COMITE D'ETHIQUE
POUR LES DONNEES
D'EDUCATION

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS
Liberté
Égalité
Fraternité

POUR L'ÉCOLE
DE LA CONFIANCE

AVIS n°2020-1

Enjeux d'éthique des usages des données numériques d'éducation dans le contexte de la pandémie

Présidente : Nathalie Sonnac

Rapporteurs : Ignacio Atal, Christine Froidevaux

Membres : Dominique Cardon, Jean-Richard Cytermann, Isabelle Falque-Pierrotin, Aurélie Jean, Michèle Laurissergues,Catherine Morin-Desailly, Jérôme Saltet, Bruno Studer.

Juillet 2020

Sommaire

Introduction

La crise sanitaire due à la pandémie de COVID-19 a nécessité la mise en place d'une continuité pédagogique hors école en utilisant massivement et de façon accélérée les outils numériques. Au-delà des objectifs de continuité, d'inclusion et d'équité indispensables à la réussite de cette transition, le recours massif aux outils numériques avec ses usages nouveaux ou renforcés s'est accompagné d'un accroissement des risques déjà existants et a mis en lumière des enjeux d'éthique qu'il convient de souligner.

Dans cette situation d'urgence où des décisions partiellement anticipées ont été prises, des points de vulnérabilité de la collecte des données et de leur utilisation dans ce contexte et dans la durée sont apparus. C'est pourquoi le comité a entrepris une réflexion pour identifier les questions éthiques liées à la gestion des données d'éducation soulevées par ces usages accentués du numérique pendant la crise, qu'il s'agisse des outils et usages institutionnels, ou d'outils et d'usages moins encadrés. Il émet dans ce rapport des alertes et des recommandations à destination de toute la communauté éducative.

Cette analyse a été initiée de façon réactive dans l'urgence de la situation et devra se poursuivre dans les phases ultérieures de gestion de la crise. Elle se concentre sur trois enjeux majeurs d'éthique de l'usage du numérique dans le domaine éducatif : protéger les données personnelles, garantir la souveraineté numérique et assurer l'égalité de l'accès aux ressources et des compétences numériques. Cette analyse qui porte sur les données d'éducation numériques prend en compte les impératifs de continuité pédagogique, le respect des valeurs au cœur de la mission pédagogique, la protection indispensable des élèves et de la communauté éducative pour une confiance partagée, de même que les opportunités d'évolution du système éducatif.

1. Données d'éducation et leur traitement

Selon le code de l'éducation, « dans chaque école, collège ou lycée, la communauté éducative rassemble les élèves et tous ceux qui, dans l'établissement scolaire ou en relation avec lui, participent à l'accomplissement de ses missions. Elle réunit les personnels des écoles et établissements, les parents d'élèves, les collectivités territoriales ainsi que les acteurs institutionnels, économiques et sociaux, associés au service public de l'éducation »[1].
De nombreuses données liées à la vie scolaire et concernant différents acteurs de la communauté éducative, dites « données d'éducation », sont produites, stockées et analysées pour différents objectifs. Ces données sont exploitées à des fins de suivi pédagogique des élèves, d'organisation du service éducatif, d'élaboration de ressources pédagogiques ainsi qu'à des fins de statistiques et de recherches.

[1] Article L. 111-3 du code de l'éducation.

1.1. Types de données d'éducation

Dans ce rapport nous nous intéressons aux données personnelles numériques d'éducation. Nous présentons les données qui sont propres à certains acteurs puis celles qui résultent d'interactions entre eux ou avec des objets numériques.

1.1.1. Données des élèves et de leur famille

Parmi les données concernant les élèves qui sont produites et/ou traitées dans le contexte scolaire on trouve des données administratives sur leur identité (nom, prénom, date de naissance, adresse postale ou numérique etc.), sur leur état de santé et sur leur suivi scolaire (présences/absences, redoublement, changement de classe/école, activités périscolaires etc.). Sont aussi produites des données relatives à leur suivi pédagogique et à leurs apprentissages telles que les évaluations, relevés de notes, productions, exercices, et notes prises en cours. Par ailleurs, sont aussi traitées des données concernant les parents des élèves comme la profession et le statut marital.

Dans le contexte du confinement ont été produites et traitées de façon massive un grand nombre de données sur les élèves, par exemple toutes les informations sur leur identité insérées dans des plateformes numériques (institutionnelles ou non), ainsi que les travaux échangés entre eux par le biais de ces plateformes (que ce soit des exercices ou des activités en ligne, ou des photos/scans de travaux nécessaires au suivi pédagogique à distance).

1.1.2. Données des enseignants

De la même façon, les données personnelles des enseignants, et de façon plus générale de tout personnel de l'éducation, incluent les données administratives sur leur identité (nom, prénom, date de naissance, adresse postale ou numérique etc.), les données concernant leur pratique pédagogique (contenus et support de cours, correction de copies etc.), ainsi que leur activité professionnelle telles que les présences/absences, congés maladies, et leur ancienneté, données utiles pour la gestion RH.

Dans le contexte du confinement, et pour assurer la « continuité pédagogique », les choix pédagogiques des enseignants, comme les ressources pédagogiques produites ou utilisées ou encore les séquences suivies, se sont accompagnés de choix de plateformes pour l'enseignement à distance. Les données personnelles qu'ils ont produites ou traitées ont été ainsi massivement stockées par les services numériques choisis par les enseignants pour faire cours ou communiquer avec leurs élèves, et ont été aussi potentiellement stockées par toute personne y ayant accès (élèves, parents, collègues).

1.1.3. Données d'interaction

En plus des données propres à un élève, à sa famille ou à un enseignant, les données relatives aux interactions ont un rôle fondamental. Il s'agit de tout ce qui relève des interactions entre élèves et enseignants (copies corrigées, questions/réponses, interpellations), entre élèves (échanges lors d'un travail collaboratif), entre enseignants (coordination entre disciplines, coordination entre classes ou entre collègues de même discipline, partage d'information sur des élèves, etc.), et aussi entre enseignants et parents (cahier de liaison, rendez-vous parents). Ces données sont donc liées directement aux élèves et/ou aux enseignants et/ou aux parents.

Lors du confinement, on a assisté à une augmentation considérable du recours au mail, aux systèmes de messagerie instantanée, aux réseaux sociaux ainsi qu'aux outils de visioconférence pour communiquer, échanger des informations, faire un cours ou travailler de façon collaborative. Ces interactions ont ainsi produit massivement des données stockées par les fournisseurs de ces services, et potentiellement stockées par toute personne ayant accès à ces espaces d'interaction.

Au-delà du domaine scolaire, il est important de signaler que le nombre de données d'interaction qui ont été produites et stockées a explosé, notamment par l'utilisation massive des réseaux sociaux par les élèves, leurs parents et les enseignants.

Le numérique permet par ailleurs un accès particulièrement précis et mémorisable aux données comportementales des élèves et des enseignants sur les plateformes et les outils mis à leur disposition. Ces données incluent par exemple les temps de connexion, les zones de la plateforme les plus visitées, et toutes formes de comportements interactifs avec l'outil tels que le nombre de clics, la distance de déroulage (scroll down), ou encore le nombre et la fréquence des messages instantanés. Là encore, pendant le confinement, la production de ces données comportementales a augmenté considérablement.

1.2. Données personnelles

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable, une personne pouvant être identifiée directement ou indirectement[2]. Le traitement des données personnelles doit se faire, hors cadre domestique, dans le respect du Règlement Général sur la Protection des Données (RGPD). Ceci inclut non seulement les données avec le nom et prénom des personnes, mais aussi les données qui permettent d'identifier indirectement les personnes.

