La technologie à l'école : protéger sans surveiller

Chaque école est responsable à un certain niveau du bien-être et de la sécurité de ses élèves. La sécurité des élèves est un vaste sujet qui couvre de nombreux domaines fonctionnels. Généralement, il est laissé à l'interprétation de l'académie ou de l'école.

C'est en effet aux établissements de déterminer les mesures de sécurité à mettre en œuvre, du filtrage des contenus respectueux de la vie privée à l'installation d'enregistreurs de frappe, qui surveillent tout ce qu'un élève tape, envoie et reçoit sur les appareils fournis par l'école.

Le document aborde :

- La signification du contrôle et de la surveillance
- Les implications plus larges de ces termes dans le contexte de l'éducation et de la confidentialité des élèves
- Les facteurs à prendre en compte afin d'élaborer des règles pour encadrer l'utilisation de la technologie et prendre des décisions éclairées quant aux mesures à appliquer.

Le problème

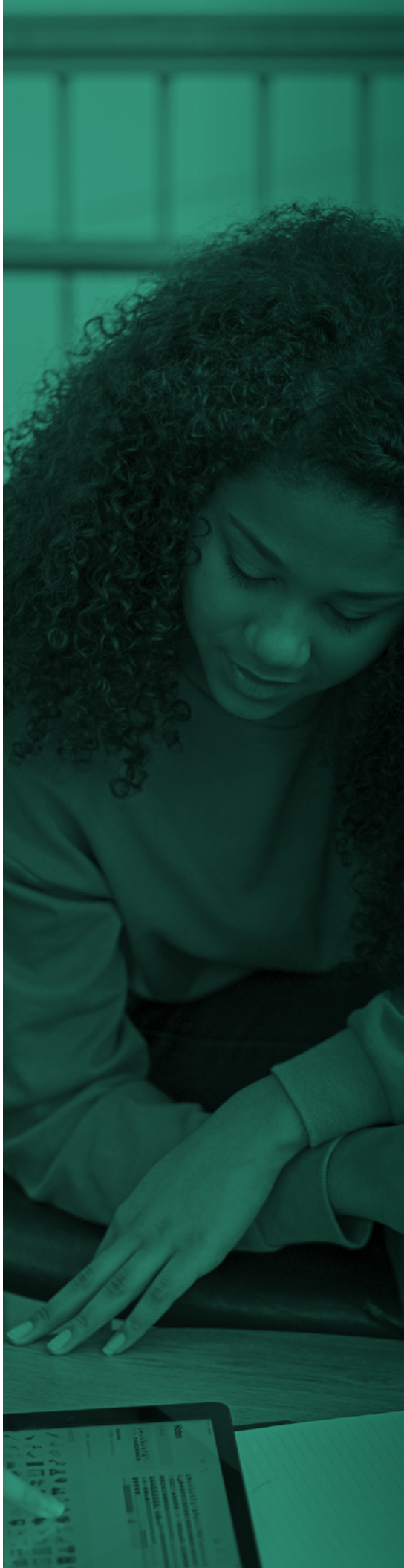
Il faut tout un village : enseignants, parents, professionnels de la santé, administrateurs informatiques, amis... la liste des personnes qui influencent la vie des élèves est longue. En moyenne, **les élèves américains passent environ mille heures par an** à l'école, réparties sur 180 jours. Les enseignants et le personnel administratif sont des acteurs clés dans la vie des élèves. Ils ont une influence sur leur éducation, leur santé mentale, leur usage des technologies, leur bien-être en général et bien d'autres aspects.

Les établissements d'enseignement restreignent l'utilisation d'Internet par les élèves au nom de leur sécurité : certains vont même jusqu'à surveiller l'utilisation de grossièretés, les indicateurs d'auto-mutilation ou de violence, et les manifestations de harcèlement scolaire. L'éducation n'est qu'une partie de la vie des élèves, et certains d'entre eux utilisent leur appareil hors du contrôle de l'établissement. Dans ce contexte, dans quelle mesure les écoles doivent-elles s'impliquer dans la supervision de leur bien-être mental et physique ? Et quelle part de cette supervision doit être liée à leur présence en ligne ? Malheureusement, il n'y a pas de réponse évidente.

