données personnelles au moyen de technologies d'IA dans le contexte éducatif à l'échelle mondiale.

En l'absence de l'élaboration et de la mise en œuvre d'un instrument juridique complet visant à encadrer les systèmes d'IA dans les contextes éducatifs, une collaboration avec des organismes des Nations Unies, comme le Comité des droits de l'enfant et l'UNESCO, ainsi qu'avec des organisations régionales comme le Conseil de l'Europe, contribuerait à l'harmonisation future des normes à l'échelle mondiale.

De plus, il importe de garder à l'esprit que la littératie en matière d'IA ne remplace pas la littératie numérique; elle en constitue plutôt un prolongement et doit y être intégrée.

Pour relever ces défis communs, les systèmes d'éducation devront aider les jeunes à développer leur sens des responsabilités, leur autonomie, leur conscience critique, leur bien-être, leurs connaissances et leurs compétences afin qu'ils puissent façonner un avenir meilleur.

Les autorités de protection des données jouent un rôle important dans l'éducation du public au sujet de ses droits en matière de protection des données et de la vie privée.

Compte tenu du rôle important que jouent les établissements d'enseignement dans la vie des enfants et de leurs familles, les activités de sensibilisation du public devraient continuer d'accorder une place prioritaire aux récentes avancées de l'IA dans les technologies éducatives.

À la lumière de la présente résolution sur l'IA dans le domaine de l'éducation, la communauté de l'Assemblée mondiale pour la protection de la vie privée devrait continuer d'intégrer la gouvernance des données dans les technologies éducatives à son plan stratégique et à ses axes de travail, notamment ceux portant sur l'IA et l'éducation numérique.

Cela enverrait un signal fort aux gouvernements et aux acteurs de l'industrie et contribuerait à favoriser l'établissement d'un cadre mondial cohérent ainsi que la mise en œuvre d'un solide programme d'apprentissage.

Boîte à outils stratégique :

Les deux documents contenus dans la Boîte à outils stratégique devraient être considérés comme des propositions du Groupe de travail sur l'éducation numérique de l'Assemblée mondiale pour la protection de la vie privée et peuvent être adaptés de façon plus poussée afin de tenir compte de contextes, de besoins et de circonstances particuliers.

Document 2 : Orientations sur la littératie en matière d'IA à l'intention des élèves et le renforcement des capacités des enseignants et éducateurs

Le volet de la Boîte à outils stratégique consacré à la littératie en matière d'IA vise à doter les enfants des différents groupes d'âge et niveaux d'enseignement, des connaissances fondamentales nécessaires en matière de protection des données et de la vie privée ainsi que de littératie numérique, informationnelle et médiatique. Ces connaissances fondamentales doivent être acquises dans une perspective critique afin de permettre aux élèves de devenir des individus compétents, responsables et autonomes, capables de comprendre les systèmes d'IA, de les remettre en question et d'en orienter l'évolution, tout en les protégeant contre leur instrumentalisation.

Ces compétences peuvent être adaptées, selon les besoins, aux niveaux primaire et secondaire, qui constituent les deux premiers niveaux de l'éducation formelle, avant le passage à l'enseignement postsecondaire.

Document 3 : Modèle de charte encadrant l'utilisation de l'IA dans les établissements d'enseignement

Le modèle de charte encadrant l'utilisation de l'IA dans les établissements d'enseignement est rédigé sous la forme d'un engagement qui s'adresse à ces établissements. Cette charte vise à énoncer certains engagements fondamentaux, de manière non exhaustive, concernant l'utilisation optimale des technologies éducatives et des outils fondés sur l'IA, ainsi qu'à témoigner d'un ferme engagement public en faveur de la protection des données et de la vie privée numérique des élèves et du renforcement de la confiance à l'égard des établissements d'enseignement. Le modèle de charte propose une approche respectueuse de la vie privée permettant de définir les responsabilités et obligations de principe des établissements d'enseignement agissant au titre de responsables de traitement. Il ne vise pas à se substituer aux obligations prévues par les lois applicables et peut servir de modèle de base à adapter en fonction du cadre juridique applicable.

