Données numériques à caractère personnel au sein de l'éducation nationale

RAPPORT N° 2018-016
Février 2018

Rapport à
monsieur le ministre de l'éducation nationale

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉDUCATION NATIONALE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

igen Inspection générale de l'Éducation nationale

igaenr Inspection générale de l'administration de l'Éducation nationale et de la Recherche

MINISTÈRE DE L'ÉDUCATION NATIONALE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE ET DE L'INNOVATION

Inspection générale de l'éducation nationale

Inspection générale de l'administration de l'éducation nationale et de la recherche

Données numériques à caractère personnel au sein de l'éducation nationale

Février 2018

Gilles BRAUN

Jean Aristide CAVAILLÈS
Jean-Marc MOULLET

Inspecteurs généraux de l'éducation nationale

Jean-Marc MERRIAUX

François PAQUIS
Stéphane PELLET

Inspecteurs généraux de l'administration de l'éducation nationale et de la recherche

Par souci de clarté et de fluidité de la lecture, la double écriture des terminaisons des mots féminin / masculin (exemple : « directeur.rice ») n'est pas appliquée, étant bien entendu que ces mots font référence aux femmes comme aux hommes.

SOMMAIRE

Synthèse **1**

Introduction **4**

1. Usages et interrogations du terrain, un paysage très hétérogène **5**

2. La place de l'École dans le nouvel environnement juridique sur la protection des données personnelles **10**

2.1. Données scolaires, données sensibles ? 10

2.2. Le foisonnement des textes juridiques 12

2.3. Une nécessaire mobilisation du ministère aux nouveaux enjeux juridiques 14

3. Le RGPD **15**

3.1. L'impact du RGPD sur le traitement et le stockage des données scolaires 15

3.1.1. La responsabilité des sous-traitants *15*

3.1.2. Questionnement autour du consentement *16*

3.1.3. Une explicitation des finalités d'utilisation des données, une information renforcée auprès des usagers de services numériques en particulier pour les mineurs *18*

3.1.4. De nouveaux droits, la portabilité et le droit à réparation des dommages matériel ou moral *18*

3.1.5. Un suivi de l'ensemble des données pour en permettre le contrôle, une gestion renforcée des données en particulier sur leurs traitements, leur stockage et leur durée de conservation *19*

3.2. Le déploiement du RGPD 20

3.2.1. Une architecture incompréhensible des dispositifs numériques actuels concernant les traitements de données *20*

3.2.2. Des flux de données au sein d'un ensemble applicatif dense dans l'éducation nationale *21*

3.2.3. L'audit en amont des acteurs privés intervenant dans le champ scolaire et utilisant des données personnelles *25*

3.2.4. Proposition d'organisation au sein de l'administration centrale et dans les services déconcentrés .. *26*

3.2.5. Gouvernance, chaine de responsabilité, dispositif pour accompagner le déploiement du RGPD dans un cadre national… *29*

3.2.6. Création d'un comité d'éthique et d'expertise sur l'intérêt public de l'utilisation de données scolaires *30*

4. De l'anonymat, à l'hébergement, où en sommes-nous sur la sécurité des données personnelles ? 32

4.1. L'anonymat n'apparaît plus comme étant le seul élément qui garantit la sécurité sur l'utilisation des données personnelles 32

4.2. La problématique de l'hébergement des données sur le territoire national 32

4.3. Le *e-privacy* ou règlement sur la « vie privée et les communications électroniques » 33

4.4. Les recherches dans le domaine de la traçabilité des données 34

5. De l'ouverture des algorithmes à la souveraineté pédagogique des données scolaires 35

5.1. La transparence des algorithmes, une différence entre le privée et le public 35

5.2. Le traitement des données scolaires par les logiciels de vie scolaire 35

5.2.1. Une gestion de la vie scolaire des lycées et des collèges publics hors du contrôle de l'État 35

5.2.2. Le stockage des données des élèves et des professeurs sans aucun regard de l'État sur la sécurité des serveurs les accueillant 36

5.2.3. Le cryptage et la portabilité des données d'apprentissage 37

5.2.4. Des traitements, en particulier statistiques, qui devraient interroger le ministère 38

5.2.5. Continuité et adaptabilité du service public d'éducation 38

5.2.6. La protection des données rejoint l'objectif stratégique de souveraineté éducative et l'articule à celui de la sécurisation des process 38

Conclusion 40

Rappel des préconisations 43

Annexes 45

SYNTHÈSE

Ce rapport sur les données numériques à caractère personnel au sein de l'éducation nationale dresse un état des lieux de leur gestion actuelle et une analyse des différentes problématiques qu'elles soulèvent dans le champ scolaire à l'heure de la mise en œuvre du règlement européen sur la protection des données.

