Mondialisation.ca
Centre de recherche sur la mondialisation

# Normaliser la surveillance dès le plus jeune âge : De plus en plus d'écoles utilisent la reconnaissance faciale et les technologies d'IA pour surveiller les enfants

Les parents et les élèves sont préoccupés par l'utilisation croissante des technologies d'intelligence artificielle en classe, selon une enquête du Centre pour la démocratie et la technologie. Les experts en protection de la vie privée mettent en garde contre le fait que ces technologies visent à "manipuler et à contrôler le comportement des enfants en leur inspirant de la peur".

Par Michael Nevradakis
Thème: Science et médecine
Mondialisation.ca, 05 janvier 2024
The Defender 22 décembre 2023

Les parents et les élèves sont de plus en plus préoccupés par l'utilisation des technologies d'intelligence artificielle (IA) en classe, en particulier la technologie de reconnaissance faciale, selon une enquête du Center for Democracy and Technology (Centre pour la démocratie et la technologie, CDT ).

Le rapport du CDT, publié le 12 décembre, révèle que plus de la moitié des parents et des élèves interrogés s'inquiètent de l'utilisation de la reconnaissance faciale et d'autres technologies d'intelligence artificielle, y compris les systèmes de localisation, dans les écoles.

Les enseignants, qui ont également été interrogés, ont montré un degré d'acceptation plus élevé des technologies.

Selon le rapport, un nombre croissant d'écoles ont mis en place de tels outils.

Les partisans de ces technologies affirment qu'elles peuvent contribuer à protéger les environnements scolaires contre les menaces violentes, telles que les tireurs dans les écoles.

Les défenseurs de la vie privée soutiennent que les technologies qui présentent un risque pour la vie privée et les données personnelles des élèves n'ont pas prouvé qu'elles renforçaient la sécurité dans les écoles..

**Un fossé profond entre les écoles, les parents et les élèves**

Selon le CDT, "des outils de sécurité expérimentaux et potentiellement dangereux sont utilisés sans tenir compte des préoccupations des élèves et des parents", y compris des technologies "que nous considérions auparavant comme trop extravagantes".

Il s'agit notamment de l'analyse prédictive, de la surveillance à distance, de la reconnaissance faciale, du partage des données des forces de l'ordre, des systèmes de détection d'armes et de la géolocalisation des étudiants.

Poussées par [l'industrie de] l'IA, ces technologies "sont déployées dans les écoles pour répondre aux fusillades de masse, à la crise de la santé mentale des jeunes et à d'autres menaces permanentes pour la sécurité du personnel et des élèves", a déclaré le CDT – une tendance "alarmante" selon laquelle les écoles poursuivent le déploiement de ces technologies en dépit des "niveaux élevés d'inquiétude" des parents et des élèves.

Ces "niveaux élevés d'inquiétude" étaient évidents dans les résultats de l'enquête:

- 58 % des parents et 55 % des élèves (et 33 % des enseignants) sont préoccupés par l'utilisation de caméras de reconnaissance faciale pour vérifier qui devrait être autorisé à entrer dans un bâtiment scolaire ou qui est autorisé à s'y trouver.
- 71 % des parents et 74 % des élèves (et 36 % des enseignants) se sont dits préoccupés par l'utilisation de ces technologies pour localiser physiquement les élèves.
- 60 % des parents et 58 % des élèves (et 31 % des enseignants) s'inquiètent de l'utilisation de caméras d'IA "pour remarquer des mouvements physiques inhabituels ou irréguliers".
- 55% des parents et 45% des élèves (et 27% des enseignants) ont exprimé leur inquiétude quant à l'utilisation de ces technologies pour détecter les coups de feu dans l'enceinte de l'école.
- 69 % des élèves et des parents (et 36 % des enseignants) sont préoccupés par le fait que les données relatives aux élèves sont analysées afin de prédire quels élèves sont les plus susceptibles de commettre un crime, un acte violent ou un acte d'automutilation.
- 66 % des parents et 65 % des élèves (et 38 % des enseignants) ont exprimé leur inquiétude quant à la possibilité que les informations scolaires des élèves, telles que leurs notes et leur assiduité, soient communiquées aux forces de l'ordre.
- 68 % des parents et 71 % des élèves (et 37 % des enseignants) s'inquiètent de l'utilisation de ces technologies pour surveiller les comptes de médias sociaux des élèves.

