

[Espace Presse et Actualités](#)[Événements](#)[Partenariats](#)[Gouvernance](#)[Liens utiles](#)

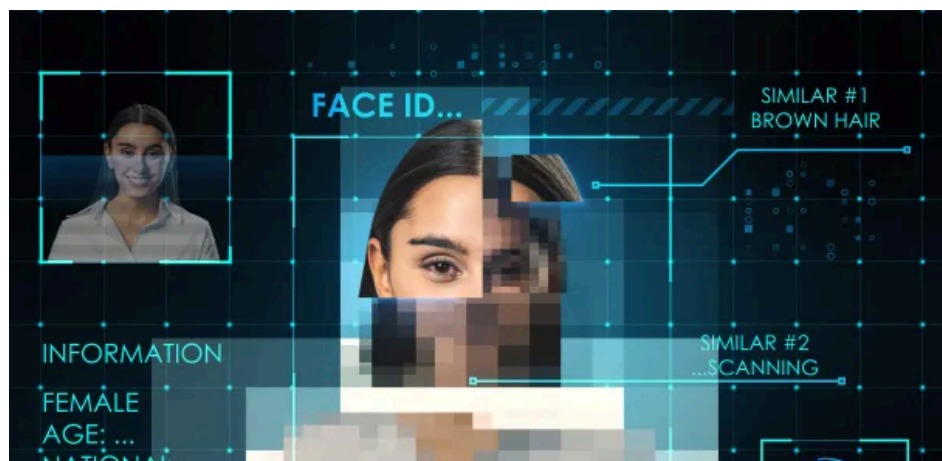
Français

[Idée >](#)

Les deepfakes et la crise du savoir

À mesure que les deepfakes brouillent la réalité, l'éducation doit aller au-delà de la simple détection : elle doit apprendre aux étudiants à naviguer entre vérité, connaissance et incertitude à l'ère de l'intelligence artificielle.

27 octobre 2025



Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).



Pilier 2 : construction organisationnelle du savoir

Pilier 3 : écosystèmes intersectoriels de connaissance

L'occasion des sociétés apprenantes : architecturer les écosystèmes de connaissance


Conclusion

Références

Biography

Par Dre. Nadia Naffi, Université Laval

À mesure que les médias synthétiques et la désinformation générée et diffusée par l'intelligence artificielle se multiplient, les établissements d'enseignement se hâtent de développer des outils techniques de détection et des programmes d'éducation aux médias et à l'information (EMI).

En termes simples, les médias synthétiques désignent tout contenu — audio, image ou vidéo — créé par intelligence artificielle. Cela inclut les *deepfakes*, ces contrefaçons numériques si réalistes qu'elles peuvent imiter de façon convaincante la voix ou l'apparence d'une personne ([Forum canadien des organismes de réglementation numérique](#) , 2025).

Les *deepfakes* diffèrent fondamentalement de la désinformation traditionnelle : ils sont convaincants, évolutifs et de plus en plus accessibles. Le simple soupçon d'une génération par IA sème le doute.

Et si cette course technologique aux armements nous aveuglait face à une perturbation plus profonde ? Et si notre

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

"Dans un monde de médias synthétiques avancés, la littératie en IA ne consiste pas seulement à savoir utiliser des outils d'IA — elle consiste à survivre dans une réalité médiée par l'IA, où voir et entendre ne suffisent plus à croire."


Ce texte de réflexion remet en question le paradigme centré sur la vérification qui domine nos réponses aux hypertrucages. S'appuyant sur la théorie de l'apprentissage, la pensée systémique et l'épistémologie, j'avance que nous ne faisons pas seulement face à une crise de la désinformation — c'est-à-dire des faussetés diffusées dans le but délibéré de tromper, par opposition à la mésinformation, transmise à l'insu de celui ou celle qui la partage — mais à une crise du savoir elle-même. Les hypertrucages n'introduisent pas simplement de la fausseté dans notre écosystème informationnel : ils érodent les mécanismes mêmes par lesquels les sociétés construisent une compréhension commune.