Il s'appuie sur une large consultation des différents interlocuteurs concernés, parmi lesquels figurent des organisations syndicales, des associations de parents d'élèves, des services de l'administration centrale et déconcentrée de l'éducation nationale ainsi que des organismes en charge du numérique et des données personnelles, des entreprises du secteur du numérique, des associations de défense des droits de l'Homme, des experts et des chercheurs spécialistes dans le domaine.

Un questionnaire a été transmis à l'ensemble des délégués académiques au numérique éducatif, aux directeurs des systèmes d'information et aux doyens des groupes disciplinaires et de spécialité de l'inspection générale.

Les membres de la mission ont aussi mené de nombreux entretiens en établissement scolaire avec les équipes éducatives (chefs d'établissement et enseignants).

Il en ressort qu'aujourd'hui dans le champ scolaire les utilisateurs ne connaissent pas le devenir des données qu'ils renseignent et sont peu conscients de l'impact des traitements de ces données par les systèmes mis en œuvre aussi bien par l'État ou les collectivités territoriales que par des entreprises privées. Ces dernières mettent parfois en place, de façon opaque, une politique de monétisation des données. Il convient donc de former rapidement les enseignants et les chefs d'établissement aux enjeux de l'utilisation des données scolaires numériques dans le cadre d'usages pédagogiques et administratifs. Ils devront, à leur tour, former leurs élèves aux dimensions éthiques, sociales et économiques de l'utilisation des données numériques à caractère personnel. Il est proposé dans ce rapport de compléter l'article 38 de la loi d'orientation et de refondation de l'École (formation à l'utilisation des outils numériques) par former « aux dimensions éthiques, sociales et économiques de l'utilisation des données numériques, en particulier celles à caractère personnel ».

Une sensibilité croissante de la communauté éducative sur ce sujet est cependant perceptible, probablement en raison de la mise en application prochaine du règlement général européen sur la protection des données (RGPD) et des aménagements de la loi informatique et liberté qui seront discutés très prochainement au parlement. Afin de rassurer celle-ci, la mission préconise, au-delà des seules données à caractère personnel, d'adopter le principe suivant : interdire, soit par circulaire auprès des chefs d'établissement et des enseignants soit en intégrant cette interdiction dans un code de conduite, les services numériques qui opèrent des traitements sur les données scolaires autres que ceux nécessaires à des utilisations pédagogiques ou administratives. La mission a aussi fait le constat que le ministère, aussi bien au niveau national qu'académique, est peu préparé à la mise en œuvre de ces nouveaux textes législatifs qui auront des conséquences importantes aussi bien dans le domaine de la gestion administrative que dans la mise en œuvre de pratiques pédagogiques s'appuyant sur les outils numériques.

Les questions posées n'étant pas toutes de nature juridique, la mission propose également qu'un comité consultatif d'éthique et d'expertise sur l'intérêt public de l'utilisation de données scolaires

soit constitué pour analyser la dimension éthique de la traçabilité et des finalités des traitements opérés sur celles-ci sur le modèle mis en place par le ministère des solidarités et de la santé.

Ce rapport développe la question de l'organisation qu'il est nécessaire de déployer très rapidement à tous les niveaux pour répondre efficacement à ces besoins, en particulier le positionnement des délégués à la protection des données (DPD) prévus par le règlement européen, dont le rôle est entre autres de mesurer les conséquences du traitement des données à caractère personnel dans le domaine scolaire et de produire des avis auprès des responsables du traitement des données (le DASEN pour le premier degré, les chefs d'établissement pour le second degré). Il serait souhaitable que ces derniers diligentent systématiquement des études d'impact sur ces traitements de données scolaires en s'appuyant sur l'expertise des DPD.

Il convient de souligner que la mise en place de cette organisation qui s'appuie sur les DPD et les responsables de traitement (chefs d'établissement et DASEN principalement) devra s'accompagner d'une campagne d'information et de formation à laquelle l'administration ne s'est pas encore préparée malgré la proximité des échéances.

Les questions soulevées dans ce rapport interrogent fortement le service public d'éducation quant à sa capacité à assurer :

- une continuité dans la gestion des établissements scolaires en cas par exemple d'arrêt des activités des sociétés éditrices de logiciels de vie scolaire (impossibilité par exemple d'assurer une rentrée scolaire normale faute de pouvoir disposer des emplois du temps) ;

- une mutabilité de ces services afin qu'ils puissent suivre les évolutions souhaitées par le ministère (mise en place de réforme ayant des conséquences sur la gestion d'emploi du temps, des absences, etc.) ou permettre l'accès à de nouveaux services pour lesquels les chefs d'établissement demandent un accès via leurs outils quotidiens).