Par exemple, si l'on dispose du numéro de téléphone, ou du numéro de sécurité sociale d'une personne, ou de l'Identifiant National Élève (INE)[3] d'un élève, il est *a priori* facile d'identifier la personne concernée. Aujourd'hui, il est même possible d'identifier automatiquement une personne à partir d'un enregistrement de sa voix ou d'une photo de son visage. Il est aussi possible d'identifier une personne par le

[2] https://www.cnil.fr/fr/definition/donnee-personnelle

[3] Arrêté du 16 février 2012 portant création d'un traitement dénommé « répertoire national des identifiants élèves, étudiants et apprentis », https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025554438

croisement de plusieurs données, comme un élève si on connaît l'école qu'il fréquente, le jour de son anniversaire, et le métier de ses parents. De même, la géo-localisation d'une personne à plusieurs moments de la journée peut permettre de trouver son identité (les localisations fréquentes en journée et en soirée correspondent généralement au lieu de travail et au domicile, respectivement). Une copie d'examen ainsi que les corrections des évaluateurs, même si celles-ci n'incluent pas l'identifiant de l'élève, doivent être considérées comme des données personnelles si on peut identifier indirectement l'élève[4].

Une donnée d'éducation peut ne plus se rapporter à une personne identifiable si elle a été soumise à un processus d'anonymisation (mais souvent on procède à une simple pseudonymisation, par exemple en retirant des éléments directement identifiants tels que le nom et le prénom sur un texte écrit, ce qui n'assure pas l'anonymisation[5]) ou bien si elle a été agrégée aux données d'autres personnes, comme par exemple la proportion de redoublements dans une région, de sorte que le groupe soit suffisamment grand. De telles données ne sont alors plus des données personnelles et ne relèvent pas du RGPD, à l'inverse des données pseudonymisées[6]. Il est à noter toutefois que dans le cas de données agrégées, même si on ne sait pas si un élève a redoublé, savoir qu'il appartient à un groupe caractérisé par une propriété (fort taux de redoublement) donne des indications sur lui et peut être stigmatisant.

1.3. Traitement des données

Selon la CNIL, un traitement de données personnelles est toute opération portant sur des données personnelles (comme stocker, modifier, analyser ou croiser avec d'autres données), quel que soit le procédé utilisé[7].

1.3.1. Avec quels outils et à quelles fins ?

Les données d'éducation sont traitées par de nombreux acteurs à de nombreuses fins et avec des outils très divers.

Lors du confinement on a assisté à une augmentation spectaculaire de l'usage des outils numériques pour communiquer et partager des données d'éducation. La proportion de recours à des outils non-institutionnels pendant le confinement est difficile à évaluer, mais dans les premiers jours de la mise en place de la continuité pédagogique, faute d'autres solutions rapides à mettre en œuvre, cette proportion n'a pas été négligeable.
Ensuite, très rapidement le Ministère a mis à disposition des enseignants et des élèves un certain nombre de ressources numériques éducatives utiles pour la continuité pédagogique, indiquées sur le site Eduscol[8] et donné des directives aux enseignants pour l'utilisation des outils institutionnels qui ont été de pair avec le développement d'outils comme Ma Classe à la Maison du CNED. La CNIL a diffusé

[4] https://gdpr-info.eu/issues/personal-data/

[5] Il n'est pas toujours possible d'anonymiser les données et il n'existe pas de méthode universelle. Voir la note (mai 2020) de la CNIL : https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

[6] https://gdpr-text.com/fr/read/recital-26/

[7] https://www.cnil.fr/cnil-direct/question/un-traitement-de-donnees-caractere-personnel-cest-quoi?visiteur=part

[8] https://eduscol.education.fr/cid150648/ressources-numeriques-educatives.html

le 8 avril des conseils pour aider au choix d'outils numériques qui se conforment aux règles de protection des données[9].

Les données scolaires des élèves sont utiles à de nombreux égards : elles permettent la gestion administrative, pédagogique et financière des élèves ou encore le suivi des résultats scolaires. Elles sont précieuses pour l'équipe enseignante, dans la mesure où elles permettent d'améliorer la pédagogie au service des élèves et des enseignants, mais peuvent l'être aussi pour l'élève lui-même (il peut consulter son parcours d'apprentissage) ainsi que pour ses responsables légaux. Dans le contexte de l'enseignement à distance, les données des élèves (connexions, réponses à des questionnaires) permettent à l'équipe enseignante de suivre les apprentissages de chaque élève dans son individualité, mais aussi de l'ensemble des élèves d'un groupe pour ajuster son enseignement aux besoins de ce groupe. Dans ce cas, toutes les traces d'apprentissage sont reliées à des élèves identifiés.

Les données d'éducation sont aussi précieuses pour les chercheurs en sciences de l'éducation pour comprendre les phénomènes sociologiques et cognitifs des processus d'enseignement et d'apprentissage, ainsi que pour identifier des pratiques pédagogiques prometteuses. D'autres champs de la recherche tels que les *learning analytics* ou l'*educational data-mining* pourraient utiliser les traces numériques d'apprentissage pour créer des modèles d'apprenants afin de développer des plateformes d'enseignement s'adaptant automatiquement aux individualités des élèves. Notons toutefois que les chercheurs n'ont pas forcément besoin de données personnelles, mais que des données anonymisées ou agrégées peuvent suffire.

Ces données permettent également d'extraire des statistiques sur le système d'éducation par classe d'âge, classe sociale, ville, région ou à l'échelle du pays. Ces statistiques sont fondamentales pour évaluer la situation du pays en matière d'éducation nationale (et les possibles disparités géographiques et sociales), son évolution dans le temps, ainsi que pour évaluer l'efficacité de différentes réformes. Là encore, des données personnelles anonymisées peuvent être utilisées à de telles fins.

1.3.2. Responsables de traitement

Selon le RGPD, le responsable d'un traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement et est soumis au droit des données »[10]. Concernant les données traitées dans le cadre scolaire, le guide élaboré par la DAJ et le DPD, avec le soutien de la CNIL, et présenté par le réseau Canopé décrit précisément qui est le responsable du traitement dans différentes situations et quelles sont ses obligations[11].

A côté du responsable de traitement, on trouve les sous-traitants qui sont des personnes physiques ou morales (entreprise ou organisme public) qui traitent des

[9] https://www.educnum.fr/fr/outils-de-la-continuite-pedagogique-les-conseils-de-la-cnil
[10] Article 4 du RGPD, §7 : https://www.privacy-regulation.eu/fr/4.htm
[11] https://www.reseau-canope.fr/les-donnees-a-caractere-personnel/le-responsable-de-traitement-et-ses-obligations.html

données pour le compte d'un autre organisme (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation[12].
Les responsables de traitement et les sous-traitants sont tenus de désigner un DPD (Délégué à la Protection des Données) lorsque le traitement est effectué par une autorité publique ou un organisme public, ce qui est le plus souvent le cas des données d'éducation[13].

Ces différents traitements doivent être effectués en respectant les cinq grands principes relatifs à la protection des données personnelles : finalité, proportionnalité et pertinence, durée de conservation, sécurité et confidentialité[14].

2. Des données spécifiques au cœur de la souveraineté numérique

Nous reprenons à notre compte la définition proposée par les représentants de la CERNA lors de leur audition au Sénat[15] et dans leur rapport « La souveraineté à l'ère du numérique - Rester maîtres de nos choix et de nos valeurs »[16]. La souveraineté numérique est la capacité pour une entité donnée - Etat, entreprise ou individu - de maitriser des attributs numériques (données, informations, connaissances, algorithmes) sur des objets dont elle revendique l'observation voire le contrôle. La souveraineté numérique ne peut ainsi se résumer à un enjeu économique ou politique, elle porte aussi des enjeux d'éthique, qui concernent notamment le droit de chaque individu à préserver sa vie privée.

2.1. Respecter les libertés fondamentales des acteurs de l'éducation

Comme toute personne, les acteurs de l'éducation disposent de droits sur les traitements de leurs données personnelles, leur permettant de garder la maîtrise des informations les concernant : droit à l'information, recueil du consentement, droit d'opposition, droits d'accès et de rectification[17].