Internet offre aux institutions de grandes opportunités d'éducation. Les possibilités d'approches pédagogiques individualisées et l'accès à d'innombrables ressources sont un appui pour l'apprentissage des élèves dans notre monde axé sur l'information. Mais bien sûr, ce pouvoir implique une responsabilité : il est essentiel de réfléchir à la manière dont les élèves interagissent avec le contenu disponible en ligne, qui peut être dangereux.

L'éducation ne s'arrête pas à l'exploration des connaissances en ligne. Les écoles veulent autonomiser les élèves pour qu'ils deviennent des internautes responsables, tout en assurant leur sécurité. Il n'existe pas de méthode définie pour équilibrer ces concepts, et l'on trouve donc un large éventail d'approches de la sécurité des élèves en ligne. Devons-nous simplement informer l'élève sur le bon usage d'Internet et le lancer sur la toile sans garde-fou ? Ou faut-il tout verrouiller pour que les élèves n'aient accès qu'aux sites que nous aurons choisis et vérifiés au préalable ?

Ces deux extrémités du spectre offrent un bon aperçu d'une problématique essentielle de l'éducation : liberté d'explorer ou accès limité. Et si nous autorisions une certaine liberté d'exploration tout en gardant un œil sur les élèves ? Est-ce que l'un de ces deux extrêmes résout réellement le problème de la sécurité des élèves, ou existe-t-il de meilleures solutions ? Comment assurer la sécurité des élèves de manière globale, même hors du cadre de l'école ?



Comprendre les différentes approches

Voyons quelques approches du traitement des données des élèves. La première est la **supervision**.

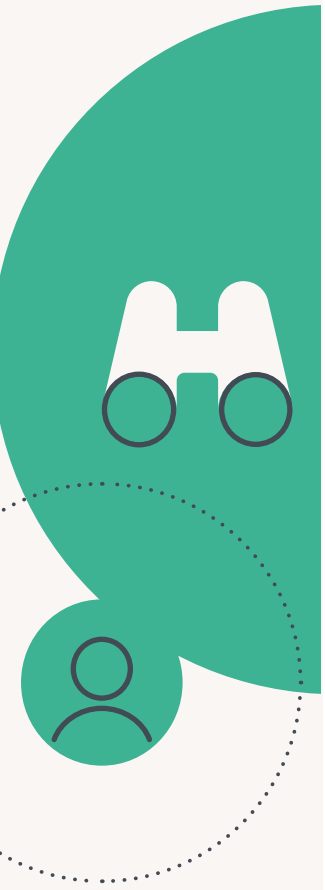
Supervision

La supervision de l'utilisation de l'internet par les élèves permet de recueillir des données sur les sites auxquels ils accèdent, ainsi que le moment et la durée des visites. Ces données permettent aux institutions de dégager des tendances :

- Quels types de ressources les élèves recherchent-ils ?
- À quel moment de la journée font-ils des recherches ? Pendant les cours ou en dehors ?
- Sur quels contenus les élèves passent-ils le plus de temps ?

La supervision se concentre sur les données – les sites web consultés – plutôt que sur les élèves eux-mêmes. Elle permet de comprendre le comportement général d'un groupe d'élèves et de réagir à d'éventuels problèmes.

Les modalités de collecte et de stockage des données peuvent être adaptées pour minimiser la quantité d'informations personnelles identifiables (IPI). On va ainsi protéger la confidentialité des utilisateurs tout en obtenant des informations utiles. En collectant des données anonymes, on minimise également la quantité d'informations nominatives perdues en cas de violation – un phénomène de plus en plus courant.



La deuxième est la **surveillance.**

Surveillance

La surveillance va plus loin en associant les données à des individus, généralement dans le but d'identifier un comportement inapproprié en temps réel. Son champ peut être très large : enregistrement de l'historique de recherche, analyse de ses frappes au clavier et même consultation de ses messages privés. Certaines académies n'installent ces outils de surveillance que sur les appareils de l'école, mais d'autres surveillent également le comportement des élèves **sur les réseaux sociaux**.

