Novembre 2020 T-PD(2019)06rev

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION

DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ

DES DONNÉES À CARACTÈRE PERSONNEL

Convention 108

La protection des données personnelles des enfants dans les systèmes éducatifs : enjeux et solutions possibles

Direction générale Droits de l'homme et État de droit

Rapport de Jen Persson, directrice de defenddigitalme

SOMMAIRE

1 Contexte 5

1.1 Introduction 5

1.1.1 L'approche actuelle met des droits en péril 6

1.1.2 Nombre et diversité des acteurs dans le secteur des données, sur la scène éducative 7

1.1.3 Exploration et exploitation de données 8

1.1.4 Des visées prédictives non affichées 9

1.1.5 Bâtir un environnement respectueux des droits tout au long de la vie 9

1.1.6 La réglementation doit revenir à l'application stricte des principes de base 10

1.1.7 Le paysage éducatif et les perspectives technologiques 11

1.1.8 Considérations relatives au champ de l'étude 12

2 Enjeux et recommandations 15

2.1 Capacité d'action et de décision 15

2.1.1 Le consentement doit être libre et éclairé 15

2.1.2 Le consentement ne peut être refusé qu'au détriment de la personne concernée et ne peut être considéré comme donné librement. 16

2.1.3 Le consentement ne peut être pleinement éclairé dans le cadre des pratiques actuelles17

2.1.4 Étude de cas sur le consentement présumé 18

2.1.5 Repenser les modalités du consentement et du contrat dans le contexte des écoles peut être nécessaire. 18

2.1.6 Capacité d'action et de décision des enfants 20

2.1.7 Écoles et contrats d'achat» uniformisés « au clic (*click-wrap agreements*) 20

2.1.8 Les extractions de données opérées par l'État et le gouvernement font peser des obligations sur les écoles 21

2.1.9 Les élèves et les responsables légaux ont peu d'influence sur les conditions qui s'appliquent à eux 21

2.2 Le dossier permanent 22

2.2.1 L'importance du principe de la table rase 22

2.2.2 Un enfant ne peut contrôler la conservation excessive de données, d'où le risque d'abus 22

2.2.3 Les enfants ont un droit à la protection de leur réputation 23

2.2.4 Les demandes commerciales ou à des fins de marketing de conservation excessive devraient être rejetées 24

2.3 Gestion de l'identité 25

2.3.1 Vérification de l'âge et de l'identité 26
2.3.2 Vérification de l'identité au moyen des identifiants des médias sociaux 27
2.3.3 Vérification de l'identité au moyen de données biométriques 28
2.4 Sources de données et traitement opaque 29
2.4.1 Données cachées 29
2.4.2 La réorientation des données doit pouvoir être empêchée en pratique 30
2.5 Le rôle de l'implication des parents dans les questions relatives aux données des enfants à l'école 30
2.5.1 Prévenir les utilisations abusives à l'école : mission impossible pour les parents 31
2.5.2 Compréhension des enjeux par les parents 31
2.5.3 Aperçu des avis des parents en Angleterre 32
2.5.4 Les parents attendent des écoles qu'elles protègent et réalisent les droits de l'enfant 33
2.5.5 Les droits des parents concernant leurs propres données à caractère personnel 34
2.6 Le rôle des enseignants et du personnel scolaire 34
2.6.1 Non formés, les enseignants font confiance au système et aux prestataires 34
2.7 La charge d'investigation 35
2.7.1 À la fin de la scolarité obligatoire, on ne peut plus repérer l'empreinte numérique d'un enfant 36
2.8 Assistance, représentation et voies de recours pour les personnes concernées 36
2.9 Technologies spécifiques, essais et nouvelles problématiques 37
2.9.1 La participation à des tests de produits en conditions réelles est-elle sans danger pour la construction des enfants ? 38
2.9.2 L'enseignement public peut-il être façonné sans risque sous emprise commerciale ? 39
2.9.3 La valeur de l'éducation d'un enfant ne se mesure-t-elle qu'aux données ? 40
2.10 Intelligence artificielle et éducation 40
2.10.1 La discrimination et les biais dans les données sont des problèmes universels 41
2.10.2 Les choix faits dans la conception des produits peuvent porter atteinte aux droits des enfants 42
2.11 Données biométriques 43
2.11.1 Les données biométriques doivent-elles être considérées comme une denrée prisée ou devenir finalement des données courantes ? 44
2.11.2 Détection de visage et reconnaissance faciale 44

2.12 Protection et lutte contre l'extrémisme violent 46
2.12.1 Cela pourrait exacerber plutôt que diminuer la vulnérabilité des enfants aux risques. 48
2.12.2 Le couplage des données sous couvert de protection de l'enfant crée un panoptique de surveillance 48
2.13 Analyse prospective : sciences cognitives, incitations affectives et comportementales 49
2.13.1 Quelles sont les protections dont disposent nos enfants à l'école contre des technologies de modification du cerveau et du comportement et immersives ? 50
2.13.2 Quel devrait être le visage de l'éducation ? 52
2.14 Les outils de protection de la vie privée dans le cadre éducatif 53
2.14.1 Évaluation des risques pour la vie privée 53
2.14.2 Minimisation des données 54
2.15 Mécanismes d'audit 55
2.16 Rapports d'accès et d'utilisation 55
2.17 Le rôle des développeurs et de l'industrie 56
2.17.1 Effort disproportionné 56
2.17.2 Bibliothèques de développeurs tiers 57
2.17.3 Base licite pour le traitement 58
3 Conclusion : Qui encadrera l'avenir ? 59
4 Définitions 61
5 Remerciements 62
6 Références 63

1 Contexte

1.1 Introduction

Il ne faut pas sous-estimer le caractère sensible des données numérisées des élèves et des étudiants. (Document de travail du Groupe de travail international sur la protection des données dans le domaine des télécommunications, relatif aux plateformes d'apprentissage électronique, avril 2017).

> « Certaines de ces plateformes d'apprentissage électronique et l'analyse de l'apprentissage qu'elles facilitent peuvent apporter une immense contribution au développement de pratiques d'apprentissage novatrices et efficaces. Utilisées de façon optimale, elles peuvent améliorer et compléter les échanges entre élèves, parents et éducateurs dans l'environnement éducatif et aider chacun à réaliser son plein potentiel. Cela dit, elles peuvent également présenter des risques pour la vie privée de ces personnes, résultant de la collecte, de l'utilisation, de la réutilisation, de la divulgation et de la conservation de leurs données à caractère personnel » (Résolution de la Conférence internationale des commissaires à la protection des données et de la vie privée sur les plateformes d'apprentissage en ligne, 2018).

Le risque de préjudice lié à une mauvaise utilisation de simples informations sur l'éducation numérisées peut sembler modéré en comparaison avec d'autres technologies plus complexes déjà mises en œuvre dans l'éducation. Cependant, si l'on considère le volume des bases de données d'élèves qui contiennent des centaines d'éléments de données personnelles de personnes nommément identifiées, soit des millions d'enregistrements sur un plan national, on voit déjà mieux les risques, notamment d'atteinte à la réputation, auxquels la moindre perte de données peut exposer les personnes et les institutions concernées.

Il est aussi important de reconnaître que, quelque soient les différences dans les paysages éducatifs dans le monde, les enfants sont communément utilisés comme bancs d'essai pour de nouvelles technologies, autant par des entreprises dans l'élaboration de leurs produits que par des intervenants étatiques avant de les adopter à grande échelle.

Peu de recherches portent sur des questions pourtant importantes relatives à la santé et à la sécurité humaine et sur les questions d'éthique et de gouvernance liées à l'introduction de nouvelles technologies dans les salles de classe, telles que le mal des transports dans la réalité virtuelle immersive. Les neurotechnologies et la science à l'ère post-numérique appellent une attention concertée de la part des chercheurs en éducation (Williamson, 2019) ainsi que de la part des autorités législatives et de régulation.

Alors que les autorités de contrôle de la protection des données sont aux prises avec la protection des données et de la vie privée dans un large éventail de secteurs, défendre les droits des enfants dans l'éducation n'a bénéficié que de peu d'attention concertée et d'action systémique jusqu'à présent, la tendance étant à regarder ce qui est plutôt qu'à étudier l'horizon.

En 2009, le groupe de travail Article 29 a publié un avis (2/2009) sur la protection des données personnelles des enfants (Recommandations générales et cas particulier : les établissements scolaires). Il a reconnu que « d'un point de vue statique, l'enfant est une personne qui n'a pas encore atteint la maturité physique et psychologique. Dans une perspective dynamique, l'enfant se développe sur le plan physique et mental pour devenir un adulte. Les droits de l'enfant et l'exercice de ces droits, et notamment du droit à la protection des données, devraient s'exprimer en tenant compte de ces deux dimensions ».

Vus sous cet angle, les enfants, dans les différents systèmes d'éducation, chacun avec son propre ressenti quant aux transformations culturelles, sociales, économiques et politiques, n'ont peut-être pas beaucoup changé en dix ans, mais les technologies disponibles dans leurs salles de classe se sont, elles, rapidement multipliées.

Les écoles ont ouvert leurs portes et leurs bases de données d'informations personnelles et confidentielles d'enfants à un nombre croissant d'acteurs commerciaux. Les enfants sont peut-être déjà soumis à des outils d'imagerie cérébrales, des caméras 360° avec captation audio, des systèmes de surveillance RFID et utilisent des casques de réalité augmentée en classe. Les entreprises et leurs soutiens financiers cherchent à exploiter les nouveaux marchés de l'éducation là où les États délaissent les modèles nationaux pour des modèles plus commerciaux. De même, les entreprises les plus florissantes sur les marchés existants comme ceux des caméras de sécurité s'étendent en direction du secteur éducatif. Pourtant les conséquences en termes d'exposition des enfants à un vaste éventail de technologies de traitement des données sont passées largement inaperçues.

Les droits des enfants au titre de la législation sur la protection des données sont restés quasi inchangés en une décennie : leur respect dépend en grande partie des sociétés qui œuvrent en coulisse et de la surveillance exercée par les autorités de régulation, les contrôles et garanties pouvant être insuffisants au niveau de l'école.

Comme l'ont fait remarquer Lupton et Williamson en 2017,

> « Les enfants deviennent les objets d'une multitude de dispositifs de surveillance qui génèrent des données les concernant, mais ces pratiques commencent tout juste à éveiller l'attention des chercheurs en données critiques et des défenseurs de la vie privée ».

1.1.1 L'approche actuelle met des droits en péril

Croire que les enfants ne se soucient pas de la protection de leur vie privée est un mythe. Ce n'est simplement pas vrai. De nombreux témoignages nous renseignent sur leurs attentes. Il en ressort que les enfants et les jeunes peuvent être plus conscients des risques que ne le pensent de nombreux adultes (Paterson, L. et Grant, L. (sous la dir. de, 2010)), ils sont soucieux de leur vie privée ou craignent que leurs données ne tombent « entre de mauvaises mains ».

Le Commissaire à l'enfance d'Angleterre considère que nous manquons à notre devoir fondamental, en tant qu'adultes, de doter les enfants des outils dont ils ont besoin pour être les acteurs de leur propre vie (Children's Commissioner, 2017).

Au niveau national, les pouvoirs publics devraient peut-être revoir leur politique en matière de réemploi des données dont ils disposent à l'échelle de la population dans le domaine de l'éducation, pour des finalités secondaires comme l'établissement de profils de risque pour des interventions ou la recherche sur les politiques publiques, c'est-à-dire bien au-delà des finalités pour lesquelles elles avaient été recueillies à l'origine.

L'utilisation de données relatives à l'éducation par l'administration publique risque d'être de plus en plus compromise s'il est jugé que « les mégadonnées ont rendu les stratégies actuelles de protection de la vie privée et des libertés civiles obsolètes » (Mundie, 2014).

Une prise de conscience croissante de l'utilisation abusive des données entraînera une multiplication des refus des collecte de données (Against Borders for Children (UK) (2016-2018)), ce qui à long terme sera préjudiciable aux intérêts publics comme commerciaux (Parent Coalition for Student Privacy, (US) InBloom, 2012-14) et pourrait même menacer les bénéfiques qu'elle présente pour l'intérêt supérieur de l'enfant.

L'introduction commerciale de produits et de méthodes doit faire l'objet de davantage de précaution et de consultations plus poussées. Lorsque le programme d'apprentissage en ligne Summit a imposé des modèles commerciaux centrés sur la technologie dans l'éducation publique, il y a eu une vive opposition de la part des parents (Summit schools, Kansas, 2019).

La confiance est fragile et certaines pratiques altèrent l'image que le public a des technologies courantes dans un internet des objets qui ne cesse de se développer et fait progressivement son chemin jusque dans les salles de classe. Une utilisation de données qui continuerait à ne pas tenir compte de cette réalité accroît le risque général au détriment des autres entreprises qui utilisent les données personnelles. Comme l'a fait observer le rapport du Conseil norvégien des consommateurs #Toyfail en 2016,

> « Si l'idée que nos secrets les plus intimes et nos appareils puissent être piratés ne pas suffi à nous effrayer, peut-être le fait d'entendre des étrangers parler à nos enfants via un babyphone ou un jouet ébranlera-t-il davantage notre confiance dans les appareils connectés ».

La question de savoir combien de temps les modèles actuels sont viables pour la collecte de données en termes de fiabilité et de niveaux de tolérance sociétale est mise à l'épreuve par l'arrivée des nouvelles technologies émergentes dans les salles de classe, comme la reconnaissance faciale. (CNIL, 2019)

Les régulateurs jouent un rôle vital dans l'application de l'État de droit qui devrait offrir des cadres fiables et durables pour s'assurer que chaque enfant laisse une empreinte numérique la plus réduite possible jusqu'à sa vie d'adulte.

En outre, malgré une prolifération toujours croissante d'institutions qui émettent une documentation sur l'éthique et l'empreinte numérique, on attend toujours une prise en compte réelle et holistique de l'effet de ces technologies dans la vie de l'enfant, dans le présent et dans son avenir, ainsi qu'une évaluation de leur impact sur l'empreinte carbone de chaque enfant et sur la question de savoir si nous pouvons construire des modèles de matériel informatique plus durables afin de ne pas alourdir leur monde futur par leurs interactions dans l'environnement numérique actuel.

L'héritage croissant de certaines écoles en matière de TIC issu d'équipements précoces a la forme d'un placard rempli d'appareils inutilisables qu'elles ne peuvent se permettre de remplacer, construits sur des systèmes d'exploitation qui n'ont plus de maintenance.

Toute évaluation étique de l'impact des technologies émergentes doit aussi inclure leur impact environnemental ainsi que les modalités de responsabilisation des entreprises aux mesures nécessaires pour réduire leur consommation de ressources et d'énergie.

Les risques inhérents aux systèmes obsolètes comprennent l'exposition à des *ransomware* et autres menaces sur la sécurité[1].

1.1.2 Nombre et diversité des acteurs dans le secteur des données, sur la scène éducative

Le volume de données créées et collectées dans les systèmes scolaires à des fins administratives et pédagogiques a des incidences énormes pour l'« enfant mis en données » (Lupton, Williamson 2016).

[1] Les petits établissements scolaires sont des cibles particulièrement faciles à atteindre par des ransomware du fait de leur faible budget pour les technologies de l'information et leurs ressources de sécurité limitées - ArsTechnica (2019) https://arstechnica.com/information-technology/2019/08/rash-of-ransomware-continues-with-13-new-victims-most-of-them-schools

Dans les établissements d'éducation, les types d'acteurs impliqués dans le traitement des données personnelles d'enfants et provenant des écoles peuvent être en grande partie regroupés entre ceux qui ont une relation directe avec l'enfant (enseignants, personnel administratif) et ceux qui n'en ont pas (administrateurs régionaux traitant les données à des fins d'analyse, de performances des enseignants et de mesures des progrès des élèves).

Mais la grande majorité des personnes impliquées dans le traitement courant des données correspondant à une journée, une année ou la vie entière d'un enfant, difficiles à imaginer du fait de leur gros volume, ne sont pas dans les locaux des écoles mais en dehors, dans les centaines d'entreprises qui traitent des données à partir du cloud.

Les types de données recueillies peuvent être de façon générale regroupés en données administratives et données d'apprentissage.

Dans le domaine de l'éducation, les finalités du traitement de données peuvent porter sur la gestion des présences et absences, l'évaluation et le suivi des résultats scolaires, la surveillance des comportements, les relations avec les parents et leur participation, la gestion des locaux et des plans de salle, les paiements sans espèces, la protection et la lutte contre l'extrémisme violent, le suivi des ressources, la responsabilité et la performance du personnel, ou encore le benchmarking. Et tout cela avant que les données soient traitées pour évaluer l'intelligence des élèves, les accompagner dans leurs apprentissages et leurs devoirs ou à des fins de recherche. La technologie est utilisée pour enseigner, suivre les progrès des étudiants et les tester.

Sans contrôles adéquats compte tenu de la multitude de prestataires qui interviennent chaque jour que l'enfant passe dans le système éducatif, la collecte et la réutilisation des données des enfants sur toute une scolarité peuvent pendre une ampleur qui échappe aux établissements eux-mêmes comme aux responsables légaux.

1.1.3 Exploration et exploitation de données

Pour diverses raisons, les acteurs commerciaux et les technologies nouvelles connaissent une croissance rapide sur le marché global des technologies éducatives, favorisée par des investisseurs providentiels et des accélérateurs de technologie sur les marchés anglophones des États-Unis et du Royaume-Uni, mais aussi partout ailleurs dans le monde. Les estimations de la valeur du marché et du montant des investissements sont très variables : le chiffre de 8 milliards de dollars est avancé, mais selon l'étude de Metaari intitulée « The 2018 Global Learning Technology Investment Patterns: The Rise of the Edtech Unicorns », les sociétés chinoises de technologies éducatives auraient été les principales bénéficiaires des investissements globaux du secteur en 2018 en captant 44,1 % d'un marché total de 16,34 milliards de dollars de dépenses.

Dans le même temps, sous la pression mondiale pour assurer un enseignement public à bas coûts et de la marchéisation, les infrastructures utilisées pour l'enseignement public et les enfants en leur sein sont exposés à un risque supplémentaire lié aux « gratuiciels » (*freeware*), ces logiciels que des entreprises proposent sans frais, mais souvent moyennant un échange non-explicite de données[2].

L'introduction de nouvelles technologies s'accompagne souvent de formations et d'une gestion du changement insuffisantes, avec des matériels pédagogiques peu adaptés et des et des enseignants sous-qualifiés (Sabates, R. 2010).

[2] Par exemple, en 2019, le groupe NetDragon Websoft était "en route pour monétiser sa base d'utilisateurs" à partir de la communauté en ligne d'Edmodo. (page 4 (6/84) http://file.download.99.com/down/ir_e_20191011f.pdf)

1.1.4 Des visées prédictives non affichées

Dans une expérimentation menée à Espoo en Finlande, en coopération avec la société Tieto, l'intelligence artificielle a été utilisée pour analyser des données sur la santé et l'aide sociale relatives à l'éducation durant la petite enfance, entre 2002 et 2016 (Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch 2019).

En Angleterre, le conseil du comté d'Essex utilise l'analyse prédictive pour identifier les enfants qui ne seraient pas "prêts pour l'école" à leur cinquième anniversaire, et le conseil municipal de Bristol expérimente de nouvelles capacités algorithmiques en prenant en compte des données sur les élèves, extraites de nuit[3], dans ses analyses prédictives en vue d'actions de protection sociale des enfants (Pegg, McIntyre, 2018)

La nature prédictive de tels traitement de données appliqué à des interventions précoces pourrait avoir un impact significatif et des conséquences à long terme non voulues sur les enfants dès leur plus jeune âge.

Les logiciels vendus comme utilisant l''intelligence artificielle sont aussi utilisés pour prédire des risques de comportement relatifs à de produits de contrôle d'internet, dans des plateformes d'apprentissage personnalisé et même pour la prise de petites décisions au niveau de salles de classe comme l'assignation de places à partir des données comportementales des élèves sur des applications, analysées de manière opaque pour définir des configurations de salle optimisées (ClassCharts).

Les conclusions de Regan et Steeves (2019) suggèrent que

> « Les discours concurrents sur l'apprentissage personnalisé tournent autour de significations contestées sur le type d'expertise nécessaire à l'apprentissage au XXIe siècle, sur ce à quoi devrait ressembler l'apprentissage autodirigé, si l'éducation concerne le processus ou le contenu, et sur le type de preuves nécessaires pour établir si un apprentissage personnalisé conduit ou non à de meilleurs résultats chez l'élève ».

Les implications générales potentielles pour la sécurité et la stabilité des infrastructures éducatives du secteur public et l'interaction avec d'autres secteurs publics où les données des enfants sont utilisées pour des interventions dans leur vie, les coûts personnels pour les enfants en termes de vie privée, et les effets de la normalisation des prises de décision automatisées peuvent dépasser la durée de vie de cette génération de données.

1.1.5 Bâtir un environnement respectueux des droits tout au long de la vie

La technologie et ses effets sur les relations humaines et le rôle de l'humain dans la société sont depuis longtemps source de préoccupation. En 1946, l'autrice Anaïs Nin évoquait dans son journal « cette époque dangereuse où les voix mécaniques, radios et téléphones remplacent l'intimité, et l'idée d'être en relation avec des millions d'individus appauvrit toujours plus les relations humaines » (Le journal d'Anaïs Nin, vol. 4 : 1944-1947).

Le volume, la vitesse et la simplicité du transfert de données ont augmenté de façon exponentielle depuis la création d'internet et du web, tandis que le coût de la conservation des données a baissé. L'accessibilité accrue des données a réduit les obstacles à leur copie et à leur distribution, mais elle s'est également accompagnée d'un recul des protections offertes dans la pratique aux personnes concernées, les entreprises et les institutions négligeant leurs obligations en la matière.

[3] http://specification.sifassociation.org/Implementation/UK/2.0/html/

Au paragraphe 8 de son Observation générale n° 1 sur les buts de l'éducation, le Comité des droits de l'enfant de l'Organisation des Nations Unies a affirmé en 2001 :

> « Les enfants ne sont pas privés de leurs droits fondamentaux du seul fait qu'ils franchissent les portes de l'école. Ainsi, par exemple, l'éducation doit être dispensée dans le respect de la dignité inhérente de l'enfant et doit permettre à l'enfant d'exprimer ses opinions librement conformément au paragraphe 1 de l'article 12 et de participer à la vie scolaire ».

Comme indiqué dans la Recommandation CM/Rec (2018)7 du Comité des Ministres, les États membres ont un devoir de respecter, protéger et réaliser les droits de l'enfant dans l'environnement numérique. Il ne faudrait pas utiliser les produits des fournisseurs qui ne respectent pas ces droits.

Le traitement de données durant l'enfance à des fins de profilage, et en particulier d'analyse prédictive, risque d'avoir des effets opaques à vie pour la personne concernée. Dans les milieux scientifiques, beaucoup accueillent avec enthousiasme l'idée d'entreprendre avant même la naissance cette mise en données des individus à des fins de stratification des risques et d'interventions. L'intelligence – la capacité à apprendre, à raisonner et à résoudre des problèmes – est au premier plan dans la recherche génétique comportementale (Plomin, Stumm 2018).

Les prédictions basées sur l'analyse automatique de grands ensembles de données personnelles, les décisions automatisées qui apportent des changements à l'écran et hors écran à l'expérience vécue par l'enfant simplement en poussant les interactions à l'écran, et les interventions personnalisées effectuées en conséquence par les adultes, sont toutes déjà possibles à des niveaux d'invasivité et de manière cachée ou opaque que la plupart des familles et le personnel scolaire eux-mêmes ne voient pas. Les raisons de l'échec des obligations de transparence et les moyens d'y remédier exigent une approche systémique différente pour aider les enfants et les familles à comprendre comment leurs propres données sont traitées par d'autres.

Certaines applications des technologies reposant sur la capture, l'exploration et l'interprétation des données des enfants devraient être jugées trop intrusives et préjudiciables au plein et libre épanouissement des enfants pour que l'on accepte qu'ils y soient exposés dans le cadre éducatif. La réglementation devrait suivre une approche proactive en exigeant une coopération entre les autorités de protection des données et celles chargées des lois sur la sécurité du consommateur dès lors que des produits et services sont introduits en classe ou utilisés dans le cadre d'interventions auprès des enfants. Mais cela ne doit pas signifier l'imposition d'essais et de tests de produits sur les enfants en classe dans le cadre des systèmes d'enseignement public obligatoire au profit principal des fabricants de produits.

1.1.6 La réglementation doit revenir à l'application stricte des principes de base

Les droits de l'homme consacrés par la Convention des Nations Unies relative aux droits de l'enfant, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (STE n° 5) et leurs protocoles doivent être pleinement respectés, protégés et réalisés dans l'éducation.

Les principes fondamentaux que sont la limitation des finalités, la minimisation des données et la transparence sont souvent insuffisants dans la pratique s'ils ne sont pas accompagnés de mesures fortes et dissuasives pour les faire respecter.

Il incombe par ailleurs aux adultes de veiller non seulement à ce que les protections offertes aux enfants soient adaptées à leurs besoins tout au long de leur enfance, mais également

qu'elles leur permettent d'atteindre l'âge adulte sans entrave et de s'épanouir pleinement et librement, en donnant le meilleur d'eux-mêmes.