[12] https://www.cnil.fr/fr/definition/sous-traitant
[13] Article 37 du RGPD, 1.
[14] https://www.cnil.fr/fr/cnil-direct/question/quels-sont-les-grands-principes-des-regles-de-protection-des-donnees
[15] http://www.senat.fr/compte-rendu-commissions/20190603/ce_souverainete.html#toc4
[16] http://cerna-ethics-allistene.org/digitalAssets/55/55160_AvisSouverainete-CERNA-2018-05-27.pdf
[17] https://www.cnil.fr/fr/respecter-les-droits-des-personnes

2.1.1. Des données révélant des informations sensibles sur les personnes

Les données d'éducation révèlent de nombreuses informations sur les personnes, de façon directe ou indirecte. Le travail effectué par un élève fournit des informations sur son niveau de connaissances sur le sujet en question. Le contenu des cours utilisés par un enseignant fournit des informations sur sa façon d'enseigner et ses choix pédagogiques. Mais aussi les moments ou lieux de connexion d'un élève ou d'un enseignant sur une plateforme numérique fournissent des informations sur leur mode de vie. Ces informations mobilisées par des données deviennent plus riches à mesure que les méthodes de traitement de celles-ci évoluent. Par exemple, le rythme de frappe sur un clavier d'un individu peut donner des informations sur son état émotionnel[18].

Les données de comportement des élèves ou enseignants sur une plateforme numérique peuvent aussi être utilisées algorithmiquement pour catégoriser les utilisateurs et ainsi, par association, les orienter vers des contenus ou encore personnaliser le service qui leurs est fourni sur la plateforme. Cette catégorisation algorithmique poussée à l'extrême induit le phénomène bien connu de « bulle » qui enferme les individus et peut devenir une source de discrimination et de perte d'objectivité.

Au sens du RGPD, les ***données personnelles sensibles*** sont des données qui sont vues comme étant particulièrement à risques, notamment pour les droits et libertés fondamentales et dont le régime juridique de protection est renforcé. « Ce sont les informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Ce sont également les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Il est interdit de recueillir et d'utiliser ces données, sauf dans certains cas précis »[19]. Les traitements des données personnelles sensibles sont donc plus contraints juridiquement.

Concernant les données d'éducation, certaines données sont clairement identifiées comme données sensibles au sens du RGPD car relatives par exemple à la santé (allergies alimentaires ou handicaps) et sont traitées dans le cadre scolaire (régime alimentaire à la cantine ou aménagement d'épreuves), tandis que d'autres peuvent être perçues comme sensibles d'un point de vue social, parce qu'elles peuvent entraîner des dommages pour les élèves, sans pour autant être reconnues explicitement comme sensibles au sens du RGPD. Par exemple, les données scolaires relatives aux bulletins peuvent être discriminantes pour les élèves et nuire à leur future carrière si elles sont sorties du contexte scolaire et connues de futurs employeurs.

Les données scolaires sont également des données qui peuvent être croisées avec d'autres données, révélant ainsi des informations « sensibles » au sens du RGPD. Par exemple, si l'on note une corrélation entre les absences répétées d'un élève et les dates de fêtes religieuses il serait possible d'inférer sa religion. Aussi, des difficultés scolaires, apparaissant dans des copies, évaluations ou dossiers

[18] Identifying Emotional States using Keystroke Dynamics. CHI 2011, May 7–12, 2011, Vancouver, BC, Canada
[19] https://www.cnil.fr/fr/cnil-direct/question/une-donnee-sensible-cest-quoi et RGPD, art. 9.

administratifs d'école, peuvent être corrélées à des données de santé comme des troubles spécifiques de l'apprentissage comme la dyslexie ou la dyspraxie. Enfin, la connaissance de données sur des enfants permet de mieux les connaître et éventuellement d'orienter leurs choix avec un risque de manipulation.

2.1.2. Protection des données d'éducation et consentement

L'ensemble des données d'éducation des élèves, selon le RGPD[20], ne sont pas considérées comme des données à caractère personnel sensibles du point de vue des libertés et des droits fondamentaux et qui, par suite, mériteraient une protection spécifique. Comme le préconise la déclaration conjointe France-Estonie (EIGS 2019) présentée en annexe 3, il faudrait reconnaître un statut spécifique aux données pédagogiques personnelles des élèves.

Actuellement, le RGPD protège ces données en tant que données personnelles de mineurs nécessitant une attention particulière[21] et protège de façon spécifique celles des données éducatives reconnues comme sensibles – telles que des données de santé – lorsque celles-ci peuvent être traitées dans le cadre éducatif.

Dans ce cadre, plusieurs cas sont prévus[22]. Le principe est que les traitements de données d'éducation à caractère personnel sont majoritairement fondés sur l'exécution d'une mission d'intérêt public. Si le traitement n'est pas compatible avec ce fondement, un autre fondement sera recherché parmi ceux de l'exercice de l'autorité publique, du respect d'une obligation légale ou de l'intérêt légitime du responsable de traitement. Ce n'est, le plus souvent, qu'à défaut que le traitement sera fondé sur le consentement, celui-ci devant être ni contraint ni influencé. Le nombre de traitements mis en œuvre par l'école ou tout autre acteur dans le cadre éducatif reposant sur le consentement est ainsi en principe peu important.

Un exemple de cas où le consentement des responsables légaux (ou de l'élève s'il est majeur) peut être valablement demandé est par exemple le cas où on veut utiliser les photos d'un élève sur le site de l'école afin de documenter des activités organisées par l'école. Le consentement serait ici le fruit d'un véritable choix dès lors que les élèves/responsables légaux ne se verront pas privés de tout enseignement ou de tout service, et pourront refuser sans aucun préjudice[23].
Soulignons ici que lorsque le consentement doit être recueilli, l'élève doit pouvoir refuser, sans que ce refus n'entraîne une rupture d'égalité avec les autres élèves.

De son côté le Ministère a pris acte que de nombreux usages pédagogiques s'appuient aujourd'hui sur l'utilisation des données personnelles des élèves et a édité en partenariat avec la CNIL une fiche à destination des enseignants pour leur conseiller d'adopter des réflexes pour enseigner avec le numérique[24]. Cette fiche

[20] RGPD articles 9 et 10, et considérant 51.
[21] Considérants 38, 58, 65, 71 et 75 du RGPD. Concernant les droits des mineurs, le RGPD considère les enfants comme vulnérables, et ce critère doit donner lieu, combiné à un autre critère issu des lignes directrices du G29, à la réalisation d'une analyse d'impact (AIPD), pour construire des traitements respectueux de la vie privée (https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd)
[22] https://www.privacy-regulation.eu/fr/6.htm
[23] Lignes directrices sur le consentement au sens du règlement 2016/679A : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf
[24] https://www.education.gouv.fr/les-enjeux-de-la-protection-des-donnees-au-sein-de-l-education-7451

présente dix principes clés, cinq concernant le choix des outils tels que « privilégier l'usage de logiciels libres ou développés par le ministère » ou encore « utiliser de préférence des logiciels ou applications hébergés dans l'Union européenne », et cinq portant sur la protection des données des élèves dans toute activité pédagogique tels que « limiter toute collecte de données personnelles aux informations indispensables au bon déroulement de l'activité et veiller à ce qu'elles soient supprimées ou archivées selon la réglementation », ou encore « respecter le droit à l'image des élèves ». Dans cette fiche le 8ème principe recommande aux enseignants de « sensibiliser les élèves aux enjeux de la protection des données personnelles ».

Pour que ces conseils soient compris et suivis il faut que les enseignants soient eux-mêmes sensibilisés à l'importance de ces principes avec la conscience des conséquences de leur non-respect. La tâche est multiple. Il faut sensibiliser non seulement les élèves, mais aussi leurs familles et bien sûr les enseignants qui se doivent d'être exemplaires dans le respect des droits fondamentaux. Si des actions de sensibilisation sont déjà en cours[25], il faut les généraliser et les intensifier en diversifiant les mesures.