Ces résultats montrent "un profond décalage entre les priorités des écoles, des parents et des élèves en ce qui concerne les décisions d'achat d'edtech [educational data and technology] ", écrit le CDT.

**Les écoles utilisent les fonds de récupération COVID pour acheter des technologies de surveillance**

L'enquête s'appuie sur un rapport du CDT, publié en septembre, sur les outils edtech qui filtrent et bloquent les contenus, surveillent les activités des élèves ou utilisent l'IA générative.

Selon ce rapport, la pandémie de COVID-19 a contribué à accélérer l'adoption de ces technologies en milieu scolaire – une évolution que la CDT considère d'un œil critique.

“L’utilisation de logiciels de suivi des activités des étudiants s’est rapidement développée dans le cadre de l’apprentissage à distance et est restée très présente dans la vie des étudiants. Malheureusement,

il continue de nuire aux étudiants qu’il est censé aider”, indique le rapport.

Selon le rapport, ces préjudices vont des mesures disciplinaires à la divulgation d’informations sur les élèves sans leur consentement et à l’établissement d’un contact avec les forces de l’ordre.

Le rapport comprend également des données indiquant que 88 % des enseignants déclarent que leur école utilise un logiciel de surveillance des activités des élèves, 40 % des enseignants déclarent que leur école surveille les appareils personnels des élèves et 38 % des enseignants déclarent que leur école surveille les élèves en dehors des heures de classe – bien que, notamment, il y ait eu une diminution de 9 points de pourcentage dans cette mesure par rapport à l’année scolaire 2021-22.

Kenneth Trump, président de National School Safety and Security Services, a déclaré à Education Week en octobre : “Les écoles ont utilisé les fonds de récupération COVID pour acheter des équipements et du matériel de sécurité”.

Les entreprises technologiques ont “intensifié” la commercialisation de ces produits auprès des districts scolaires ces dernières années, selon M. Trump, qui a déclaré que ces achats “ont été utilisés pour résoudre des problèmes politiques et de relations avec les communautés, et pas tellement des problèmes de sécurité dans les écoles”.

“Lorsqu’il y a utilisation ou confiscation d’armes à feu sur un campus, nous voyons les conseils d’administration des écoles et les directeurs prendre des décisions irréfléchies et jouer sur les besoins émotionnels de sécurité des parents et du personnel”, a ajouté M. Trump.

Au Royaume-Uni, Sky News a rapporté en octobre 2021 que 27 écoles avaient commencé à utiliser un système de reconnaissance faciale pour servir le déjeuner aux élèves et que 15 autres étaient prêtes à mettre en œuvre cette technologie – une mesure censée réduire le risque de transmission du Covid-19.

Sky News a rapporté que les parents et les activistes “ont mis en garde contre la normalisation de l’exposition des enfants à la surveillance biométrique, et se sont plaints qu’ils n’étaient pas sûrs que les étudiants soient correctement informés du risque pour la vie privée”.

Malgré le taux élevé de consentement des parents, Sky News a rapporté à l’époque que les défenseurs de la vie privée des enfants, Jen Persson et Pippa King, avaient déclaré au commissaire à l’enfance d’Écosse : “Il ne faut pas confondre taux de participation élevé et consentement”, notant que les formulaires de consentement fournis aux parents donnaient l’impression que l’acceptation était obligatoire.

Ces plaintes ont conduit l’Information Commissioner’s Office, l’organisme britannique de surveillance des données, à ouvrir une enquête. Le conseil écossais de North Ayrshire a suspendu son déploiement de la technologie, tandis que la Chambre des Lords britannique a

débattu de la question en novembre 2021.

Greg Glaser, avocat plaidant en Californie pour les initiatives de protection de la vie privée de Children Health Defense, a déclaré au Defender que “pendant l’ère des masques et des fermetures poir le Covid, les parents ont été témoins d’une normalisation forcée des salles de classe Zoom, mais Zoom n’était pas la seule technologie normalisée pour les jeunes”.

M. Glaser a ajouté :

“Cette situation n’est pas surprenante pour les écoles publiques. La bureaucratie n’est pas organisée pour remédier aux problèmes de fond de la société, mais pour traiter les symptômes. Rien ne s’améliorera vraiment dans les écoles publiques tant que la société ne décidera pas d’apprendre la leçon la plus profonde, à savoir pourquoi les enfants échouent dans un système conçu pour échouer. Pourquoi le système a-t-il été conçu pour blesser les enfants ?