Les principes de nécessité, de proportionnalité et d'application effective des périodes de rétention de données devraient être renforcés pour prévoir une limitation légale par défaut de la durée de conservation des données individuelles identifiables dans les dossiers scolaires des enfants.

Le principe de minimisation des données est au cœur de ce dont les enfants ont besoin pour que la protection des données ait un effet significatif sur la protection de leur personne et de leur dignité humaine, et pas seulement pour permettre un traitement sûr, équitable et licite de leurs données. Les limites de la portée de l'approche proposée par le groupe d'experts de haut niveau sur l'intelligence artificielle (HLEG-AI) dans ses recommandations de politique et d'investissement pour une intelligence artificielle fiable en avril 2019 devrait être appliquée pour assurer une meilleure protection dans l'environnement éducatif et ne devrait pas être déterminée par les acteurs étatiques ou les désirs commerciaux, mais plutôt par les besoins et l'intérêt supérieur de l'enfant, afin de lui permettre de se développer pleinement et librement à l'âge adulte. :

> « Il faudrait assurer aux enfants un espace de développement libre et non surveillé, et faire table rase de toutes les données publiques ou privées conservées à leur sujet lorsqu'ils atteignent l'âge adulte ». (HLEG-AI, 2019)

1.1.7 Le paysage éducatif et les perspectives technologiques

L'activité législative et les procédures de passation de marchés publics à tous les niveaux de l'administration doivent respecter l'Observation générale n° 16 (2013) du Comité des droits de l'enfant sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant.

> « Un État ne devrait pas commettre, encourager ou laisser commettre des violations des droits de l'enfant lorsqu'il a lui-même un rôle commercial ou entretient des relations commerciales avec des entreprises privées. Par exemple, les États doivent prendre des mesures pour que les marchés publics soient attribués à des soumissionnaires qui s'engagent à respecter les droits de l'enfant. Les organismes et institutions de l'État, notamment les forces de sécurité, ne devraient pas participer à la commission d'atteintes aux droits de l'enfant ou laisser commettre de tels actes par des tiers. En outre, les États ne devraient pas investir de l'argent public ou d'autres ressources dans les activités d'entreprises qui portent atteinte aux droits de l'enfant ».

Le champ évolutif de ce qui est autorisé, possible et acceptable dans l'éducation reste théorique pour de nombreux universitaires et responsables politiques. Trois ans pour tester un produit et le mettre sur le marché, ou pour mesurer l'efficacité et l'utilité pédagogique d'un outil de technologie éducative suffisent à peine et peuvent sembler courts aux yeux des développeurs, mais peuvent représenter plus du quart du temps passé par un enfant dans l'enseignement obligatoire.

L'espoir et l'engouement qu'avaient suscité les formations en ligne ouvertes à tous (MOOC) en 2012 (New York Times, 2012) que les cours en ligne allaient pouvoir apporter le meilleur de l'éducation dans les régions les plus reculées du monde, former sans effort les professionnels tout au long de leur carrière et « étendre les réseaux intellectuels et personnels » sont quelque peu retombés.

Certains restent réservés quant au modèle économique des MOOC, dans lequel les conférenciers sont incités en permanence à participer à la prestation de cours, et se

demandent si le bénéfice intellectuel pour les étudiants et les facultés est à la hauteur du gain financier pour les investisseurs (Davidson, C. 2017).

Cependant, bien que la croissance des certaines plateformes d'apprentissage ait peut-être été inférieure aux prévisions, de nouvelles plateformes promettant souvent des technologies perçues plus récentes et des fonctionnalités d'intelligence artificielle et d'apprentissage-machine, sont en plein essor. Une multitude de nouveaux outils administratifs font leur apparition dans le secteur de l'éducation, souvent assortis de la promesse d'accroître l'efficacité du personnel tout en réduisant sa charge de travail et d'améliorer les résultats scolaires des élèves. En parallèle, du moins au Royaume-Uni, où le secteur est de plus en plus géré comme une entreprise, la marchéisation est encouragée, le nombre d'enseignants est en baisse dans l'enseignement public et les dépenses consacrées à l'éducation diminuent.

Ce résumé de l'état de l'utilisation des données à caractère personnel donne un aperçu des technologies disponibles et mises en œuvre, et invite à s'interroger sur l'efficacité des réglementations en vigueur en matière de protection des données et ses mécanismes de contrôle qui reposent sur des plaintes individuelles, à tenir compte des droits de l'enfant dans l'environnement éducatif.

1.1.8 Considérations relatives au champ de l'étude

Aux fins du présent rapport, les définitions utilisées seront celles de la convention. En l'occurrence, la « personne concernée » est l'enfant et, selon la Convention des Nations Unies sur les droits de l'enfant, (UNCRC par. 1) un enfant est « tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable ». Dans les références, on pourra trouver selon le pays les termes « élève » ou « étudiant » ; ils sont employés ici de manière interchangeable.

Par l'évocation du traitement de données dans le secteur de l'éducation, il n'est fait ici aucune distinction entre les différents modèles d'éducation proposés à travers le monde et le type d'enseignement, obligatoire, privé ou public. Le choix est plutôt de présenter une sélection de domaines relevant de la prestation de services éducatifs, dans lesquels les données des enfants peuvent faire l'objet d'un traitement par les autorités et par des tiers commerciaux – une pratique déjà courante, qui s'étend au-delà des frontières nationales.

Les enfants vivant aux États-Unis ne rencontreront peut-être pas les mêmes problèmes de mobilité que ceux d'Afrique subsaharienne, du Ghana, du Malawi ou d'Afrique du Sud (Porter, 2010) pour accéder aux services éducatifs, mais du point de vue de la surveillance, les conséquences de l'utilisation d'outils numériques sur un téléphone mobile ou une tablette seront les mêmes pour tous.

Bridge International, par exemple, affirme que son application pour smartphone « permet aux directeurs de ses Académies de synchroniser facilement les tablettes de leur école, d'améliorer l'assiduité des élèves et des enseignants, de gérer le paiement des droits de scolarité, de superviser l'instruction et plus encore ».

Les critiques exprimées sur son « solutionnisme technologique » et l'utilisation dans un but lucratif d'une pédagogie high-tech standardisée développée depuis son siège aux États-Unis se retrouvent dans d'autres pays (ESCR-Net- International Network for Economic, Social & Cultural Rights (2018)). En mars 2018, 88 organisations de la société civile ont uni leurs voix dans une lettre demandant aux grands investisseurs financiers de renoncer à soutenir les Bridge International Academies (BIA), réseau multinational à but lucratif gérant plus de 500 écoles au Kenya, au Libéria, au Nigéria, en Ouganda et en Inde.

Lorsque Mark Zuckerberg a essayé d'exporter des solutions du type Silicon Valley dans le cadre du modèle d'éducation des Summit Schools financé par Facebook au Kansas, un État

du Midwest américain, elles ont été accueillies avec de fortes objections, même de la part des enfants eux-mêmes (Bowles, 2019).

Les plus grands contributeurs commerciaux à la refonte des infrastructures éducatives sont les mêmes qui façonnent le monde des affaires : Google, Microsoft et Apple. En outre, certains des plus grands éditeurs du monde sont également impliqués dans la fourniture d'outils éducatifs en ligne, par exemple Pearson et Wiley et NewsCorp. Les entreprises qui suivent les écrits et le contenu universitaires créent également des balises de contenu en ligne, ce qui permet d'en suivre l'utilisation à une échelle que le contenu non numérique ne permet pas. Selon les mots de Jose Ferreira, alors PDG de la société d'éducation Knewton, en 2012,

> « La race humaine est sur le point d'entrer dans une existence totalement minée par les données... l'éducation se trouve être aujourd'hui, de loin, l'industrie la plus exploitable au monde. »

Cela soulève toujours la question de savoir qui possède les méga données ? (Ruppert 2015), car les données numériques sont utilisées par des organisations techniques de plus en plus puissantes pour produire des connaissances et orienter la prise de décision. (Williamson, 2017) Et comme les connaissances extraites des données dans l'éducation sont de plus en plus utilisées pour pousser et prédire le comportement à l'intérieur et à l'extérieur de la classe, l'équilibre des pouvoirs dans la vie d'un enfant est modifié d'une manière qui n'est pas évidente pour lui.

Le rôle de la protection des données dans la protection de l'enfant dans un cadre éducatif a donc de multiples rôles importants. Il devrait être moins axé sur la transformation des mots en actions, sur la mise en conformité du traitement légal des données, et plus sur une focalisation de l'enfant sur la protection et l'exercice de ses droits. La protection des données relatives à un enfant est la protection de l'enfant lui-même pour garantir son développement libre et sa dignité, et devrait créer un équilibre des pouvoirs et des influences auxquels l'enfant est exposé. La vie privée est également un facteur de renforcement des droits.

Les enfants devraient disposer des informations et des compétences nécessaires pour jouir de leur vie privée, protéger leur réputation et exercer leur liberté d'expression en ligne (Nyst, 2018) en fonction de l'évolution des capacités de l'enfant.

Le rôle du droit à la vie privée et à la protection des données n'est pas souvent aussi clairement démontré que les droits habilitants, comme c'est le cas dans l'éducation, ce qui sous-tend les liens entre l'article 29 (1=) et la lutte systémique contre la discrimination raciale, la xénophobie et l'intolérance qui y est associée.

Les buts énoncés dans les cinq alinéas de l'article 29 (1) de la Convention des Nations Unies relative aux droits de l'enfant sont tous directement liés au respect de la dignité humaine et des droits de l'enfant, compte tenu de ses besoins spéciaux en termes développement et de ses capacités évolutives.

Alors que l'éducation et les outils numériques sont inégalement répartis dans le monde, les problèmes qui accompagnent certains outils d'éducation numérisés sont nouveaux pour certaines populations. Les agences et les acteurs du développement reconnaissent que certains réfugiés évitent activement certains camps de réfugiés pour que leurs identifiants biométriques ne soient pas saisis. Des effets similaires de la surveillance des données peuvent être constatés dans le domaine de l'éducation.

L'universalité des principes de la Convention des Nations Unies relative aux droits de l'enfant devrait servir de base à une approche respectueuse des droits en matière de protection des données de chaque enfant.

(article 3) « Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale ».

(article 16) « (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 ».

Reconnaissant que les données à caractère personnel peuvent faire l'objet d'un traitement pour les besoins de l'administration de l'éducation et dans l'intérêt des enfants, le droit relatif à la protection des données, à l'article 5(4) de la Convention 108 modernisée et à l'article 5(1)(a) du RGPD, exige que les données soient traitées loyalement et de manière transparente envers la personne concernée. En ce qui concerne les services internet, le traitement de données doit être tel qu'il permet aux personnes concernées de bien comprendre ce qu'il advient de leurs informations personnelles. Le principe d'équité va au-delà de la transparence : il s'agit de veiller à ce que le traitement soit conforme à l'éthique et aux attentes raisonnables des personnes concernées.

Nous nous intéresserons ici aux enjeux de protection des données et de respect de la vie privée spécifiques à certaines technologies. Les effets plus généraux ne relevant pas de l'éducation ou n'étant pas du ressort du Conseil de l'Europe, comme les effets sur la sécurité nationale d'une généralisation de la biométrie à l'école, et notamment de la collecte de données vocales et d'empreintes digitales, seront en revanche exclus du champ de l'étude.

Le présent rapport entend aider les acteurs concernés à assurer la mise en œuvre effective des droits consacrés par les conventions et normes européennes et internationales en matière de droits de l'homme, et en particulier la Convention 108 modernisée.

2 Enjeux et recommandations

2.1 Capacité d'action et de décision

Nous disposons déjà de lois générales sur la protection des données, alors pourquoi l'éducation a-t-elle besoin de plus ?

2.1.1 Le consentement doit être libre et éclairé

Les plus grands défis aux droits et libertés de l'enfant dans l'environnement éducatif sont peut-être aussi le point de départ de la raison pour laquelle le secteur mérite une attention plus spécifique, au-delà des normes existantes de protection universelle des données.

1. L'éducation est obligatoire pour les enfants et les jeunes.

2. Le consentement en tant qu'outil ultime de l'autonomisation personnelle est fondamentalement défectueux et difficile à donner librement sans nuire à la relation entre l'enfant et l'adulte, entre la famille et l'institution.

Conformez-vous, ou vous n'aurez pas votre place dans cette école. (Taylor, 2015) Au fond, la scolarité obligatoire peut être en contradiction avec l'article 12 de la CDE qui veut que les opinions de l'enfant soient dûment prises en compte en fonction de son âge et de sa maturité. Ce déséquilibre peut être ou non un environnement d'apprentissage souhaitable, en lien avec les normes culturelles, les politiques et les législations nationales spécifiques, mais il n'entre pas dans le cadre du présent rapport.

En réalité, ce déséquilibre de pouvoir signifie que les droits des enfants sont rarement protégés par des principes qui défendent les droits individuels en vertu de la Convention 108+ et du RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). La pratique quotidienne des établissements d'enseignement peut souvent exiger la perte de pouvoir par défaut.

> « Comme on peut le constater, la surveillance dans l'éducation publique implique beaucoup plus que l'observation et la discipline des élèves. La surveillance est la logique d'organisation dominante des institutions modernes, façonnant toutes les opérations (Lyon 2007). [..} Nous définissons la surveillance comme la surveillance, le suivi, la supervision ou l'analyse de données à des fins de contrôle. La surveillance, en tant que forme de production de connaissances, s'appuie sur les catégories normatives d'apparence et de comportement et les requalifie de ce fait. La surveillance est une opération de pouvoir. Comme Michael Foucault (1980) l'a fait remarquer il y a longtemps, le pouvoir n'est pas simplement le contrôle d'une personne sur une autre, mais signifie plutôt tout un appareil de relations matérielles, sociales et symboliques dans lequel les acteurs humains sont pris au piège ». (Monahan et Torres 2009)

Dans le domaine de l'éducation, le consentement n'est pas la norme, même s'il est souvent demandé et recueilli au moyen d'une case à cocher obligatoire, qui n'est pas un processus de consentement mais plutôt une reconnaissance du traitement que l'école a communiqué à une famille, avec une explication plus ou moins précise des conditions. Du point de vue de l'enfant, l'éducation est généralement obligatoire, même lorsqu'elle n'est pas prévue par la loi. Que ce soit par le choix des parents ou par l'application des politiques et des règles par le personnel scolaire, l'enfant en éducation, quel que soit son âge, n'est pas en position de pouvoir.

L'autorité suédoise de protection des données l'a reconnu dans sa décision d'août 2019, concernant le *Skellefteå kommun*, et que l'introduction d'un système de reconnaissance faciale aux fins d'inscription des présences était illégale, et a condamné l'autorité scolaire à payer une amende dissuasive de 200 000 couronnes suédoises (20 700 $) pour violation des lois relatives à la protection des données et à la vie privée. Le consentement n'avait pas pu être donné librement pour la collecte de données sensibles, il n'y avait pas eu de consultation préalable avec l'autorité de contrôle et l'évaluation des risques en matière de protection des données avait été inadéquate.

Il est important que cette décision vise à protéger les droits de l'enfant et n'accepte pas l'utilisation inappropriée d'un " consentement " fabriqué.

2.1.2 Le consentement ne peut être refusé qu'au détriment de la personne concernée et ne peut être considéré comme donné librement.

Une autre façon de recueillir le « consentement » consiste à offrir une procédure pour s'y opposer. Toutefois, cela pose certains des mêmes problèmes que l'obtention du consentement actif en matière de déséquilibre des pouvoirs. Les familles et les enfants ne peuvent pas facilement refuser ou décider contre une option (*opt ou*) sans éprouver un certain malaise ou se sentir stigmatisé comme étant une parent différent ou « difficile ». Même lorsqu'une approche « *opt-out* » ou un refus du traitement est proposée comme modèle alternatif à la collecte du consentement, l'alternative peut signifier « passer à côté de quelque chose » et s'accompagner du sentiment qu'un plus faible niveau de soutien ou d'enseignement sera offert aux enfants qui donnent la priorité à leur vie privée ou à l'engagement parental sur l'utilisation de produits commerciaux en classe. Il incombe donc aux prestataires de services éducatifs de le faire dans le respect des droits, de manière à permettre un processus digne de confiance fondé sur de bonnes pratiques qui ne laisse pas les familles sans moyens pratiques d'exercer l'ensemble des droits relatifs aux données (droit d'accès, de minimisation et d'opposition au traitement ou au profilage automatisé) et sans autre alternative que de s'opposer à l'utilisation des technologies quotidiennes en classe afin de protéger les droits de leurs enfants à la vie privée.

Le niveau de base des normes attendues en matière de traitement des données à l'aide de fournisseurs de technologie doit être relevé, tout en maintenant un niveau égal d'alternatives éducatives acceptable (c'est-à-dire une objection à l'utilisation d'un fournisseur ne devrait pas entraîner une expérience scolaire moindre pour l'enfant).

Le consentement ne peut être donné librement et ne convient au traitement des données relatives aux enfants dans le domaine de l'éducation qu'à des fins très limitées, lorsque l'objection ne porte pas préjudice à l'éducation de l'enfant (par exemple, les photographies d'événements scolaires utilisées par la presse).

Souvent, on recueille des données sur l'enfant, mais pas auprès de l'enfant.

Des données que l'enfant et sa famille ne voient jamais peuvent être créées sur l'enfant par le personnel de l'école.

Souvent, un traitement ultérieur est expressément prévu par la loi.

L'article 8 (3), sur la transparence en vertu de la convention réduit le droit des personnes concernées dans des circonstances qui imposent q'elles soient informées de la manière dont leurs données sont traitées, à supposer que ces cas soient exceptionnels et que le consentement soit le statu quo :

> « lorsque les données à caractère personnel ne sont pas collectées auprès des personnes concernées, le responsable du traitement n'est pas tenu de fournir ces

> informations lorsque le traitement est expressément prévu par la loi ou lorsque cela s'avère impossible ou implique des efforts disproportionnés. »

Dans le domaine de l'éducation, cependant, le consentement au traitement des données n'est pas le statu quo, même s'il peut être demandé aux responsables légaux et aux enfants sous la forme d'accords entre le foyer et l'école ou de politiques acceptables pour l'utilisation de l'informatique.

Dans d'autres environnements, la relation entre le parent et l'enfant peut offrir un niveau supplémentaire de protection et d'attente de de surveillance, entre le vendeur et l'enfant, par exemple lors de l'achat d'une application à la maison, pour usage personnel. On s'attend à ce que ce rôle évolue avec le temps et que le droit de l'enfant d'être entendu augmente avec la maturité.

> « Le fait que l'on accorde de plus en plus d'importance à l'opinion de l'enfant ne signifie pas pour autant que l'opinion des parents sur les questions touchant leurs enfants peut tout simplement être ignorée comme non pertinente, ou que leur responsabilité primordiale peut être remplacée ou ignorée lorsque cela est pratique. Il s'agit plutôt d'un processus de changement progressif dans l'équilibre des pouvoirs et des responsabilités des parents vers leurs enfants à mesure que l'expérience, la maturité et la capacité de chaque enfant à comprendre les implications des actions et des décisions augmentent. (Anderson et al. 2009) »

Dans l'environnement scolaire, cette relation a encore un rôle important à jouer, mais n'offre pas le même niveau de protection dans les faits, et les familles peuvent trouver que leurs propres préférences sont en conflit avec les politiques scolaires.

2.1.3 Le consentement ne peut être pleinement éclairé dans le cadre des pratiques actuelles

La mise en œuvre des technologies dans cet environnement prive encore plus les enfants de leur pouvoir dans la mesure où elle introduit de nouveaux intervenants avec davantage de contrôle et de pouvoir sur la façon dont l'enfant interagit avec l'application ou la plate-forme que l'enfant, sa famille et souvent, son enseignant.

La multitude d'entreprises et de développeurs à l'origine d'un seul produit est cachée, en particulier lorsque les données personnelles peuvent être traitées dans d'autres finalités que celles directes de l'école comme les devoirs, le suivi du comportement, les communications domicile-école ou le traitement des paiements, par les nombreuses organisations partenaires, filiales et prestataires des entreprises et que les conditions générales des entreprises peuvent exercer leur autorité en cas de vente, fusion ou reprise de société sur les données personnelles à des fins d'actifs.

En plus du traitement direct des données par des tiers, une autre couche de traitement des données personnelles peut être introduite par les développeurs qui empruntent du code à des bibliothèques de codes, copient du code conçu par d'autres personnes et l'insèrent dans leurs propres créations. Cela peut conduire au comportement d'applications et à un traitement de données personnelles que même le développeur qui les vend ou les distribue ne peut pas entièrement comprendre ni contrôler, et peut avoir des conséquences imprévues.

Il est donc impossible pour les écoles d'obtenir un consentement légalement valide pour le traitement des données personnelles au nom de leurs fournisseurs.

Les enfants et les responsables légaux ne peuvent tout simplement pas comprendre ce à quoi ils consentent.

Mais c'est le volume même des interactions visibles avec des tiers qui amène les écoles à dire qu'elles ne peuvent pas gérer le consentement.

Cela peut expliquer en partie pourquoi actuellement les écoles considèrent qu'il est compliqué d'obtenir le consentement, et les entreprises peuvent prétendre que cela crée un « obstacle à l'innovation ». Les écoles peuvent ignorer le consentement parce qu'il est trop complexe à gérer et elles donnent souvent leur « consentement par procuration ».

Cela permet bien la divulgation d'informations dans un contexte d'urgence qui, de par sa nature même, est spécifique dans la prise en charge directe d'un enfant dans son intérêt vital ou supérieur, et pour une durée limitée. Les écoles négligent ainsi à tort les familles et les droits de l'enfant dans les tâches courantes de traitement des données.

2.1.4 Étude de cas sur le consentement présumé

En Angleterre, le groupe de réflexion " Nesta " a lancé mi-2019 un programme d'essai des produits edTech en collaboration avec le ministère de l'Éducation. En ce qui concerne le traitement des données à caractère personnel, ils suggèrent qu'il n'est pas nécessaire de demander le consentement, mais confondent leur traitement commercial effectué par des tiers avec celui des écoles relevant de la mission publique, et ne tiennent pas compte des exigences supplémentaires liées aux données de catégorie spéciale (sensibles).

> « Étant donné que ce projet produit des données probantes sur des produits qui aident à atteindre les objectifs actuels des écoles et des collèges, et qu'il est dans l'intérêt public, il n'est pas nécessaire d'obtenir le consentement individuel. » (Nesta, EdTech Innovation Testbed, 2019)

L'incitation économique à développer edTech pour l'exportation est claire. La manière d'éviter l'exploitation de la population enfantine d'un État dans ce contexte dépendra de l'État de droit et de la capacité de ses sujets à s'appuyer sur son application, là où la pratique est guidée par des décisions basées sur des positions éthiques inadéquates de la part des décideurs politiques ou par des buts politiques.

Le défi est donc double :

- Comment assurer la protection des données et de la vie privée de l'enfant lorsque le consentement n'est pas la base légale du traitement des données et que les écoles interprètent la situation une non obligation de fonctionner de manière consensuelle ;

- Comment obtenir le consentement de façon appropriée lorsqu'il est la base légale valide our le traitement des données et requis, en tenant compte du rôle du parent / de la famille et du rôle de l'enfant, ainsi que de leur relation entre eux et avec l'établissement.

2.1.5 Repenser les modalités du consentement et du contrat dans le contexte des écoles peut être nécessaire.

Le modèle de pouvoir patriarcal de la majorité des établissements d'enseignement occidentaux et son déséquilibre de pouvoir intrinsèque exigent un modèle d'autonomisation différent pour les enfants et les familles, au-delà de ce que la loi actuelle sur la protection des données ne nous permet. Les modèles actuels prônent l'autonomie individuelle et le consentement en tant que garantie solide pour le contrôle des données.

Les opinions des enfants doivent être entendues en fonction de leur âge et de leurs capacités et les limites fixées par la loi à cet égard qui varient selon la juridiction, comme l'âge de la

responsabilité pénale, de 10 ans au Royaume-Uni. Lorsqu'il s'agit de l'école, ils sont généralement représentés par leur tuteur légal ou leur institution.

Ce modèle institutionnel peut être souhaitable ou non en termes d'autonomie et de droits individuels, mais à moins que les écoles ne soient prêtes à réduire de manière significative le nombre d'acteurs impliqués dans le traitement des données, il n'y a peut-être pas d'autre modèle réalistement possible.

Cela signifie toutefois qu'un cadre législatif solide est nécessaire pour que les flux de données à l'entrée et à la sortie de l'institution soient étroitement contrôlés et que les responsabilités soient clairement définies.

Par exemple, en vertu de la loi américaine sur l'éducation, la FERPA exige que les établissements financés par le gouvernement fédéral, dans le cadre de programmes administrés par le département de l'Éducation des États-Unis, se conforment à certaines procédures concernant la divulgation et la tenue des dossiers scolaires.

Cela peut être un modèle possible pour gérer la communication des entreprises et des tiers avec lesquels l'école a l'intention de partager des données personnelles au cours de l'année scolaire de l'enfant.

La protection des données qu'offre le modèle américain comprend de fortes attentes eu égard au comportement des entreprises. Les termes et conditions des contrats sont convenus au niveau de l'État régional. La norme approuvée par la FERPA ne peut être respectée que par les entreprises désireuses de respecter et de maintenir des conditions de conformité communes convenues au préalable tout au long de leur cycle de vie.