L'accent mis par l'[UNESCO](#) sur l'intelligence artificielle dans l'éducation identifie à juste titre la nécessité d'approches inclusives et équitables de la littératie en IA (UNESCO, 2025). Toutefois, il faut aller plus loin : dans un monde de médias synthétiques avancés, la littératie en IA ne consiste pas seulement à savoir utiliser des outils d'IA — elle consiste à survivre dans une réalité médiée par l'IA, où voir et entendre ne suffisent plus à croire.



En réponse, je propose trois piliers selon lesquels l'éducation doit évoluer : l'agentivité épistémique individuelle, la



Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

Pilier 1 : agentivité épistémique individuelle

La menace de la mésinformation et de la désinformation, désormais massivement amplifiée par les médias synthétiques, figure parmi les principaux risques mondiaux selon le Forum économique mondial, qui souligne la frontière de plus en plus floue entre les contenus générés par l'IA et ceux produits par des humains ([Elsner et al., 2025](#) ) .

Pourtant, notre réponse demeure technique : détecter les faux, vérifier les sources, repérer la manipulation.

Cette approche est insuffisante ([Naffi et al., 2024](#) ) . Le marché de l'IA générative devrait croître de 560 % entre 2025 et 2031 pour atteindre 442 milliards USD ([Statista, 2025](#) ) .

Quarante-six pour cent des experts en fraude ont été confrontés à des fraudes par identité synthétique, 37 % à des hypertrucages vocaux et 29 % à des hypertrucages vidéo ([Statista, 2024](#) ) . En janvier 2024, des fraudeurs utilisant la technologie d'hypertrucage ont usurpé l'identité d'un directeur financier lors d'un appel vidéo, trompant un employé et lui faisant transférer 25 millions USD. Deloitte prévoit que l'IA générative pourrait faire passer les pertes liées à la fraude aux États-Unis de 12,3 milliards USD en 2023 à 40 milliards USD en 2027 — soit un taux de croissance annuel de 32 % ([Lalchand et al., 2024](#) ) .

"Nous approchons d'un seuil de réalité synthétique — un point au-delà duquel les humains ne pourront plus


Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).


technologie d'hypertrucage pour créer des contenus harcelants et à caractère sexuel mettant en scène des camarades ou des enseignants, laissant les législateurs peiner à adapter les lois existantes sur la cyberintimidation à cette nouvelle menace ([Laws Struggle to Address Students Making Deepfakes, 2025](#) [↗](#)). Parallèlement, le milieu médical fait face à ce que certains appellent une « crise de la preuve », alors que des acteurs malveillants utilisent des vidéos d'hypertrucage de médecins pour promouvoir des arnaques médicales, et que la possibilité de falsifier des données cliniques menace les fondements mêmes de la médecine fondée sur les preuves ([Lee Myers et al., 2025](#) [↗](#)).

Les dangers spécifiques sont clairs. Les outils de clonage vocal alimentés par l'IA permettent aux escrocs d'imiter la voix de proches à partir de quelques secondes d'enregistrement, créant des scénarios d'urgence crédibles qui poussent leurs victimes à envoyer de l'argent ([Bethea, 2024](#) [↗](#); [Vellani & Common, 2025](#) [↗](#)). Les recherches confirment que les humains ne peuvent pas identifier de manière fiable les voix générées par IA, les percevant souvent comme identiques à celles de vraies personnes ([Barrington et al., 2025](#) [↗](#)).


"La possibilité de rejeter des enregistrements authentiques comme des faux probables (Schiff et al., 2024) — crée un double piège où ni la croyance ni l'incrédulité face aux preuves ne peuvent être justifiées."

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

d'actualités sur les réseaux sociaux sont plus vulnérables aux hypertrucages, et cet effet persiste indépendamment des capacités cognitives ([Ahmed et al., 2024](#) .