Le ministère doit s'assurer que les flux, les traitements, et l'hébergement des données scolaires assurent efficacement le respect de la vie privée, la sécurité des données et leur interopérabilité.

Pour que le système éducatif conserve la maitrise de son fonctionnement administratif, de sa spécificité pédagogique, pour qu'il puisse mettre en œuvre les orientations souhaitées et éviter qu'il subisse des évolutions imposées par des agents extérieurs, le contrôle du traitement des données scolaires s'impose. Une clause d'explicitation des principes sur lesquels reposent les algorithmes utilisés dans les traitements de données à caractère personnel devrait être intégrée dans les contrats passés avec les développeurs privés. Au-delà, la mission préconise que le champ du scolaire intègre les secteurs d'activité industriels stratégiques soumis à une autorisation préalable du gouvernement français en cas d'investissements étrangers.

Il ne s'agit pas de tomber dans l'excès d'une réglementation trop restrictive qui risquerait de complexifier inutilement la gestion du système éducatif et de freiner la recherche et les développements d'applications pédagogiques innovantes. En effet, au-delà des enjeux économiques – et des inquiétudes qu'ils engendrent chez de nombreux interlocuteurs –, les avancées dans le traitement d'un nombre très important de données (*big data*) laissent présager des développements prometteurs dans le domaine pédagogique qu'il serait dommageable de freiner en France pénalisant ainsi les entreprises nationales par rapport à des sociétés de pays ayant des règles moins strictes.

Il convient toutefois de rester prudent et critique, aussi bien sur le catastrophisme que sur l'enthousiasme que peuvent susciter de tels travaux.

Quoi qu'il en soit, si l'éducation nationale se doit de mettre la puissance des développements numériques actuels et à venir au service de la pédagogie et de la gestion de son administration, elle doit aussi se porter garante du respect de la vie privée de l'ensemble des membres de la communauté éducative et de la souveraineté de la France sur son système éducatif et ainsi garantir sa mission de service public.

Introduction

L'utilisation quotidienne et massive des technologies de l'information et de la communication dans la sphère privée par les élèves, leur famille, les enseignants et les personnels administratifs, a des incidences fortes sur les usages numériques dans le cadre scolaire, de la maternelle à l'université. Les premiers retours sur ces pratiques questionnent l'utilisation potentielle qui peut être faite des données personnelles sous leur forme numérisées. *A contrario*, l'analyse de ces données peut offrir de véritables opportunités dans le domaine de la pédagogie.

En effet, l'exploitation des données des élèves présente plusieurs intérêts :

- pour l'élève d'abord : l'analyse détaillée, sur un temps assez long, des résultats obtenus à différents tests d'évaluation permettrait, grâce à des services numériques spécifiques, de lui proposer des parcours pédagogiques mieux adaptés à son stade d'acquisition de connaissances et de compétences ;
- pour le professeur, qui pourrait disposer d'outils de pilotage pédagogique plus fins que ceux dont il a l'usage actuellement ;
- pour la recherche didactique, par l'utilisation statistique des données, sur des échelles diverses, pour mieux comprendre les situations d'apprentissage.

L'observation des usages réalisée par la mission montre qu'il existe actuellement une profonde méconnaissance des enjeux de la récolte, du traitement et de l'analyse des données captées, stockées voire traitées en flux continu, à l'insu des usagers par les services numériques utilisés dans le cadre scolaire, qu'ils aient été ou non spécifiquement conçus pour ces usages. Les utilisateurs sont peu conscients de la réutilisation qui peut être faite de leurs activités numériques par des systèmes généralement peu transparents et pratiquant une politique de monétisation des données parfois opaque.

On constate aujourd'hui l'existence de plateformes de stockage et de traitement de données qui ne donnent pas d'information claire sur leur lieu d'hébergement, la sécurisation et la nature des opérations qui sont effectuées sur celles-ci[1]. C'est le cas de certains acteurs privés, sur lesquels l'institution a un pouvoir de régulation très limité, qui proposent des services aujourd'hui massivement utilisés par les chefs d'établissement, les enseignants et leurs élèves. Le ministère de l'éducation nationale doit être à même d'offrir transparence, protection et traçabilité sur les traitements des données de ses usagers, tout particulièrement pour les applications de tiers que l'institution utilise dans le cadre de ses missions de service public.