En effet, il devrait être exceptionnel qu'un tiers commercial devienne le responsable du traitement des données plutôt qu'un sous-traitant du traitement des données personnelles d'enfants d'âge scolaire collectées pendant leur scolarité.

Former suffisamment le personnel dans le système scolaire au niveau régional pour qu'il puisse prendre des décisions d'achat en fonction des résultats d'évaluations approfondies de la protection des données et de l'impact éthique, et conclure des contrats avec des entreprises permettant ainsi aux écoles de conclure des contrats avec elles localement est un moyen d'alléger le poids pour les familles d'effectuer des recherches individuelles.

Les individus et les familles peuvent accéder à la protection des données et aux évaluations éthiques en ligne ou à la demande d'une école, et donc poser des questions et être étroitement informés, s'ils le souhaitent et des règles du jeu équitables sont créées pour que tous aient un niveau de confiance similaire dans la norme de conformité attendue afin de permettre à une entreprise de s'engager avec le système d'éducation publique.

La FERPA classe les informations protégées en trois catégories : les informations éducatives, les informations personnellement identifiables et les informations de répertoire et les limites imposées varient en fonction de chaque catégorie.

Toutefois, le modèle américain ne suffit pas à protéger correctement la vie privée ainsi que toutes les données à caractère personnel qui peuvent appartenir à l'une de ces catégories parce qu'il est impossible de séparer les données à caractère personnel en catégories distinctes et nettes. En effet, la nature des données étant personnelles, elle ne dépend pas

seulement de l'élément lui-même, mais de son contexte, et le responsable du traitement peut posséder ou parvenir à posséder d'autres données personnelles qui permettraient de rendre le premier ensemble de données identifiant.

Afin de faire respecter les droits, les écoles sont tenues de s'opposer à l'utilisation des services d'un tiers fournisseur, et les écoles ont la responsabilité de maintenir un niveau approprié de modes d'éducation alternatifs si les familles ou l'enfant s'opposent au produit.

Davantage de clarté et d'orientation sont nécessaires au personnel scolaire pour comprendre les limites de ce qui est permis et requis en vertu du consentement plutôt que d'autres motifs légitimes. Des considérations pratiques doivent être prises en compte quant à la manière dont les écoles communiquent efficacement avec les enfants et les familles, et pas seulement pour remplir leur liste de contrôle des obligations légales.

2.1.6 Capacité d'action et de décision des enfants

La navigation en ligne peut particulièrement être problématique pour des enfants qui souvent ne comprennent pas la nature commerciale des services numériques auxquels ils ont recours ni la manière dont ces derniers utilisent leurs données. S'il est déjà difficile pour les enfants de savoir comment leurs données personnelles sont recueillies, traitées, partagées et monétisées en ligne lorsqu'ils s'inscrivent eux-mêmes à ces services, cela devient quasi impossible lorsque c'est le personnel de l'école qui prend cette décision en leur nom. Même bien informés et sensibilisés à la gestion de leur vie privée, les enfants ne peuvent le faire quand les établissements choisissent pour eux les applications et les plateformes auxquelles ils auront accès. On demande rarement aux enfants ce qu'ils veulent. (Stoilova, Livingstone et Nandagiri, 2019)

Les données personnelles des enfants contenues dans le système de gestion des informations scolaires peuvent être envoyées à des prestataires commerciaux en ligne sans que les familles ou les enfants en soient préalablement avertis. L'enjeu majeur s'agissant du rôle des écoles dans la gestion des données relatives à l'éducation serait peut-être qu'elles reconnaissent que leur mission publique d'éducation, qui nécessite une part de traitement de données personnelles, ne doit pas consister par défaut à transmettre ces données à des fournisseurs d'applications et de plateformes qui n'ont aucune obligation légale d'assurer un enseignement, et que les sociétés qui traitent l'information avec leur propres finalités, comme le développement de produits, sortent du cadre de la mission publique.

Dans le système éducatif, les élèves ne disposent que de peu d'autonomie ou de possibilités de contrôler la diffusion de leurs données personnelles. De plus en plus, les écoles perdent elles aussi la mainmise sur ces éléments. Il est courant de voir des données collectées ou créées à l'origine dans un contexte éducatif se transmettre en chaine d'un responsable du traitement à un autre.

2.1.7 Écoles et contrats d'achat» uniformisés « au clic (*click-wrap agreements*)

Les écoles établissent de multiples contrats avec des tiers extérieurs et acceptent souvent des conditions types qui demandent aux utilisateurs de confirmer leur acceptation en cochant une case lors de leur premier accès au service ou à l'application. Ces accords sont communément appelés « contrats d'achat au clic » (*click-wrap agreements*). Ils peuvent prévoir l'extraction de volumes importants de données concernant les élèves à partir des systèmes de gestion des informations scolaires, aux conditions du prestataire, sans que l'école ait la possibilité de

limiter au strict nécessaire les données transmises (US Department for Education (Privacy Technical Assistance Center), 2015). Des systèmes de paiement de services de restauration pourraient donc avoir accès à des données sur la religion ou l'origine ethnique.

Il arrive également qu'il ne soit pas possible de refuser les changements apportés à ces conditions sans arrêt du service. Les modifications en question peuvent être transmises par courrier électronique à l'administrateur du système de l'école par des sociétés comme Google for Education, et les nouvelles conditions de même que les changements apportés au traitement par l'entreprise seront rarement communiquées aux responsables légaux ou aux enfants.

2.1.8 Les extractions de données opérées par l'État et le gouvernement font peser des obligations sur les écoles

Au déséquilibre des pouvoirs dans les contrats entre les sociétés prestataires et les établissements qui souhaitent acquérir des services s'ajoute un rapport de forces inégal entre les écoles et les pouvoirs publics aux local et national. Les établissements financés par l'État n'ont guère de possibilité, sur le plan administratif, de s'opposer aux demandes nationales de données et n'ont pas les moyens techniques nécessaires pour empêcher la collecte de certaines données par les systèmes d'extraction automatisés ou la collecte de données à des fins de recensement, pour laquelle des champs requis sont prédéfinis par l'État. Les écoles peuvent ne pas avoir d'autre choix que de transmettre les données en leur possession lorsque la loi les y oblige.

Les gouvernements ne devraient exiger la mise à disposition ou le partage de données personnelles sensibles que pour des finalités limitées et strictement définies ; le mieux, dans la plupart des cas, serait de conserver les données sensibles sur des systèmes locaux plutôt que nationaux (Anderson et autres, 2009) :

> « La politique gouvernementale et les activités des enfants en ligne posent de nombreuses questions de confidentialité et d'intégrité des données et placent au cœur des préoccupations celle, essentielle, de savoir qui peut ou devrait donner son consentement à la collecte, à la conservation et au partage des données confidentielles des enfants » (Dowty, 2009). »

2.1.9 Les élèves et les responsables légaux ont peu d'influence sur les conditions qui s'appliquent à eux

Selon le Bureau du Commissaire à l'information britannique (ICO), les pouvoirs publics, les employeurs et autres organisations en position de force pourraient avoir plus de difficultés à démontrer l'existence d'un consentement valable, donné librement. Il ne faudrait donc pas considérer d'office qu'un tel consentement a été donné au traitement courant de données essentielles.

Les enfants et les familles contestent depuis longtemps et de plus en plus les solutions centrées sur la technologie qui leur sont imposées dans l'éducation en prétendant redonner aux enfants une capacité d'action qu'ils n'avaient plus. Alors que Summit et ses fondateurs parmi lesquels Bill Gates, Mark Zuckerberg et l'initiative Chan Zuckerberg affirment tous que les élèves des écoles Summit « s'approprient davantage leurs activités d'apprentissage », en réalité, les étudiants de la ville de McPherson (Kansas) prennent de plus en plus le contrôle

de leur éducation et organisant des sit-in pour s'opposer à l'introduction du programme d'apprentissage Summit dans leur établissement (Parent Coalition for Student Privacy, 2019).

Lorsqu'ils quittent l'environnement scolaire, les enfants ne sont généralement plus en relation permanente avec l'institution, mais celle-ci peut poursuivre le traitement de leurs données ou maintenir des liens avec des vendeurs tiers qui, eux, le font. Des informations sur les données conservées et leur traitement devraient être transmises à l'enfant et à sa famille tant que leurs données continuent de faire l'objet d'un traitement, ce qui pourrait être fait sur une base annuelle.

2.2 Le dossier permanent

2.2.1 L'importance du principe de la table rase

En 2009, le groupe de travail Article 29 a reconnu que « Les enfants se développent, si bien que les données qui les concernent changent et peuvent vite devenir obsolètes et inadaptées aux finalités pour lesquelles elles avaient été collectées à l'origine. Dans ce cas, les données ne devraient plus être conservées ».

Dix ans plus tard, en juin 2019, le groupe d'experts de haut niveau sur l'intelligence artificielle (HLEG-AI) a fait la proposition suivante dans ses recommandations de politique et d'investissement pour une intelligence artificielle digne de confiance :

> « Il faudrait assurer aux enfants un espace de développement libre et non surveillé, et faire table rase de toutes les données publiques ou privées conservées à leur sujet lorsqu'ils atteignent l'âge adulte ».

Bien souvent, ces recommandations, ainsi que la réglementation en vigueur en matière de conservation de données, ne sont pas prises en compte dans l'éducation, soit sur la base de revendications subjectives d'exemptions à des fins de recherche, soit du fait d'un amalgame entre désidentification et anonymisation ou de politiques de gestion des informations à risque qui ne considèrent pas les données excessives comme un actif toxique. Des mesures s'imposent pour assurer que la réglementation en matière de conservation des données est respectée.

Les progrès technologiques ont permis de conserver des volumes illimités d'informations personnelles sur chaque enfant d'une école, d'un pays voire du monde entier dans des dossiers potentiellement permanents.

2.2.2 Un enfant ne peut contrôler la conservation excessive de données, d'où le risque d'abus

Les enregistrements peuvent être rapidement diffusés à d'autres ordinateurs dans des services sur le cloud et copiés un nombre illimité de fois pour un nombre indéterminé de personnes, à l'infini. Tout le dossier scolaire d'un enfant peut être partagé en un simple clic. Des informations qui auparavant seraient restées dans des archives locales où elles auraient occupé un vaste espace rempli d'armoires de classement, peuvent aujourd'hui être stockées sur un appareil portable. De la même manière, il est possible de dupliquer et de télécharger rapidement une base de données contenant des millions d'enregistrements. L'histoire regorge d'exemples dans lesquels des informations conservées par les gouvernements sur l'origine ethnique, la nationalité ou la religion ont été utilisées contre des communautés.

Le ministère de l'Intérieur britannique avait utilisé les bases de données nationales des élèves de manière abusive à des fins de contrôle de l'immigration, ce qui a été dévoilé en 2016 après que le ministère de l'Éducation ait ajouté le critère de la nationalité au recensement scolaire (defenddigitalme, 2016). L'utilisation de données par le gouvernement à des fins non éducatives présente des risques trop importants qui justifieraient de ne pas conserver les données nationales à l'échelon individuel et identifiable.

En Angleterre, le premier recensement scolaire général des enfants âgés de 2 à 19 ans a eu lieu en 2002 et incluait les noms des élèves. Le ministre d'État à l'Éducation et à la Formation professionnelle d'alors avait assuré aux parlementaires, au sujet des modifications apportées à la « base de données centrale des élèves », que « le ministère n'avait aucun intérêt à connaître l'identité des élèves en tant que telle et qu'il n'utiliserait la base de données qu'à des fins statistiques et seul le personnel technique directement impliqué dans le processus de recueil de données aurait accès aux noms des élèves. »

Treize ans plus tard, sous un gouvernement différent et en catimini, les noms, dates de naissance, sexe et adresses des enfants ont été comparés aux données recueillies mensuellement par le ministère de l'Intérieur à des fins de contrôle de l'immigration.

2.2.3 Les enfants ont un droit à la protection de leur réputation

Les effets durables d'un dossier permanent et des décisions qui en découlent peuvent suivre les enfants jusqu'à l'âge adulte à la suite d'interventions étatiques et commerciales. Ces données peuvent également être exploitées des années plus tard et réorientées facilement à d'autres fins sans que la personne concernée le sache.

La réputation des enfants est de plus en plus façonnée par la quantité croissante d'informations disponibles en ligne à leur sujet. Cela n'a pas seulement une influence sur leurs rapports interpersonnels, mais également sur leur capacité à accéder à des services et à l'emploi à l'âge adulte (UNICEF, Children's Online Privacy and Freedom of Expression, Discussion Paper and Industry toolkit, 2018).

La question des cycles de vie des données doit être abordée avec une attention particulière lorsqu'il s'ait d'enfants qui doivent avoir le droit à ce que la divulgation de données aux sociétés privées soit retreinte afin d'assurer leur plein développement et leur épanouissement en tant qu'adultes. Cela vaut en particulier pour les données sensibles qui peuvent ne pas toujours répondre aux critères des catégories particulières de données. Par exemple, il devrait être possible d'exclure de la diffusion sans consentement les données scolaires relatives au comportement pour des finalités qui dépassent la prise en charge directe de la personne concernée. Les antécédents judiciaires de violence, de comportements sexuels répréhensibles ou de consommation de drogues peuvent être retirés de la diffusion s'ils sont de nature pénale mais en tant qu'indicateurs de comportement et données **non** pénales, ils peuvent être transmis continûment à des tiers, à l'insu de l'enfant (puis de l'adulte) ou envoyées au-delà de l'établissement ou à d'autres juridictions.

Le rapport de forces entre les autorités scolaires et l'enfant est très inégal pour ce type de traitement de données ; par conséquent, une discussion devrait avoir lieu avec la famille avant toute diffusion d'informations à des tiers. L'option de retrait *(opt-out)* n'est pas un mécanisme de protection suffisamment robuste au vu des énormes quantités de données qu'il est possible d'extraire des établissements de façon automatisée.

Lorsque les décideurs humains ne peuvent exercer un contrôle effectif sur les décisions de l'intelligence artificielle, la question de l'opportunité d'utiliser ces systèmes en lieu et place des méthodes faisant appel à l'humain se pose plus largement, notamment pour le traitement des données relevant de catégories particulières (Mantelero, 2018).

2.2.4 Les demandes commerciales ou à des fins de marketing de conservation excessive devraient être rejetées

Bien que les fournisseurs de produits éducatifs commerciaux (technologies éducatives edTech) facilitent la portabilité des données et permettent le transfert de fichiers aux établissements successifs par un même prestataire, ils ne devraient pas conserver les données uniques des enfants permettant de les identifier, pour des finalités autres que celles nécessaires à leur éducation. La conservation ultérieure à des fins d'audit devrait être effectuée par le prestataire éducatif au niveau local, et non par les fournisseurs. Les résultats d'examen renseignent sur le parcours d'une personne et doivent être accessibles tant que celle-ci souhaite y faire référence ou tant que les employeurs et autres pourraient en demander une preuve. En revanche, les données relatives au comportement en classe, aux absences pour maladie et à l'assiduité ou à l'utilisation des applications ne devraient pas être conservées dans le détail par les prestataires commerciaux.

Il arrive fréquemment que les services commerciaux éducatifs en ligne n'autorisent pas le personnel scolaire à supprimer les classes virtuelles, les comptes ou les contenus en ligne (y compris les informations des élèves) mais que les entreprises les archivent pour une période d'un ou deux ans, voire plus (IPC Ontario GPEN Privacy Sweep Report of Educational Online Services, 2017).

Certaines applications prévoient une période bien définie durant laquelle une école peut demander la suppression des données des élèves, au terme de laquelle l'entreprise les conserve indéfiniment.

Études de cas sur le dossier permanent

Mathletics, une application mathématique utilisée par les enfants du monde entier, offrait jusqu'à récemment une date dans l'année où les enseignants devaient avoir demandé que les données du compte des enfants soient supprimées, sinon l'entreprise conservait indéfiniment des données pseudonymisées. De plus, la société 3P learning considère que l'adresse IP ne constitue pas une donnée personnelle, contrairement à l'arrêt Breyer CJEU, et demande sa conservation indéfiniment, ainsi que des données d'activité comportementale.

> « En acceptant les modalités et conditions, les titulaires nous accordent le droit d'utiliser ces renseignements anonymes pour nos propres finalités, comme la préparation de rapports statistiques ou pour améliorer et modifier le contenu de nos produits. »

La plate-forme de suivi du comportement Class Dojo a déclaré, en revanche, qu'elle n'enregistrait pas les données de manières permanente :

> « Les données de profil qui ne sont pas explicitement sauvegardées par un parent ou un élève expireront et seront effacées au bout d'un an »

et elle s'engage à ne pas exploiter leurs données personnelles :

> « Nous ne vendons, ne louons ni ne partageons vos renseignements personnels (ou ceux des enfants) à aucun tiers à des fins de publicité ou de marketing ».

Cependant, un tel modèle d'entreprise est un modèle que certaines familles peuvent juger déraisonnable ou contraire à l'éthique. Des entreprises s'appuient sur l'utilisation du courrier électronique des responsables légaux lié au compte de l'enfant. Le traitement des données personnelles fournies par l'école obtenues aux fins directes de l'éducation de l'enfant par l'école, ce qui est une mission publique, ne devrait pas être utilisé afin de proposer d'autres produits aux familles, ce qui est un but lucratif de l'entreprise, en dehors de la mission publique, et peut donc être considéré comme incompatible avec la base légale de la mission publique pour traitement.

> « Nous avons l'intention de faire de l'argent grâce à des fonctions haut de gamme que nous développons et que les écoles et les parents peuvent payer ». (ClassDojo : What The New York Times Got Wrong)

2.3 Gestion de l'identité

Comment se construit l'identité chez les jeunes ? L'être et le devenir par le biais d'interactions sociales et institutionnelles sont des processus importants pour eux. À mesure qu'il grandit, l'enfant se crée et gère de multiples « persona ».

Le besoin d'anonymat des enfants en ligne est généralement associé à l'apprentissage de la sécurité en ligne et à la protection de leurs données personnelles face inconnus. Dans les dossiers scolaires, les informations personnelles sur les enfants sont généralement liées aux informations sur leur famille et sont requises dans les applications éducatives pour enregistrer les comptes. Et lorsqu'il s'agit de produits et de systèmes éducatifs, la perte de données relatives à la vie privée et à l'identité peut donc être collective et concerner toute la famille ou la communauté et pas seulement l'individu.

On considère souvent que les enfants de moins de 11 ans sont trop jeunes pour pouvoir comprendre les enjeux de la protection de la vie privée en ligne. Or, des chercheurs d'Oxford ont constaté que les enfants parvenaient bien à cerner et à expliquer certains risques pour la vie privée comme le partage excessif d'informations ou la divulgation de l'identité réelle en ligne (Zhao et autres, 2019). Cela dit, on explique rarement aux familles les asymétries entre les sociétés commerciales et les enfants à l'ère numérique qui impliquent que les enfants sont particulièrement vulnérables à une exploitation de leurs données, notamment car ils sont peu conscients des risques liés à l'accumulation de données personnelles dans le temps et font peut-être partie de la première génération dont la vie est conservée sous forme de données par des entreprises, depuis la naissance.

De récentes études ont montré que bien que les adolescents soient généralement préoccupés par le risque d'être identifiés par des inconnus utilisant leurs données personnelles et par la gestion de leur réputation, ils ne perçoivent pas le risque potentiel de réidentification à partir des différents éléments qu'ils ont partagés, par exemple des images ou une géolocalisation, lorsque ces derniers ne sont pas considérés comme des identifiants. En particulier, ils ont du mal à comprendre la notion de données longitudinales (Zhao et autres, 2019).

La nature changeante de l'enfant dans le temps contraste avec la capacité du système scolaire à créer une archive centrale permanente qui croît par ajouts successifs de données, sans ne jamais rien oublier.

La fiche d'étudiant numérisée peut également être copiée un nombre indéfini de fois. Et le contexte de la collecte de données, les déductions faites et la qualité d'un dossier peuvent être perdus à chaque copie et utilisation partagée.

L'individu est au cœur de l'idée de personnalisation qui imprègne de nombreuses technologies d'apprentissage. L'individuation consiste à transformer « l'identité » humaine, d'un certain « état d'être » à une « tâche » de devenir (Livingstone, 2016).

Le droit de faire des choix libres, sans interférence, est fondamental pour l'autonomie et le plein et libre développement de la personnalité.

La protection contre toute ingérence illégitime de l'État est à la base du droit fondamental au respect de la vie privée. C'est une condition essentielle pour que chacun puisse construire librement sa propre identité dans une société démocratique (Hildebrandt, 2015).

Le dossier scolaire permanent et le fait qu'il soit partagé avec d'autres augmentent le risque de perte d'identité, de contrôle sur les décisions de la vie privée par le biais d'influences, de décisions prises par d'autres pour des interventions dans notre vie et de discrimination fondée sur la représentation que le système s'est construit de nous, à la fois au cours de l'enfance et à l'âge adulte.

La résolution de la Conférence internationale des commissaires à la protection des données et de la vie privée sur les plateformes d'apprentissage en ligne, qui peut être appliquée plus largement à toutes les données personnelles dans un environnement éducatif, recommande :

> « Conformément au principe de minimisation des données et autant que possible, l'identité des individus et l'identifiabilité de leurs données à caractère personnel traitées par la plateforme d'apprentissage électronique doivent être réduites au strict nécessaire ».

2.3.1 Vérification de l'âge et de l'identité

On voit aujourd'hui se multiplier les appels à rendre obligatoire l'utilisation de l'identité réelle et à recourir à des mécanismes de vérification de l'âge pour valider celle des enfants. Cela aurait néanmoins un coût sur le plan de la vie privée des enfants et ferait perdre l'espace de liberté qu'offre l'anonymat.

La vérification de l'âge est une forme limitée d'« assurance de l'identité » reposant sur la définition d'un seul attribut (l'âge). Aucune méthode n'est préconisée en particulier, mais il serait illogique de vouloir protéger les enfants et leur vie privée en créant plus de nouvelles bases de données, et donc potentiellement plus de risques (Booth, P. 2017).

En 2008, le Berkman Center for Internet & Society de l'Université Harvard a publié un rapport sur les enfants dans l'environnement en ligne et a conclu que la vérification de l'âge n'était pas une solution appropriée.

> « La vérification/authentification de l'âge/de l'identité n'est pas une solution car elle s'applique aux réseaux sociaux et autres entités de l'environnement en ligne où les mineurs interagissent avec des adultes. Elle n'apporte pas de bénéfice là où les risques sont depuis longtemps considérés comme élevés » (Déclaration de Symantec, 2018).

Les applications et les plateformes sécurisées autorisées dans l'école après vérification et validation dans le cadre d'un appel d'offres adéquat, assorties d'un système approprié de filtrage/blocage de contenus, devrait suffire à créer un environnement ne nécessitant pas de protections supplémentaires liées à l'âge.

Cela dit, le système éducatif externalise également la gestion de l'identité à diverses entreprises, y compris des courtiers en données, pas seulement pour l'audiovisuel, mais aussi pour les plateformes de médias sociaux. Nombre d'entre eux autorisent le recours aux identifiants des réseaux sociaux pour autoriser la connexion à d'autres applications et plateformes, utilisées pour le travail à la maison et les activités en classe.

2.3.2 Vérification de l'identité au moyen des identifiants des médias sociaux

La Conférence internationale des commissaires à la protection des données et de la vie privée (2018) recommande aux écoles :

> « d'éviter l'utilisation des identifiants de connexion des médias sociaux car cela peut déboucher sur une collecte et une divulgation excessives de données de profil détaillées et d'autres informations identifiables entre le site de réseau social et la plateforme d'apprentissage en ligne. Cela limite la capacité des élèves à empêcher le suivi de leurs activités en ligne sur l'ensemble du Web ».

Facebook, par exemple, est fréquemment utilisé dans certaines écoles comme outil d'administration de groupes, en particulier pour les enfants plus âgés, ainsi que dans les établissements techniques et de formation continue, mais l'entreprise est de plus en plus critiquée par les autorités de régulation américaines et européennes pour la manière dont elle traite l'information des utilisateurs et des non-utilisateurs par le suivi et l'analyse de sites Web. Sa politique de l'identité authentique (« vrai nom ») et d'enregistrement implique l'utilisation de données à caractère personnel qui peuvent être fusionnées avec les comptes scolaires lorsque le personnel le demande.

Le personnel des établissements scolaires devrait garder à l'esprit son obligation de protéger avec le plus grand soin les données des élèves et de l'école lorsqu'il sollicite le recours à ce type de plateformes, et procéder à un examen attentif de leur base légale. Les usages cachés de données personnelles et la manipulation des fils d'information des utilisateurs de Facebook à leur insu pour générer des réponses émotionnelles semblent rendre ses valeurs incompatibles avec l'obligation des prestataires de services éducatifs de respecter les droits et libertés de l'enfant (Forbes, 2014).

Ce constat n'empêche pas les promoteurs des technologiques de prêcher en faveur de son utilisation en classe (Education Foundation, 2013). Ils ont affirmé en 2013 que la plateforme « était déjà largement utilisée dans les lycées et universités du Royaume-Uni et dans le monde, mais qu'il pourrait y avoir « un avant et un après Facebook pour les enseignants, les écoles et la classe. C'est un « couteau suisse » truffé d'outils permettant de libérer l'apprentissage des jeunes, en cours et au-delà ».