2.1.3. Enjeux d'éthique et recommandations

Nous relevons ici un certain nombre de risques pour les données d'éducation relatifs aux libertés fondamentales :

- Les données sont susceptibles d'être récupérées par de nombreux acteurs publics ou privés, français et internationaux, donnant des indications d'ordre privé sur des élèves, pouvant entraîner des risques de perte de confidentialité pour ceux-ci.
- La connaissance des données comportementales des élèves et des enseignants sur les plateformes numériques peut donner lieu à des incitations à consulter des contenus ciblés, pouvant conduire à des manipulations et des enfermements.
- Les données scolaires qui pourraient être collectées et stockées par l'État peuvent être exposées à des risques de piratage si le système de cybersécurité n'est pas suffisant. Or on ne souhaite pas anonymiser toutes les données pédagogiques des élèves en raison du suivi pédagogique personnalisé si bien que des données personnelles des élèves pourraient être ainsi divulguées, et le procédé de pseudonymisation n'exclut pas la possibilité de ré-identification.
- L'espace physique - clos et limité - de la classe n'existe plus lors d'une séance de téléenseignement conduisant à une ingérence possible de membres extérieurs à la classe dans l'espace virtuel, avec de plus un abolissement des frontières entre espace privé et espace scolaire. Cette situation peut entraîner un risque d'ingérence dans la vie privée par l'usage des outils numériques avec des dérives telles que par exemple le cyberharcèlement et la pornodivulgation (*revenge porn*).
- Les conditions générales d'utilisation des données (CGU) des plateformes ou des outils sont peu lisibles et peuvent évoluer rapidement.

[25] https://www.cnil.fr/fr/signature-dune-convention-triennale-sur-la-protection-des-donnees-personnelles-dans-les-usages, décembre 2018.

- La signification de la mention « conforme au RGPD » n'est pas évidente pour tous et n'a pas de valeur juridique à l'heure actuelle. Par ailleurs, utiliser, en tant que responsable de traitement, un outil qui affirme être « conforme RGPD », ne retire aucune des obligations du responsable de traitement.
- La question de savoir qui donne le consentement se pose. Des outils délèguent aux enseignants l'obtention du consentement des parents et il existe également le risque que le consentement soit donné par des élèves n'ayant pas la capacité juridique de le faire, à la place de leurs parents.
- Il pourrait exister un risque de discrimination en cas de non consentement de l'élève ou de ses parents, et/ou de mise à l'écart du suivi pédagogique dans les cas où il faudrait y faire recours.

Enjeux d'éthique et tensions

- Risque d'atteinte à la vie privée : perte de confidentialité des données personnelles des individus ou des groupes d'individus
- Risque de manipulation, de harcèlement et d'enfermement
- Risque de discrimination
- Risque de perte d'autonomie
- Tension entre respect de la vie privée de l'élève et besoin d'assurer un suivi pédagogique individualisé avec des données personnelles
- Tension entre une protection juridique exigeante de l'ensemble des données d'éducation et lourdeur des traitements qui en résulterait

Recommandations

1. Engager une réflexion sur l'opportunité d'introduire dans le RGPD le statut de données sensibles pour les données d'éducation, à l'instar des données de santé, à des fins de protection de la vie privée des élèves et des enseignants.
2. Donner un statut juridique plus protecteur pour les données d'éducation, au niveau français en instituant un code de bonne conduite sur les données d'éducation pour l'ensemble des acteurs (publics comme privés).
3. Attirer l'attention des différents acteurs (enseignants, élèves, familles, entreprises, acteurs académiques, politiques) sur le caractère « spécifique » des données d'éducation et continuer à responsabiliser ces acteurs dans leur utilisation de ces données.
4. Intensifier la formation au droit à la protection des données, en particulier de celles qui sont liées aux usages pédagogiques numériques, pour les enseignants, les élèves et leurs familles, en illustrant avec des cas pratiques.
5. Accentuer la sensibilisation des différents responsables de traitements aux principes de protection des données exigés par le RGPD pour la collecte des données personnelles en les explicitant, en les expliquant et en les exemplifiant.
6. Continuer et intensifier les démarches de sensibilisation de l'équipe éducative et des élèves aux risques d'ingérence dans la vie privée par

l'usage des outils numériques (dont cyberharcèlement). Ces démarches de sensibilisation doivent s'inscrire bien au-delà du domaine de l'éducation et concerner aussi les usages des réseaux sociaux par les élèves.

7. Proposer un label (ou une certification) ouvert à tous les acteurs des EdTech remplissant un certain nombre de critères qui garantissent le respect de la vie privée des acteurs de la communauté éducative.
8. Offrir des garanties de sécurité des outils que l'Etat recommande ou met à la disposition des acteurs de l'éducation, et évaluer le risque que fait courir leur perte éventuelle de confidentialité.
9. Mettre en place des accords avec les acteurs privés dont les élèves et les enseignants utiliseraient les outils, afin de garantir une minimisation de l'usage de la donnée à une liste définie par le Ministère, ainsi qu'un effacement régulier des données.

2.2. Garantir la souveraineté numérique en matière d'éducation

La question de la souveraineté numérique implique la question de la formation des acteurs de la communauté éducative, qui doit être prioritaire.

2.2.1. Recours à une offre privée internationale

Le recours à l'offre du privé dans l'EdTech (française ou internationale) de moyens numériques pour échanger des documents et converser à distance a augmenté de façon considérable pendant la période de confinement. A la fin mars, on constatait que des outils très variés étaient communément utilisés par les enseignants, parmi lesquels figuraient dans le top 20 WhatsApp, Google Suite, Zoom ou Discord[26]. Il est à noter qu'il a été difficile pour les utilisateurs de s'assurer de la conformité au RGPD de ces outils, comme Discord qui a fait l'objet de critiques dans la presse[27].

L'offre publique n'a pas pu dans un premier temps assurer le flux des demandes, ni proposer des outils disposant de toutes les fonctionnalités nécessaires à la continuité pédagogique dans le respect du RGPD. Dans un second temps, l'offre publique a grandi en puissance et le ministère de l'Education Nationale a donné des directives, comme vu en section 1.3.1. Il faut noter toutefois que ces directives n'ont pas été suivies par tous.

On a pu observer peu d'adhésion des différents acteurs à l'offre publique, probablement en raison de l'accoutumance à l'usage des technologies privées, et au fait que les outils privés peuvent s'avérer plus conviviaux et plus robustes pour une utilisation par un grand nombre de participants. Pour exemple, on peut citer la formidable augmentation des utilisations de ZOOM, un logiciel de visioconférence privé américain, dont pourtant très vite des failles de sécurité menaçant la vie privée ont été détectées et rapportées dans la presse[28], puis assez vite corrigées.

[26] https://lewebpedagogique.com/2020/03/29/comment-travaillent-les-profs-pendant-le-confinement/
[27] https://www.liberation.fr/checknews/2020/03/27/les-enseignants-peuvent-ils-faire-cours-sur-discord-pendant-le-confinement_1783162
[28] Article du 31 mars de France 24 : https://www.france24.com/fr/20200331-coronavirus-zoom-l-appli-vid%C3%A9o-au-m%C3%A9pris-de-la-vie-priv%C3%A9e et article du Monde du 2 avril : https://www.lemonde.fr/pixels/article/2020/04/02/securite-donnees-usages-cinq-questions-sur-zoom-le-service-de-videoconference-qui-cartonne_6035309_4408996.html.

Par ailleurs, les utilisateurs peuvent se laisser bercer par l'illusion que les entreprises privées leur offrent gratuitement leurs outils numériques sans contrepartie. Or comme dit l'adage « si c'est gratuit, c'est que c'est vous le produit ». Une méconnaissance du modèle économique sous-jacent au marché des données peut conduire à une telle illusion. Il s'ensuit un enjeu d'équité pour permettre aux plus démunis de disposer d'outils numériques efficaces et conviviaux qui ne mettent pas en péril leurs données personnelles.

2.2.2. Les données d'éducation : une richesse stratégique nationale

Comme on l'a vu précédemment[29], les données permettent d'extraire des statistiques sur le système d'éducation par ville, par région voire à l'échelle du pays. Les données agrégées permettent d'évaluer la situation d'un pays en matière d'éducation nationale et son évolution dans le temps, et constitue de fait un enjeu stratégique national.
La connaissance de ces données par d'autres pays étrangers peut constituer une vulnérabilité pour notre pays, si elles sont utilisées à mauvais escient. Le pays doit pouvoir rester maître de la diffusion de ces informations.
Par ailleurs, ces données d'éducation constituent une véritable mine pour la recherche et l'innovation, tant pour les acteurs publics que privés, qu'ils soient nationaux ou internationaux dans le but de développer des ressources éducatives.
Enfin, si l'éducation n'est pas en soi une marchandise, comme les biens éducatifs se répandent et se multiplient, ils s'inscrivent dans des mécanismes de marché. Relevons qu'il existe un véritable marché des données d'éducation, et il faut définir une stratégie de gouvernance de ces données qui soit respectueuse de nos valeurs.
Les données scolaires agrégées sont donc une richesse nationale et à ce titre l'Education est un actif stratégique national de l'Etat au même titre que les activités de transport, de communication numérique, ou de santé publique.