La surveillance permet de détecter les comportements nuisibles des élèves avant qu'ils ne deviennent dangereux pour les autres ou pour eux-mêmes. Et c'est la raison pour laquelle certains districts scolaires optent pour cette approche. Mais elle est très difficile à mettre en œuvre sans violer la confidentialité des élèves ni susciter une **méfiance à l'égard de l'établissement**. Elle présente également le défaut de générer de fausses alertes et de **cibler de manière disproportionnée certains groupes démographiques**.

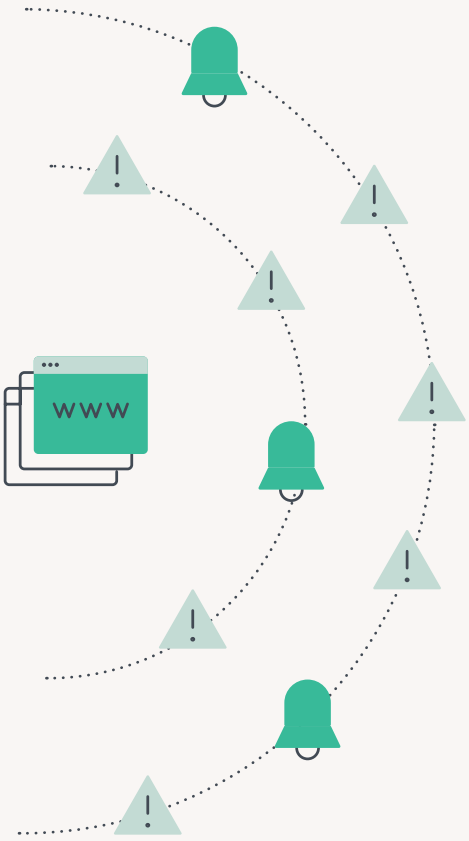
Selon une étude récente du **Center for Democracy and Technology** , 44 % des enseignants affirment connaître un élève qui a été contacté par les forces de l'ordre sur la base des données recueillies par leur école. **Et 29 % des étudiants LGBTQ+ déclarent** que cette technologie a divulgué leur situation ou celle d'une connaissance.

C'est indéniable : la surveillance affecte tous les aspects de la vie des élèves, et pas seulement à l'école. Les adultes ne toléreraient pas un tel niveau de contrôle : pourquoi en faire une norme dans le contexte éducatif ?

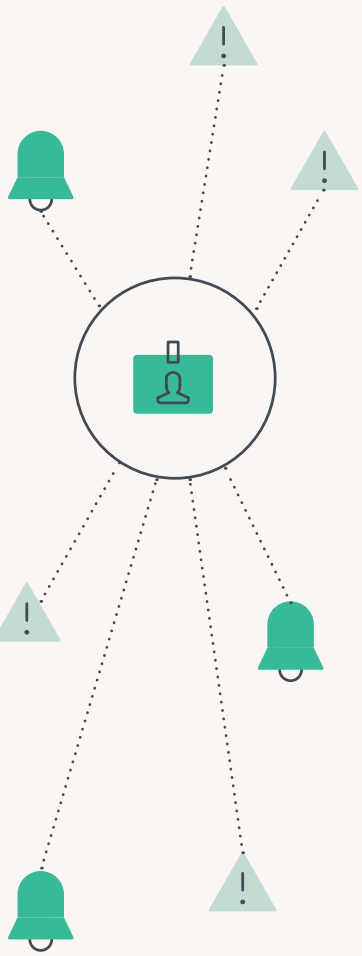
L'accumulation des données multiplie les problèmes

La collecte et l'utilisation des informations personnelles des étudiants peuvent poser un certain nombre de problèmes.

En premier lieu, les étudiants des tranches de revenus inférieures ne bénéficient pas du même niveau de confidentialité. Les élèves qui n'ont pas accès à un appareil personnel et ne peuvent utiliser que l'appareil fourni par l'école sont soumis à un niveau de surveillance accru. Les élèves des milieux plus aisés ont accès à un appareil personnel, un iPhone ou un iPad par exemple, qui préserve davantage leur vie privée. Selon un **rapport McKinsey de 2020** portant sur l'effet de l'apprentissage à distance sur les étudiants, environ 9 % des étudiants n'avaient pas un accès régulier à Internet à la maison, et les personnes noires et hispaniques étant 3 à 4 % moins susceptibles d'y avoir accès. Ces inégalités rampantes en matière de technologie peuvent rendre ces groupes démographiques plus sensibles à la surveillance et les exposer davantage à ses conséquences.