Les enfants et les jeunes ne comprennent pas ce qu'une entreprise peut derrière les choix qu'ils font, officiellement pour configurer leurs paramètres de confidentialité, en utilisant les données personnelles qu'ils fournissent lors de leur enregistrement en tant qu'utilisateurs. De telles pratiques devraient être évitées dans l'éducation.

Pour respecter le principe de finalité, les écoles et les applications edTech ne doivent pas utiliser les médias sociaux et autres données personnelles sur les enfants ou les membres de leur famille, obtenues de sources publiques.

2.3.3 Vérification de l'identité au moyen de données biométriques

La gestion de l'identité peut être menée à l'école de multiple manière, mais c'est souvent par les échanges en interne entre les écoles et des fournisseurs tiers de technologies, sur site ou par le biais de services connectés à internet. Les données biométriques permettent d'établir l'identité avec un degré de certitude qui même s'il n'est pas parfait, reste élevé. Cela dit, il nous faut encore débattre de la question de savoir s'il y a véritablement lieu d'utiliser ces méthodes pointues de vérification de l'identité pour des transactions de faible niveau comme c'est le cas aujourd'hui dans les écoles, par exemple pour enregistrer les prêts de livres à la bibliothèque ou payer les repas à la cantine scolaire par des moyens de paiement sans numéraire.

Les technologies de détection et de reconnaissance faciale sont utilisées depuis un certain temps dans le système éducatif pour contrôler l'identité des élèves et des visiteurs dans les écoles. Cependant, à mesure que la technologie devient plus sophistiquée, ses utilisations le deviennent également.

Cette technologie est désormais utilisée pour lire des expressions et suivre des personnes dépersonnalisées, de caméra en caméra dans les centres commerciaux, dans le but de déduire le sexe, l'âge et l'humeur des acheteurs (Anscombe 2017). Il est révélateur que ces applications commencent à passer de la technologie de détection à la technologie d'identification, les points de vente s'efforçant de relier les données des caméras aux informations d'achat. Lorsque les systèmes de reconnaissance faciale se généraliseront, des applications de détection (telles que la déduction de l'"humeur") seront également mises en œuvre à des fins de marketing et de sécurité. Par exemple, le ministère américain de la sécurité intérieure développe des systèmes permettant de déduire une "intention malveillante" (l'intention de nuire) à partir d'indices visuels et biométriques (Ackerman 2017). (Andrejevic et Selwyn, 2019)

Dans des circonstances moins courantes, les enfants peuvent être soumis à la reconnaissance faciale pour vérifier leur identité sur une durée particulière. Pour les examens par exemple, des systèmes d'identification biométriques faisant appel à la reconnaissance faciale sont de plus en plus utilisés pour vérifier les candidats, non seulement à l'entrée mais tout au long de l'épreuve en recueillant régulièrement leurs caractéristiques biométriques.

En août 2019, l'autorité de régulation suédoise a jugé que la mise en place d'un système de reconnaissance faciale pour l'identification des élèves dans le cadre de l'enregistrement des présences était contraire à la loi (voir : II. 6.2 données biométriques). L'introduction de systèmes similaires par Aurora Computer Services avait déjà fait l'actualité en 2010 en Angleterre.

D'autres systèmes de reconnaissance faciale et systèmes portables biométriques sont en train d'être mis au point pour collecter des données sur les émotions, la participation et l'attention des élèves en milieu scolaire dans le but de fournir aux enseignants des informations en retour sur les compétences et caractéristiques sociales et émotionnelles des élèves (IEEE, 2018) et de « personnaliser » l'enseignement. Le présent rapport aborde cette question dans la partie II.7.2 Données biométriques.

Le Forum économique mondial a plaidé en faveur d'un recours accru à la "promotion de l'apprentissage social et émotionnel par la technologie" en 2016.

Il est peu probable que la législation actuelle sur la protection des données soit suffisante pour protéger les enfants contre les utilisations de plus en plus invasives d'informations personnelles sur leurs caractéristiques corporelles, notamment l'analyse de la démarche et des émotions qui sont collectées non pas dans le but de vérifier l'identité d'une personne unique, en vertu de l'article 6 et des catégories spéciales de données de la Convention, mais plutôt pour déduire leurs émotions et leurs intentions.

2.4 Sources de données et traitement opaque

Les données ne sont pas toutes semblables et, en particulier, on ne devrait pas reconnaître que de grandes quantités de données sur les enfants dans le contexte éducatif sont des opinions, ou des déductions. Dans le domaine de l'éducation, il y a de grandes différences entre les sources de données. Elles peuvent être :

. fournies par la famille ;
. fournies par l'enfant ;
. créées par les enseignants ;
. créées par les systèmes administratifs de l'école ;
. créées par les pouvoirs publics ;
. créées par les outils et plateformes éducatives d'une société commerciale, que les enfants et les familles voient et
. créées par des tiers extérieurs au système éducatif, comme les courtiers en données, des entreprises de médias sociaux et peuvent être liées aux dossiers scolaires.

2.4.1 Données cachées

Les données cachées incluent les enregistrements basés sur les données et/ou métadonnées dont les entreprises se servent pour créer des profils d'utilisateurs concernant l'usage d'une application, par exemple, et cibler ainsi les élèves ou leurs parents à des fins publicitaires ou de marketing. Elles ne sont pas vues par les enseignants, les parents ou les représentats légaux et peuvent violer les lois sur la confidentialité des données en ligne et la protection des consommateurs, ainsi que les lois sur la protection des données.

On peut citer en exemple la tendance croissante à utiliser des applications de santé mentale et de bien-être au Royaume-Uni dans les salles de classe, qui présentent sans aucun doute les mêmes failles que les applications de santé mentale conçues pour des adultes étudiées en 2019 par Privacy International.

Cette ONG a publié une étude de 136 pages Web très populaires liées à la santé mentale en France, en Allemagne et au Royaume-Uni qui montre comment des sites partagent les données personnelles des utilisateurs avec des publicitaires, des courtiers en données et de grandes entreprises technologiques comme Google, Facebook et Amazon.

Certains transmettent à des tiers les réponses et résultats des tests sur la dépression qu'ils proposent aux internautes. L'étude conclut que certains sites Web de santé mentale traitent les données personnelles de leurs visiteurs comme une marchandise et ne respectent pas leurs obligations découlant du droit européen relatif à la protection des données et de la vie privée (Privacy International 2019).

Des données cachées renferment aussi des nouvelles informations ou indications obtenues par couplage ou réutilisation secondaire de données recueillies pour l'éducation mais utilisées par les collectivités locales pour d'autres analyses sociétales comme l'évaluation prédictive des risques sociaux.

Ces usages analytiques de données réorientées vont bien au-delà de ce à quoi de nombreuses personnes peuvent raisonnablement s'attendre lorsqu'elles envoient leurs enfants à l'école, et ils ont de profondes répercussions sur la vie privée et familiale.

2.4.2 La réorientation des données doit pouvoir être empêchée en pratique

La collecte unique pour un usage multiple peut être jugée efficace, mais elle peut donner lieu involontairement à une utilisation abusive des données lorsque les finalités ne sont pas compatibles ou transparentes pour l'enfant ou la famille.

Les administrations locales et nationales peuvent exercer des pressions, dans les systèmes éducatif, pour une réutilisation des données collectées pour les finalités directes de l'école pour des finalités indirectes comme l'analyse de données pour le benchmarking, le regroupement des données des élèves dans des lacs de données à usage de tiers, et le couplage des données des élèves des écoles avec celles des étudiants de l'enseignement supérieur et d'autres ensembles de données longitudinales des ministères (données LEO Graduate Outcomes ministère de l'Education britannique, données sociales et fiscales).

De plus en plus, les données relatives à l'éducation sont couplées à grande échelle avec d'autres données administratives sur l'enfant ou les familles, pour mesurer des scores de risque à des fins d'interventions prédictives pour repérer les cas de maltraitance des enfants et de violence domestique, ainsi que pour réduire les exclusions scolaires (Cardiff Data Justice Lab, 2018). Or, les données en question n'ont jamais été destinées à cet usage ou collectées dans ce but et les risques sont grands lorsque des décisions reposent sur des opinions, plutôt que sur des faits.

De nombreuses entreprises partent du principe qu'il est acceptable de traiter les données personnelles des élèves pour créer des données désidentifiées qui seront utilisées à d'autres finalités, sans en informer les familles ou les écoles, puisque les lois de protection des données ne s'appliquent pas aux données anonymes. Ce raisonnement est toutefois incorrect, ne serait-ce que parce que le processus d'anonymisation des données est déjà en lui-même un traitement de données personnelles. Il est également difficile de rendre des données anonymes tout en conservant les identifiants de l'école ou du lieu, même s'ils ne sont pas considérés comme des données à caractère personnel, car ils peuvent eux aussi accroître considérablement le risque de réidentification.

Les enfants et les familles n'ont aujourd'hui aucun moyen d'être informés de la réorientation des données avant qu'elle ait lieu. Une telle violation des principes de protection des données doit être prévenue par un contrôle strict de l'application des dispositions en vigueur.

2.5 Le rôle de l'implication des parents dans les questions relatives aux données des enfants à l'école

Des responsables du traitement ont tendance à négliger les droits des enfants dans l'environnement scolaire en s'appuyant sur les arguments avancés par des tiers selon lesquels les écoles peuvent donner leur consentement au nom des enfants, en lieu et place des

parents. Cela dit, les établissements ne prennent pas toujours leurs décisions en fonction de l'intérêt supérieur de l'enfant, mais selon ce qui leur est le plus pratique ou facile.

Bien que les pratiques en classe soient très variables d'un lieu à l'autre, l'apparition d'objets connectés à bas coût, d'appareils portables, de l'intelligence artificielle et d'objets vocaux facilement utilisables en classe sans que les parents le sachent, le permettent ou le surveillent menace les droits des enfants à un degré sans précédent à l'échelle mondiale, et notamment leur droit au respect de leur vie privée, leur autonomie et leur capacité à gérer leur empreinte numérique.

2.5.1 Prévenir les utilisations abusives à l'école : mission impossible pour les parents

Faut-il établir le cas échéant une distinction entre la communication d'informations aux responsables légaux sur la mise en service d'un produit destiné aux activités quotidiennes en classe et une expérimentation ponctuelle à des fins de recherche ? Quels critères un produit pilote devrait-il remplir pour recevoir l'approbation de la commission d'éthique de l'école ? Comment atteindre le degré élevé de consentement requis pour le traitement de catégories particulières de données sans que le choix se fasse au détriment de l'enfant s'il ne peut donner son consentement en raison de son âge et, en tout état de cause, si le rapport de forces ne lui permet pas (ou à ses parents), indépendamment de leur âge, de donner un consentement réellement libre et éclairé dans l'environnement scolaire ?

La protection des droits des enfants doit s'inscrire dans une approche prospective fondée sur les principes de la Convention 108 qui seront les piliers de leur développement sans entrave et de leur plein épanouissement.

Les écoles ne devraient pas passer outre aux responsabilités des parents à l'égard de l'empreinte numérique de l'enfant, ou en créer une qu'ils n'auraient pas créés eux-mêmes et qu'il ne serait pas possible de contrôler ou d'effacer à la fin de la scolarité. Cela affaiblirait les droits des responsables légaux et réduirait leurs capacités d'action.

2.5.2 Compréhension des enjeux par les parents

Les données relatives à l'éducation doivent être accessibles aux responsables légaux pour favoriser leur compréhension des enjeux. C'est aujourd'hui mission impossible si l'on considère qu'il peut y avoir à tout moment plus d'une trentaine d'intervenants externes procédant au traitement des données d'un enfant. La question se pose également de savoir si les enfants sont épaulés par leurs parents pour tout ce qui concerne les risques pour leur vie privée en ligne, et qui les soutient eux-mêmes sur ces questions (Zhao J., 2018).

Zhao affirme que :

> « Les parents des 6-11 ans croient souvent que leurs enfants sont trop jeunes pour saisir et affronter les problèmes de vie privée en ligne et adoptent souvent une attitude protectrice pour restreindre ou contrôler les contenus accessibles aux enfants en ligne (à leur domicile), au lieu d'aborder ces questions avec eux. Ils mettent tout en œuvre pour assurer la sécurité de leurs enfants en ligne. Cela dit, on ne sait pas grand-chose de leur niveau de connaissance des risques liés à la collecte implicite de données à caractère personnel par les entreprises qui se cachent directement ou indirectement derrière les applications mobiles utilisées par leurs enfants, et donc de leur capacité à les protéger contre ce type de risques ».

Les outils employés dans l'environnement scolaire et les risques qu'ils présentent sont encore moins connus des familles. Pour l'heure, les institutions semblent sous-estimer le niveau de risque et le degré de préoccupation qui entourent le traitement de données dans les écoles, qui restent d'ailleurs plutôt faibles au regard de l'étendue du traitement de données du fait d'un manque d'information des parents en la matière. Il reste à voir si les écoles laissent délibérément les responsables légaux « dans le flou » ou si elles partent du principe qu'il n'y aura pas d'opposition vu qu'il n'existe aucun mécanisme pour en tenir compte.

Il est nécessaire de disposer d'outils et de processus pour permettre aux écoles d'exercer leurs obligations de transparence de manière à pouvoir être ouvertes sur le traitement des données avant qu'il n'ait lieu, et à démontrer leur responsabilité après le traitement. Il peut être nécessaire de mettre en place une législation et un contrôle indépendant pour garantir que les écoles remplissent ces obligations.

2.5.3 Aperçu des avis des parents en Angleterre

En 2018, defenddigitalme a commandé un sondage d'opinion auprès des parents. L'étude sur l'état des données 2018 a été menée en ligne : 1 004 parents d'enfants de 5 à 18 ans scolarisés dans l'enseignement public en Angleterre ont été interrogés sur la collecte des données des enfants et l'utilisation qui était faite des technologies de tous les jours en classe. On a recueilli leurs réponses à des questions détaillées sur les données personnelles de leurs enfants à l'école et leur compréhension du type de technologies utilisées, ainsi que leur avis sur l'utilisation des données personnelles confidentielles des enfants au niveau national par des tierces parties.

Un parent sur quatre (24 %) a affirmé qu'il ne savait pas si son enfant avait été enregistré dans un système au moyen de données personnelles. La plupart ignoraient que des données sur chaque enfant d'âge scolaire (2-18 ans) étaient transmises au ministère de l'Éducation lors du recensement scolaire et ne savaient pas comment étaient utilisées les données personnelles des enfants issues de la base de données nationale des élèves. 69 % des parents ont indiqué qu'ils n'avaient pas été informés que le ministère de l'Education pouvait divulguer à des tiers des données issues de la base de données nationale des élèves.

Il est ressorti nettement de la consultation que les parents considéraient les données des enfants ayant des besoins éducatifs spéciaux comme des données sensibles nécessitant un examen particulier avant d'être transmises par l'établissement au ministère de l'Éducation en vue d'utilisations secondaires. Ces données ne sont pas traitées comme des données de santé ou des catégories particulières de données, bien qu'elles soient révélatrices de besoins sociaux, émotionnels et de santé mentale, de handicaps physiques, de troubles du spectre autistique ou de troubles de l'audition et de la vue (service de l'Éducation, SEND, 2019).

- 81 % des parents étaient d'accord pour affirmer que le consentement des parents devrait être recueilli avant le partage de données sur les besoins éducatifs spéciaux d'un enfant.

- 60 % des parents estimaient que le consentement des parents devrait être recueilli avant la transmission de données par les établissements à la base de données nationale des élèves du ministère de l'Éducation.

- Pour 65 % d'entre eux, le ministère de l'Éducation devrait demander le consentement des parents avant de transmettre les données personnelles des enfants à des sociétés commerciales d'analyse de données.

- Plus de trois quarts (79 %) des parents, s'ils devaient accéder aux données de leur enfant dans la base de données nationale des élèves, choisiraient de le faire au moyen d'une demande d'accès aux données personnelles (Subject Access Request).

Afin de concrétiser l'intention et les objectifs des protections de la Convention, il doit y avoir un droit parental d'opposition aux finalités secondaires indirectes du traitement des données, celles au-delà desquelles un parent ne s'attend pas à ce que les données de son enfant soient traitées dans le cadre de son éducation.

2.5.4 Les parents attendent des écoles qu'elles protègent et réalisent les droits de l'enfant

Conformément à la Recommandation CM/Rec (2018)7 sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique,

> « Les États et les autres parties prenantes devraient veiller à ce que les enfants soient informés des modalités d'exercice de leur droit au respect à la vie privée et à la protection des données, en tenant compte de leur âge et de leur degré de maturité, et, si nécessaire, avec l'orientation et les conseils de leurs parents, des personnes qui en ont la charge, des tuteurs ou des autres personnes légalement responsables de l'enfant, d'une manière qui corresponde au développement des capacités de l'enfant ».

Par ailleurs,

> « Les données personnelles des enfants et des jeunes méritent une protection spécifique et leur traitement ne devrait être autorisé que s'il repose sur une base légale suffisante. Les enfants et les jeunes ont le droit à la protection de leur vie privée et doivent pouvoir exercer leurs droits en matière de protection des données avec le soutien de leurs parents ou tuteurs. Les parents doivent pouvoir aider leurs enfants et participer activement à l'exercice de ces droits » (Résolution de la Conférence internationale des commissaires à la protection des données et de la vie privée sur les plateformes d'apprentissage en ligne, 2018).

Or, les preuves d'un manque de connaissance et d'information, de l'école aux tuteurs légaux, signifient que les familles sont démunies et ne peuvent pas agir pour protéger les droits de leur enfant à l'école. À moins que la législation n'autorise les responsables légaux à refuser l'utilisation des données personnelles de l'enfant déjà conservées par l'école, il n'existe aucun mécanisme qui leur permette de s'opposer à un traitement de données sans consentement éclairé. Les écoles appliquent peut-être le principe de la collecte unique pour un usage multiple et dans ce cas, n'informent pas les responsables légaux que les données pourront faire l'objet d'un traitement secondaire, sans finalités claires et précises, après avoir été collectées à l'origine pour l'inscription de l'enfant à l'école. L'obligation de protéger les droits et libertés fondamentaux de l'enfant ne doit pas incomber seulement aux parents.

2.5.5 Les droits des parents concernant leurs propres données à caractère personnel

Les données personnelles des responsables légaux contenues dans le dossier de leur enfant peuvent également être transférées à leur insu à des sociétés commerciales d'éducation par l'intermédiaire du système de l'école.

Les modèles commerciaux particulièrement manipulateurs basés sur un « prix d'appel » devraient être interdits dans l'éducation. Ils encouragent les écoles à accepter des produits gratuits, mais leur facturent la poursuite ou l'extension du service ou ciblent les enseignants et les responsables légaux dans le cadre d'opérations de marketing direct par courrier électronique, en leur envoyant de la publicité sur des applications ou en faisant la promotion de contenus commerciaux supplémentaires.

Les écoles et organismes éducatifs peuvent également considérer les données personnelles des responsables légaux comme une source de données extractible. L'inspection britannique de l'éducation, Ofsted, était en pourparlers en 2017 avec le ministère de l'Éducation pour un projet de sciences des données qui visait à étudier la possibilité d'utiliser des données en quasi-temps réel et des informations provenant des médias sociaux et d'autres sources pour prédire et prévenir la baisse des résultats scolaires. Cette forme d'espionnage des pages des responsables légaux et des élèves sur les médias sociaux pour observer si le niveau d'une école baissait a rencontré les critiques et des syndicats d'enseignants et de groupes de défense des libertés civiles, préoccupés par le manque de fiabilité de données pouvant reposer sur des informations fausses ou des rumeurs et l'effet préjudiciable que cela pourrait avoir sur la confiance du public dans la surveillance institutionnelle (i-news, 2017).

2.6 Le rôle des enseignants et du personnel scolaire

En Angleterre, des chercheurs de la London School of Economics ont conclu en 2019 que les « enseignants ne savent pas exactement ce qu'il advient des données des enfants et quelle est la part des données de l'école transmises à l'extérieur » (Stoilova, Livingstone et Nandagiri. 2019).

Ils ont également conclu que les enseignants reconnaissaient « les nombreux défis que leur pose le programme de connaissance du numérique – du format des cours à l'intégration des technologies dans le processus d'apprentissage en passant par la recherche de contenus plus impliquants centrés sur les opportunités et les messages positifs ».

Compte tenu du volume de données traitées au cours d'une journée type dans la vie d'un enfant scolarisé – communications entre l'école et la maison, inscription et présence, gestion des équipements et des locaux, plateformes et applications d'apprentissage, outils utilisés en classe, gestion des comportements et protection, applications pour les devoirs – et des usages cachés des données à caractère personnel des enfants à des fins de benchmarking et de mesure des performances de l'école et des enseignants, il peut être surprenant de constater que le système étatique prépare si peu les enseignants à gérer des données qui exigent tant d'eux.

2.6.1 Non formés, les enseignants font confiance au système et aux prestataires

Les enseignants peuvent discuter de la conformité des pratiques de l'établissement avec le RGPD mais ils se déclarent simplement « confiants dans la réglementation adéquate et le bon fonctionnement du système de l'école. » (Stoilova, Livingstone et Nandagiri. (2019)).

Les fondements de la protection des données et les droits des enfants ne sont pas systématiquement abordés dans la formation initiale et continue des enseignants. Des entreprises extérieures peuvent fournir une technologie à des enseignants non formés, dont on attend simplement qu'ils apprennent par la pratique.

La formation à la protection des données est considérée comme un complément et non une partie intégrante de la formation des enseignants du secteur public, si bien qu'ils n'ont pas les qualifications nécessaires pour évaluer la licéité d'une technologie mise en place à l'école et procéder à une mise en balance des intérêts en jeu avec les droits de l'homme.

La prudence lors de l'introduction d'une technologie et les processus d'audit ultérieurs doivent s'inscrire dans une boucle d'évaluation des risques active pendant toute la durée de la scolarité de l'enfant et du traitement de ses données, et non dans un processus statique limité à la phase de collecte des données.

Quand un enseignant demande à ses élèves d'utiliser une application donnée, il se peut qu'aucun n'ait les informations nécessaires pour comprendre si les conditions d'utilisation sont équitables ou comment les données personnelles de l'enfant seront traitées tout au long de sa vie.

Un délégué à la protection des données est un rôle indispensable dans une école, même s'il ne s'agit pas nécessairement joué par un membre du personnel détaché à ces fonctions. Il convient de préciser qu'en vertu des obligations complémentaires prévues dans la Convention (article 10 (1)), un tel délégué est nécessaire aux organismes qui traitent les données des enfants dans l'éducation et qu'il doit disposer des moyens nécessaires à l'accomplissement de son mandat.

En 2009, Dowty et Korff ont constaté que le niveau de formation des praticiens sur les questions de sécurité de l'information variait considérablement et que dans certaines collectivités locales britanniques, l'imprécision des recommandations et l'inadéquation des procédures en matière de sécurité étaient préoccupantes.

Il est aujourd'hui courant que les finalités légales du traitement des données personnelles des enfants dans l'éducation soient interprétées à tort comme faisant toutes partie intégrante d'une obligation statutaire ou d'une mission de service public. Or, les tierces parties n'ont pas de mission de service public ; les conditions d'utilisation de la plupart des applications indiquent d'ailleurs que le traitement est effectué sur la base du consentement. Une formation des enseignants et du personnel est donc nécessaire, et les écoles devraient procéder à des audits des pratiques en vigueur.

2.7 La charge d'investigation

S'il ne fait aucun doute que la capacité d'action et de décision des enfants est essentielle et qu'ils doivent être davantage sensibilisés à leur empreinte numérique et à la manière dont leurs données personnelles sont collectées, il existe également un consensus sur le fait que l'on ne peut ni ne doit attendre d'eux qu'ils naviguent seuls dans un environnement en ligne très complexe (Livingstone, 2019).

Le travail d'analyse à mener pour comprendre les produits, procéder à une évaluation adéquate des risques, extraire les informations à transmettre aux personnes concernées et faire en sorte de respecter et défendre les droits des utilisateurs représente actuellement une

charge trop importante pour les écoles. Cela n'est donc pratiquement pas fait et le personnel accepte souvent d'utiliser un produit sans en savoir plus au détriment des enfants.

2.7.1 À la fin de la scolarité obligatoire, on ne peut plus repérer l'empreinte numérique d'un enfant

Les modifications des conditions contractuelles, le partage de données brutes, les transferts de données à l'étranger, le recours à de nombreux sous-traitants par les sociétés spécialisées dans les technologies éducatives et les sessions d'entreprises et changements de propriétaire sont tels que même les parents et les enfants les plus informés au moment de la collecte de données pourraient se retrouver, à la fin de la scolarité obligatoire, sans aucun moyen de comprendre jusqu'où l'école a permis que leur empreinte numérique s'étende et soit diffusée.

Les enfants n'étant pas toujours suffisamment épaulés par leurs représentants légaux s'agissant des risques pour la vie privée en ligne, il appartient aux écoles et aux autres parties au contrat de communiquer sur toute rétention de données et tout traitement qui se poursuivrait après que l'enfant a quitté le système éducatif.

Les entreprises ont elles aussi l'obligation d'adopter des pratiques et de proposer des produits respectueux des droits.