2.2.3. Utiliser des outils qui mobilisent les valeurs européennes

En France et dans l'Union Européenne, les données personnelles sont soumises au RGPD qui est une réglementation mobilisant les valeurs de protection de la vie privée et des libertés individuelles. Il est fondamental que toutes les données personnelles d'éducation, dont on a vu qu'elles sont spécifiques et constituent un enjeu stratégique national, soient traitées par des outils qui respectent une telle réglementation, et que soit exclu tout recours à des outils ne respectant pas les valeurs fondamentales européennes. Il en va de la souveraineté numérique de la France. « Il faut donner aux citoyens français la capacité d'utiliser des solutions technologiques qui reflètent leurs valeurs »[30], leur permettant ainsi de garder la maîtrise du choix de société dans laquelle ils veulent vivre.

2.2.4. Enjeux d'éthique et recommandations

Nous relevons ici un certain nombre de risques pour les données d'éducation relatifs à la souveraineté numérique :

[29] Voir section 1.3.1.
[30] Audition de Bernard Benhamou le 12 mai.

- Un grand nombre de ces données peuvent tomber dans les mains d'acteurs publics ou privés, français ou étrangers, dont les usages peuvent être difficilement contrôlés. Cela pose la question du devenir de l'utilisation de ces données, de qui en disposera, de qui les stockera, or on a vu qu'il s'agit d'une ressource stratégique et sa non maîtrise peut constituer une menace sur le fonctionnement démocratique de nos institutions avec un risque d'ingérence dans les choix de société.
- L'absence actuelle d'outils développés au niveau Français ou Européen ayant les mêmes robustesses (e.g. passage à l'échelle) et fonctionnalités (en termes d'ergonomie ou en termes d'analyse des données) que certains outils étrangers qui peuvent ne pas respecter le RGPD, ainsi que le manque d'interopérabilité des outils, peuvent générer un risque pour la protection des données.
- Les plus démunis peuvent être enclins à choisir des outils numériques « gratuits » même s'ils ne sont pas respectueux des valeurs fondamentales.

Enjeux d'éthique

- Risque d'ingérence dans nos choix de société et risque de perte d'autonomie
- Risque de perte de confidentialité

Recommandations

1. Définir une stratégie nationale et portée par l'Europe concernant le développement de produits numériques d'éducation respectant les valeurs fondamentales Européennes.
2. Assurer une offre gratuite à l'échelle nationale ou européenne d'outils de téléenseignement de bonne qualité, relative à un minimum de fonctionnalités (telles que des actions de partage collaboratif), à leur convivialité (rapidité d'exécution, facilité de prise en main) et à leur robustesse (outils adaptés à un grand nombre de participants) qui respectent les valeurs éthiques européennes portées par le RGPD.
3. Encourager les utilisateurs (élèves, enseignants, parents), au besoin par des formations dédiées, à recourir à l'offre publique, chaque fois qu'elle est suffisante.
4. Identifier au niveau national les offres dont le fonctionnement peut poser à moyen ou long termes des problèmes éthiques liés aux données.
5. Effectuer une veille et une analyse des principaux outils de communication, de partage et de collaboration qui peuvent s'avérer utiles dans le cadre de l'enseignement scolaire, développés par des acteurs publics ou privés français ou européens qui sont respectueux de nos libertés fondamentales.
6. Sensibiliser les différents acteurs (enseignants, élèves, familles, entreprises, acteurs académiques, politiques) aux enjeux de souveraineté numérique dans le domaine des données scolaires numériques.

3. Assurer l'égalité d'accès au numérique

Les données d'éducation sont de plus en plus souvent produites et échangées à travers des outils numériques. On a vu toutes les potentialités offertes par ces données. Afin de les valoriser pleinement, pour des raisons éthiques, il convient de veiller à ce que cette production et ces échanges puissent être effectués de façon égale par tous et pour tous.

3.1. Etat de l'accès au numérique

Si l'équipement numérique et la connexion à Internet sont évidemment des conditions indispensables pour bénéficier d'un accès au numérique, et par là aux documents scolaires échangés par internet, les dernières statistiques de l'INSEE mettent en évidence que ce ne peut être le seul critère pour répondre à la question de l'accessibilité. En effet, l'utilisation d'Internet ne garantit pas de posséder les compétences numériques de base. La question de la formation au numérique est donc indispensable.

3.1.1. Etat de l'équipement et de la connexion numérique

Selon les résultats de l'enquête menée au niveau des rectorats, déclarative, à destination des écoles et établissements à laquelle environ la moitié des directeurs et chefs d'établissement ont répondu, 272 000 élèves des 1er et 2nd degrés vivent dans des familles n'ayant ni PC, ni tablettes, 91 000 n'ont pas de connexions internet, 37 000 pas de smartphone et 130 000 avec un forfait bloqué. Les chiffres de cette enquête directe sont probablement sous-estimés si on les rapporte à ceux du CREDOC[31] qui permet d'obtenir un ordre de grandeur des élèves de 12 à 17 ans non équipés de 570 000 (contre un peu plus de 106 000 élèves du second degré repérés grâce à l'enquête portant sur la moitié des établissements interrogés) ; ce chiffre de 570 000 représentant 9 % des 6 328 600 collégiens et lycéens (même si la tranche d'âge retenue par le CREDOC ne correspond pas exactement à celle des élèves du second degré).

La pratique des enseignants au début du confinement a été observée par différents sondages. D'après le sondage SynLab du 31 mars 2020, 17 % des enseignants n'ont pas réussi à établir de lien avec les familles, principalement dans les lycées où le taux monte à près de 40%. 20% des enseignants mettent en avant le manque de matériel ou de connexion pour les familles avec lesquelles le lien n'a pu être établi et n'ont d'autre recours que les relances par téléphone. 6% des enseignants n'ont ni matériel ou connexion adaptés pour travailler à domicile, le double dans les lycées professionnels[26].

Outre les mesures relatives à la continuité pédagogique relative aux à l'utilisation d'outils institutionnels (cf § 1.3.1), le Ministère (MENJ) a mis en place trois mesures notables : (i) une opération « fracture numérique » portée par le GIP Trousse à Projets en partenariat avec le MENJ qui a consisté en l'achat de matériels et services informatiques de base au bénéfice de familles qui en sont totalement démunies,

[31] https://www.economie.gouv.fr/files/files/directions_services/cge/barometre-numerique-2019.pdf. L'enquête a été réalisée en juin 2019 auprès d'un échantillon représentatif de la population française âgée de 12 ans et plus, sélectionné selon la méthode des quotas : 2.259 personnes ont été interrogées à leur domicile (2.052 adultes et 207 jeunes).

dans le cadre d'un dispositif d'urgence financé par les dons de fondations investies dans le champ social et éducatif ; (ii) une opération MENJ-La Poste en France métropolitaine et en Outre-mer pour assurer l'acheminement des matériels informatiques aux élèves en situation de déconnexion numérique afin qu'ils puissent recevoir des devoirs par courrier postal grâce au dispositif « Devoirs à la maison »[32] ; (iii) un dispositif expérimental de gratuité accordée aux élèves pour leurs connexions aux sites dédiés à la continuité pédagogique dans les académies d'Outre-Mer, dans le cadre d'un partenariat entre les académies et les opérateurs de réseaux.