Nous approchons d'un seuil de réalité synthétique — un point au-delà duquel les humains ne pourront plus distinguer les médias authentiques des médias fabriqués sans assistance technologique. Les outils de détection accusent un retard sur les technologies de création, dans une course aux armements impossible à gagner ([Cal Alumni Association, 2024](#) .

Pendant ce temps, le dividende du menteur — la possibilité de rejeter des enregistrements authentiques comme des faux probables (Schiff et al., 2024) — crée un double piège où ni la croyance ni l'incrédulité face aux preuves ne peuvent être justifiées.

Une première étape cruciale consiste à faire de l'éducation un vecteur d'agentivité épistémique, c'est-à-dire la capacité individuelle à interagir de manière responsable avec le savoir lorsque les preuves traditionnelles deviennent incertaines. Ce concept s'appuie sur les principes de l'apprentissage des adultes de [Knowles, \(1978](#) ) , en mettant l'accent sur l'autodirection et les cadres expérientiels. L'agentivité épistémique consiste à aider les apprenants à développer leurs propres cadres d'évaluation plutôt que d'accepter des critères de vérification prédéfinis.

Des exemples concrets émergent. Certaines familles instaurent des mots de passe pour vérifier l'identité lors d'appels, contournant ainsi les arnaques par clonage vocal. Lors d'appels vidéo, on utilise des défis du type « prouve que tu es bien en direct » : on demande à la personne à l'écran

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

doit encourager ces pratiques de savoir, qui dépassent le perfectionnement des seules compétences techniques de détection.

Pilier 2 : construction organisationnelle du savoir

Le défi des médias synthétiques dépasse l'individu : il touche les institutions. Les organisations de tous les secteurs reposent sur des flux d'information fiables. Les *deepfakes* menacent cette confiance à sa racine — que ce soit par la falsification de dossiers médicaux ([Waier & Shillair, 2024](#) [↗](#)), l'usurpation d'identité de dirigeants ([Robins-Early, 2024](#) [↗](#) ; [Leonard, 2025](#) [↗](#)) pouvant faire chuter les cours boursiers ([McConvey, 2025](#) [↗](#)), ou la production de fausses preuves soumises aux assureurs (Kapani, 2025).

La plupart des organisations réagissent par des correctifs techniques : déployer de nouveaux détecteurs, mettre à jour les protocoles de vérification, former le personnel. Or, cette approche passe à côté du changement épistémologique en cours. Elle traite les *deepfakes* comme des menaces isolées plutôt que comme les symptômes d'une fragilité plus profonde dans la manière dont les institutions produisent, valident et partagent le savoir.

"Nous ne devons donc pas seulement former les individus — nous devons reconcevoir les systèmes qui les font échouer."

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

savoir. Cela signifie concevoir ce que l'on peut appeler des écosystèmes du savoir : des environnements où diverses perspectives, méthodes et expériences interagissent pour générer une compréhension plus résiliente.

Les organisations doivent dépasser l'idée que la vérification est une compétence individuelle et l'ancrer dans leur architecture institutionnelle. Il s'agit d'intégrer la vérification dans les processus de travail et de valoriser la vigilance au-delà de la seule efficacité. Comme l'a noté Geary Rummler : « Placez un bon exécutant dans un mauvais système, et c'est le système qui gagne à chaque fois » ([Zemke, 1983](#) [🔗](#)). Nous ne devons donc pas seulement former les individus — nous devons reconcevoir les systèmes qui les font échouer.

Pilier 3 : écosystèmes intersectoriels de connaissance

Les défis posés par les médias synthétiques dépassent les frontières institutionnelles, alors que nos réponses demeurent cloisonnées. Les établissements d'enseignement, par exemple, tentent d'élaborer des techniques de vérification ; les institutions financières inventent leurs propres solutions ; les systèmes de santé découvrent des schémas de manipulation inconnus des autorités publiques ; et les concepteurs de technologies développent de nouvelles capacités synthétiques sans dialogue suffisant avec les professionnels concernés.