> « Faire preuve de transparence en communiquant les résultats obtenus à l'aide du mécanisme, au moyen de statistiques, d'études de cas ou d'autres informations plus détaillées sur l'instruction de certaines affaires peut être important pour démontrer la légitimité dudit mécanisme et préserver la confiance qu'il suscite de façon générale ». (Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (2011))

L'étude Privacy Sweep du Global Privacy Enforcement Network de 2017 a noté que « les liens vers les politiques de confidentialité et les conditions d'utilisation sont souvent absents ou difficiles à trouver lors de la création d'un compte. Autrement dit, l'enseignant ou l'étudiant ne pourra les retrouver facilement après avoir cliqué sur 'j'accepte' ».

2.8 Assistance, représentation et voies de recours pour les personnes concernées

En vertu des articles 9 et 12 de la Convention 108 modernisée du Conseil de l'Europe, toute personne doit pouvoir exercer ses droits de recours quant au traitement de données personnelles la concernant. Pour les enfants, le système judiciaire est inaccessible, incompréhensible et intimidant (Lignes directrices pour une justice adaptée aux enfants, adoptées par le Comité des Ministres du Conseil de l'Europe (2010)).

Sans accompagnement, il sera donc impossible pour un enfant de contester judiciairement une décision ou une pratique. L'assistance aux personnes concernées, à l'article 18, ne fait aucune référence particulière aux enfants. Ce point pourrait être développé dans le document d'orientation.

La Stratégie du Conseil de l'Europe 2016-2021 pour les droits de l'enfant dit clairement que les droits de tous les enfants sont considérés comme égaux à ceux des adultes et que leurs opinions doivent être entendues en conséquence, jusqu'à leur majorité à l'âge de 18 ans.

« Les enfants ont le droit d'être entendus et de prendre part aux décisions qui les concernent, à la fois à titre individuel et en tant que groupe. En effet, tout individu a droit à la liberté d'expression, garantie par l'article 10 de la Convention européenne des droits de l'homme. La CIDE reconnaît aux enfants le droit d'exprimer librement leur avis sur toutes les questions qui les concernent, cet avis devant être dûment pris en compte en fonction de l'âge et de la maturité de l'enfant ».

> « En vertu de la CIDE, les enfants ont le droit d'être entendus dans toute procédure judiciaire et administrative qui les concerne et d'avoir accès à des mécanismes de recours compétents, indépendants et impartiaux en cas d'atteintes à leurs droits. De plus, les États parties à cette convention reconnaissent le droit de chaque enfant en conflit avec la loi d'être traité d'une manière propre à favoriser son sens de la dignité et qui tienne compte de son âge, en ayant à l'esprit l'objectif de le réinsérer dans la société. Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale » (Stratégie 2016-2021 du Conseil de l'Europe pour les droits de l'enfant, par. 37 et 52).

L'Observation générale n° 16 (2013) des Nations Unies sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant souligne combien il est difficile, en particulier pour les enfants, d'accéder à un recours en cas de problèmes en ligne.

> « Il est particulièrement difficile d'obtenir réparation lorsque l'infraction a été commise dans le cadre d'activités exercées par une entreprise à l'échelle internationale » (par. 67). « Les États qui n'ont pas mis en place de procédures de plaintes collectives (plaintes en nom collectif, action en justice visant à défendre l'intérêt général, etc.) devraient instaurer ce type de recours afin de donner les moyens à un grand nombre d'enfants touchés de la même manière par les activités d'une entreprise de saisir la justice plus facilement. Dans certains cas, ils devront fournir une assistance spéciale aux enfants qui ont des difficultés à accéder à la justice, notamment en raison de leur langue, d'un handicap ou de leur très jeune âge » (par. 68).

Il n'est pas facile pour les enfants d'assurer le respect de leurs droits sans faire appel à des tiers. Le coût financier d'une action en justice contre un ministère ou une entreprise internationale peut être pénalisant.

2.9 Technologies spécifiques, essais et nouvelles problématiques

La conclusion du rapport « Des données et des hommes : droits et libertés fondamentaux dans un monde de données massives » d'Antoinette Rouvroy s'applique aussi bien à l'éducation qu'aux usages du traitement de données à grande échelle, dans leur ensemble.

> « Aussi est-ce à une vigilance constante et à un examen continuellement renouvelé de la pertinence et de l'adéquation des instruments juridiques de protection des droits et libertés fondamentaux qu'invite la 'révolution numérique' ».

Questions posées par les données à grande échelle dans le domaine de l'éducation comme dans les autres secteurs

Le présent rapport n'entend pas dresser une liste exhaustive des enjeux actuels et à venir du traitement de données à grande échelle – parfois appelées « mégadonnées » - dans l'éducation. Il donnera tout au plus quelques exemples illustrant les questions pertinentes du point de vue de la protection des données et plus généralement, de la protection des droits et libertés fondamentaux de l'enfant.

Les plus grands défis en matière de protection des droits de l'enfant, de leur dignité et de leur développement libre et complet sans interférence favorisant leur épanouissement humain à l'âge adulte, proviennent peut-être de la promesse de l'apprentissage et de la prédiction automatiques, utilisant de grandes quantités de données collectées à l'école, passées par des états d'éducation et analysées pour des interventions précoces. La présomption que cela est possible et souhaitable se poursuit par l'éducation dans la vie des étudiants également.

> « Les algorithmes d'IA peuvent être utilisés pour identifier les problèmes en se basant sur l'analyse d'informations courantes – Garder ses étudiants est devenu un problème majeur pour les universités, et des institutions analysent désormais des données afin de déterminer quand et pourquoi les étudiants risquent d'abandonner leurs études, y compris la fréquence à laquelle ils accèdent à leur système de gestion, visitent la bibliothèque ou soumettent leurs devoirs. Repérer les causes inquiétantes permet aux universités de s'occuper activement des étudiants en difficulté et de leur offrir soutien et assistance au plus tôt.
>
> En plus d'augmenter les taux de rétention des étudiants, cela aide les universités à améliorer leur bien-être en identifiant les problèmes et en offrant une assistance plus tôt, plutôt que de leur laisser la responsabilité de demander un soutien. Cela permet également aux établissements d'intervenir précocement auprès d'étudiants ayant des problèmes personnels ou de santé psychologique ».

Cela dit, le principal défi immédiat lié aux technologies les plus récentes, envers les enfants de tous âges, est le souhait des vendeurs comme et des chercheurs de développer et de tester leurs produits.

2.9.1 La participation à des tests de produits en conditions réelles est-elle sans danger pour la construction des enfants ?

Dans leur rapport de 2019 sur l'intelligence artificielle et les nouvelles technologies à l'école, commandé par le gouvernement australien, Southgate et autres affirment :

> « L'intelligence artificielle et les technologies les plus récentes nécessitent un temps 'd'incubation' dans divers environnements scolaires, y compris dans les écoles des zones rurales et à faibles revenus, pour détecter d'éventuels problèmes pratiques, techniques, de sécurité ou d'éthique. Cette 'incubation' doit être accompagnée de travaux de recherche solidement étayés par la théorie sur le potentiel pédagogique et l'impact de ces technologies sur les apprenants et l'apprentissage ».

Cependant, cette 'incubation ' et en fait des projets pilotes et tests en conditions réelles, pourraient se révéler contraires aux bonnes pratiques consistant à appliquer le principe de précaution, comme l'ont montré les conclusions de l'autorité suédoise de protection des données en août 2019 concernant des essais qui avaient recours à la reconnaissance faciale.

Il est crucial que les « problèmes pratiques, techniques, de sécurité ou d'éthique » soient mis en évidence avant qu'une technologie soit appliquée à des enfants qui n'ont pas d'autre option que d'aller en cours.

Les enfants qui sont tenus de participer à des essais ne peuvent pas consentir librement et, comme nous l'avons déjà dit, le concept de consentement légitime en milieu scolaire est fondamentalement problématique. L'absence de consentement ne devrait jamais entraîner l'indisponibilité de services essentiels, mais le consentement ne peut pas non plus être rejeté et les produits testés dans le cadre d'une tâche publique si les écoles disposent de moyens moins invasifs pour mener à bien leurs travaux éducatifs courants.

Le développement de systèmes algorithmiques ne doit pas signifier que les tests ou le déploiement entraînent des risques ou des coûts pour les individus, les familles ou les communautés, et cela nécessite un soutien législatif.

2.9.2 L'enseignement public peut-il être façonné sans risque sous emprise commerciale ?

Le secteur compte d'importants acteurs globaux qui influent sur les technologies disponibles et leur adoption à grande échelle. Leurs pratiques ne sont pas toujours conformes à l'éthique ou au droit. L'Allemagne a par exemple ordonné à la plateforme mondiale Google de modifier ses méthodes de traitement des données d'utilisateurs ; dont l'autorité de protection des données avait conclu en 2015 qu'elles violaient les lois du pays sur le profilage, et à nouveau en 2019, pour que les données à caractère personnel ne soient pas traitées en dehors du territoire allemand.

La culture et les finalités de l'éducation sont dictées par les entreprises internationales à mesure que celles-ci prennent le contrôle des infrastructures de gestion des données de grandes parties du secteur.

Google a développé son propre langage et sa propre terminologie dans le domaine de l'éducation, de la même manière que son nom est devenu synonyme de « rechercher des informations sur internet » ; la rhétorique de l'innovation de Google consiste également à créer des types de sujets particuliers commençant par internaliser les valeurs de la plateforme et à les proposer gratuitement au personnel scolaire (Sujon, Z., 2019).

> « Les campagnes de promotion de GE (Google Education) visent à recruter des gens ordinaires, volontaires pour étendre gratuitement l'univers Google. Les 70 millions d'utilisateurs de GFE et de GE oeuvrent également pour Google qui leur promet en contrepartie un enrichissement éducatif et personnel. C'est le cœur de la stratégie d'expansion de GFE – un constat qui rejoint la littérature sur le *soft power* de Google, son capitalisme de surveillance et plateforme et de son « colonialisme en matière de données » (Srnicek 2016 ; Zuboff 2019, Couldry et Meijas 2018 ; Sandoval, 2014 ; Fuchs 2014 ; Hillis et autres, 2013). GE est ainsi une spectaculaire illustration du pouvoir de Google de fabriquer, proposer et définir les termes du travail éducatif et d'affirmer ses ambitions quant au futur de l'éducation.
>
> À mi-chemin entre enrichissement et colonialisme, cette stratégie apportera sans doute une contribution utile aux études sur l'éducation et les technologies. Mais elle doit également nous amener à nous interroger sur ce qui est véritablement en jeu ici. Quelles sont les données que Google extrait des établissements scolaires, où vont-

> elles et comment la société tire-t-elle des bénéfices – économiques ou stratégiques – de cette activité ? Et surtout : quelles sont les incidences concrètes d'un renforcement de la place de Google dans la vie des jeunes ou au sein des infrastructures publiques et des institutions sociales »? (Sujon, Z., 2019)

Au moment où nous écrivons, la contestation de cette position dominante a commencé aux États-Unis, en Suisse et aussi chez des représentants légaux en Espagne (Ars Technica, 2019). Le procureur général de l'État du Nouveau-Mexique a intenté une action en justice en février 2020 contre Google LLC, affirmant que l'utilisation de Google Éducation et d'autres produits Google " a un coût très réel que Google occulte délibérément". (*Balderas, Nouveau-Mexique, contre Google LLC, 2020*). L'Autorité norvégienne de protection des données a également annoncé qu'elle enquêtait sur la légalité de l'utilisation de Google dans les écoles. (Aftenposten, février 2020). Des autorités et des parents, commencent à rejeter une entreprise qui paraissait pourtant être un cadeau bienvenu pour les infrastructures scolaires en période d'austérité (Republik, 2019).

2.9.3 La valeur de l'éducation d'un enfant ne se mesure-t-elle qu'aux données ?

L'analyse de données étant utilisée de plus en plus couramment pour demander des comptes aux enseignants et évaluer la qualité de leur travail à partir des données des enfants, la question de savoir comment nous continuerons à valoriser ce qui, dans l'éducation, ne peut pas être mesuré par des machines (Smith, S. 2016) nécessite de notre part une action volontaire pour choisir les valeurs que notre société souhaite voir transmises par l'éducation de demain.

Si nous restons passifs, les entreprises décideront pour nous et leurs valeurs seront les fondements des sociétés futures et celles des citoyens formés par nos systèmes éducatifs.

Dans son Observation générale n° 1 (2011) : les buts de l'éducation (article 29), le Comité des droits de l'enfant de l'Organisation des Nations Unies demande instamment que les instances internationales concernées par les politiques éducatives et l'éducation aux droits de l'homme s'efforcent d'améliorer leur coordination pour une mise en œuvre plus efficace des dispositions du paragraphe 1 de l'article 29.

Les lois de protection de la vie privée et des données personnelles peuvent établir des paramètres définissant les limites de ce qui est acceptable dans le champ des possibles. Il est urgent que les valeurs de ceux qui façonnent nos enfants par l'éducation reposent sur des droits fondamentaux universels qui donnent la priorité aux personnes et à leur épanouissement en tant qu'êtres humains ; cela implique de reconnaître que pour servir l'intérêt général, l'utilisation de données créées dans le secteur public devrait viser à promouvoir la pleine participation de tous à une société libre, plutôt que le simple profit privé.

2.10 Intelligence artificielle et éducation

Le recommandations émises devraient s'appuyer sur les normes existantes du Conseil de l'Europe et la jurisprudence pertinente de la Cour européenne des droits de l'homme, ainsi que sur la dimension des droits de l'homme des techniques automatisées de traitement de données actuelles et en cours de développement, en particulier les algorithmes et les possibles implications en termes de normes et de réglementation.

> « Il n'existe pas à l'heure actuelle de définition communément admise de l' «intelligence artificielle ». Toutefois, aux fins de la présente recommandation, l'IA est une expression générique utilisée pour désigner de façon générale un ensemble de sciences, de théories et de techniques dont le but est d'améliorer la capacité des machines à réaliser des tâches requérant des facultés cognitives. Un système d'IA est un système informatique qui formule des recommandations, établit des prévisions ou prend des décisions en fonction d'une série donnée d'objectifs. » (Conseil de l'Europe, mai 2019

Des plateformes d'apprentissage personnalisées au dépistage automatique de la dyslexie chez les enfants (AlgorithmWatch, 2019), l'intelligence artificielle accapare une grande part de l'attention et des ressources financières disponibles dans le monde universitaire, le secteur privé et les milieux dirigeants :

> « Les entreprises s'investissent pleinement pour réinventer les capacités, compétences et dispositions requises de la part des jeunes et des professionnels de l'enseignement dans une période de mutations économiques et technologiques. Fin 2016, IBM et Pearson ont uni leurs forces dans un nouveau partenariat global » (Williamson, 2017, Big Data in Education).

Le Consensus de Beijing de l'UNESCO sur l'intelligence artificielle publié en 2019 donne des orientations et des recommandations sur la meilleure façon d'exploiter les technologies de l'intelligence artificielle pour atteindre l'ODD4. Cela dit, les préconisations de ce type posent rarement la question de savoir si, comment et pourquoi la personnalisation améliorerait la pratique ou les résultats en matière d'éducation. À ce jour, les preuves – limitées – de ces bénéfices sont apportées par ceux qui développent ou commercialisent les produits.

Lorsque l'on cherche des recommandations, la première chose à faire serait de ne pas utiliser du tout l'expression « intelligence artificielle », dont il n'y a pas de définition juridique, avec ses définitions vagues mais limitées, mais « système intelligent autonome » ou « prise de décision algorithmique »". La seconde serait de traiter le traitement des données à l'aide de ces outils, avec les mêmes attentes élevées que les autres méthodes de données décisionnelles.

2.10.1 La discrimination et les biais dans les données sont des problèmes universels

Le Consensus a conclu à propos de l'intelligence artificielle dans l'éducation que, du point de vue des droits,

> « le développement et l'utilisation de l'intelligence artificielle dans l'éducation ne doivent pas accroître le fossé numérique et être exempts de tout préjugé à l'égard de groupes minoritaires ou vulnérables ».

La question de savoir si les solutions personnalisées « monétisables » s'attaquent aux causes des inégalités et peuvent mieux les combattre commence seulement à être examinée par des tiers indépendants (Davies, H., à paraître).

La puissance de traitement de données et les pratiques et prises de décisions potentiellement opaques qui caractérisent les nouvelles technologies ont d'importantes répercussions sur le service public de l'éducation, notamment en tant que cadre de travail, que ce soit pour le recrutement, l'analyse de données ou les prédictions et interventions.

S’agissant des applications portant sur de grands volumes de données, comme lorsque l’IA collecte des données d’interactions toutes les deux secondes, le rôle des comités d’éthique attire de plus en plus l’attention du secteur de l’intelligence artificielle, même s’il n’y a pas encore de consensus unanime sur leur nature, leur indépendance ou leur mission. Les études théoriques, documents d’orientation et initiatives des entreprises proposent tous des solutions différentes, et quelquefois contradictoires, de ce point de vue.

2.10.2 Les choix faits dans la conception des produits peuvent porter atteinte aux droits des enfants

Même si vie privée et innovation ne sont pas forcément incompatibles, le développement de produits dans de nouveaux domaines comme l’apprentissage-machine, l’intelligence artificielle, la biométrie et la reconnaissance faciale peut très vite porter atteinte à certains droits. La protection des données et le respect de la vie privée dès la conception (« *privacy by design* ») suivent une approche basée sur le principe de précaution, ce qui est particulièrement important lorsque des données sont traitées dans le cadre d’interventions auprès d’enfants.

Dans leur rapport de 2019 sur l’intelligence artificielle et les nouvelles technologies à l’école, commandé par le gouvernement australien, Southgate et autres affirment :

> « Luckin et ses collègues (2016) mettent également en avant un risque d’utilisation des assistants d’enseignement basés sur l’intelligence artificielle pour surveiller subrepticement ou indûment les performances des enseignants (au moyen des données des élèves), et sont rejoints sur ce point par Campolo et autres (2018) qui recommandent de « multiplier les recherches et les directives générales sur l’utilisation des systèmes d’intelligence artificielle dans la gestion et la surveillance dans l’environnement professionnel » (p. 1). D’autres préoccupations concernent la manière dont l’intelligence artificielle vise à modifier les comportements d’apprentissage en ayant recours à des recommandations, à la persuasion et à la remontée d’informations, ce qui n’est finalement pas toujours dans l’intérêt supérieur de l’apprenant. Certains avancent que les « compagnons d’apprentissage » basés sur l’intelligence artificielle, destinés à soutenir les élèves tout au long de leur cursus d’apprentissage pourraient aboutir à l’enregistrement permanent de leurs échecs au détriment de leurs futurs progrès (Luckin et autres, 39).

La remarque faite par Boyd et Crawford (2012) sur les mégadonnées est particulièrement pertinente dans le contexte de l’intelligence artificielle :

> « Nombre (de personnes) n’ont pas conscience de la multiplicité des acteurs et des algorithmes qui recueillent et conservent actuellement leurs données en vue d’une utilisation ultérieure’. (p. 673). Cela nous amène au troisième volet de la sensibilisation : les élèves, parents et enseignants doivent être pleinement informés des modalités de collecte, de conservation et de partage de données par l’intelligence artificielle, les parents devant y donner leur consentement exprès et éclairé avec l’assentiment de l’élève. Les recommandations de l’IEEE (2017) vont également dans ce sens ».

Le 17 octobre 2017, le groupe de travail Article 29 a publié ses Lignes directrices sur les décisions individuelles automatisées et le profilage aux fins du Règlement 2016/679 (RGPD).

Il n'interprète pas le considérant 71 comme une interdiction absolue des décisions prises sur le seul fondement d'un traitement automatisé lorsque la personne concernée est un enfant, mais note que cela devrait être limité à certaines situations bien définies (par exemple pour protéger les intérêts vitaux de l'enfant).

Quoi qu'il en soit, la réglementation de ces outils pourrait nous conduire à accepter des utilisations de la technologie pour des finalités dont la nécessité devrait faire l'objet d'un questionnement plus intense.

> « En résumé, les casse-têtes informatiques qui nous préoccupent nous font passer à côté du problème, beaucoup plus important, de l'asymétrie colossale entre le coût pour la société et les bénéfices privés du déploiement des systèmes automatisés. Ils nous privent également de la possibilité de nous interroger sur l'opportunité même de développer de tels systèmes.
>
> « L'intelligence artificielle évoque une toute-puissance objective et mythique mais elle est soutenue par les forces bien réelles de l'argent, du pouvoir et des données. Au service de ces forces, nous sommes abreuvés de discours convaincants qui nous entraînent vers une utilisation et une dépendance généralisées à l'égard de systèmes de classification régressifs basés sur la surveillance, faisant de nous les sujets d'une expérience sociétale sans précédent dont il est difficile de ressortir. Aujourd'hui plus que jamais, il nous faut riposter avec fermeté, courage et imagination » (Powles, 2018).

La sensibilisation et l'éducation sont essentielles mais ne sont pas la panacée. Certaines technologies impliquant un traitement de données peuvent porter atteinte aux droits, même si le traitement est transparent, car certains risques seront peut-être décalés dans le temps. Les États doivent reconnaître la nécessité d'éduquer les enfants à l'importance de leurs données personnelles et à l'usage qui en est fait, pour qu'ils comprennent bien l'impact de leur histoire numérique sur leur avenir dans le système éducatif puis dans la vie active, mais aussi pour qu'ils puissent contester les décisions automatisées lorsqu'elles semblent inéquitables, conformément à l'article 9(1)(a) de la Convention, et s'épanouir ainsi pleinement.

2.11 Données biométriques

L'utilisation des données biométriques d'une personne est un moyen d'accès aux services scolaires plus intrusif pour la vie privée qu'un code PIN ou une carte magnétique. Diverses technologies biométriques sont employées dans les écoles. La plus courante est l'empreinte digitale qui a été introduite dans les écoles britanniques en 1999 (King, P. 2019).

Ces technologies existent depuis un certain temps. L'école Marie-José de Liège, en Belgique, a été équipée en 2007 malgré des critiques grandissantes.

Les mesures biométriques sont déjà utilisées dans les systèmes éducatifs du monde entier pour gérer les systèmes de paiement, les casiers et le matériel d'impression, et plus généralement pour authentifier l'identité des élèves, protéger l'intégrité académique et assurer la sécurité.

Selon les estimations, plus de 2 millions d'enfants auraient été contraints d'accepter le traitement de leurs empreintes digitales dans les écoles britanniques et par les prestataires de

services de restauration avant 2012, date à laquelle la loi de protection des libertés (« chapitre 2, protection des données biométriques des enfants à l'école ») a été mise en place en Angleterre et au Pays de Galles pour régler la question du consentement nécessaire au traitement des données biométriques des enfants par les écoles. Depuis le 1er septembre 2013, les écoles doivent obtenir le consentement écrit des parents pour toute conservation ou tout traitement des données biométriques d'un enfant. Cela dit, une étude commandée par defenddigitalme en 2019 a montré que sur 1 000 parents dont les enfants utilisaient des technologies biométriques à l'école, 38 % n'avaient pas reçu d'invitation à donner leur accord. La question se pose donc de savoir si l'utilisation de ces catégories particulières de données, qui représentent un enjeu considérable et peuvent être essentielles à la vérification de transactions importantes à l'âge adulte, doit être autorisée à l'école pour des opérations banales de comparaison.

2.11.1 Les données biométriques doivent-elles être considérées comme une denrée prisée ou devenir finalement des données courantes ?

Dans le cadre de leurs travaux de recherche auprès d'enfants, rassemblés dans leur publication Invisibly Blighted (UCL IOE Press, 2017), Sandra Leaton Gray et Andy Phippen ont relevé des manifestations préoccupantes de cette normalisation de la surveillance biométrique et constaté que les écoles recueillaient librement des données biométriques en se souciant guère du droit des enfants au respect de leur vie privée :

> « Alors que techniquement, l'utilité des données biométriques ne fait aucun doute pour les administrateurs, il est préoccupant de constater que leur valeur comparativement élevée pour l'individu n'est pas prise en compte. Il semblerait en effet que celle-ci soit sous-évaluée du fait que les données biométriques sont associées à des choses aussi banales et quotidiennes que la cafétéria ou la bibliothèque de l'école. Vu l'âge des personnes concernées et l'influence encore forte que l'institution qui les entoure, en l'occurrence l'école, exerce sur leurs identités sociales, cela n'est pas sans conséquences ».

Les technologies biométriques comme l'utilisation des empreintes digitales et les scanners d'iris deviennent de plus en plus courantes dans les écoles et même dans les universités pour vérifier l'identité des élèves, protéger l'intégrité académique et assurer la sécurité (Paul, 2017).

Les scanners d'iris et l'oculométrie sont souvent utilisés dans le cadre des plateformes d'apprentissage et des solutions automatisées de surveillance en ligne. Ces dernières servent à authentifier et réauthentifier l'identité en ligne grâce à la reconnaissance faciale par webcam et à la collecte régulière de données lors d'examens.

2.11.2 Détection de visage et reconnaissance faciale

Les technologies de détection de visage et de reconnaissance faciale existent depuis quelque temps dans le système éducatif chinois (Greene, 2018) et commencent à être utilisées de diverses manières dans un nombre toujours plus grand de contextes scolaires.