3.1.2. Compétences numériques

Au-delà des inégalités de répartition des ressources numériques et d'accès à ces ressources, on constate également une inégalité d'utilisation de ces moyens numériques, liée à un manque de culture numérique, rendant l'utilisation de ces moyens impossible, ou en tout cas difficile.
L'étude des compétences numériques de l'INSEE 2019[33] s'appuie sur des indicateurs portant sur 4 domaines identifiés par Eurostat[34] : la recherche d'information (sur des produits et services marchands ou administratifs, etc.), la communication (envoyer ou recevoir des courriels, etc.), l'utilisation de logiciels tels que traitement de texte, et la résolution de problèmes (par exemple, accéder à son compte bancaire par Internet)[35]. L'échelle varie entre 0 (correspondant à une compétence nulle), 1 (pour compétence basique) ou 2 (pour une compétence plus que basique). Ainsi, le non-usage d'Internet au cours de l'année implique la note 0. Toutes ces compétences sont liées, et en les sommant, on obtient un indicateur global de capacités numériques : une personne n'a ainsi aucune capacité numérique si elle obtient 0 dans chaque domaine (*illectronisme*[36]) et des capacités plus que basiques si elle obtient 2 dans les quatre domaines. Entre les deux, Eurostat distingue les capacités faibles (au moins une compétence est notée à 0 et au moins une vaut 1) et basiques (aucune des compétences n'est égale à 0 et au moins une est égale à 1).

En 2019, 15 % des personnes de 15 ans ou plus n'ont pas utilisé Internet au cours de l'année et l'illectronisme concerne 17 % de la population. 38 % des usagers manquent d'au moins une compétence numérique de base ; une personne sur quatre ne sait pas s'informer et enfin une sur cinq est incapable de communiquer via Internet[36]. Concernant les compétences numériques, l'étude de l'INSEE relève des disparités en fonction des territoires et aussi du niveau de formation initiale, et souligne aussi qu'elles varient en fonction de l'âge. Ces inégalités de compétences numériques touchent aussi les élèves par le biais de leurs familles.

[32] http://documents-pleiade.education.fr/delcom2/Lettres_reperes/reperes_624.html
[33] Enquête INSEE 2019 sur l'utilisation d'internet et le compétences numériques : https://www.insee.fr/fr/statistiques/4241397
[34] https://ec.europa.eu/eurostat/cache/metadata/en/tepsr_sp410_esmsip2.htm
[35] Ces compétences sont mesurées à partir des déclarations sur le fait d'effectuer certaines tâches dans l'enquête annuelle auprès des ménages sur les technologies de l'information et de la communication, menée dans tous les pays de l'Union européenne. Note de l'INSEE.
[36] Illectronisme ou illettrisme numérique.

3.2. Former au numérique et à la citoyenneté numérique

Les compétences numériques de base doivent être maîtrisées par tous les acteurs de la communauté éducative, en particulier les élèves, leurs familles et les enseignants, mais aussi plus généralement par tous les citoyens pour des usages responsables du numérique. Cela signifie qu'il faut veiller à ce que tous les citoyens possèdent des compétences de base du numérique, qui leur permettent de comprendre et d'appliquer les conseils de sécurité prodigués à des fins de protection des données personnelles. Mais cela implique également de leur faire appréhender le modèle économique sous-jacent aux offres soi-disant gratuites du privé et qui ne le sont pas dans les faits, pour une utilisation éclairée des outils gratuits qu'ils choisissent. C'est grâce à ces compétences numériques de base que pourra s'acquérir la citoyenneté numérique, c'est-à-dire, « la capacité de s'engager positivement, de manière critique et compétente dans l'environnement numérique, en s'appuyant sur les compétences d'une communication et d'une création efficaces, pour pratiquer des formes de participation sociale respectueuses des droits de l'homme et de la dignité grâce à l'utilisation responsable de la technologie »[37].
Il existe ainsi un enjeu majeur d'éthique de formation de tous les citoyens au numérique et à la citoyenneté numérique.

3.2.1. Besoins de formation au numérique des élèves et de leur famille

Depuis quelques années, l'informatique est enseignée au collège (en mathématiques et en technologie) et depuis septembre 2019, un enseignement de Sciences Numériques et Technologie (SNT) a été introduit dans toutes les classes de Seconde générale et technologique. Cela permettra certainement à la longue de résoudre le problème du manque de compétences en numérique des futurs citoyens, mais cette réforme ne touche pas l'ensemble des enseignants, ni les enfants de primaire et leurs parents.

Or, dans certains cas, comme par exemple en classe de CP où les élèves ne savent ni lire ni écrire, la communication doit passer par les parents. Si ceux-ci ne sont pas à l'aise avec le numérique, la communication est difficile. Par ailleurs, on a pu observer pendant le confinement le rôle joué par les grands-parents, plus ou moins à l'aise avec les outils du numérique. Plus généralement, la crise a souligné le rôle important et intéressant que pouvaient jouer les familles.

3.2.2. Besoins de formation des enseignants au numérique accentués par la crise

Les enseignants exprimaient déjà avant la crise le besoin de formation au numérique.

[37] Citoyenneté numérique et éducation à la citoyenneté numérique, Conseil de l'Europe : https://www.coe.int/fr/web/digital-citizenship-education/digital-citizenship-and-digital-citizenship-education. Voir le rapport, Digital citizenship education, Council of Europe, Overview and new perspectives, 2017 : https://rm.coe.int/prems-187117-gbr-2511-digital-citizenship-literature-review-8432-web-1/168077bc6a

Selon la note d'information de la DEPP de 2019 relative à l'enquête de internationale Talis, donnant une photographie du métier de professeur des écoles[38], seuls 16 % des enseignants français interrogés expriment un avis positif s'agissant du niveau de préparation au numérique (TICE) en formation initiale (contre 1/3 de leurs voisins européens en moyenne). De plus, 35% des enseignants du premier degré expriment un besoin élevé de formation pour acquérir des compétences numériques.
Dans le second degré, enquête Profetic de 2018, 22 % des enseignants déclarent qu'ils utiliseraient davantage le numérique s'ils étaient formés à son utilisation pédagogique. La grande majorité estime l'offre insuffisante. 2/3 des enseignants du secondaire déclarent privilégier des démarches personnelles pour se former au numérique.

3.2.3. Position à l'international

Une étude de l'OCDE[39] parue le 27 mars 2020 analyse comment 98 pays qui ont répondu à l'enquête sont préparés à la continuité pédagogique dans le contexte de la pandémie. Cette étude s'appuie sur les résultats de PISA 2018, pour laquelle les principaux des établissements ont été interrogés. Il en ressort que les jeunes Français se placent au-dessus de la moyenne de l'OCDE pour l'équipement par ordinateur ou l'accès à Internet, mais en dessous de la moyenne OCDE pour la puissance de calcul des moyens numériques dans les établissements ou la bande passante et la vitesse d'internet. Ce qui est encore plus dommageable pour la continuité pédagogique est le mauvais taux d'enseignants qui sont préparés à intégrer le numérique dans leur enseignement. En effet, les principaux pensent que seulement 55% des enseignants ont les compétences techniques et pédagogiques pour intégrer le numérique dans leur pratique pédagogique (65% pour la moyenne de l'OCDE), ce qui place la France au 59e rang sur les 77 pays classés sur ce critère dans PISA 2018.

3.3. Enjeux d'éthique et recommandations

Nous indiquons un certain nombre d'enjeux pour les données d'éducation relatifs aux accès au numérique et aux compétences numériques, ainsi qu'à la citoyenneté numérique :

- Il y un enjeu d'équité pour les citoyens français :
    - en termes d'accès à internet. Si les collectivités territoriales sont toutes engagées dans des plans de généralisation de la fibre à l'habitant, elle n'est pas encore installée sur tout le territoire, et les moyens informatiques nécessaires pour échanger les données scolaires sont loin d'avoir la même qualité partout. Par ailleurs, certains élèves sont dépourvus d'accès internet, ainsi que certains enseignants, comme

[38] Note de la direction de l'évaluation, de la prospective et de la performance (DEPP), n° 19-22 (juin 2019) qui fait la synthèse d'une enquête internationale Talis réalisée tous les 5 ans par l'OCDE : https://www.education.gouv.fr/pratiques-de-classe-sentiment-d-efficacite-personnelle-et-besoins-de-formation-une-photographie-12581

[39] A framework to guide an education response to the COVID-19 Pandemic of 2020: https://www.hm.ee/sites/default/files/framework_guide_v1_002_harward.pdf

cela a été noté par le MENJ dès le début du confinement dans son *vadémécum*[40].