Prenons l'exemple d'une mère ciblée par un clonage vocal

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

ou des fraudes financières. Ces menaces exigent des réponses coordonnées.

Nous avons besoin de biens communs épistémiques — des espaces partagés où des parties prenantes diverses peuvent échanger et co-crée des stratégies. Cela suppose la mise en place de réseaux de partage de connaissances en temps réel et de partenariats interdisciplinaires : des éducateurs apprenant des experts en cybersécurité ; des gouvernements, à tous les niveaux, façonnant politiques et régulations ; la société civile contribuant à la conception technologique ; et des instances internationales facilitant l'élaboration de normes éthiques.

La pensée cybernétique (Wiener, 1948) peut nous guider ici. Dans ce modèle, les écosystèmes de connaissance fonctionnent comme des boucles de rétroaction s'adaptant aux nouvelles menaces et aux nouveaux savoirs. L'éducation doit contribuer à cultiver ces boucles adaptatives, favorisant l'humilité, la réflexivité et la réactivité — plutôt que des curriculums rigides ou des listes de vérification de la véracité, qui deviennent rapidement obsolètes.

L'occasion des sociétés apprenantes : architecturer les écosystèmes de connaissance

Ce moment de perturbation épistémique représente une occasion de mener un changement de paradigme mondial — passer du soutien à l'éducation traditionnelle à l'architecture d'écosystèmes de connaissance pour l'ère synthétique.

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

essentielles pour naviguer dans l'ambiguïté et la connaissance relationnelle.

Ce dialogue doit inclure activement les agences gouvernementales, les entreprises, les institutions d'enseignement, les systèmes de santé et les services financiers, car chacun apporte des pratiques de savoir distinctes qui, intégrées, produisent des compréhensions plus résilientes.

Au-delà du dialogue, ces secteurs devraient co-développer des normes internationales pour une « conception enrichissante du savoir » dans l'IA — des spécifications techniques et des principes éthiques mettant l'accent sur la transparence, la contextualisation et les garde-fous nécessaires à la préservation du sens collectif.

Nous devons bâtir des infrastructures mondiales pour partager les pratiques épistémiques émergentes à travers les frontières sectorielles. À mesure que les capacités synthétiques évoluent rapidement, nos réponses ne peuvent demeurer prisonnières des silos industriels ni attendre les cycles traditionnels de diffusion académique ou politique.

"Dans un monde où la réalité elle-même peut être programmée, notre défi ultime n'est pas seulement de détecter la tromperie, mais de nous engager dans le projet collectif de reconstruire la manière dont nous produisons le savoir et décidons de ce qui mérite d'être cru."


Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).


citoyennes et citoyens à y faire face. La tâche ne consiste pas seulement à enseigner de nouvelles techniques de vérification, mais à reconstruire notre relation même au savoir dans une ère où nos sens peuvent être trompés.

Cela nécessite de cultiver une littératie métacognitive approfondie — la capacité de réfléchir à la façon dont nous savons ce que nous savons. La finalité la plus élevée de l'éducation devient alors de nourrir les capacités humaines uniques que l'IA ne peut reproduire : la conscience contextuelle, le raisonnement éthique et la création collaborative de sens.

La voie à suivre n'est donc pas uniquement technique, mais profondément philosophique. Dans un monde où la réalité elle-même peut être programmée, notre défi ultime n'est pas seulement de détecter la tromperie, mais de nous engager dans le projet collectif de reconstruire la manière dont nous produisons le savoir et décidons de ce qui mérite d'être cru.