Les enseignants affirment que les outils de suivi les aident à identifier les jeunes en difficulté et à leur apporter l'aide dont ils ont besoin, à une époque où la dépression et l'anxiété sont en hausse dans cette classe d'âge. Pourtant, les résultats d'une **enquête nationale menée par le Center for Democracy and Technology** (CDT), un organisme à but non lucratif, dessine une autre réalité : au lieu de recevoir de l'aide, de nombreux élèves sont punis pour avoir enfreint le règlement. Et dans certains cas, les résultats de l'enquête suggèrent que les étudiants sont victimes de discrimination. Cela qui soulève à nouveau la question : la technologie aide-t-elle réellement les élèves ? Les avis et les pratiques divergent d'une école à l'autre, une chose semble claire : la technologie seule ne suffit pas.



Des mesures de surveillance drastiques renforcent nécessairement la sécurité, n'est-ce pas ? En réalité, les possibilités techniques offertes la collecte de toutes ces données ont une efficacité médiocre et augmentent les risques juridiques pour les écoles qui font ce choix. Les détections reposent sur un ensemble de mots-clés qui génèrent une alerte lorsqu'ils apparaissent. La quantité de faux positifs est considérable, mais l'école est tout de même tenue de réagir à chaque alerte.

Les vraies alertes peuvent en effet être le signe d'un problème potentiel avec un élève. Mais elles sont rarement le premier. Les véritables indicateurs sont généralement des aspects que les humains sont plus susceptibles de remarquer en premier : le comportement général de l'élève, son apparence, ses résultats scolaires, ses échanges avec ses camarades, son humeur, son assiduité et bien d'autres choses encore. S'appuyer sur la technologie pour repérer les élèves en difficulté peut s'avérer aussi lent qu'inefficace.

Prévenir plutôt qu'inspecter

De nombreux établissements scolaires veulent que les élèves puissent naviguer en toute sécurité sur Internet, et limitent à cette fin l'accès aux sites inappropriés – jeux d'argent, contenus pour adultes, jeux vidéo et autres sites incompatibles avec l'apprentissage. Le filtrage de contenu peut être très utile en bloquant l'accès en amont. Cette approche s'oriente davantage vers un accès libre – mais sécurisé – à Internet. Les étudiants peuvent explorer librement dans un environnement contrôlé qui évite qu'ils consultent des sites potentiellement dangereux.

Quand les élèves sont protégés par un dispositif de filtrage des contenus, la surveillance des sites qu'ils consultent n'est plus nécessaire. Et se pose à nouveau la question de la confidentialité des élèves : les établissements doivent-elles examiner tout ce que fait un étudiant, ou enquêter uniquement en cas d'inquiétude ?

En bloquant en amont l'accès à certains sites et domaines de contenu, les établissements peuvent faire d'Internet un outil d'apprentissage et d'enseignement en classe au quotidien. Les élèves peuvent enrichir leurs connaissances autour du contenu exploré dans le programme, à l'abri des contenus néfastes. Certains outils sont capables de limiter Internet à une poignée de sites approuvés ou, plus souplement, à certaines catégories de contenu. Dans le contexte de la classe, cela permet aux élèves d'explorer différentes sources de connaissances et d'apprendre à faire un usage constructif d'Internet, en toute autonomie. Autrement dit, les élèves approfondissent leurs connaissance tout en devenant de bons citoyens numériques – un acquis précieux pour le reste de leur vie.

Une approche plus réactive consisterait à analyser les contenus consultés puis à intervenir. Mais cela présuppose une surveillance. Il faudrait également que du personnel dédié, appuyé par une assistance informatique, passe en revue les sites visités et intervienne après-coup.

La solution ?