  - en termes de messageries numérique. Les comptes de messagerie personnelle des enseignants ne permettent pas tous d'échanger des gros fichiers (par exemple avec des images).
  - en termes d'équipement informatique. Dans les familles, même lorsqu'un ou plusieurs équipements numériques existent, ils ne sont pas toujours disponibles pour chaque enfant (fratrie, parents en télétravail sur les mêmes équipements, etc.), et les conditions de logement ne sont pas les mêmes pour toutes les familles (par exemple, s'il n'y a qu'une seule pièce pour travailler - pas de pièce pour s'isoler).

- Comme le souligne le Conseil de l'Europe, il y a un risque pour ceux qui ne sont pas des « natifs du numérique » ou qui n'ont pas la possibilité de devenir des « citoyens numériques » d'être marginalisés dans la société[41].
- Si le temps passé à l'école tend à réduire les inégalités sociales (bien que le rapport 2019 de l'Observatoire des inégalités constate que « La situation des inégalités scolaires semble figée »[42]), ce sont les mêmes familles - les mêmes milieux sociaux[43]-, qui sont pénalisés par le manque d'accès au numérique et aux compétences numériques, ainsi que par le manque de temps passé à l'école, les exposant en quelque sorte à une double peine, par un renforcement de la fragilité scolaire.
- Les élèves, leurs familles et les enseignants ne sont pas tous conscients du modèle économique sous-jacent aux offres soi-disant gratuites du privé et qui utilisent leurs données personnelles numériques comme une marchandise, impliquant un risque pour la confidentialité de leurs données.
- En raison du téléenseignement promu en temps de pandémie, les élèves sont sollicités pour une utilisation massive et continue des outils numériques de communication et sont par suite exposés plus largement aux informations qui circulent sur la toile. En tant que mineurs, ils sont plus vulnérables et plus facilement influençables. De plus, il est difficile pour eux de discerner parmi le flot d'informations qu'ils voient passer et portées par les médias, les fausses informations[44].

Enjeux d'éthique :

- Accentuation des inégalités territoriales, sociales et familiales pour l'accès au numérique et son utilisation pendant la pandémie
- Renforcement des inégalités scolaires par les inégalités d'accès au numérique (équipement et connexion) et par les manques de compétences numériques
- Vulnérabilité des élèves et des familles par le manque de compétences

[40] https://www.education.gouv.fr/sites/default/files/2020-03/coronavirus-covid-19-vademecum-continuit-p-dagogique-66201.pdf

[41] "Decision makers and policy framers need to be sensitised to the fact that the lack of DCE [Digital Citizenship Education] poses risks of youth exclusion if such basic literacy is not provided in order to empower them as citizens and creative and critical actors" , in Digital citizenship education. Overview and new perspectives, Council of Europe, octobre 2017 : https://rm.coe.int/prems-187117-gbr-2511-digital-citizenship-literature-review-8432-web-1/168077bc6a

[42] https://www.inegalites.fr/L-essentiel-des-inegalites-d-education?id_theme=17

[43] En 2015, l'école française est celle où l'origine sociale des enfants pèse le plus lourd dans les résultats scolaires, parmi les pays de l'OCDE : https://www.avise.org/articles/en-france-les-inegalites-scolaires-saggravent

[44] https://www.ccne-ethique.fr/sites/default/files/cnpen-desinformation-2020-07-21.pdf

numériques pour appréhender les enjeux du modèle économique des marchands de données numériques
- Vulnérabilité des élèves face aux fausses informations
- Risque d'exclusion de ceux qui ne pourraient pas devenir des « citoyens numériques »

Recommandations

1. Dans un contexte de ressources numériques limitées, coordonner de façon équitable leur distribution dans les écoles pour faciliter l'accès aux familles, et s'assurer de leur utilisabilité en cas d'éducation à distance.
2. Veiller à ne pas discriminer les élèves n'ayant pas pu bénéficier de la continuité pédagogique par manque d'accès au numérique pendant la période de confinement.
3. Mettre en œuvre une stratégie de formation des familles et des équipes pédagogiques dédiée aux outils numériques pour l'éducation, incluant une sensibilisation aux modèles économiques du marché des données, et évaluer son efficacité à réduire les inégalités sociales et territoriales dans l'usage de ces outils. Une formation au numérique tout au long de la vie devrait être également mise en place pour tous les citoyens.
4. Mettre en place des systèmes alternatifs permettant d'acheminer les contenus éducatifs en conditions dégradées d'accès au numérique.
5. Concevoir un enseignement qui sensibilise aux enjeux de cybersécurité et de la maîtrise des outils permettant de préserver la vie privée et d'alerter sur différentes formes de manipulation facilitées par les médias numériques, dès l'école primaire et dans les classes du secondaire.
6. Eduquer aux médias et éduquer par les médias : enfants, familles et enseignants doivent aussi être sensibilisés aux services en ligne, à la vérification des faits et à l'analyse critique des informations disponibles (lutte contre les fausses informations et les manipulations d'information).
7. Définir les compétences en termes de valeurs, attitudes et connaissances, que doivent acquérir tous les élèves pour devenir des « citoyens numériques ».
8. Mettre en œuvre pour tous une véritable éducation à la citoyenneté numérique.

Récapitulatif des recommandations

Respecter les libertés fondamentales des acteurs de l'éducation

1. Engager une réflexion sur l'opportunité d'introduire dans le RGPD le statut de données sensibles pour les données d'éducation, à l'instar des données de santé, à des fins de protection de la vie privée des élèves et des enseignants.
2. Donner un statut juridique plus protecteur pour les données d'éducation, au niveau français en instituant un code de bonne conduite sur les données d'éducation pour l'ensemble des acteurs (publics comme privés).
3. Attirer l'attention des différents acteurs (enseignants, élèves, familles, entreprises, acteurs académiques, politiques) sur le caractère « spécifique » des données d'éducation et continuer à responsabiliser ces acteurs dans leur utilisation de ces données.
4. Intensifier la formation au droit à la protection des données, en particulier de celles qui sont liées aux usages pédagogiques numériques, pour les enseignants, les élèves et leurs familles, en illustrant avec des cas pratiques.
5. Accentuer la sensibilisation des différents responsables de traitements aux principes de protection des données exigés par le RGPD pour la collecte des données personnelles en les explicitant, en les expliquant et en les exemplifiant.
6. Continuer et intensifier les démarches de sensibilisation de l'équipe éducative et des élèves aux risques d'ingérence dans la vie privée par l'usage des outils numériques (dont cyberharcèlement). Ces démarches de sensibilisation doivent s'inscrire bien au-delà du domaine de l'éducation et concerner aussi les usages des réseaux sociaux par les élèves.
7. Proposer un label (ou une certification) ouvert à tous les acteurs des EdTech remplissant un certain nombre de critères qui garantissent le respect de la vie privée des acteurs de la communauté éducative.
8. Offrir des garanties de sécurité des outils que l'Etat recommande ou met à la disposition des acteurs de l'éducation, et évaluer le risque que fait courir leur perte éventuelle de confidentialité.
9. Mettre en place des accords avec les acteurs privés dont les élèves et les enseignants utiliseraient les outils, afin de garantir une minimisation de l'usage de la donnée à une liste définie par le Ministère, ainsi qu'un effacement régulier des données.

Garantir la souveraineté numérique en matière d'éducation

1. Définir une stratégie nationale et portée par l'Europe concernant le développement de produits numériques d'éducation respectant les valeurs fondamentales Européennes.
2. Assurer une offre gratuite à l'échelle nationale ou européenne d'outils de téléenseignement de bonne qualité, relative à un minimum de fonctionnalités (telles que des actions de partage collaboratif), à leur convivialité (rapidité d'exécution, facilité de prise en main) et à leur robustesse (outils adaptés à un grand nombre de participants) qui respectent les valeurs éthiques européennes portées par le RGPD.