Document 2 : Orientations sur la littératie en matière d'IA à l'intention des élèves et du renforcement des capacités des enseignants et éducateurs

Avant d'envisager des exigences en matière de littératie de l'IA pour les élèves, les établissements d'enseignement devraient veiller à ce que les services d'IA utilisés dans le cadre éducatif soient adaptés à l'usage prévu, sûrs et conformes au cadre juridique applicable. La littératie en matière d'IA ne devrait pas être considérée comme pouvant remplacer ces mesures de sécurité.

Établir des bases solides en matière d'éducation numérique afin de permettre aux élèves d'acquérir des compétences en IA, du primaire au postsecondaire.

L'intégration de l'IA dans les contextes éducatifs exige que les élèves acquièrent un ensemble de compétences fondamentales avant de commencer à utiliser des outils d'IA. Ces compétences constituent le niveau minimal de littératie en matière d'IA que les autorités éducatives et les établissements d'enseignement devraient veiller à transmettre à l'ensemble des élèves, en collaboration avec les autorités de protection des données et les autres parties prenantes.

- **Comprendre les différences entre les secteurs public et privé**

Les élèves doivent comprendre de façon générale les intérêts qui sous-tendent les activités des secteurs public et privé, ainsi que les différences dans leur façon de traiter les données personnelles. Il est important que les services liés à l'IA utilisés par les élèves dans les contextes éducatifs leur soient bénéfiques et respectent le cadre juridique applicable régissant le traitement des données personnelles. Il est également essentiel que les élèves qui utilisent des technologies et des outils d'IA en éducation, comme les agents conversationnels, sachent reconnaître lorsqu'ils interagissent directement avec une entreprise du secteur privé qui recueille leurs données personnelles.

Les élèves du primaire peuvent comprendre que certains organismes, infrastructures et services relèvent du secteur public. Par exemple, l'hôtel de ville, la bibliothèque publique, le service d'incendie, les écoles publiques, le réseau routier et les transports en commun. Ils peuvent aussi comprendre que les entreprises et les commerces relèvent du secteur privé et vendent des produits ou des services dans le but de réaliser des profits.

Les élèves du secondaire peuvent comprendre que le secteur public comprend les organisations qui sont sous l'autorité de l'État, des administrations locales (régions, départements, municipalités) ou des établissements publics. Sa mission première est de répondre aux besoins collectifs et d'assurer à l'ensemble de la population l'accès à des services essentiels, sans but lucratif. Ils peuvent également comprendre que le secteur privé est composé d'entreprises ou d'organisations appartenant à des personnes, à des actionnaires ou à des investisseurs. Sa principale raison d'être est de générer des profits tout en répondant aux besoins des consommateurs.

- **Savoir définir les données personnelles et les données personnelles sensibles**

Les élèves devraient être en mesure de définir ce que sont les données personnelles, c'est-à-dire toute information qui, seule ou combinée à d'autres renseignements, permet d'identifier un individu. Les élèves devraient également comprendre que certaines catégories de données personnelles bénéficient d'une protection accrue, notamment les données relatives à la santé, à l'origine ethnique,

aux croyances religieuses, à l'orientation sexuelle, les données génétiques et les données biométriques.

Dans le contexte éducatif, cela signifie reconnaître que certaines données qui peuvent sembler anodines au premier abord, comme les travaux scolaires remis par les élèves et enregistrés par un logiciel de surveillance, peuvent néanmoins révéler des informations relevant de catégories de données bénéficiant d'une protection renforcée. Les données relatives aux élèves sont conservées à des fins d'analyse, ce qui soulève d'importantes questions s'agissant de leur conservation sur le long terme et de l'utilisation qui pourrait en être faite au fil du temps.