La Convention des Nations unies relative aux droits de l'enfant énonce **des orientations concernant le respect de la vie privée des enfants :**

1. Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

C'est un excellent principe pour la protection de la vie privée des enfants. Mais il ne fournit pas d'indications explicites sur la mise en œuvre d'une règle technologique équilibrée qui mette les élèves à l'abri du danger. Les élèves ne peuvent pas se prévaloir de leur « droit à la confidentialité » pour échapper à la surveillance des appareils scolaires, et n'ont donc que peu ou pas de contrôle sur la manière dont leur école traite leurs informations. Ce contrôle peut même s'étendre aux appareils personnels présents sur les réseaux scolaires, par le biais des règles d'utilisation acceptables (RUA) qui peuvent inclure une collecte des données. En d'autres termes, les élèves n'ont aucun choix face aux pratiques de collecte de leur établissement scolaire, et ceux qui n'ont pas leur propre forfait de données ou ne disposent pas d'un appareil personnel sont particulièrement touchés.

Les écoles doivent donc élaborer leurs règles et procédures en s'appuyant sur leur vision de la sécurité des élèves. Il est vrai que le danger peut venir de partout : d'Internet, de leur camarades de classe et, parfois, d'eux-mêmes. Les écoles sont obligées de répondre à la pression de la communauté et cherchent par-dessus tout à empêcher le pire scénario : la perte de la vie d'un élève.

La technologie n'est pas une panacée

La question est donc de savoir ce que les écoles doivent faire concrètement. Encore une fois, il faut un village pour élever un enfant, et la technologie seule ne peut pas assurer la sécurité des élèves. Les élèves doivent composer avec Internet, leurs relations avec leur famille et leurs amis, leur propre santé mentale et leur identité, et leur niveau de vie à la maison. Il est essentiel que les conseillers scolaires, les enseignants, les professionnels de santé et les administrateurs des établissements scolaires continuent d'entretenir avec les élèves des relations étroites, qui restent la meilleure façon d'évaluer le bien-être d'un individu. Plutôt que d'envahir toute la vie de l'élève, la technologie doit être une partie seulement de la solution. La surveillance ne doit être envisagée que lorsque des professionnels pensent qu'un étudiant présente un risque, et non comme une pratique généralisée à tous les élèves. Quand un étudiant aura obtenu son diplôme, il sera libre d'explorer entièrement Internet. Mais si son campus verrouille le Web, comment se préparera-t-il aux menaces qu'il risque d'y croiser ?

Un bon filtrage des contenus peut limiter les distractions et les dangers quand les élèves sont encore à l'école, sans leur donner l'impression que tout ce qu'ils disent, font ou pensent est scruté à la loupe dans un climat de suspicion (et de sanction). Le filtrage s'applique à tous les élèves, quels que soient les revenus de leur famille et leurs caractéristiques démographiques, ce qui réduit les inégalités.

Au-delà du filtrage des contenus, les écoles doivent respecter les bonnes pratiques de cybersécurité pour protéger les données qu'elles collectent. Elles doivent notamment :

- Mettre en place des processus clairs pour la création des comptes des élèves et le contrôle d'accès
- Appliquer des contrôles d'accès stricts à tous les appareils et applications qui ont accès aux informations des élèves
- Développer un plan de réponse clair en cas d'attaque informatique
- Sécuriser les terminaux à l'aide de logiciels de détection et de réponse adaptés
- Effectuer des sauvegardes régulières des données en vue d'une restauration
- Chiffrer les serveurs de données et les appareils
- Mettre en œuvre un logiciel de gestion des informations et des événements de sécurité (SIEM)
- Développer un programme de formation approprié pour enseigner aux enseignants, au personnel et aux étudiants les risques liés à la présence en ligne

Principaux points à retenir

- Les écoles ont la responsabilité de protéger les élèves contre les contenus préjudiciables en ligne, mais rien ne permet de dire clairement dans quelle mesure l'activité des élèves doit être surveillée
- Une surveillance constante peut avoir un effet négatif sur le bien-être des élèves
- Ces approches peuvent être discriminatoires à l'égard de certains groupes d'élèves
- L'observation humaine des élèves offre un moyen bien plus fiable que la technologie d'identifier les élèves en difficulté
- La surveillance et le contrôle doivent être mis en œuvre avec soin et parcimonie, en gardant en tête que ce n'est qu'une solution partielle pour la sécurité des élèves
- Les établissements doivent élaborer des règles de sécurité strictes pour protéger les données des élèves

Découvrez comment Jamf peut enrichir votre solution de gestion de la technologie, de sécurité et de filtrage de contenu en visitant Jamf.com

En savoir plus