Pendant ce temps, l’industrie de l’éducation, qui réalise des milliards de dollars de bénéfices en “luttant” contre l’échec, continuera à proposer ses prétendues solutions. C’est tellement lassant – on peut repérer l’escroquerie à un kilomètre”.

**Inquiétudes quant aux “effets paralysants” des technologies de reconnaissance faciale dans les écoles**

Selon le CDT, les technologies utilisées “au nom de la sécurité des élèves” présentent des capacités dont les responsables de l’éducation et les décideurs politiques devraient se préoccuper.

Il s’agit notamment d’un manque d’efficacité et de précision, dû à des limitations techniques, à des “faux positifs” qui pourraient conduire à des “mesures disciplinaires non fondées” à l’encontre des étudiants, et à des difficultés d’audit de ces systèmes.

Une autre série de préoccupations, selon le CDT, concerne les “effets de refroidissement”. Selon le CDT, “l’intégration de divers outils technologiques de sécurité invasifs dans l’environnement d’apprentissage d’un élève peut en fait faire en sorte que les élèves se sentent moins en sécuritédans la salle de classe”.

“Un contrôle et une surveillance excessifs peuvent entraver la liberté d’expression, d’association et de mouvement, ainsi que l’accès aux ressources vitales”, a déclaré le CDT.

Ces préoccupations ont été reprises dans un article publié en 2020 dans la revue Learning, Media and Technology par Mark Andrejevic, Ph.D., et Neil Selwyn, Ph.D., de l’université Monash en Australie, selon lequel ces technologies peuvent modifier “la nature des écoles et de l’enseignement selon des critères de division, d’autoritarisme et d’oppression”.

“Le principal défi auquel sont confrontés les éducateurs est de savoir s’il existe ou non une perspective future réaliste de remodeler ces technologies à des fins plus bénéfiques et/ou bénignes. Sinon, s’agit-il d’une forme de technologie numérique qui ne devrait pas être appliquée “pédagogiquement” sous quelque forme que ce soit ?”, écrivent les auteurs.

Tim Hinchliffe, rédacteur en chef de The Sociable, a déclaré à The Defender : “La reconnaissance faciale dans les écoles vise à manipuler le comportement et à normaliser la surveillance totale dès le plus jeune âge”.

“Dans les salles de classe, la reconnaissance faciale apprend aux enfants qu’ils n’ont pas de vie privée et que tout ce qu’ils disent ou font peut être et sera utilisé contre eux. Cela permet aux gouvernements et aux entreprises de contrôler plus facilement les générations futures, car elles sont éduquées dans l’idée que la vie privée n’existe pas et qu’elles feraient mieux de faire ce qu’on leur dit, sinon”, a-t-il ajouté.

M. Hinchliffe a cité un reportage de l’émission “Good Morning America” de 2020 qui montrait une vidéo d’une classe en ligne de l’école primaire de Parkland au Texas. Lorsque la connexion Zoom d’un enseignant de deuxième année a été interrompue, les élèves ont d’abord réagi, avant de se rendre compte que l’appel était toujours enregistré.

“Les enfants ont d’abord commencé à faire des siennes, mais lorsqu’un élève s’est rendu compte qu’il était toujours enregistré, ils se sont tous conformés de peur d’avoir des ennuis avec le directeur de l’école. C’est cette peur qui rend le système si puissant et qui pousse les enfants à se conformer”, a-t-il déclaré.

Pin Lean Lau, docteur en droit de la Brunel Law School de Londres, a raconté une conversation avec sa fille qui, lorsqu’on lui a demandé si elle s’inquiéterait de l’utilisation de la technologie de reconnaissance faciale par la cafétéria de son école, a répondu : “Pas vraiment. Cela rendrait les choses beaucoup plus rapides à la caisse”.

Selon Mme Lau, “ses propos confirment la préoccupation selon laquelle les enfants sont beaucoup moins conscients de leurs droits en matière de données que les adultes”.

“À l’échelle macroéconomique, une population qui se sait surveillée modifiera son comportement pour se conformer aux normes, et ses citoyens se surveilleront eux-mêmes”, a déclaré M. Hinchliffe.

Le rapport du CDT aborde également l’impact potentiellement disproportionné de ces technologies sur les catégories d’étudiants protégés, le manque de ressources dont disposent de nombreuses écoles pour entretenir et mettre à jour ces technologies, le manque de clarté des mécanismes de gouvernance supervisant l’utilisation de ces technologies, et les risques pour la vie privée tels que les violations de données.