Jusqu'à présent, ces technologies ont été largement considérées comme des ajouts courants aux systèmes scolaires dans des contextes culturels de suivi et de surveillance déjà étendus. Cela présente un certain nombre de problèmes et de préoccupations d'ordre social qui méritent une attention particulière. C'est notamment la probabilité que la technologie de

reconnaissance faciale modifie la nature des écoles et de la scolarité selon des lignes de division, d'autoritarisme et d'oppression. (Andrejevic et Selwyn (2019)

Les préoccupations croissantes du public commencent à se refléter dans des mesures réglementaires. Dans une décision d'août 2019 sur le *Skellefteå kommun*, l'autorité suédoise de protection des données a déclaré illégale l'introduction d'un système de reconnaissance faciale pour l'enregistrement des présences et a condamné l'administration scolaire à une sanction pécuniaire de 200 000 couronnes suédoises (soit 20 700 $) pour violation de la loi sur le respect de la vie privée et la protection des données. Le consentement à la collecte de données sensibles ne pouvait être donné librement et il n'y avait eu ni consultation préalable de l'autorité de supervision, ni évaluation d'impact adéquate du risque pour la protection des données.

Il est important de noter que cette décision visait à protéger les droits des enfants en refusant le recours inapproprié à un « consentement » artificiel. L'infrastructure permettant une adoption généralisée des systèmes de détection de visage et de reconnaissance faciale à l'école et dans le reste de la société inquiète beaucoup les groupes de défense des libertés civiles et une partie du monde universitaire, mais à ce stade, la prise de conscience de l'introduction de ces technologies dans les écoles est encore faible chez les responsables légaux.

En février 2020, les tribunaux français ont respecté la décision de la CNIL selon laquelle l'utilisation de la reconnaissance faciale dans les écoles était illégale.

Les écoles disposent déjà couramment de bases de données images de tous leurs élèves et beaucoup utilisent des caméras de télévision en circuit fermé pour la surveillance de leur site, souvent comme mesure de sécurité. Cela facilite la possibilité de mettre en œuvre des systèmes de reconnaissance faciale. Comme l'a noté Selwyn dans le projet Data Smart Schools, auquel ont participé des chercheurs des universités de Monash et de Deakin,

> « Un autre facteur qui accélère l'introduction des systèmes de reconnaissance faciale dans les écoles est l'usage très répandu de la vidéosurveillance, avec des caméras installées partout, de la cour aux toilettes des élèves. L'engouement des écoles pour les technologies de surveillance est tel qu'il a même été proposé d'équiper les enseignants de caméras piéton ou de recourir à l'inscription par empreintes digitales ou au marquage RFID des élèves » (Selwyn, Data Smart Schools, 2019).
>
> « La RFID est déjà couramment utilisée dans des pays comme le Brésil où l'introduction d'un niveau supplémentaire de surveillance des élèves pour les protéger contre des menaces potentielles est la bienvenue dans le paysage socioculturel » (Taylor, 2017).

La vidéosurveillance comporte à elle seule des risques pour le droit des enfants au respect de leur vie privée et à la protection de leurs données. On dispose de nombreux témoignages sur la manière dont les enfants vivent et voient la vidéosurveillance, le fait qu'elle empiète sur le besoin d'intimité des individus dans les espaces sanitaires, la méfiance qu'elle suscite et les effets et conséquences inattendus des alternatives à la surveillance par la technologie. L'introduction de la vidéosurveillance dans les écoles se poursuit au même rythme, ses usages au-delà de la lutte contre la délinquance sont très rarement remis en question et les opinions critiques et dissidentes ne trouvent guère d'expression (Taylor, Rooney (2017)).

La vidéosurveillance à l'école est présumée avoir pour seul but la prévention de la délinquance mais dans la pratique, les usages répertoriés au Royaume-Uni incluaient la surveillance des examens, le suivi des performances des enseignants et la recherche d'un effet dissuasif sur le comportement des élèves.

L'analyse de l'actualité mondiale relative à la mise en œuvre des technologies fait clairement apparaître des disparités d'un pays à l'autre et au sein des pays s'agissant des normes culturelles et des attentes en matière de respect de la vie privée des enfants et des parents. Il en ressort également que les droits de l'enfant ne sont pas reconnus partout de la même manière.

Ainsi, en juillet 2019, il a été rapporté que le gouvernement de Delhi prévoyait d'installer pour novembre des caméras de vidéosurveillance dans toutes les écoles publiques. Les données ne resteraient cependant pas sur site mais sur le cloud, afin que les responsables légaux puissent obtenir des flux vidéo en direct des caméras de surveillance et surveiller le comportement de leur enfant à l'école « pendant une durée limitée, via l'application mobile 'DSG live' » (Vatsalya, Youth Ki Awaaz 2019).

Ces systèmes sont souvent introduits dans les écoles avec des moyens techniques limités. Toute erreur peut ouvrir une brèche dans le système, comme celle découverte en février 2018 lorsqu'il a été constaté que des images de vidéosurveillance prises dans des écoles britanniques étaient diffusées en direct sur un site Web américain au moyen de flux de données provenant de caméras non sécurisées, « montrant des centaines d'élèves vaquant à leurs occupations quotidiennes ». Dans ce cas, la vidéosurveillance ne prenait pas d'images des espaces privés dans les toilettes. Mais cette pratique peut être courante.

L'usage de caméras piéton et de caméras frontales se répand également dans les écoles qui choisissent de s'en servir pour surveiller les comportements.

Il est également possible d'activer des webcams à distance. En 2010, l'affaire *Robbins c. Lower Merion School District* a révélé que des écoles pouvaient photographier les enfants à leur insu, dans l'intimité de leur foyer en utilisant les logiciels installés sur les ordinateurs portables des enfants. La nature hautement invasive de telles pratiques s'est accrue depuis avec les politiques consistant à faire apporter par les enfants leurs propres équipements dans le cadre de programmes visant à combattre des extrémismes violents en Australie, aux États-Unis et au Royaume Uni, et ce sans réel débat ni contrôle.

2.12 Protection et lutte contre l'extrémisme violent

En 2009, le groupe de travail Article 29 a suggéré qu'il « ne devrait jamais arriver que pour des raisons de sécurité, les enfants fassent l'objet d'une surveillance excessive qui limiterait leur autonomie. Dans ce contexte, il convient de ménager un juste équilibre entre la protection de l'intimité et de la vie privée des enfants et leur sécurité » (Avis 2/2009 sur la protection des données à caractère personnel des enfants).

Aujourd'hui, au contraire, le PDG de la société Gaggle spécialisée dans les logiciels de protection des écoles, Jeff Patterson, reconnaît que certains logiciels de protection utilisés dans les écoles sont très intrusifs. « La vie privée est passée à la trappe ces cinq dernières années. Pour le bien de la société, pour la protection des enfants » (Education Week, mai 2019).

Durant ces dix années, l'absence de contrôle des applications pratiques a conduit les fournisseurs de l'éducation à minimiser l'importance du respect de la vie privée des enfants et à ne plus le considérer comme un droit, mais comme une marchandise. C'est à ce prix que se paie la sécurité que ces entreprises promettent en contrepartie.

Dans les Principes pour le respect de la vie privée et la liberté d'expression des enfants en ligne (Fonds des Nations Unies pour l'enfance (UNICEF) 2018) et la boîte à outils pour les chefs d'entreprise qui l'accompagne, Carly Nyst énumère un certain nombre de risques liés aux logiciels employés pour assurer la sécurité en ligne dans les écoles.

> « Ceux qui cherchent à exploiter les enfants et à abuser d'eux en utilisant internet pour entrer en contact avec eux et les solliciter à des fins sexuelles, ou pour partager des contenus montrant des abus sexuels sur mineurs portent gravement atteints à la vie privée des enfants en ligne. Cependant, elle est également menacée par les mesures prises pour les protéger contre ces dangers. Les lois conçues pour faciliter la prévention et la détection des crimes contre les enfants en ligne prévoient souvent des mesures de suivi et de surveillance sur internet, contraignent les intermédiaires à générer et à conserver des informations personnelles et autorisent les pouvoirs publics à accéder à des données privées. Dans le même temps, à la maison, des dispositifs courants de contrôle parental visant à surveiller et à restreindre l'accès à internet promettent d'exposer dans les moindres détails l'activité des enfants en ligne ».

Une évaluation des principaux prestataires de logiciels de ce type au Royaume-Uni et aux États-Unis menée par defenddigitalme en 2018-2019 a montré que le traitement des données personnelles avait lieu en dehors du territoire du pays concerné et qu'il était courant qu'aucune information ne soit fournie aux responsables légaux ou aux enfants sur le fonctionnement des systèmes ou les profils qu'ils génèrent.

Des informations contradictoires circulent quant à la capacité du personnel à modifier les enregistrements et à supprimer les erreurs. Des requêtes avec les mots-clés « précipice » et « rhinocéros noirs » ont déclenché des avertissements de sécurité, respectivement pour risque de suicide et appartenance à un gang. Il s'agit tout bonnement de mauvais appariements, mais le personnel n'est pas toujours apte ou disposé à les supprimer, au contraire : « si un mot-clé déclenche une correspondance que l'école considère comme erronée, il est possible d'ajouter une note permettant à l'analyste d'expliquer pourquoi ». Autrement dit, des informations inexactes peuvent être enregistrées sur un enfant sans qu'il puisse voir l'enregistrement en question ou le faire corriger.

L'étude a également montré que la moitié des écoles imposent une politique du « *bring your own device* » (« apportez votre équipement personnel de communication »), ce qui constitue un niveau de surveillance opaque des biens personnels, actifs dès qu'ils sont connectés au réseau de l'école voire en continu, indépendamment de la connexion au réseau.

Les effets comportementaux que cela peut avoir sur l'utilisation d'internet par les enfants n'ont pas encore été suffisamment étudiés mais les retours qualitatifs semblent indiquer un effet dissuasif sur les recherches concernant la sexualité, la santé et les questions de développement des adolescents.

2.12.1 Cela pourrait exacerber plutôt que diminuer la vulnérabilité des enfants aux risques.

S'agissant du filtrage, le rapporteur spécial des Nations Unies a affirmé dans son rapport de 2014[4] sur le droit de l'enfant à la liberté d'expression :

> « En adoptant des définitions vagues et larges de ce qui constitue une information nuisible, par exemple lors de la détermination de la façon de paramétrer les systèmes de filtrage sur Internet, on risque d'empêcher les enfants d'avoir accès à des informations qui peuvent les aider à prendre des décisions en connaissance de cause, notamment dans le cas de renseignements impartiaux, objectifs et adaptés à leur âge sur des questions telles que celles relatives à l'éducation sexuelle et à l'abus de drogue. Cela peut exacerber, plutôt que de diminuer, la vulnérabilité des enfants aux risques ».

Les moyens de lutter contre l'extrémisme violent faisant l'objet d'une attention accrue de la part des pouvoirs publics depuis 2001, les éléments considérés comme significatifs par ces logiciels sont progressivement passés de l'intention claire de passer à l'action qualifiée de terrorisme aux notions plus larges et plus vagues d'« extrémisme » et de « radicalisation ». Alors qu'auparavant, le système devait évaluer dans une certaine mesure l'intention et la capacité d'action pour signaler un élément suspect ou pouvant constituer un risque potentiel, aujourd'hui, des interceptions et interventions pourront être déclenchées par des présomptions – potentiellement insignifiantes – d'une disposition à l'égard de telles idées.

Ces collectes de données aboutissent entre autres à la création de profils d'enfants classés avec des étiquettes telles que « terrorisme et extrémisme », « automutilation » et « problèmes de santé mentale ».

Une analyse des informations provenant de 4 507 écoles anglaises (sur 6 950) ayant procédé à des auto-évaluations de la sécurité électronique, menée par le professeur Andy Phippen, montre que le personnel scolaire n'a pas à sa disposition les outils qui lui permettraient de se prononcer sur les résultats obtenus par le biais de ces technologies ou les remettre en question.

2.12.2 Le couplage des données sous couvert de protection de l'enfant crée un panoptique de surveillance

L'application de la vidéosurveillance aux espaces scolaires et la surveillance de l'activité personnelle des enfants en ligne peuvent être poussées plus loin encore en les associant dans un panoptique regroupant les autorités, la lutte contre la criminalité et les communications privées de l'enfant.

En réponse à des préoccupations similaires des établissements d'enseignement, les technologies de reconnaissance faciale ont été perfectionnées et permettent aujourd'hui de proposer des outils de « détection des émotions » pour repérer les manifestations de violence scolaire. (Guardian, 2019)

[4] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf

En juin 2018, dans le cadre des mesures prises pour prévenir les fusillades dans les écoles, les législateurs de l'État de Floride (États-Unis) ont autorisé la création d'une base de données centralisée qui regrouperait les casiers judiciaires de chacun des élèves, leur dossier auprès des services sociaux et des informations provenant de leurs comptes personnels sur les médias sociaux (Herold, Education Week).

> « Le cas de la Floride nous donne un aperçu des immenses possibilités de réappropriation, de recyclage et de recombinaison des données scolaires. Il nous rappelle également la nécessité de nous entourer de précautions avant de générer un élément de données simple sur un élève ou un enseignant, susceptible d'être relié à d'autres renseignements permettant de les identifier.
>
> De nombreux responsables politiques et parents de Floride voient logiquement dans ce projet de l'État une utilisation valable des données des élèves au nom de la 'sécurité de l'école' ». C'est une question très sensible et peu de solutions effectives y sont apportées dans un pays qui semble se refuser à mettre en place un contrôle efficace des armes à feu. Dans ces circonstances, le renforcement de la surveillance numérique est une alternative intéressante pour les responsables politiques et chefs d'établissement soucieux de montrer qu'ils agissent ».

Cela dit, les études montrent que les outils actuels vont souvent à l'encontre des valeurs des parents et des jeunes en matière de respect de la vie privée, et qu'ils préféreraient avoir à leur disposition des outils pour faciliter la médiation par les parents de l'utilisation des technologies par les enfants, plutôt que des moyens de surveillance (Zhao, 2019).

2.13 Analyse prospective : sciences cognitives, incitations affectives et comportementales

Les milieux éducatifs ont de plus en plus recours à des technologies en ligne qui identifient et gèrent les élèves par les affects. Ces formes de suivi peuvent être considérées comme une méthode d'approche des élèves à travers le prisme de la psychologie positive (Nemorin, 2018).

En 2017, le magazine Wired a révélé que l'unité « *nudge* » ou unité d'introspection comportementale du gouvernement britannique avait expérimenté l'usage d'algorithmes d'apprentissage-machine de conception opaque pour évaluer les performances des établissements :

> « Les données relatives à l'origine ethnique et à la religion des élèves ont été délibérément exclues de l'ensemble de données pour prévenir les biais algorithmiques. Bien que certains facteurs influencent davantage la décision algorithmique que d'autres, Sanders a refusé de dire lesquels. Il a expliqué que cela était dû en partie au fait qu'il ne voulait pas que les établissements sachent comment les algorithmes prennent les décisions et en partie parce qu'il était difficile de connaître exactement leur fonctionnement ; « le processus ressemble un peu à une boîte noire, et c'est en quelque sorte le but de la manœuvre ».

L'option consistant à réglementer une technologie en particulier se révèle souvent inefficace car un changement mineur dans le design peut la faire sortir du champ des protections prévues. Cela dit, il est possible que dans la décennie à venir, les données des étudiants soient recueillies au moyen de technologies de plus en plus pointues et intrusives sur le plan

physique et psychométrique, capables par exemple de détecter des caractéristiques psychologiques individuelles, des traits physiques, l'activité neuronale du cerveau et des informations génomiques à partir de l'ADN. Si les États décident d'utiliser ces technologies à grande échelle pour évaluer leurs institutions ou leur population de manière cachée, ou s'ils n'en comprennent pas bien le fonctionnement, il faudra des protections importantes contre leurs effets dommageables insoupçonnés.

Les enfants, en phase de croissance physique et mentale et encore malléables, seront les plus vulnérables de ce point de vue.

2.13.1 Quelles sont les protections dont disposent nos enfants à l'école contre des technologies de modification du cerveau et du comportement et immersives ?

Des chercheurs australiens ont récemment conclu que

> « la réalité virtuelle immersive posait des problèmes d'éthique et de sécurité. Chez les jeunes enfants, elle peut notamment provoquer de faux souvenirs et un phénomène de « mal du virtuel » (s'apparentant au mal des transports). La création et le partage de contenus de réalité virtuelle par les élèves et les enseignants, en particulier, soulèvent des préoccupations d'ordre éthique et juridique concernant le droit au respect de la vie privée, la propriété intellectuelle et le droit d'auteur ».

Ils en sont arrivés à la même conclusion s'agissant de la réalité augmentée :

> « Il existe des préoccupations éthiques et légales touchant aux domaine de la vie privée, de la propriété intellectuelle et du droit d'auteur, en particulier lorsque les enseignants et les étudiants partagent ou créent de contenus de réalité augmentée ».

Ben Williamson, de l'Université d'Édimbourg, a apporté une contribution importante à la réflexion sur certains enjeux actuels liés à l'utilisation des technologies dans l'éducation et à la manière dont les enfants peuvent exercer leur pouvoir d'action et de décision.

> « La 'psychométrie numérique' et le 'phénotypage numérique', qui ont fait leur apparition dans le domaine de la psychologie, permettent de construire un profil psychologique détaillé des individus à partir de leurs activités en ligne, mais ont été ternis en étant associés au microciblage à des fins de publicité politique (Mats, S., Wired, 2017).
>
> Cependant, certains aspects de la psychométrie numérique commencent à poindre dans l'éducation. L'étude de l'OCDE sur les compétences sociales et émotionnelles, par exemple, utilisera un outil de sondage en ligne pour évaluer les jeunes selon le modèle de personnalité OCEAN (OCDE, 2018) à cinq facteurs, qui est le même que celui utilisé par les spécialistes en psychométrie numérique de l'Université de Cambridge dans le test myPersonality proposé via Facebook. D'autres organisations impliquées dans l'évaluation des apprentissages et des compétences sociales et émotionnelles explorent également d'autres technologies novatrices pour faire entrer la psychométrie numérique dans le secteur de l'éducation (McKown, 2017).
>
> Les technologies biométriques comme les capteurs cutanés portables et la reconnaissance faciale ont très vite suscité de l'intérêt pour leurs usages dans l'éducation (Hand, 2019). Le domaine dans lequel les applications de la biométrie

portable sont sans doute les plus évidentes est celui de l'éducation physique où divers dispositifs ont été mis en œuvre pour recueillir les données physiologiques des élèves (Pluim, 2016).

Des 'neurotechnologies' comme les interfaces cerveau-machine et les neurostimulateurs sont déjà mises au point et testées en vue de recueillir des données sur l'activité neuronale des élèves lors d'activités éducatives. (Williamson, B. 2019). BrainCo par exemple, a conçu un bandeau frontal qui capte les données des ondes cérébrales et les transmet en temps réel au tableau de bord de l'enseignant pour lui indiquer le niveau d'attention et de participation de la classe et servir de base à des programmes d'entraînement cérébral reposant sur le neurofeedback pour améliorer la concentration des élèves (Jing, M., 2019).

De même, des chercheurs de l'Université de Cambridge ont élaboré un appareil « biométrique cognitif » portable qui enregistre les « signaux neuro-respiratoires du diaphragme » comme indicateurs des états de concentration et d'éveil. FOCI utilise l'apprentissage-machine pour analyser et visualiser les résultats, ainsi qu'un coach mental à base d'IA s'appuyant sur l'entraînement cognitif, le renforcement positif et les techniques de neurofeedback pour fournir en temps réel des conseils permettant d'améliorer l'attention et d'optimiser la concentration. D'autres innovations dans le domaine de la neurostimulation sont conçues pour intervenir plus activement sur l'état cérébral des élèves (FOCIAI, 2019).

Les techniques de neurostimulation comme la stimulation électrique transcrânienne (SET) ont été explorées pour leur capacité à améliorer la cognition chez les jeunes.

Selon une analyse des travaux de recherche en neurostimulation appliquée à l'éducation, des liens ont pu être établis entre l'utilisation des techniques de SET et des améliorations parfois durables dans plusieurs domaines de la cognition dont la mémoire, l'attention, le langage, les mathématiques et la prise de décisions (Schuijer, J., 2017).

Les spécialistes des neurosciences appliquées à l'éducation s'intéressent de plus en plus aux possibilités offertes par la neurostimulation (UCL, Centre de neurosciences éducatives, 2019) qui dynamise également tout le secteur des technologies d'amélioration cognitive proposées directement au consommateur.

La bio-informatique est l'étude informatique de l'ADN humain. Récemment, des études de bio-informatique suivant la méthode du « score polygénique » ont commencé à faire leur apparition dans l'éducation, pour faire des prédictions concernant les résultats scolaires, le niveau d'études et l'intelligence des élèves, à partir de leurs données génétiques (Williamson, B 2018). Ces études de « mégadonnées » en bio-informatique laissent entrevoir la possibilité d'une utilisation croissante des données génétiques pour « personnaliser » l'enseignement en fonction des propensions héréditaires et des caractéristiques comportementales des élèves. D'autres sociétés, comme les fabricants de kits ADN à bas coût pour la mesure génétique du QI dans les écoles, d'« applications d'intelligence » ou d'autres produits des technologies éducatives basés sur la génétique, pourraient également voir dans la génomique éducative un marché potentiel (Zimmer, 2018)

2.13.2 Quel devrait être le visage de l'éducation ?

Le fait, qu'au Royaume Uni, un ministère national de l'Éducation et une commission parlementaire se soient intéressés au rôle de la génétique dans les mauvais résultats scolaires de garçons issus de la classe ouvrière devrait faire réfléchir (Underachievement in Education (2014) House of Commons Education Committee).

La notation polygénique devrait-elle jouer un rôle dans l'éducation ? Si les prédictions génétiques venaient à être acceptées comme outils de prévision des capacités futures d'un enfant dans l'éducation, de nouvelles méthodes de sélection artificielle des générations futures (Conley, Fletcher 2017) ou de ciblage des interventions pourraient voir le jour, annonçant un « eugénisme 2.0 » qui sélectionnerait les enfants « plus intelligents » (Regalado, 2017) ou introduirait des différences de traitement entre les élèves, non pas en fonction de leur dossier et de leurs besoins individuels, tels qu'ils auront été identifiés par les enseignants, mais selon ce que leurs données auront décidé.

> « Des entreprises, telles que les start-up productrices de kits d'ADN bon marché pour les tests de QI dans les écoles, d'"applications d'intelligence" ou d'autres produits génétiques de technologie électronique peuvent voir un potentiel de marché dans la génomique éducative.
>
> Des entreprises comme 23andMe exploitent le séquençage du génome humain pour lancer commercialement des services de test génétique et incarnent la tendance, dans le domaine biomédical, à donner à des entreprises privées la mainmise sur des données à caractère personnel (Stevens, 2016b). La semaine de parution de l'étude SSGAC, *23andMe* a conclu un accord de 300 millions de dollars avec le géant pharmaceutique *GlaxoSmithKline* pour analyser à des fins de recherche médicale et d'innovation pharmaceutique les données de ses 5 millions de clients au moyen de l'apprentissage-machine et de l'intelligence artificielle. La société se positionne ainsi comme un acteur à part entière de l'infrastructure et de la bioéconomie de l'industrie pharmaceutique génétique, mais aussi de l'éducation » (Zimmer, 2018).

Les critiques affirment que les éléments que nous associons à l'intelligence sont trop complexes et ambigus pour être définis de manière aussi simpliste. Les eugénistes utilisent quant à eux le nouveau concept d'intelligence dans leur campagne visant à refonder la société (Zimmer, 2018).

D'autres enfin plaident en faveur d'une réglementation pour permettre aux enfants d'atteindre l'âge adulte en ayant préservé le plus possible leur intégrité, sans avoir été perturbés par la réalité modifiée ou par des incitations comportementales reposant sur la neurotechnologie ou l'usage opaque de données et en ayant maintenu leur autonomie intacte pour pouvoir prendre leurs propres décisions dans un monde qui s'emploie de plus en plus activement à créer des incitations cachées, les « nudges », pour influencer nos comportements et nos états émotionnels à notre insu.

2.14 Les outils de protection de la vie privée dans le cadre éducatif

2.14.1 Évaluation des risques pour la vie privée

Compte tenu de l'augmentation du volume et de la vitesse de collecte et de transfert des données, et de l'accès dès à présent des élèves aux technologies de la génération suivante dans le cadre d'essais en classe, une réglementation s'impose d'urgence pour défendre les droits des enfants de manière concrète et efficace.

Les risques liés au traitement de données ne sont pas des risques isolés, limités aux premiers stades de la collecte de données ; au contraire, ils sont disséminés tout au long du processus. Certains des risques les plus importants pourraient même être transférés au futur adulte. Ce la devrait être pris en compte lors de l'analyse des risques et intégré aux informations fournies par la suite aux enfants et aux familles, au début, pendant et à l'issue du traitement de leurs données personnelles. Les personnes concernées seraient alors mieux renseignées et les responsables du traitement prendraient davantage conscience des risques et de leurs responsabilités.

Pour certains, les évaluations d'impact relatives à la protection des données des enfants doivent être spécialement adaptées à leur cas (The Danish Institute for Human Rights, 2016) et aussi expliquer correctement la notion de collecte passive de données et ses risques. Les informations invisibles concernant un enfant scolarisé (RFID, balises, assistants virtuels en classe et objets connectés à internet) peuvent former une vaste empreinte numérique constituée de données que ni les familles, ni les enfants, ni même les enseignants n'auront probablement pas fournis directement.