De plus, toutes les personnes participant au système, notamment les enseignants, les élèves et les administrateurs, peuvent alimenter ces données, ce qui accroît le risque d'incohérences ou d'utilisations inappropriées. Plus important encore, l'accès à ces données n'est pas réservé au seul personnel scolaire. Des organisations externes peuvent également y avoir accès. Il est donc essentiel de mettre en place des politiques claires et transparentes afin de protéger la vie privée des élèves et de veiller à ce que leurs données personnelles soient traitées de façon responsable.

Les élèves du primaire peuvent comprendre que les données personnelles comprennent toutes les informations qui les concernent ou qui permettent de les identifier, comme leur nom, leur lieu de résidence ou les activités qu'ils aiment pratiquer.

Les élèves du secondaire peuvent comprendre que les données personnelles désignent toute information permettant d'identifier une personne, directement ou indirectement.

- **Comprendre l'identité numérique**

Les élèves devraient apprendre à créer et à maintenir une présence numérique saine :

  - comprendre ce qu'est une empreinte numérique;
  - comprendre de quelle façon leur empreinte numérique se forme;
  - comprendre pourquoi leur empreinte numérique est importante;
  - comprendre comment leurs propres actions et celles des autres peuvent influer sur leur réputation;
  - comprendre leur droit de contrôler leurs données personnelles et de gérer leur présence en ligne;
  - comprendre quels aspects de leur empreinte numérique sont sous leur contrôle et lesquels reposent sur les déductions faites par des entreprises;
  - être capables de se projeter dans l'avenir afin d'imaginer l'identité numérique qu'ils souhaitent construire et de la façonner.

- **Savoir comment et pourquoi protéger les données personnelles**

Les élèves devraient apprendre des règles pratiques en matière de sécurité et de protection des données et la vie privée, notamment :

- utiliser des noms d'utilisateur et des mots de passe robustes et uniques qui ne révèlent pas leur identité et ne permettent pas de l'établir; s'ils choisissent de rédiger une description de profil, veiller à ce qu'elle ne contienne aucune information permettant de deviner qui ils sont, où ils vivent ou quelles sont leurs activités préférées;

- éviter de communiquer des données personnelles non nécessaires lors de l'inscription à des outils d'intelligence artificielle, notamment des informations pouvant servir à établir leur profil;
- comprendre que les données communiquées aujourd'hui peuvent être conservées, réutilisées ou transférées à des tiers pendant de nombreuses années.

Les élèves devraient être conscients que des bases de données scolaires insuffisamment sécurisées ont déjà été la cible de cyberattaques, ce qui a mis en péril les données personnelles de milliers d'enfants. La protection des données est donc à la fois une responsabilité collective et une responsabilité individuelle. Si leurs données ne sont pas protégées, les conséquences peuvent largement dépasser le cadre scolaire et avoir des répercussions sur leur avenir, leur réputation et leur sécurité.

C'est pourquoi la littératie numérique doit reposer sur une véritable culture de la responsabilité à l'égard des données, qui concerne autant les élèves que les enseignants et éducateurs, les administrateurs scolaires et les concepteurs des outils utilisés dans les contextes éducatifs. La protection des données ne relève pas uniquement de considérations techniques; elle constitue un droit fondamental et une responsabilité collective à l'ère du numérique.

- **Connaître ses droits et savoir comment les exercer**

Selon les lois applicables en matière de protection des données et de la vie privée, les personnes, y compris les mineurs représentés par leur tuteur légal lorsque nécessaire, peuvent bénéficier des droits suivants :

- Droit d'accès : savoir quelles données personnelles une plateforme détient à leur sujet.
- Droit de rectification : faire corriger des données inexactes ou incomplètes.
- Droit à l'effacement (ou droit à l'oubli) : demander la suppression de données personnelles qui ne sont plus nécessaires aux fins pour lesquelles elles ont été recueillies.
- Droit à la limitation du traitement : demander que l'utilisation de certaines données soit restreinte dans certaines circonstances.
- Droit à la portabilité des données : recevoir ses données personnelles dans un format structuré, couramment utilisé et lisible par machine, et les transférer à un autre service ou à une autre plateforme sans obstacle.
- Droit d'opposition et droit de ne pas faire l'objet d'une prise de décision automatisée : s'opposer à certains traitements de données personnelles, y compris l'établissement de profils.

