Des consensus sur l'IA en éducation

publié le 06/12/2023 - mis à jour le 19/01/2026

Descriptif :

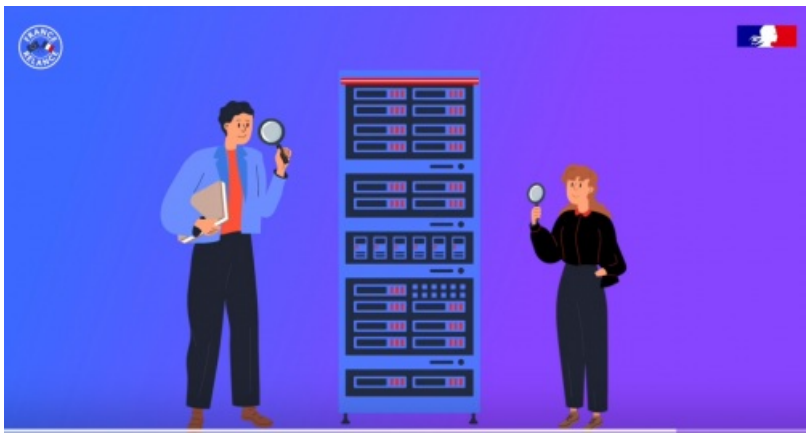
Consensus de Beijing sur l'intelligence artificielle et l'éducation (UNESCO), rapport de la direction du numérique éducatif. Stratégies, points de vigilance.

Sommaire :

Le **Consensus de Beijing** sur l'intelligence artificielle et l'éducation permet en 10 pages de présenter les conclusions tirées en 2019 par l'UNESCO.
Le nom Intelligence Artificielle ne doit pas nous éblouir : il s'agit en fait de puissance calculatoire, et rien n'est magique. Cette puissance doit être transparente et il s'agit de la placer au service du bien commun.

Des textes à connaître

Le consensus (version française de 15 à 25).
En tant qu'institution des Nations Unies spécialisée pour l'éducation, l'UNESCO est chargée de diriger et de coordonner l'agenda Éducation 2030, qui fait partie d'un mouvement mondial visant à éradiquer la pauvreté, d'ici à 2030, à travers 17 Objectifs de développement durable. L'éducation est au coeur de l'Objectif 4 qui vise à « assurer l'accès de tous à une éducation de qualité, sur un pied d'égalité, et promouvoir les possibilités d'apprentissage tout au long de la vie ».



Le rapport de la DNE[1] "Intelligence artificielle et éducation, Apports de la Recherche et enjeux pour les politiques publiques") présente un état des lieux (avril 2023) sur :

- la diversité des définitions et des approches,
- les enjeux pour les politiques publiques,
- les **enjeux éthiques**,
- les domaines d'application,
- des **pistes de travail** pour **former** et **enseigner**,
- les perspectives avec le tournant actuel de l'IA générative et des grands modèles de langage.

Ses 40 pages commencent par des résumés et infographies pour les personnes qui ne souhaitent pas tout lire.

● Comment s'acculturer ?

- Des regards croisés et **pluridisciplinaires** sont proposés dans les parcours de formations à l'intelligence artificielle et les séminaires actuellement mis en oeuvre (ex dans la formation des cadres),
- des dispositifs permettent de tester des nouvelles pratiques pédagogiques associant l'IA dans des conditions conformes aux règles de protection des données, par exemple en utilisant des ressources innovantes présentes dans le médiacentre des ENT,
- les ressources dont la pertinence a été validée par **EduUP** ou qui ont été accompagnées par le programme **P2IA** (cycle 2) ont bénéficié de l'évaluation qui est recommandée dans le consensus,
- les personnes qui souhaitent s'engager dans des projets pédagogiques sont invitées à se faire accompagner par des expert.es, et à veiller à l'équilibre des angles de vue (disciplines, **genres**) de manière à ce que la **plus value** puisse être estimée collégialement et mise en balance avec les **risques**,
- l'acculturation des élèves à la **connaissance** et à la **compréhension** de l'IA peut s'appuyer sur les ressources adaptées à chaque âge, qui contribuent au développement de l'esprit critique. Exemple de vidéographie proposée dans Lumni. Exemple de vidéographie sur l'IA générative proposée par Canopé dans la Canotech.
- les parcours Pix et Pix+ Edu incluent des questions et des capsules sur l'IA et les enjeux associés. Ils sont accessibles à tous et toutes gratuitement, pour ne pas aggraver la fracture sociale. Exemple de capsule Pix+ Edu.
- Dans le livre "Le fabuleux chantier, rendre l'intelligence artificielle robustement bénéfique" (2019), les vulgarisateurs scientifiques Lê Nguyên Hoang et El Mahdi El Mhamdi[2] analysent les effets secondaires présents et les risques futurs du déploiement massif des algorithmes. Voir le résumé sur le site Cairn.