On peut soutenir que les évaluations des risques devraient être des documents techniques et complets comprenant un résumé en termes simples des explications de la fonctionnalité et des risques qui peuvent être extrapolées. Les évaluations de l'impact des données doivent être systématiquement intégrées dans les processus d'achat.

Une protection adéquate des données, la protection de la vie privée et l'évaluation de l'impact éthique doivent être intégrées à l'introduction de toute technologie et exigent des niveaux appropriés de connaissances et de formation. Les services partagés sont susceptibles de fournir un niveau plus élevé de compétences dignes de confiance et pourraient renforcer la confiance des écoles dans l'introduction de nouvelles technologies, ainsi que réduire la charge de travail au niveau local que les niveaux de diligence raisonnable nécessaires devraient exiger. Cela serait particulièrement utile lorsqu'il s'agit d'adopter un modèle de contrat régional, avec des normes minimales reconnues, dans le cadre de codes de pratiques réglementaires.

Les évaluations d'impact des données doivent être intégrées systématiquement aux processus de passation de marchés. Le travail législatif et les marchés publics à tous les niveaux de l'administration doivent respecter l'Observation générale n° 16 (2013) du Comité des droits de l'enfant, sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant.

La législation et les marchés publics à tous les niveaux de gouvernement doivent respecter l'Observation générale n° 16 (2013) des Nations unies sur les obligations des États concernant l'impact du secteur des entreprises sur les droits de l'enfant.

Dans le secteur public, les évaluations d'impact des données doivent être publiées – notamment dans l'éducation et lorsque le traitement concerne des données relatives à des enfants – pour que la société civile et les familles puissent surveiller les activités de traitement de données par des tiers.

2.14.2 Minimisation des données

Dans le domaine de la protection des données, le principe de minimisation des données doit être respecté au moment de la collecte pour que l'enfant ait la possibilité de minimiser l'empreinte numérique créée lors de la scolarité. Le traitement de données personnelles doit être adéquat, pertinent et non excessif au regard des finalités poursuivies, mais dans l'éducation les finalités se confondent en raison du grand nombre d'utilisateurs de données dans et en dehors du système éducatif. Il conviendrait de ne collecter que la quantité minimale de données nécessaire pour une finalité donnée.

De plus en plus, les données personnelles traitées dans le domaine de l'éducation sont conservées non seulement par l'administrateur scolaire, mais également transférées vers des lieux de stockage externes, « les établissements faisant appel à des prestataires externes pour conserver et traiter les données des élèves dans le cloud » (document de travail du groupe de travail international sur la protection des données dans le domaine des télécommunications, sur les plateformes d'apprentissage électronique, avril 2017).

L'importation et l'exportation de données s'effectuent rapidement et à grande échelle. Diverses entreprises interviennent pour l'intégration de données et leurs services en tant qu'intermédiaires pour les transferts contrôlés de données. Cela dit, la baisse du coût de stockage des données s'est accompagnée d'une hausse du volume de données collectées, ce qui accroît les possibilités de profilage longitudinal et de couplage des données.

Selon Mantelero dans les Lignes directrices sur les la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, (2017), il est reconnu que le principe de minimisation des données créée des difficultés à l'entraînement des produits de l'intelligence artificielle. Cela dit, plutôt que de rechercher les solutions qui préservent le plus la vie privée des enfants, le secteur des technologies semble souvent se contenter d'accepter qu'elle soit une contrepartie dans le marché conclu avec l'intelligence artificielle. Face aux demandes souvent insistantes d'augmentation du volume de données pour alimenter les systèmes d'intelligence artificielle, les organismes de régulation devraient éviter de confondre souhaits et nécessité. Une diversité de techniques de préservation de la vie privée peut être utilisées pour minimiser le traitement de données lors des phases d'entraînement.

Dans un blog récent sur le cadre d'audit IA de l'ICO, Binns, R (2019), chercheur associé en intelligence artificielle et Gallo, V. conseiller en politiques relatives à la technologie, examinent quelques-unes des techniques que les organisations pourraient mettre en œuvre pour respecter leurs obligations de minimisation de données lorsqu'elles adoptent des systèmes d'intelligence artificielle :

> « Certaines techniques impliquent de modifier les données d'entraînement pour limiter les possibilités de remonter jusqu'aux personnes physiques concernées tout en conservant leur utilité pour entraîner des modèles performants. Cela pourrait consister à modifier au hasard les valeurs des points de données appartenant à des individus – ce que l'on appelle « perturber » ou « ajouter du bruit » aux données – d'une manière

qui préserve certaines propriétés statistiques de ces éléments (voir par exemple l'algorithme RAPPORT)[5].

Ces types de techniques de préservation de la vie privée peuvent être appliquées aux données d'entraînement après leur collecte. Cependant, elles devraient dans la mesure du possible être appliquées avant la collecte de données personnelles, pour éviter la création d'ensembles de données personnelles importants.

Une technique analogue de préservation de la vie privée est l'apprentissage fédéré. Il permet à plusieurs parties d'entraîner des modèles en s'appuyant sur leurs propres données (modèles « locaux ») puis de combiner certains schémas identifiés par ces modèles (les « gradients ») en un modèle unique « global » plus précis, sans avoir à s'échanger des données d'entraînement. L'apprentissage fédéré est relativement récent mais il a plusieurs applications majeures parmi lesquelles l'autocorrection et les modèles de saisie intuitive sur smartphones, mais aussi pour la recherche médicale nécessitant de réaliser une analyse dans de multiples bases de données de patients.

Bien que le partage d'un gradient issu d'un modèle entraîné au niveau local présente un risque moindre pour la vie privée que le partage des données d'entraînement elles-mêmes, un gradient pourra tout de même révéler certaines informations personnelles sur les personnes dont il provient, et ce d'autant plus que le modèle est complexe et comporte beaucoup de variables à grains fins. Les responsables de traitement devront donc encore évaluer le risque de réidentification. Dans le cas de l'apprentissage fédéré, les organisations participantes seront probablement considérées comme des co-sous-traitants, même si elles n'ont pas accès aux données les unes des autres ».

Les autorités de surveillance devraient encourager les organisations et les gouvernements à défendre un cadre de droits et des valeurs qui évitent les modèles de traitement de données reposant sur une protection payante de la vie privée, lesquels sont par essence défavorables aux enfants sur le plan financier et accentueront l'exploitation disproportionnée d'enfants, de jeunes et de familles pauvres les plus marginalisés.

2.15 Mécanismes d'audit

Les écoles devraient adopter des mécanismes d'audit pour permettre aux enfants et aux familles de savoir « qui sait quoi sur moi » (Children's Commissioner (2017), UK). Ils pourraient prendre la forme de rapports annuels des écoles et de leurs intégrateurs de données, permettant d'obtenir plus facilement une vue d'ensemble des tiers qui ont eu accès aux données, du nombre de personnes physiques qui les utiliseront et des finalités poursuivies. L'affichage d'une politique générale de traitement des données sur le site Web d'un établissement n'est pas suffisant pour permettre à la famille de comprendre les utilisations qui ont été faites des données à caractère personnel de l'enfant.

2.16 Rapports d'accès et d'utilisation

La confiance dans l'utilisation des données confidentielles repose sur de nombreux facteurs parmi lesquels la compréhension des mécanismes de sécurisation et d'anonymisation des

[5] http://www.chromium.org/developers/design-documents/rappor

données, l'autonomie et le contrôle sur les données, ainsi que savoir qui y aura accès, quel est leur degré d'exactitude, qui gère et régit la base de données, comment les personnes concernées seront informées des changements et quels sont les moyens mis en œuvre pour les protéger contre les préjugés et la discrimination pendant toute la durée d'utilisation de leurs données.

Il faudrait aussi donner, de façon régulière, des informations prévisionnelles sur la conservation et la suppression des données lorsqu'un enfant quitte un établissement scolaire ou chaque fois qu'il termine un cycle de l'instruction obligatoire (maternelle, primaire, secondaire, supérieur).

Les établissements scolaires devraient publier chaque année un rapport d'audit sur la protection des données à leur niveau, comprenant un registre des données à caractère personnel diffusées à des tiers, les études d'impact sur la protection des données, les déclarations de confidentialité et toute modification importante, rendre compte de toute violation ainsi que tout rapport d'audit mené sur les sociétés commerciales ou les utilisateurs des données des élèves.

2.17 Le rôle des développeurs et de l'industrie

2.17.1 Effort disproportionné

Les orientations devraient préciser que permettre l'exercice de tous les droits prévus à l'article 9 de la Convention est une exigence de la protection des données dès la conception (*protection by design*) et non une option supplémentaire et qu'une conception qui repose sur un effort disproportionné *dès la conception* pour que les écoliers exercent leurs droits, devrait être considérée comme inéquitable et illégale. En ce moment, on rencontre des produits et des responsables de traitement qui déclarent que leur base de données de personnes concernées est trop énorme pour qu'il soit possible de communiquer avec, comme cela a été mis en évidence dans le cas de la première amende imposée par la DPA polonaise en vertu du RGPD et de la loi polonaise sur la protection des données personnelles du 10 mai 2018 qui le met en œuvre. La décision apporte des indications limitées sur l'interprétation de l'expression "effort disproportionné" au sens de l'article 14, paragraphe 5 (b), du RGPD. Nous suggérons que cela en soi doit être considéré comme un manquement au respect de l'article 25 et non comme une excuse pour priver les personnes concernées de leurs droits. C'est donc le traitement qui devrait être considéré comme illicite, et non pas soutenir l'idée que l'exclusion de la capacité d'exercer des droits est acceptable.

Ekambaranathan et Zhao (2019) ont constaté que des concepteurs de technologies axées sur la famille estiment en grande partie qu'il est contraire à l'éthique de recueillir et de vendre les données sur les enfants comme un produit (5/5 personnes interrogées et 71/81 répondants au sondage). Certains développeurs refuseraient également l'accès aux données de leurs utilisateurs par des tiers en échange de gains monétaires pour des raisons morales et de responsabilité. Toutefois, on constate encore souvent que les pratiques de protection de la confidentialité des données sont insuffisantes dans ces technologies qui s'adressent aux enfants.

2.17.2 Bibliothèques de développeurs tiers

Dans le développement de logiciels, la réutilisation des bibliothèques de codes existantes mises en place par d'autres est acceptée comme pratique essentielle permettant aux communautés de développement de réduire les frais généraux et de faire un meilleur usage des ressources existantes (comme l'informatique dans les nuages). Cependant, l'utilisation de ces bibliothèques de code signifie souvent que le développeur ne voit pas ou ne comprend pas pleinement l'étendue des leurs effets et de leurs interactions avec les siennes. Cela peut être pour des raisons innocentes - par exemple, les bibliothèques de codes sont souvent créées par des développeurs dans des pays qui n'ont pas de cadres de protection des données, et qui par conséquent ne connaissent pas les cadres légaux du CdE ou de l'UE. - ou moins innocentes, par exemple les bibliothèques de codes créées par des développeurs financés par l'adTech. Cela peut signifier que le logiciel peut distribuer des données d'utilisateurs à des tiers sans que le développeur en ait pleinement conscience.

> « Les bibliothèques tierces sont de plus en plus répandues dans les applications d'aujourd'hui. L'un des principaux facteurs en est que les développeurs comptent sur la publicité ciblée pour générer des revenus qui à son tour utilise des bibliothèques tierces pour recueillir des données ciblées. De plus, cela simplifie également le développement, apporte des fonctionnalités accrues et peut être plus sûr que des modules logiciels propriétaires. Cependant, ces bibliothèques sont autorisées à collecter des données sensibles, ont fréquemment accès à la géolocalisation, au journal des appels, à l'historique du navigateur et aux informations de contact pour les besoins de publicités ciblées, même si ce n'était pas la fonctionnalité prévue. » (Zhao et al, 2019 à venir)

Il n'y à qu'à regarder le Software Developer Kit de Facebook, par exemple, et comment la dont les applications android partagent des données avec Facebook (même sans compte Facebook). (Privacy International, 2019)

> « Les développeurs d'applications partagent des données avec Facebook par le biais du kit de développement logiciel (SDK) de Facebook, un ensemble d'outils de développement logiciel qui peuvent être utilisés pour développer des applications pour un système d'exploitation spécifique. Le SDK pour Android de Facebook permet aux développeurs d'applications d'intégrer leurs applications à la plate-forme Facebook et contient un certain nombre de composants de base : Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links. Par exemple : utiliser le SDK de Facebook permet l'authentification basée sur "Login with Facebook", avec lequel les utilisateurs peuvent se connecter en utilisant un numéro de téléphone d'adresse e-mail avec leur mot de passe Facebook. Le SDK de Facebook offre également Analytics (données, tendances et aperçu agrégé de l'audience sur les personnes qui interagissent avec l'application), ainsi que Ads et la possiblilité de lire et d'écrire sur l'API Graph de Facebook. »

Les conditions générales relatives aux produits suggèrent souvent que le consentement est une base nécessaire au traitement des données, non pas en raison des finalités dans lesquelles l'école utilisera les données personnelles d'un écolier, mais de la manière dont le produit et ses fournisseurs l'utiliseront. Cependant, lorsque l'on accepte que le consentement soit un fondement légal du traitement des données, il ne peut être donné librement et ne peut donc pas être légal en milieu scolaire pour des tâches courantes en raison du déséquilibre de

pouvoir dans les relations entre les enfants, les familles et le personnel scolaire - et avec seulement une relation indirecte entre l'enfant et les propriétaires des produits. Cela signifie que les attentes des tiers quant à ce qu'ils sont autorisés à faire doivent changer.

2.17.3 Base licite pour le traitement

Selon les Lignes directrices 2/2019 du Comité européen pour la protection des données relatives au traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées (octobre 2019) dans la plupart des cas, un utilisateur conclut un contrat pour utiliser un service existant. Si la possibilité d'apporter des améliorations et des modifications à un service peut être systématiquement incluse dans les clauses contractuelles, un tel traitement ne peut généralement pas être considéré comme objectivement nécessaire à l'exécution du contrat avec l'utilisateur, et c'est particulièrement vrai dans l'environnement scolaire où il n'existe aucune relation directe entre un enfant et une entreprise.

En ce qui concerne le traitement de catégories particulières de données à caractère personnel sensibles, dans les lignes directrices sur le consentement, le groupe de travail a également observé que l'article 9, paragraphe 2, du TPIR ne reconnaît pas que "nécessaire à l'exécution d'un contrat" constitue une exception à l'interdiction générale du traitement de catégories particulières de données. Il s'ensuit donc que "nécessaire à la performance d'un produit" ne constitue pas un motif substantiel pour demander une exemption à la législation sur la protection des données. En d'autres termes, les écoles, les entreprises et les concepteurs de produits ne devraient pas s'attendre à être exemptés de mesures d'application, simplement parce que le produit fonctionne d'une manière qui ne respecte pas les droits.

Si la majorité des services et outils de traitement des données mis à la disposition des écoles aujourd'hui ne répondent pas aux normes élevées de la loi ainsi qu'aux attentes éthiques quant à ce qui doit être fait avec les données personnelles des enfants, alors une nouvelle approche est nécessaire.

Même les États-Unis, qui ont traditionnellement résisté à la législation sur la protection de la vie privée, sont en train de changer leur fusil d'épaule. Au moment de la rédaction du présent document, la Federal Trade Commission des États-Unis a ouvert une consultation sur la mise en œuvre de la Children's Online Privacy Protection Rule (COPPA). On y demande si l'exigence relative au consentement a permis de protéger efficacement la vie privée et la sécurité des enfants en ligne. Compte tenu de la quantité de données sur les enfants en Europe collectées ou traitées par les entreprises américaines, la consultation COPPA doit être suivie de près.

Des orientations à l'intention des développeurs dans le contexte de l'edTech sont nécessaires

Un instrument pour le traitement des données relatives aux enfants dans le secteur de l'éducation devrait fixer des normes élevées par défaut qui répondent à des niveaux de qualité acceptables et à l'État de droit. Cela doit s'appuyer sur une combinaison de lignes directrices sectorielles, de codes de pratique statutaires et d'une application plus spécifique au secteur par les autorités réglementaires.

Ces normes peuvent être définies dans des codes de bonnes pratiques et il est impératif que leur rédaction fasse l'objet d'une large coopération avec les concepteurs et l'industrie, les praticiens de l'éducation, les milieux universitaires, les organisations représentant les enseignants et les familles, et la société civile.

3

Qui encadrera l'avenir ?

Les décideurs politiques ne devraient pas avoir peur de la question de savoir dans quelle mesure la croissance rapide de la technologie destinée aux écoliers et l'automatisation de leur administration scolaire sont dans l'intérêt supérieur de l'enfant.

> "Dans l'ensemble, les preuves corrélationnelles et expérimentales n'offrent pas de preuves convaincantes de l'impact général de la technologie numérique sur les résultats d'apprentissage. Cela ne veut pas dire qu'il ne vaut pas la peine d'investir dans l'utilisation de la technologie pour améliorer l'apprentissage. Mais cela devrait nous encourager à être prudents face aux solutions technologiques aux défis de l'éducation. Il faut bien réfléchir pour utiliser la technologie au mieux." (Higgins, S., Xiao, Z. et Katsipataki, M., 2012)

Il est tout aussi sage de faire preuve de prudence à l'égard des allégations de marketing d'entreprises dans toutes les technologies émergentes.

> "Ce que l'on entend lorsque les organisations appliquent l'IA à un problème est impossible à distinguer de l'application de l'informatique, de la statistique ou même de la preuve. L'usage de l'expression est devenu tellement comiquement ambigu et général que c'est presque comme dire que pour résoudre un problème d'infrastructure urbaine, il faut " utiliser des outils électriques "...
>
> Ben Green aborde ces questions dans son récent ouvrage, The Smart Enough City, qui souligne la nécessité de considérer la technologie comme un outil parmi tant d'autres qui pourraient être utilisés pour parvenir à une fin complexe et négociée au niveau social. L'accent devrait être mis sur l'élimination des "lunettes de protection technologiques" pour identifier des problèmes, des défis et des besoins, et pour ne pas avoir peur de découvrir que d'autres options politiques sont supérieures à un investissement technologique". (Veale, M. 2019)

La Convention 108 a pour objet d'assurer sur le territoire de chaque Partie, pour toute personne, quelle que soit sa nationalité ou sa résidence, le respect de ses droits et libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données"). Le respect de sa "vie privée et familiale, de son domicile et de sa correspondance, sous réserve de certaines restrictions qui sont "conformes à la loi" et "nécessaires dans une société démocratique", signifie le droit de ne pas être inquiété.

Ce rapport devrait aider les décideurs politiques à comprendre la nécessité de passer d'une culture de conformité à une culture de respect des droits dans le traitement des données

relatives à l'éducation. Les recommandations doivent reconnaître l'autonomie professionnelle, et également garantir la prescription supplémentaire de normes élevées attendues.

Si nous maintenons le cap actuel et son orientation en ce qui concerne le traitement des données dans l'éducation, l'équilibre des pouvoirs sera à jamais en faveur des géants de l'informatique. Ce sont eux qui détermineront l'offre, la sécurité et la mémoire institutionnelle des systèmes éducatifs publics et leurs effets sur des millions d'enfants chaque jour.

La base de connaissances que l'État et l'entreprise ont des vies individuelles stockées dans les systèmes de gestion de l'information de l'école, dans des milliers d'applications et de systèmes de plate-forme suivra un enfant sans entrave à travers chaque étape de son éducation vers l'emploi. Le personnel de l'école s'appuiera sur de vastes volumes de données du passé, craignant de plus en plus que son jugement humain ne soit moins valable que celui d'une décision prise à l'aide d'une machine. Les prédictions prédétermineront le programme d'études et les choix de vie des enfants à un âge de plus en plus précoce.

Les différences génétiques entre les enfants seront utilisées pour les classer dès la naissance et appliquer les interventions éducatives différemment ou pas du tout. La sélection du lieu de scolarité d'un enfant, qui façonne une grande partie de sa vie aujourd'hui, pourrait passer à une sélection dès l'utérus fondée sur les caractéristiques cognitives qui seront considérées comme souhaitables et d'autres comme des anomalies, ou sur la question de savoir si un enfant ayant des besoins particuliers aura une place dans le monde.

Ou encore, les décideurs peuvent donner la priorité aux moyens d'appliquer et de mettre en pratique les valeurs des droits de l'homme qui sous-tendent la Convention.

Si cette génération ne doit pas être freinée par le poids des données de son passé, mais avoir les libertés nécessaires pour le façonner, les enfants doivent pouvoir exercer leur droit à l'éducation d'une manière qui ne soit pas préjudiciable à leur propre avenir et à leur avenir collectif. L'équilibre des pouvoirs entre les organisations et les institutions par rapport à celui de l'enfant et de la famille doit être modifié d'urgence,

"Les yeux de toutes les générations futures sont sur vous. Et si vous choisissez de nous décevoir, je vous le dis, nous ne vous le pardonnerons jamais." Greta Thunberg, Sommet des Nations Unies sur le climat, New York, 23 septembre 2019.

4 Définitions

1. Aux fins de la présente recommandation, on entend par

a. "Données à caractère personnel" : toute information concernant une personne physique identifiée ou identifiable ("personne concernée").

b. Par "données sensibles", on entend les données à caractère personnel sur lesquelles une personne peut s'attendre à de la confidentialité, telles que les marqueurs de comportement qui indiquent un comportement violent mais qui n'ont pas été déterminés par un tribunal et qui ne sont donc pas techniquement des "condamnations pénales" ou un revenu familial, mais qui ne relèvent pas nécessairement des définitions des données de catégorie spéciale selon le droit sur la protection des données.

c. "Données de catégorie spéciale" a la même signification que l'article 6 de la Convention modernisée 108+. « Le traitement : de données génétiques ; de données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes ; de données biométriques identifiant un individu de façon uniqu; de données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle ; n'est autorisé qu'à la condition que des garanties appropriées, venant compléter celles de la présente Convention, soient prévues par la loi. Ces garanties doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination. »

d. "Traitement" : toute opération ou ensemble d'opérations effectués partiellement ou totalement à l'aide de procédés automatisés, et appliqués à des données à caractère personnel, telles que l'enregistrement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, l'appariement ou l'interconnexion, ainsi que l'effacement ou la destruction.

e. "Profil" (n) désigne un ensemble de données qui caractérise une catégorie d'individus ou de comportements et qui est destiné à être appliqué à un individu ou à un groupe d'individus

f. Par "profilage", est une technique de traitement automatisé des données qui consiste à appliquer un « profil » à une personne physique, de l'insérer dans une catégorie ou de faire correspondre des attributs à ce modèle, notamment pour prendre des décisions concernant le sujet, ou pour intervenir, ou pour analyser ou prévoir leurs préférences, comportements et attitudes personnelles. Celles-ci peuvent être créées à partir de données que la personne concernée fournit ou qui sont opaques pour elle, telles que des données d'interaction provenant de l'utilisation d'une plate-forme, qui sont envoyées de l'appareil à l'entreprise, mais que les utilisateurs ne voient pas.

g. Par "service de la société de l'information", on entend tout service, normalement fourni contre rémunération, à distance, par voie électronique et répondant à la même définition que l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535.

h. "Responsable de traitement" comprend la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou avec la collaboration d'autres, détermine les finalités et les moyens de la collecte et du traitement des données à caractère personnel.

i. "sous-traitant" : désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

j. Les " contrats d'achat au clic " s'entendent des ententes sur les modalités et conditions que l'entreprise ou le vendeur du produit ne permet pas à l'école ou à l'utilisateur de modifier. Ils se présentent sous la forme d'un paquet que l'école ne peut qu'accepter ou refuser, et le refus signifiera qu'elle ne pourra plus continuer à utiliser le produit ou la plate-forme.

k. Par " transmission en chaine ", on entend une série de transactions qui sont reliées entre elles et qui permettent à plusieurs tiers d'extraire ou de recevoir des données de la partie précédente dans la chaîne. L'image est celle d'une chaîne de fleurs enchaînée que les enfants peuvent généralement réunir, du fait de son nom anglais « daisy-chain ».

5 Remerciements

L'auteure tient à exprimer ses remerciements aux très nombreuses personnes qui ont partagé leurs propres travaux et idées à l'appui de ces travaux, en particulier à ceux qui ont le plus contribué de façon significative sur leurs sujets spécialisés, le Dr Ben Williamson, Chancellor's Fellow au Centre for Research in Digital Education et au Edinburgh Futures Institute et le Dr Jun Zhao, Senior Research Fellow au Département des sciences informatiques, Université Oxford.