3. Encourager les utilisateurs (élèves, enseignants, parents), au besoin par des formations dédiées, à recourir à l'offre publique, chaque fois qu'elle est suffisante.
4. Identifier au niveau national les offres dont le fonctionnement peut poser à moyen ou long termes des problèmes éthiques liés aux données.
5. Effectuer une veille et une analyse des principaux outils de communication, de partage et de collaboration qui peuvent s'avérer utiles dans le cadre de l'enseignement scolaire, développés par des acteurs publics ou privés français ou européens qui sont respectueux de nos libertés fondamentales.
6. Sensibiliser les différents acteurs (enseignants, élèves, familles, entreprises, acteurs académiques, politiques) aux enjeux de souveraineté numérique dans le domaine des données scolaires numériques.

Assurer l'égalité d'accès au numérique

1. Dans un contexte de ressources numériques limitées, coordonner de façon équitable leur distribution dans les écoles pour faciliter l'accès aux familles, et s'assurer de leur utilisabilité en cas d'éducation à distance.
2. Veiller à ne pas discriminer les élèves n'ayant pas pu bénéficier de la continuité pédagogique par manque d'accès au numérique pendant la période de confinement.
3. Mettre en œuvre une stratégie de formation des familles et des équipes pédagogiques dédiée aux outils numériques pour l'éducation, incluant une sensibilisation aux modèles économiques du marché des données, et évaluer son efficacité à réduire les inégalités sociales et territoriales dans l'usage de ces outils. Une formation au numérique tout au long de la vie devrait être également mise en place pour tous les citoyens.
4. Mettre en place des systèmes alternatifs permettant d'acheminer les contenus éducatifs en conditions dégradées d'accès au numérique.
5. Concevoir un enseignement qui sensibilise aux enjeux de cybersécurité et de la maîtrise des outils permettant de préserver la vie privée et d'alerter sur différentes formes de manipulation facilitées par les médias numériques, dès l'école primaire et dans les classes du secondaire.
6. Eduquer aux médias et éduquer par les médias : enfants, familles et enseignants doivent aussi être sensibilisés aux services en ligne, à la vérification des faits et à l'analyse critique des informations disponibles (lutte contre les fausses informations et les manipulations d'information).
7. Définir les compétences en termes de valeurs, attitudes et connaissances, que doivent acquérir tous les élèves pour devenir des « citoyens numériques ».
8. Mettre en œuvre pour tous une véritable éducation à la citoyenneté numérique.

Annexes

Annexe 1 – Auto-saisine

Auto-saisine du Comité d'éthique pour les données d'éducation

La crise sanitaire due à la pandémie de Covid 19 a nécessité la mise en place de la continuité pédagogique hors école/établissement scolaire en utilisant massivement et de façon accélérée des outils numériques.

Au-delà des objectifs de continuité, d'inclusion et d'équité indispensables à la réussite de cette transition, le recours aux outils numériques avec des usages nouveaux ou renforcés ne va pas sans un accroissement des risques déjà existants et sans l'émergence de risques nouveaux.

Dans cette situation d'urgence des décisions partiellement anticipées, des points de vulnérabilités justifient une attention particulière quant à la nature des données d'éducation collectées et leur utilisation dans ce contexte et dans la durée.

Qu'il s'agisse des outils et usages institutionnels, ou d'outils et d'usages moins encadrés, une réflexion du comité pour identifier les questions éthiques liées à la gestion (stockage et réutilisation) et à la protection des données d'éducation des élèves, à l'égalité (ou l'inégalité) d'accès des élèves devant ces services en ligne, mais aussi à la souveraineté numérique nationale, soulevées par ces usages accentués du numérique, permettra d'éclairer le ministère afin qu'il puisse émettre des alertes et des recommandations à destination de la communauté éducative, des élèves et de leurs familles. Ces recommandations doivent renforcer les principes en lien avec la réversibilité des données, l'accès à/et la protection des données personnelles ainsi que la conformité au RGPD.

Cette analyse des enjeux éthiques liés à la collecte, l'échange et le traitement des données d'éducation est initiée de façon réactive dans l'urgence de la situation et devra se poursuivre dans les phases ultérieures de gestion de la crise. Elle prendra en compte les impératifs de continuité pédagogique, le respect des valeurs au cœur de la mission pédagogique, la protection indispensable des élèves et de la communauté éducative pour une confiance partagée de même que les opportunités d'évolution du système éducatif.

Annexe 2 – Experts consultés

La rédaction de ce rapport a bénéficié des avis de deux experts qui ont été auditionnés :

M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique et M. François Taddei, directeur du Centre de Recherches Interdisciplinaires (CRI),

ainsi que de commentaires sur une version intermédiaire de M. Claude Kirchner, directeur du comité national pilote d'éthique du numérique.

Annexe 3 – Déclaration conjointe France Estonie

Joint declaration France Estonia

EIGS 2019

- Advanced digital technologies allow collecting, processing and analyzing large amounts of data. This increasing digitalization entails an exponential growth of data.

- Les technologies numériques avancées permettent la collecte, le traitement et l'analyse de grandes quantités de données. Cette digitalisation croissante entraîne une croissance exponentielle des données.

- The use of data collected in school offers many prospects in term of improving teaching methods, learning opportunities to pupils and the management of education systems..

- L'utilisation des données recueillies à l'école offre de nombreuses perspectives en termes d'amélioration des méthodes d'enseignement, de possibilités d'apprentissage pour les élèves et de pilotage des systèmes éducatifs.

- These potential benefits also mean that the student must have the necessary skills and be aware of some of the risks associated with the use of these digital tools and his personal data.

- Ces avantages potentiels signifient également que l'élève doit avoir les compétences nécessaires et être informé de certains risques liés à l'utilisation de ces outils numériques et celle de ses données personnelles.

- For national education policies, the main challenge is to prepare pupils to use digital technologies effectively and safely, and to prevent any misuse in ways of collecting and using learner data. *In that sense, we consider that pupils' data should have a specific status.*

- Pour les politiques éducatives nationales, le principal défi consiste à préparer les élèves à utiliser les technologies numériques de manière efficace et sûre, et à prévenir toute utilisation abusive dans la collecte et l'utilisation des données relatives aux apprenants. **En ce sens, nous considérons que les données relatives aux élèves devraient avoir un statut spécifique.**

- There are already some data protection frameworks such as the European Union's General Data Protection Regulations and the Council of Europe's Data Protection Convention which aim to protect citizens' personal data.

- Il existe déjà certains cadres de protection des données, tels que les règlements généraux de l'Union européenne sur la protection des données et la convention du Conseil de l'Europe sur la protection des données, qui visent à protéger les données personnelles des citoyens.

- The confident and critical use of digital technology are closely linked with transparency and respect for ethics, and should be encouraged by a fully secure framework ensured by all stakeholders.

- L'utilisation confiante et critique de la technologie numérique est étroitement liée à la transparence et au respect de l'éthique, et devrait être encouragée par un cadre pleinement sécurisé assuré par toutes les parties prenantes.

- We are commited to strengthen Digital competency education, in order to help pupils use the digital environment and technologies ethically and responsibly, in learning and other environments.

- Nous nous engageons à renforcer l'éducation aux compétences numériques, afin d'aider les élèves à utiliser l'environnement numérique et les technologies de manière éthique et responsable, dans l'apprentissage et d'autres environnements.

- We therefore invite digital companies to build, with a view to the next summit, a framework of trust for the use of educational data and to explore two ways: the development by companies of a code of conduct, on the one hand, and the exploration of a specific status for educational data, on the other. The objective of such an approach is to provide a framework of trust for all users: students, teachers and parents and also to provide a framework for companies to better use this data and improve their services. This provides a balanced framework for developing the use of educational data.

- Nous invitons donc les entreprises du numérique à construire, en vue du prochain sommet, un cadre de confiance pour l'utilisation des données d'éducation et pour cela d'explorer deux voies : l'élaboration par les entreprises d'un code de conduite, d'une part, et d'autre part, l'exploration d'un statut spécifique des données d'éducation. L'objectif d'une telle approche est de fournir un cadre de confiance à tous les utilisateurs : élèves, enseignants et parents et également de fournir un cadre aux entreprises pour mieux utiliser ces données et améliorer leurs services. Ceci constitue un cadre équilibré propre à développer l'utilisation des données d'éducation.