● La délicate question des données à caractère personnel

Dans son article "Les institutions éducatives au défi des GAFAM, des NATU et des BATX", paru dans le numéro 180 (2023/4) de la revue Administration & Éducation, p. 71-78, Jean-François Cerisier constate qu'en dépit des combats menés par les agences nationales européennes et des organisations non gouvernementales pour la protection des données personnelles, beaucoup d'entreprises s'immiscent au cœur de nos vies personnelles et professionnelles, de manière discrète voire opaque.

Le manque d'informations claires rend difficile le fait de décider "si un risque de fuite de données personnelles concernant des apprenants (identité et adresse électronique par exemple) doit interdire l'utilisation d'un service numérique, quand celle-ci permettrait d'améliorer notablement l'efficacité du dispositif de formation considéré".

Ce qui fait consensus actuellement c'est qu'avec l'IA... le risque est élevé.

○ De quelles données parle-t-on ?

Ces données personnelles relèvent de différentes catégories :

- *celles qui nous identifient et répondent à la question* ***« qui ? »*** *(nom, prénom, photographie, numéro de téléphone, adresse électronique, numéro de carte bancaire mais aussi adresse IP de notre smartphone ou de notre ordinateur, données de géolocalisation…),*

- *les données d'**engagement** qui décrivent nos interactions avec les différents services numériques et qui répondent à la question **« quoi ?** » (nos requêtes Google, nos courriels, nos publications sur les réseaux socionumériques, les prompts que nous adressons aux intelligences artificielles génératives comme ChatGPT ou Bard…),*
- *les données relatives à nos comportements numériques qui répondent à la question **« comment ? »** (nos habitudes et pratiques numériques)*
- *et tous les indicateurs attitudinaux qui peuvent être **calculés** à partir des données des trois premières catégories : nos attentes, nos opinions, nos critères d'achat mais aussi nos valeurs, nos orientations sexuelles, nos engagements politiques…*

Énumération à l'évidence incomplète !

De quels risque de fuite parle-t-on ?

*Les risques sont le plus souvent attachés à l'exploitation des données personnelles par des entreprises tierces qui les ont achetées à la plateforme qui les a collectées et qui les utilisent pour des **finalités** qui échappent totalement au consentement et au contrôle de ceux qui, le plus souvent à leur insu, les ont fournies. (...)*

*On trouve sur les **Dark web** toutes sortes de données, allant des mots de passe des services numériques que vous utilisez aux numéros et codes de vos cartes bancaires. Ce sont souvent les **failles** de sécurité des principales plateformes qui alimentent ce marché illégal des données. Si ces fuites de données ne sont pas intentionnelles de leur part, il leur est souvent reproché de ne pas prendre toutes les mesures de sécurisation nécessaire. Ainsi, 235 millions d'identifiants de comptes Twitter avec leurs mots de passe hackés ont-ils été vendus le 4 janvier 2023 pour une somme dérisoire selon une équipe de spécialistes du Daily Dark web9. (...)*

Quelles influences sont à craindre ?

- *être la cible de **publicités ciblées** non souhaitées (...).*
- *Les autres risques (...) attachés aux spécificités des applications utilisées comme l'**exposition** des jeunes à la pornographie, aux radicalismes, aux révisionnismes, aux violences, aux différents types de harcèlement ou bien aux complotismes et aux contre-vérités.*

Comment limiter les risques ?

- utiliser des **adresses mail temporaires**
- utiliser des **appareils** fournis par l'établissement scolaire pour limiter l'impact des cookies
- sensibiliser au lien entre technologies et influences et au fonctionnement des IA, y compris des compagnons IA.
- utiliser des **navigateurs** adaptés (Qwant, par exemple)
- prévoir des **scénarios "déconnectés"** (par exemple comparaison de résultats de requêtes qui dispensent l'élève d'utiliser l'IA)
- inclure l'**éducation** à la notion de données à caractère personnel et aux enjeux associés (Compétence 4.2 du CRCN Protéger les données personnelles et la vie privée).

(1) Direction du Numérique pour l'Education, au sein du Ministère de l'Education Nationale et de la jeunesse

(2) A propos des auteurs