6 Références

ftenposten (2020) Datatilsynet undersøker om det er lovlig å bruke Google i skolen. The Norwegian Data Protection Authority has announced it is investigating whether it is legal to use Google in schools. (accessed February 21, 2020) https://www.aftenposten.no/norge/i/pLvba6/datatilsynet-undersoeker-om-det-er-lovlig-aa-bruke-google-i-skolen

Avis 2/2009 du groupe de travail Article 29 sur la protection des données personnelles des enfants (Recommandations générales et cas particulier : les établissements scolaires) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

Against Borders for Children (2016) https://www.schoolsabc.net/2016/09/letter-justine-greening/ (consulté en août 2019)

Alim, F., et al (2017). (Electronic Frontier Foundation) Spying on Students: School-Issued Devices and Student Privacy, https://www.eff.org/files/ 2017/04/13/student-privacy-report.pdf

Andrejevic, M. and Selwyn, N. (2019) Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, DOI: 10.1080/17439884.2020.1686014

Anderson, R., Brown, I., Clayton, R., Dowty, T., Korff, D. et Munro, E., (2009), Children's Databases - Safety and Privacy. Rapport pour le Commissaire à l'information du Royaume-Uni. (accessed October 2019) https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

Ars Technica, Cox, K. (2019) 50 states and territories launch massive joint probe into Google https://arstechnica.com/tech-policy/2019/09/50-states-and-territories-launch-massive-joint-probe-into-google/

Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch (2019) https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf

Balderas (New Mexico) vs Google LLC, 2020 https://cdn.vox-cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf (accessed February 24, 2020)

The Berkman Centre for Internet And Society at Harvard (2008) Enhancing Child Safety and Online Technologies report https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (consulté en novembre 2017)

Binns et autres () Measuring third party tracker power across web and mobile. WebSci'18. https://ora.ox.ac.uk/objects/uuid:86310ed1−762e−4037−a4d2−80568c5ee7c4 (2018) (consulté en septembre 2019)

Binns et autres (2018) Third Party Tracking in the Mobile Ecosystem. TOIT. https://arxiv.org/abs/1804.03603 (2018) (consulté en septembre 2019)

Big Brother Watch (2014), rapport : Biometrics in Schools https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf (consulté le 12 novembre 2017) et Classroom Monitoring ; Another Brick in the Wall (2016) https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/11/Classroom-Management-Software-Another-Brick-in-the-Wall.pdf (consulté le 12 novembre 2017)

Binns, R. et autres 2018. "It's Reducing a Human Being to a Percentage" ; Perceptions of Justice in Algorithmic Decisions. ArXiv:1801.10408 (Cs), 1–14. https://doi.org/10.1145/3173574.3173951.

Booth, P. (2017) Age Verification as the new cookie law? http://www.infiniteideasmachine.com/2017/08/age-verification-as-the-new-cookie-law/

Bowles, N., (2019) New York Times. Silicon Valley Came to Kansas Schools. That Started a Rebellion. https://www.nytimes.com/2019/04/21/technology/silicon-valley-kansas-schools.html

Boyd, D. et Crawford, K. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. 15(5) Information, Communication, & Society 662–679

Breyer c. Allemagne, http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN (consulté le 1er novembre 2017)

Bridge International (consulté en septembre 2019) https://www.bridgeinternationalacademies.com/supporting/teacher-tools/

Cardiff Data Justice Lab, Data Scores as Governance Report (2018) https://datajusticelab.org/data-scores-as-governance/

Campaign for a Commercial Free Childhood (2015) https://commercialfreechildhood.org/3-million-teachers-mcdonalds-were-not-lovin-it/

Carter, P., Laurie, G., Dixon-Woods, M. (2015) The social licence for research: why care.data ran into trouble, J Med Ethics 2015;41:404-409 doi:10.1136/medethics-2014-102374

The Children's Commissioner, (2017) (England) Growing Up Digital https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

The Chromium Projects: Rappor (Randomized Aggregatable Privacy Preserving Ordinal Responses) http://www.chromium.org/developers/design-documents/rappor

Classcharts https://www.classcharts.com/

Class Dojo What The New York Times Got Wrong.https://web.archive.org/web/20191113122736/https://www.classdojo.com/en-gb/nyt/

CNIL decision on facial recognition (lycée les Eucalyptus à Nice et lycée Ampère à Marseille) (2019) Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa positionhttps://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

Conley, D. and Fletcher (2017), The Genome Factor - What the Social Genomics Revolution Reveals about Ourselves, Our History, and the Future (2017) ISBN : 9780691164748 Princeton University Press

Stratégie du Conseil de l'Europe pour les droits de l'enfant 2016-2021, https://rm.coe.int/168066cff8 (consultée le 1er novembre 2017) par. 30 CM/Rec (2013) 2. 1.2. Lutte contre la discrimination

Conseil de l'Europe 2017. Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a

Conseil de l'Europe, Comité d'experts MSI-AUT sur la dimension droits de l'homme des traitements automatisés de données et différentes formes d'intelligence artificielle (travaux en cours) https://www.coe.int/en/web/freedom-expression/msi-aut

Conseil de l'Europe. Etude DG1(2019)05 Responsabilité et IA (rapporteur Yeung, 2019), préparée par le Comité d'experts MSI-AUT sur la dimension droits de l'homme des traitements automatisés de données et différentes formes d'intelligence artificielle : https://rm.coe.int/responsability-and-ai-fr/168097d9c6

Conseil de l'Europe (2017). Décoder l'intelligence artificielle – 10 mesures pour protéger les droits de l'homme - https://rm.coe.int/decoder-l-intelligence-artificielle-10-mesures-pour-proteger-les-droit/168094b6e2

Recommandation CM/Rec (2018)7 du Comité des Ministres aux États membres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique (adoptée par le Comité des Ministres le 4 juillet 2018 lors de la 1321e réunion des Délégués des Ministres) https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7

Davidson, C. (2017) The New Education: how to revolutionise the university to prepare students for a world in flux (Basic Books)

Department for Education, (UK) (2019) Special educational needs: an analysis and summary of data sources
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804374/Special_educational_needs_May_19.pdf

The Danish Institute for Human Rights. 2016. Human rights impact assessment guidance and toolbox (The Danish Institute for Human Rights) https://www.humanrights.dk/business/tools/human-rights-impact-assessment-guidance-and-toolbox

defenddigitalme, (2016) Timeline of school census use for immigration enforcement purposes https://defenddigitalme.com/timeline-school-census/ and https://en.wikipedia.org/wiki/England_school_census

defenddigitalme, (2016) Distribution of national pupil records to commercial companies, charities, think tanks and the press https://defenddigitalme.com/faqs/, base sur https://www.gov.uk/government/publications/dfe-external-data-shares

Denham, E. The Information Commissioner, ICO, 2017 sur “innovation”, findings on Google DeepMind and Royal Free https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Dowty, T., Korff, D. (2009), Protecting the Virtual Child: the law and children’s consent to sharing personal data https://www.nuffieldfoundation.org/sharing-childrens-personal-data

Durkin, E. (2019) The Guardian, New York school district's facial recognition system sparks privacy fears https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears

EdTech Innovation testbed, Nesta (2019) https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/ permanent record at https://web.archive.org/web/20191015162357/https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/

Education Foundation (2013) Facebook Guide for Educators https://www.ednfoundation.org/wp-content/uploads/Facebookguideforeducators.pdf Criticised by civil society in England as promotion

The Economist (2012), Learning new Lessons www.economist.com/news/international/21568738-online-courses-are-transforming-higher-education-creating-new-opportunities-best (consulté en novembre 2017)

Elliot, M., Purdam, K., Mackey, (2013) E., Data Horizons: New forms of Data for Social Research, School of Social Sciences, The University Of Manchester, 2013.) http://hummedia.manchester.ac.uk/institutes/cmist/archive-publications/reports/2013-05-Data_Horizons_Report.pdf (consulté le 11 novembre 2017)

ESCR-Net (2018) Civil society denounces for-profit ICT4D network of schools (consulté en août 2019) https://www.escr-net.org/news/2018/civil-society-denounces-profit-ict4d-network-schools and their list of Bridge International Academies Investors http://globalinitiative-escr.org/wp-content/uploads/2018/02/List-of-BIA-investors.pdf

European Union Agency for Fundamental Rights (2019) FRA has collected information on AI-related policy initiatives in EU Member States in the period 2016-2019. The collection currently includes about 180 initiatives. https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights/ai-policy-initiatives

European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

Evening Standard (2012) The CCTV in your child's school toilet: More than 200 admit using cameras in loos and changing rooms, https://www.standard.co.uk/news/education/the-cctv-in-your-childs-school-toilet-more-than-200-admit-using-cameras-in-loos-and-changing-rooms-8129753.html

Fichter, A., Der Republik (2019) Der Spion im Schulzimmer https://www.republik.ch/2019/07/02/der-spion-im-schulzimmer

Ferreira,J., CEO, Knewton (2012) https://www.youtube.com/watch?v=Lr7Z7ysDluQ Source : chaîne YouTube de l'Office pour les technologies éducatives du département de l'Education des États-Unis

FOCIAI https://fociai.com/

Forbes (2014) Facebook Manipulated User News Feeds To Create Emotional Responses (consulté en septembre 2019) https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/

Google Family Link app https://families.google.com/familylink et référence au Blog: Google Family Link for Under 13s: children's privacy friend or faux? Persson, J.(2017) http://jenpersson.com/google-family-link/

Greene,T. (2018) China's facial recognition AI has a new target: Students https://thenextweb.com/artificial-intelligence/2018/05/18/chinas-orwellian-surveillance-state-turns-its-ai-powered-gaze-on-students/

Gazette, The (2018), Parents reassured after live footage from Blackpool schools' CCTV cameras was 'hosted on US website https://www.blackpoolgazette.co.uk/education/parents-reassured-after- live-footage-from-blackpool-schools-cctv-cameras-was-hosted-on-us-website-1-9036288

Lignes directrices pour une justice adaptée aux enfants, adoptées par le Comité des Ministres du Conseil de l'Europe le 17 novembre 2010 consultées en septembre 2019 https://rm.coe.int/16804b2cf3 (voir également la Résolution 2010(2014) de l'Assemblée parlementaire « Une justice pénale des mineurs adaptée aux enfants: de la rhétorique à la réalité » et les orientations du Comité européen de coopération juridique visant à promouvoir et soutenir la mise en œuvre des Lignes directrices pour une justice adaptée aux enfants (CDCJ(2014)15)).

Hand, B (2019) Biometrics In Schools: 4 Ways Biometric Data Can Be Used To Enhance Learning https://elearningindustry.com/biometrics-in-schools-data-enhance-learning-4-ways

Herold, B. (2018) Education Week, To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts, https://www.edweek.org/ew/articles/2018/07/26/to-stop-school-shootings-fla-will-merge.html

Higgins, S., Xiao, Z. and Katsipataki, M. (2012) The Impact of Digital Technology on Learning: A Summary for the Education Endowment Foundation. School of Education, Durham University

Hildebrandt, M. (2016) Smart Technologies and the End(s) of Law : Novel Entanglements of Law and Technology (Edward Elgar Publishing).(chapitre 9)

HLEG-AI Policy and Investment Recommendations for Trustworthy Artificial Intelligence (consulté le 1er juillet 2019) (publié le 26 juin 2019) https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (copie permanente https://defenddigitalme.com/wp-content/uploads/2019/07/AIHLEGPolicyandInvestmentRecommendationspdf.pdf) (Following an open selection process, the Commission appointed 52 experts to a High-Level Expert Group on Artificial Intelligence, comprising representatives from academia, civil society, as well as industry.)

IB Times, (2017) 77 Million Accounts, Students, Teachers, Parents Stolen, de AJ Dellinger, http://www.ibtimes.com/edmodo-hacked-77-million-accounts-students-teachers-parents-stolen-education-social-2540073 (consulté le 1er novembre 2017)

ICDPPC, Résolution sur les plateformes d'apprentissage électronique (2018) (40e Conférence internationale des Commissaires à la protection des données et de la vie privée - https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

Initiative globale de l'IEEE sur les considérations éthiques liées à l'intelligence artificielle et aux systèmes autonomes. 2016. Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems, Version 1. IEEE, 2016. http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.IEEE

IEEE, (2019) Computer Vision for Attendance and Emotion Analysis in School Settings https://ieeexplore.ieee.org/document/8666488

India Today, juillet (2019), Delhi school becomes first ever to provide live CCTV video feed to parents https://www.indiatoday.in/education-today/news/story/delhi-school-becomes-first-to-provide-live-cctv-video-feed-to-parents-cm-arvind-kejriwal-1564401-2019-07-08

Document de travail du groupe de travail international sur la protection des données dans le domaine des télécommunications, sur les plateformes d'apprentissage électronique. (2017) https://epic.org/IWG/workingpapers/e-learning-platforms.pdf

i-news (2017) Ofsted to 'snoop' on parents' and pupils' social media https://inews.co.uk/news/education/teachers-given-less-days-training-safeguarding/

IPC Ontario GPEN Sweep Report (2017) https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt.pdf (consulté en août 2019)

Jing, M. (2019) BrainCo CEO says his 'mind-reading' tech is here to improve concentration, not surveillance https://www.scmp.com/tech/innovation/article/3008439/brainco-ceo-says-his-mind-reading-tech-here-improve-concentration

Jugement de la Cour suprême (2016) UKSC51 https://www.supremecourt.uk/cases/docs/uksc-2015-0216-judgment.pdf

Jugement de la Cour de Justice de l'Union européenne dans l'affaire Bara (C-201/14) http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf (octobre 2015)

King, P. Biometrics in Schools https://pippaking.blogspot.com/

The Law Society, (Royaume Uni), Event Report: Artificial Intelligence, Big Data and the Rule of Law, (consulté le 12 novembre 2017) https://www.biicl.org/documents/1798_ai_event_-_final_report_15_11_2017_002.pdf

Blog sur l'analytique de l'apprentissage consacré à l'apprentissage civil, géré par le vice-président de l'union des étudiants de l'Université de Northumbria chargé de la communication (août 2017) https://www.mynsu.co.uk/blogs/blog/tallykerr/2017/08/02/Learning-Analytics/ (consulté le 11 novembre 2017)

Livingstone, S. (2016) The GDPR: Using evidence to unpack the implications for children online, blog du LSE Media Policy Project, London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/ (consulté le 1er novembre 2017)

Livingstone, S. (2017) Online challenges to children's privacy, protection and participation: what can we expect from the GDPR?, LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2017/02/09/online-challenges-to-childrens-privacy-protection-and-participation-what-can-we-expect-from-the-gdpr/ (consulté le 1er novembre 2017)

Lievens, E., (2016) Wanted: evidence base to underpin a children's rights-based implementation of the GDPR LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based-implementation-of-the-gdpr/ (consulté le 1er novembre 2017)

Lupton, D. et Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. New Media & Society Vol. 19, Iss. 5, 780-794 ;

Grunwald, A. (2018): AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Évaluation : Computer Law & Security Review (2018), https://doi.org/10.1016/j.clsr.2018.05.017.

Grunwald, , A. (2017): Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33(5) Computer Law & Sec. Rev. 584-602.

Mantelero A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Assessment. Computer Law & Security Review (2018), https://doi.org/10.1016/j.clsr.2018.05.017.

Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33(5) Computer Law & Sec. Rev. 584-602.

Mats, S. (2018) WIRED, Psychological microtargeting could actually save politics https://www.wired.co.uk/article/psychological-microtargeting-cambridge-analytica-facebook

McKown et autres (2017) Key Design Principles for Direct Assessments of SEL: Lessons Learned from the First Design Challenge (social and emotional learning) https://measuringsel.casel.org/wp-content/uploads/2017/09/AWG-Design-Challenge-Direct-Assessments-of-SEL.pdf

Monahan, T. and Torres, R (2009) Schools Under Surveillance: Cultures of Control in Public Education (Critical Issues in Crime and Society) Rutgers University Press, ISBN: 081354680X

Mundie, C. (2014) Privacy Pragmatism, Focus on Data Use not Collection, Foreign Affairs, March/April (2014), Volume 93

Nemorin,S. (2017) University College London, Affective capture in digital school spaces and the modulation of student subjectivities. Information, Espace Society, ISSN 1755-458 http://eprints.lse.ac.uk/83298/

Nemorin,S. Selwyn, N. (2018) Everyday Schooling in the Digital Age: High School, High tech? https://www.routledge.com/Everyday-Schooling-in-the-Digital-Age-High-School-High-Tech-1st-Edition/Selwyn-Nemorin-Bulfin-Johnson/p/book/9781138069374

The Norwegian Consumer Council report #WatchOut (2017) https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children and #ToyFail https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/ (accessed 1 November 20170

The Norwegian Data Protection Authority. 2018. Artificial Intelligence and Privacy Report. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

Nyst, C. (UNICEF) (2018) Principles for Children's Online Privacy and Free Expression Industry Toolkit
https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

OCDE (2018) The OECD Study on Social and Emotional Skills (10-15 year old children) http://www.oecd.org/education/ceri/thestudyonsocialandemotionalskills.htm

Pappano, L. (2012) New York Times, The Year of the MOOC
http://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html

Paterson, L. et Grant, L. (2010) The Royal Academy of Engineering, Privacy and Prejudice: Young people's views on Electronic Patient Records.(dossier permanent http://http://jenpersson.com/wp-content/uploads/2016/08/Privacy_and_Prejudice.pdf (page 40)

Patterson.J. (2019) CEO Gaggle, Education Week,
https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html (consulté en septembre 2019)

Parent Coalition for Student Privacy : de 2012 à 2014, des citoyens se sont élevés contre les projets de certains États et districts de divulguer les données à caractère personnel des étudiants à une société créée par la Fondation Gates, inBloom Inc. https://www.studentprivacymatters.org/background-of-inbloom/ (accessed November 2017)

Parent Coalition for Student Privacy, McPherson KS students join the rebellion vs Summit and depersonalized learning and win the right to opt out (2019) https://www.studentprivacymatters.org/kansas-students-join-the-rebellion-vs-summit-and-depersonalized-learning/

Paul, J. (2017) The Rise of Biometrics in Education https://www.d2l.com/en-eu/blog/rise-biometrics-education/

Pegg, McIntyre (2018) The Guardian, https://www.theguardian.com/society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality (accessed February 2020)

Plomin, R., Stumm, S. (2018) The new genetics of intelligence https://www.nature.com/articles/nrg.2017.104

Pluim, C. et Gard, M. (2016) Physical education's grand convergence: *Fitnessgram*®, big-data and the digital commerce of children's health https://www.tandfonline.com/doi/abs/10.1080/17508487.2016.1194303

Commissaire à la protection des données polonais, première décision et amende en vertu du règlement général sur la protection des données https://uodo.gov.pl/en/553/1009 concernant l'absence de traitement loyal des données par les personnes concernées, en invoquant des efforts disproportionnés, ainsi que le traitement illicite à grande échelle de données à caractère personnel collectées auprès de sources accessibles au public.

Porter, G. (2010) Mobility, surveillance and control of children and young people in the everyday: perspectives from sub-Saharan Africa https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/sub-saharan and https://www.theimpactinitiative.net/project/impact-mobile-phones-young-peoples-lives-and-life-chances-sub-saharan-africa-three-country

Powles, J. (2018), University of Western Australia. The Seductive Diversion of 'Solving' Bias in Artificial Intelligence, https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Privacy International (2019) Report: Your Mental Health for Sale https://privacyinternational.org/campaigns/your-mental-health-sale

Privacy International Report — How Apps on Android Share Data with Facebook (even if you don't have a Facebook account. (2018) https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

Protection of Freedoms Act 2012 (England and Wales) Biometric data protection for children in schools (Chapter 2) http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2/enacted

Regan, P and Steeves, V. (2019) Education, privacy, and big data algorithms: Taking the persons out of personalized learning https://doi.org/10.5210/fm.v24i11.10094

Rouvroy, A. 2016. Des données et des hommes : droits et libertés fondamentaux dans un monde de données
massives https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020.

Sabates, R. et autres (2010) School Drop out: Patterns, Causes, Changes and Policies https://unesdoc.unesco.org/ark:/48 223/pf0000190771

Savirimuthu, J., (2016) EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids? LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/ (consulté en août 2019)

Schuijer, J., (2017) Transcranial Electrical Stimulation to Enhance Cognitive Performance of Healthy Minors: A Complex Governance Challenge https://www.frontiersin.org/articles/10.3389/fnhum.2017.00142/full

Selwyn, N., (2019) Monash University, Australia, What are the acceptable limits of school data? The case of the Florida 'school safety' database https://data-smart-schools.net/2019/06/05/what-are-the-acceptable-limits-of-school-data-the-case-of-the-florida-school-safety-database/

Selwyn, N. (2015). Data entry: towards the critical study of digital data and education. Learning, Media and Technology, 40(1), 64-82.

Selwyn, N. (2016) 'Is Technology Good For Education ?' (Polity). Chapter 4, 'Making Education More Calculable' (discussing the 'data' turn' in education' / Chapter 5, 'Making Education more Commercial' (discussing Big Tech).

Smith. S, (2016) Shadow of the smart machine: Will machine learning end? Nesta 2016 https://www.nesta.org.uk/blog/shadow-smart-machine-will-machine-learning-end (consulté en septembre 2019)

Southgate et autres (2019) Artificial Intelligence and Emerging Technologies in Schools, commande du gouvernement australien https://docs-edu.govcms.gov.au/system/files/doc/other/aiet_final_report_august_2019.pdf

The State of Data survey of parents' views on technology and data in UK schools. Survation (2018) https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

Steeves, V., Professeur agrégé, Département de criminologie, Faculté des sciences sociales. The Interdisciplinary Research Laboratory on the Rights of the Child (IRLRC) and Young Canadians in a Wired World, Phase III: Life Online https://mediasmarts.ca/ycww/life-online

Stoilova, M., Livingstone, S. et Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age, http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-

data-and-privacy-online-report-for-web.pdf
And what do children ask for? http://www.lse.ac.uk/my-privacy-uk/what-do-children-ask-for

Sujon, Z. (2019) Disruptive Play or Platform Colonialism? The Contradictory Dynamics of Google Expeditions and Educational Virtual Reality. Digital Culture and Education, 11 (1). ISSN 1836-8301

Swedish DPA decision on Facial recognition used for attendance registration in schools BBC ref https://www.bbc.co.uk/news/technology-49489154 décision originale Teaching as a Design Science, Diana Laurillard, Routledge, 2012, p. 4 (traduction en anglais à venir de l'autorité de protection des données)

Taylor, E. (2015) Discussion sur la conformité https://www.youtube.com/watch?v=QHLh485SJXc au panel du CPDP, Bentham goes to school : surveillance and student privacy in the classroom.

Taylor, E. et Rooney, T. (2017) Surveillance Futures: Social and ethical implications of new technologies for children and young people, https://www.taylorfrancis.com/books/e/9781315611402

Tucker, W and Vance, A. (2016) School Surveillance: The Consequences for Equity and Privacy. Education Leaders Report (4), National Association of State Boards of Education,. http:// www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf (permanent copy https:// defenddigitalme.com/wp-content/uploads/2019/09/Tucker_Vance-Surveillance-Final.pdf)

Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (2011) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.p

UCL, Centre for Educational Neuroscience (2019) The future of education is brain stimulation http://www.educationalneuroscience.org.uk/resources/neuromyth-or-neurofact/the-future-of-education-is-brain-stimulation/)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH, en présence de Facebook Ireland Ltd (affaire C-210/16). http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN

Comité des droits de l'enfant des Nations Unies, Observation générale n° 16 (2013) sur les obligations des États concernant les incidences du secteur des entreprises sur les droits de l'enfant https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

Comité des droits de l'enfant des Nations Unies, Observation générale n° 1(2001) sur les buts de l'éducation (article 29)
https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/a)GeneralCommentNo1TheAimsofEducation(article29)(2001).aspx

Underachievement in Education (2014) House of Commons Education Committee http://defenddigitalme.com/wp-content/uploads/2016/08/Plomin_-December-2013_142.pdf

US Department for Education (Privacy Technical Assistance Center) (2015) Protecting Student Privacy While Using Online Educational Services: Model Terms of Service,

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20%281%29.pdf

Vatsalya, Youth Ki Awaaz, 2019, CCTV in Delhi schools https://www.youthkiawaaz.com/2019/08/cctv-surveillance-in-schools-boon-or-bane/

Veale M., Binns R. 2017. Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data & Society, 4(2):2053951717743530, https://doi.org/10.1177/2053951717743530.

Veale, M. (2019). A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence. https://doi.org/10.31228/osf.io/dvx4f

Who Knows What About Me (2017) Children's Commissioner, UK https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/

Williamson, B. (2017) University of Edinburgh, Centre for Research in Digital Education and the Edinburgh Futures Institute. Big Data in Education, the digital future of learning, policy and practice (Sage)

Williamson, B. (2018) Brain Data: Scanning, Scraping and Sculpting the Plastic Learning Brain Through Neurotechnology https://link.springer.com/article/10.1007%2Fs42438-018-0008-5

Williamson, B. (2018) postgenomic science, big data, and biosocial education (on_education) https://www.oneducation.net/no-02-september-2018/postgenomic-science/

Forum économique mondial (2016) New Vision for Education: Fostering Social and Emotional Learning through Technology http://www3.weforum.org/docs/WEF_New_Vision_for_Education.pdf

Zeide, E. (2014) The Proverbial Permanent Record, New York University Information Law Institute http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2507326 https://defenddigitalme.com/wp-content/uploads/2019/09/SSRN-id2507326.pdf

Zhao et a. (2019) 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. CHI'2019. https://arxiv.org/abs/1901.10245 (consulté en septembre 2019)

Zhao J. (2018) Are Children Well−Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?. https://arxiv.org/abs/1809.10944 (consulté en septembre 2019)

Zimmer, C. (2018) The Atlantic, Genetic Intelligence Tests Are Next to Worthless https://www.theatlantic.com/science/archive/2018/05/genetic-intelligence-tests-are-next-to-worthless/561392/