Références

Ahmed, S., Bee, A. W. T., Ng, S. W. T., & Masood, M. (2024). Social media news use amplifies the illusory truth effects of viral deepfakes: A cross-national study of eight countries. *Journal of Broadcasting & Electronic Media*, 1-28. <https://doi.org/10.1080/08838151.2024.2410783> 


Barrington, S., Cooper, E. A., & Farid, H. (2025). People are poorly equipped to detect AI-powered voice clones. *Nature*. <https://doi.org/10.1038/s41598-025-94170-3> 


Barrington, S. (2024, May 17). The impact of AI-generated content on society.

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).


YouTube. <https://www.youtube.com/watch?v=38qOi2ahojc> 

Forum canadien des organismes de réglementation numérique : Les médias synthétiques dans le paysage numérique. (2025, 18 Septembre).


Gouvernement du Canada. <https://bureau-concurrence.canada.ca/fr/comment-nous-favorisons-concurrence/education-sensibilisation/publications/forum-canadien-organismes-reglementation-numerique-medias-synthetiques-dans-paysage-numerique> 

Elsner, M., Atkinson, G., & Zahidi, S. (2025). The Global Risks Report 2025 20th Edition: Insight report. Dans *World Economic Forum*. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf 

Gilbert, T. F. (1978). *Human competence: Engineering worthy performance*. McGraw-Hill.


Kapani, C. (2025, February 24). Fraud attempts with deepfakes surge over last three years. *Insurance Times*. <https://www.insurancetimes.co.uk/news/fraud-attempts-with-deepfakes-surge-over-last-three-years/1454509.article> 


Kaufman, R., Oakley-Brown, H., Watkins, R., & Leigh, D. (2003). *Strategic planning for success: Aligning people, performance, and payoffs*. Jossey-Bass.


Knowles, M. S. (1978). Andragogy: Adult learning theory in perspective. *Community College Review*, 5(3), 9-20. <https://doi.org/10.1177/009155217800500302> 


Lalchand, S., Srinivas, V., Maggiore, B., & Henderson, J. (2024, May 24). Generative AI is expected to magnify the risk of deepfakes and other fraud

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

<https://www.govtech.com/education/k-12/laws-struggle-to-address-students-making-deepfakes> 


Lee Myers, S., Callahan, A., & Rosenbluth, T. (2025, 5 September). The doctors are real, but the sales pitches are frauds. *The New York Times*. https://www.nytimes.com/2025/09/05/technology/ai-doctor-scams.html?unlocked_article_code=1.mU8.ECJr.686YhfsfI0Ms&smid=nytcore-ios-share&referringSource=articleShare 

Leonard, J. (2025, 7 mai). *Accenture: What we learned when our CEO got deepfaked*. <https://www.computing.co.uk/event/2025/accenture-what-we-learned-when-our-ceo-got-deepfaked> 

McConvey, J. R. (2025, March 25). Call me fake Ishmael: For executives, deepfakes present a gargantuan problem. *Biometric Update*. <https://www.biometricupdate.com/202503/call-me-fake-ishmael-for-executives-deepfakes-present-a-gargantuan-problem> 

Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.


Naffi, N., Chaieb, M., Goulet, J., Bassal, M. H., Vallerand, V., Kuete Tapamo, Y. J., Lapointe, E., & Côté, S. (2024). Désinformation amplifiée par l'IA: Incidents médiatisés, régulations et technologies pour contrer les manipulations par deepfakes. *Obvia*. https://www.obvia.ca/sites/obvia.ca/files/ressources/202411-OBV-Pub-Desinformation_Amplifiee_IA_0.pdf 

Robins-Early, N. (2024, 10 May). CEO of world's biggest ad firm targeted by deepfake scam. *The Guardian*. <https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam> 


Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

Statista. (2024, April 17). How many businesses are affected by deepfake fraud? *Statista Daily Data*.