Les établissements d'enseignement devraient veiller à ce que les élèves et leur famille puissent facilement trouver les coordonnées de l'autorité de protection des données compétente. Ils devraient également intégrer dans les programmes scolaires des exercices simulant le dépôt d'une plainte.

- **Comprendre que les conditions d'utilisation devraient être faciles à comprendre pour tous**

Les fournisseurs de services d'IA doivent veiller à ce que les conditions d'utilisation et les politiques de confidentialité soient claires, accessibles et faciles à comprendre, particulièrement lorsque leurs services sont destinés aux élèves ou utilisés par ceux-ci. Cette responsabilité ne devrait pas incomber

aux élèves, qui ne devraient pas avoir à déchiffrer des informations inutilement complexes. Dans le cadre de leur formation en IA, les élèves devraient néanmoins acquérir des compétences de base leur permettant de repérer et de comprendre les principales informations figurant dans les conditions d'utilisation et les politiques de confidentialité, notamment à l'aide d'une méthode de lecture structurée :

- déterminer qui est le responsable du traitement et où il est établi;
- repérer le fondement juridique de chaque fin du traitement;
- trouver la durée de conservation des données;
- vérifier si des données sont communiquées à des tiers ou vendues à ceux-ci;
- déterminer les modalités de retrait du consentement, lorsque la loi applicable prévoit cette possibilité.

Il est fortement recommandé d'intégrer dans les programmes scolaires des exercices en classe fondés sur les conditions d'utilisation réelles d'outils d'IA utilisés en éducation. Lorsque les conditions d'utilisation ne sont pas accessibles dans une langue que les élèves peuvent comprendre, cela constitue en soi un signal d'alarme qui devrait être porté à l'attention des administrateurs scolaires et, au besoin, de l'autorité de protection des données.

- **Recouper les sources d'information**

Le recoupement systématique des sources constitue une habitude d'apprentissage essentielle à l'ère de l'IA. Les élèves devraient apprendre à :

- considérer tout contenu généré par l'IA comme un point de départ à l'exploration d'un sujet, et non comme une conclusion;
- vérifier toute affirmation factuelle à l'aide d'au moins deux sources indépendantes et faisant autorité; par exemple, si un outil d'IA fournit une date historique ou une statistique, l'élève devrait la confirmer à l'aide d'une encyclopédie, d'un manuel scolaire ou d'un site Web officiel avant de la citer dans ses travaux;
- comprendre que les systèmes d'IA peuvent reproduire les biais présents dans les données sur lesquelles ils ont été entraînés et que certaines perspectives culturelles ou linguistiques dominantes peuvent être surreprésentées.

- **Savoir que les systèmes d'IA ne sont pas infaillibles**

Les élèves devraient comprendre les limites et les problèmes associés aux grands modèles de langage (GML), notamment l'obséquiosité, les hallucinations, leur mode de fonctionnement ainsi que les mécanismes d'influence et les orientations qu'ils peuvent intégrer. Particulièrement dans le cas des enfants, les systèmes d'IA ne devraient pas être anthropomorphiques (par exemple ne pas dire « je ressens… »).

- **Savoir formuler des requêtes efficaces pour les systèmes d'IA**

La capacité à formuler des requêtes consiste à adresser aux systèmes d'IA des requêtes claires, ciblées et limitées aux données nécessaires. Il s'agit d'une compétence fondamentale émergente. Les élèves devraient comprendre :

- que les requêtes soumises à des services d'IA externes sont traitées sur des serveurs exploités à distance et peuvent être utilisées pour l'entraînement des modèles, à moins que l'utilisateur n'ait expressément refusé une telle utilisation;
- qu'ils ne doivent jamais inclure de données personnelles (les leurs ou celles d'autrui) dans leurs requêtes, à moins que le service ne fournisse des garanties explicites et vérifiables concernant le caractère confidentiel du traitement. Cela signifie que la plateforme ne doit pas se contenter d'affirmer qu'elle protège les données des utilisateurs; elle doit pouvoir le démontrer au moyen de mesures concrètes et vérifiables, comme une politique de protection de la vie privée publiée et en conformité avec la législation nationale en matière de protection des données, des certifications de sécurité indépendantes ou des accords contractuels relatifs au traitement des données pouvant être examinées et invoquées afin de tenir les fournisseurs responsables;
- que la qualité et la formulation d'une requête influent directement sur la qualité du contenu généré et sur les biais qu'il peut comporter.