Un piratage datant de 2021 et touchant Verkada, un développeur de technologies de sécurité basées sur l’informatique en nuage largement utilisées dans les écoles, a exposé publiquement des flux en direct provenant de caméras de surveillance.

Irene Knapp, directrice de la technologie au sein de l’organisation à but non lucratif Internet Safety Labs, a déclaré à Education Week que les écoles devaient réfléchir attentivement à la question de savoir si elles souhaitaient assumer la responsabilité du traitement et de la protection des données biométriques des élèves.

Selon Mme Knapp, il est difficile de savoir si les données collectées par ces technologies sont partagées avec des tiers.

Selon Education Week, “il existe également un risque réel de détournement de mission”, car il est “tentant” pour les écoles d’utiliser des technologies de surveillance telles que la reconnaissance faciale à des fins non prévues à l’origine, “telles que le suivi et l’imposition d’amendes aux parents qui sont en retard pour récupérer leurs enfants à l’école”.

Molly Kleinman, Ph.D.directrice générale du programme Science, technologie et politique

publique de l'université du Michigan, a déclaré à Route Fifty en septembre, que sans réglementation, les écoles peuvent utiliser ces technologies pour des "tâches de routine" ou exiger la reconnaissance faciale pour que les élèves se connectent aux ordinateurs et tablettes appartenant à l'école.

Selon M. Hinchliffe, "même si la reconnaissance faciale commence à l'entrée des écoles pour vérifier qui entre pour de soi-disant "raisons de sécurité", ce n'est qu'une question de temps avant qu'elle n'entre dans la salle de classe, et lorsqu'elle le fera, elle privera les élèves d'une autre partie de leur enfance, et les enfants n'auront plus le droit d'être des enfants".

"Du point de vue de la législation sur la protection de la vie privée, les écoles de surveillance gouvernementales s'exposent à de nombreuses responsabilités potentielles, car leurs procédures d'acceptation, s'il y en a, ne couvriront pas la réalité de ce qu'elles et leurs partenaires commerciaux font", a déclaré M. Glaser.

"Il suffit d'une seule violation de données pour que les parents soient informés", a déclaré M. Glaser. "Et lorsque les procédures de sécurité ne sont pas respectées, des poursuites judiciaires sont engagées. Du moins, c'est ainsi que le système conçu pour échouer échouera".

Ces préoccupations ne sont pas nouvelles. Dès 2019, le magazine Wired s'est penché sur la "délicate éthique" de la mise en œuvre des technologies d'IA dans les salles de classe.

**New York interdit les technologies de reconnaissance faciale dans les salles de classe**

Ce sont ces "graves préoccupations concernant l'utilisation de la technologie de reconnaissance faciale", qui "ne l'emportent pas sur ses prétendus avantages", qui ont conduit l'État de New York à promulguer une interdiction de ces technologies en septembre, interdisant aux écoles "d'acheter ou d'utiliser la technologie de reconnaissance faciale".

Cette décision a été prise à la suite d'une analyse effectuée par l'Office of Information Technology Services et sur la base de données recueillies par l'organisation à but non lucratif The Violence Prevention Project, qui a révélé que 70 % des auteurs de fusillades dans les écoles entre 1980 et 2019 étaient des étudiants actuels.

Une étude réalisée en 2020 par l'université du Michigan sur la technologie de reconnaissance faciale et son impact dans les salles de classe a peut-être également influencé la décision de New York d'imposer une interdiction.

Selon l'étude, la technologie de reconnaissance faciale "aura probablement cinq types d'implications : exacerbation du racisme, normalisation de la surveillance et érosion de la vie privée, rétrécissement de la définition de l'étudiant "acceptable", marchandisation des données et institutionnalisation de l'inexactitude".

"La FR [facial recognition] étant automatisée, elle étendra ces effets à un plus grand nombre d'étudiants qu'un système manuel ne pourrait le faire", ajoute l'étude. "Sur la base de cette analyse, nous recommandons vivement d'interdire l'utilisation de la FR dans les écoles.

L'étude a également émis un large éventail de recommandations nationales et locales à

l'intention des écoles qui continueraient à utiliser ces technologies. Des recommandations similaires ont été formulées par le CDT dans son rapport du 12 décembre.