<https://www.statista.com/chart/32108/experiences-views-of-experts-on-advanced-identity-fraud-methods/> 

Statista. (2025, March 28). Global generative AI market size from 2021 to 2031. <https://www.statista.com/forecasts/1449838/generative-ai-market-size-worldwide> 


UNESCO. (2025, 20 février). Ce qu'il faut savoir sur les nouveaux référentiels de compétences en IA de l'UNESCO pour les élèves et les enseignants. *UNESCO*. <https://www.unesco.org/fr/articles/ce-quil-faut-savoir-sur-les-nouveaux-referentiels-de-competences-en-ia-de-lunesco-pour-les-eleves-et?hub=32618>

Vellani, N., & Common, D. (2025, March 20). Her grandson's voice said he was under arrest. This senior was almost scammed with suspected AI voice cloning. *CBC*. <https://www.cbc.ca/news/marketplace/marketplace-ai-voice-scam-1.7486437> 

Waier, J., & Shillair, R. (2024, July 29). *Deepfaking medical images: Eroding trust in medical diagnosis*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4909781 


Wiener, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. MIT Press.

Zahidi, S. (2025). *Global risks report 2025*. World Economic Forum.

Zemke, R. (1983). Geary Rummler: Training still isn't enough. *Training*, 20(8), 75-76. <https://eppic.biz/wp-content/uploads/2018/10/training-still-isnt-enough-training-magazine-1983.pdf> 

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

Biography

Dre. [Nadia Naffi](#)  est professeure agrégée en technologie éducative à l'Université Laval. Ses travaux visent à renforcer l'autonomisation et la capacité d'action des individus face à la désinformation amplifiée par l'intelligence artificielle et à l'usage non éthique des *deepfakes*, en adoptant des approches critiques et équitables de l'apprentissage tout au long de la vie.

Les futurs de l'éducation

Découvrez notre travail sur les futurs de l'éducation →

SHARE



THÈMES LIÉS

Sciences sociales et humaines

Future of education

SDG: ODD4 : 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

Cet article est lié aux **Objectifs de développement durable** des

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

Plus d'informations à ce sujet

Événement

Protéger et promouvoir la diversité culturelle et linguistique dans l'environnement numérique

17 décembre 2025



Événement

Séminaire en ligne de l'UNESCO sur les villes apprenantes « Faire tomber les barrières : l'apprentissage tout au long de la vie pour divers groupes de réfugiés et de migrants dans les villes ».

17 décembre 2025

Événement

Renforcer les compétences en IA des enseignants et des élèves : séminaire régional pour l'Amérique latine et les Caraïbes

11 décembre 2025



Événement

Cérémonie de remise du Prix UNESCO pour l'éducation à la citoyenneté mondiale



Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

Principes de l'éducation ouverte : résister aux métriques des boîtes noires de l'IA

28 octobre 2025

Idée

L'IA et le futur de l'éducation : bouleversements, dilemmes et perspectives

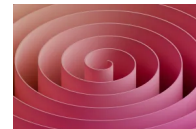
26 septembre 2025



Idée

Sortir de la boucle : remettre la pédagogie au cœur de l'ère de l'IA

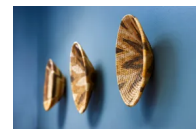
13 août 2025



Idée

L'IA dans l'éducation africaine : progrès ou perte de mémoire culturelle ?

11 août 2025



UNESCO



Actualit


Calend

In brief

Notre in

Notre E:

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).

[Portail de données](#) 

[S'abonner à nos lettres d'information](#) 

[UNESCO Shop](#) 

Conditions d'utilisation

[UNESCO Logo et Patronage](#)

[FAQ](#)

[Signaler un cas de fraude, corruption ou autre manquement](#)

[Alerte - Messages Frauduleux](#)

Politiques

[Protection des droits de l'homme \(Procédure 104\)](#)

[Politique de confidentialité](#)

[Accès à l'information](#)

[Gestion environnementale](#)

Follow us



Facebook



Threads



X



YouTube



Instagram



LinkedIn

Nous utilisons des cookies sur ce site pour améliorer votre expérience utilisateur. Pour en savoir plus sur la manière dont nous utilisons les cookies, veuillez lire [notre avis de confidentialité](#).