Document 3 : Modèle de charte encadrant l'utilisation de l'IA dans les établissements d'enseignement

Nous, , reconnaissons ce qui suit :

1. Tous les enfants ont un droit fondamental à la vie privée et à la protection de leurs données personnelles.

2. Les informations personnelles des enfants et des jeunes sont particulièrement sensibles et doivent, à ce titre, bénéficier d'une protection adéquate dans le cadre juridique régissant le traitement des données personnelles.

3. Les outils d'intelligence artificielle offrent d'importantes possibilités d'apprentissage et de développement aux élèves, mais peuvent également présenter des risques importants pour leur vie privée.

4. En tant qu'éducateurs, nous jouons un rôle essentiel dans la préparation des élèves à utiliser les outils d'IA de façon sécuritaire, à repérer et à gérer les risques pour la vie privée en ligne, et à devenir des citoyens numériques responsables.

Nous nous engageons à soutenir les élèves de la façon suivante :

Protection

1. Agir dans l'intérêt supérieur des élèves, notamment en ce qui concerne leurs données personnelles, leur vie privée et leur sécurité.

2. Veiller à ce que les outils d'IA utilisés en classe limitent la collecte, l'utilisation et la communication des données personnelles des élèves à ce qui est nécessaire à l'exécution de nos responsabilités éducatives.

3. Veiller, conformément aux lois applicables, à ce que les fournisseurs tiers d'outils et de services d'IA offrent de solides mesures de protection de la vie privée et des données lors de l'acquisition, de l'utilisation ou de toute autre forme de recours à ces outils et services.

4. Comprendre les risques pour la protection des données et la vie privée et veiller à ce qu'ils soient atténués avant l'adoption d'outils et de services d'IA.

5. Renforcer les mesures de protection des données personnelles et de la vie privée dans les outils et services d'IA, notamment en réglant les paramètres de confidentialité au niveau le plus élevé de protection par défaut.

6. Informer rapidement les élèves, les parents et les tuteurs légaux de toute atteinte importante à la vie privée et agir sans délai afin d'en atténuer les conséquences et, lorsque la loi l'exige, signaler également cette atteinte à l'autorité de protection des données compétente.

Autonomisation

1. Fournir aux élèves, aux parents et aux tuteurs légaux des avis rédigés dans un langage clair, conformes aux pratiques exemplaires ainsi qu'aux lois applicables en matière de protection des données ou de la vie privée.

2. Expliquer, dans un langage facile à comprendre pour les élèves, les parents et les tuteurs légaux, quels types de données personnelles sont collectées ainsi que les finalités pour lesquelles ils sont utilisés ou communiqués.

3. Fournir aux élèves des conseils sur la façon de protéger leurs données personnelles, y compris ceux collectés par les outils et services d'IA.

4. Recueillir les commentaires pertinents des élèves, des parents et des tuteurs légaux concernant l'utilisation des outils et services d'IA.

5. Informer les élèves de leur droit à la protection des données et à la vie privée, notamment leur droit d'accéder aux dossiers scolaires contenant leurs renseignements personnels et d'en faire corriger les informations inexactes dans le cadre d'une interaction humaine, et leur donner les moyens d'exercer ces droits.

6. Favoriser une sensibilisation continue aux risques émergents et l'apprentissage continu des enjeux liés à la protection des données et de la vie privée dans l'environnement numérique, y compris lors de l'utilisation d'outils d'IA.

La Commission fédérale du commerce des États-Unis s'abstient d'adopter cette résolution.