En 2019, Vox a noté que les écoles utilisaient de plus en plus la reconnaissance faciale pour tenter d'arrêter les fusillades, mais a estimé qu'elles devraient réfléchir à deux fois avant d'adopter cette pratique.

Les districts scolaires peuvent toujours choisir d'utiliser d'autres types de technologies biométriques, telles que les empreintes digitales, conformément à la nouvelle politique de New York.

Selon Education Week, les technologies de reconnaissance faciale et d'identification des armes par l'IA "peuvent être une solution séduisante pour les commissions scolaires et les directeurs d'école qui cherchent à rassurer les parents".

L'État de New York a mis en place un moratoire sur la reconnaissance faciale après que des parents aient contesté juridiquement l'adoption de cette technologie par le Lockport Central School Districten janvier 2020, selon le magazine Time.

"Le district de l'ouest de l'État de New York a été l'un des premiers du pays à intégrer cette technologie à la suite des fusillades meurtrières qui ont conduit les administrateurs du pays à adopter des mesures de sécurité allant du verre pare-balles aux gardes armés", a rapporté le Time.

En 2020, deux lycées français qui avaient expérimenté la technologie de reconnaissance faciale ont été poursuivis en justice, ce qui a conduit à une décision du tribunal administratif interdisant cette pratique.

Selon la décision, la mise en œuvre de la technologie "n'était ni proportionnée ni nécessaire", le consentement des étudiants n'avait pas été obtenu librement et des mesures moins attentatoires à la vie privée auraient pu être mises en œuvre.

Ailleurs, cependant, le déploiement de ces technologies se poursuit. En août, Philadelphie a annoncé qu'elle mettrait en place des drones appartenant au district "pour patrouiller dans les zones sujettes à la violence sans que la police soit présente sur le terrain".

Biometric Update a rapporté en octobre 2022 que les écoles du Montana utilisent la technologie de reconnaissance faciale de Verkada "dans le but d'améliorer la sécurité". Le district scolaire de Sun River Valley, par exemple, alimente son système de reconnaissance faciale avec "une liste de surveillance du département du shérif local, ainsi que des photos d'élèves prises dans l'annuaire de l'école (ou album de fin d'année)".

Selon M. Hinchliffe, la Chine développe capacités de reconnaissance faciale dans ses écoles "grâce à l'IA et aux dispositifs portables, afin d'inclure la reconnaissance des émotions et d'autres aspects comportementaux, de manière à pouvoir déterminer si un enfant est contrarié ou s'il n'est pas attentif".

"Encore une fois, la reconnaissance faciale dans les écoles a pour but de manipuler et de contrôler le comportement en instillant la peur chez l'enfant", a déclaré M. Hinchliffe.

L'avocat Richard Jaffe a déclaré au Defender qu'il y avait de la place pour la reconnaissance faciale dans les écoles.

“La vie privée, comme tous les droits, n’est pas absolue et doit céder le pas au droit des élèves à la sécurité.

“Je pense que la plupart des parents et la quasi-totalité des enseignants et du personnel accepteront des atteintes relativement mineures à la vie privée pour renforcer la sécurité des écoles. À moins de verrouiller toutes les écoles et de les faire garder par un peloton de policiers du SWAT armés de M16, la solution doit faire appel à la technologie et, de plus en plus, à l’intelligence artificielle et à la reconnaissance faciale”, a-t-il déclaré.

“La plupart des gens accepteront ce compromis et je doute fort que les tribunaux se prononcent en faveur des districts scolaires qui utilisent les mesures actuellement disponibles”, a ajouté M. Jaffe.

Forbes, dans un article paru en février 2023, a également estimé que les technologies de reconnaissance faciale avaient leur place dans les écoles, les qualifiant de “technologie intelligente” mais notant leur “mauvaise, mauvaise, mauvaise mise en œuvre” et affirmant qu’il y avait “des obstacles à surmonter avant que la reconnaissance faciale ne puisse être utilisée”.

Ces obstacles incluent “la recherche sur les impacts sur le bien-être et l’éthique de l’utilisation de la biométrie dans les écoles”, la garantie que ces systèmes “fonctionnent par défaut selon les plus hauts niveaux de protection des droits”, et la garantie que leur utilisation est “pleinement légale” sans “conséquences imprévues”.

**Michael Nevradakis**, Ph. D.



---

*Articles Par :* **Michael Nevradakis**