Par ailleurs, les potentiels que pourrait offrir l'accès à cette quantité importante de données dans le domaine scolaire ne sont pas encore réellement exploités. Des équipes de recherche et des entreprises mènent actuellement des travaux pour analyser la masse d'informations laissées par les traces des élèves afin de mener des recherches avec de nouveaux outils d'analyse ou développer de nouvelles applications pédagogiques[2]. Ce domaine, que l'on appelle aujourd'hui les *learnings*

[1] Cf. débat actuel sur le *Privacy Shield*, réglementation qui permet les échanges de données entre les pays européens et les USA.

[2] Différentiation pédagogique, gestion fine des parcours des élèves, analyse d'erreurs et de réussite, proposition de stratégies pédagogiques pour les professeurs se basant sur les données de leurs élèves, validation ou invalidation de théorie pédagogique.

analytics et qui appartient au champ du *big data*[3], est en expansion rapide et pourrait être source de développement économique pour des entreprises françaises de l'ed'tech[4]. Il convient toutefois d'être prudent et critique, aussi bien sur le catastrophisme que sur l'enthousiasme que peuvent susciter de tels travaux.

Le présent rapport, rédigé dans le cadre de la lettre de mission sur les données numériques à caractère personnel au sein de l'éducation nationale, intègre l'ensemble des problématiques soulevées à travers l'analyse d'un fond documentaire et d'entretiens réalisés entre novembre 2017 et fin janvier 2018 (voir liste en annexe). La mission a jugé important d'insister sur les points suivants :

- le statut des données scolaires et leur prise en compte dans la nouvelle loi informatique et liberté ;
- les conséquences pour l'institution de la mise en place au niveau européen du règlement général sur la protection des données (RGPD) qui prendra effet le 25 mai 2018. La mission s'est attachée à évaluer le niveau d'anticipation – très variable – du déploiement de ce nouveau règlement aux niveaux local, académique et central ;
- l'importance stratégique du domaine des services d'organisation et de suivi de la vie scolaire, actuellement très largement dominé par un acteur privé en situation de quasi-monopole ;
- le potentiel du traitement des traces dans le cadre de la mise à disposition de services s'appuyant sur les technologies de l'*adaptive learning* et les enjeux économiques probables de ce nouveau domaine.

La prise de conscience publique relative à ces sujets prend de l'ampleur, surtout depuis la polémique déclenchée par le message du directeur du numérique aux DAN / DSI en mai dernier[5]. Les organisations rencontrées (syndicats, fédérations de parents d'élèves, associations partenaires de l'école, ligue des droits de l'Homme, associations savantes, industriels, …) ont unanimement formulé le souhait que le ministère se positionne clairement sur la question des données scolaires. On trouvera dans ce qui suit quelques préconisations qui pourraient être autant de signes forts de l'importance que l'institution accorde à la protection et à la maîtrise des données numériques scolaires.

1. Usages et interrogations du terrain, un paysage très hétérogène[6]

Il ressort des enquêtes réalisées par la mission que les établissements scolaires questionnent régulièrement les DANE et les DSI sur des champs assez semblables d'une académie à l'autre : le droit à l'image, les possibilités d'accéder à des services au travers des adresses mél des élèves, la création de comptes mél d'élève, l'utilisation d'outils professionnels détournés, le recours à des

[3] *Big data* : ce terme anglais souvent utilisé en France, désigne le traitement automatisé de très gros volumes de données.

[4] Ed'tech : ce terme de consonance anglophone, regroupe les acteurs industriels des technologies de l'information appliquées au domaine de l'éducation.

[5] Les instructions présentes dans le mail permettaient aux acteurs académiques de donner aux GAFAM l'accès aux annuaires académiques.

[6] Synthèse des réponses à deux questionnaires envoyés aux DANE / DSI et aux doyens des groupes de l'IGEN.

services « grand public » qui créent des fichiers contenant des informations sur les élèves[7] ou opèrent des traitements sur leurs traces de navigation, les limites de l'utilisation des identifiants des élèves, le droit d'opposition aux ENT, etc. Les collectivités territoriales interpellent, elles aussi, les services académiques sur la question des données personnelles en y intégrant également la dimension matérielle (utilisation des outils nomades, dont les tablettes, utilisation des propres outils de communication des élèves, intégration de ses outils aux ENT). Certaines académies font état de contentieux avec des parents qui refusent que leurs enfants puissent être identifiés sur des ENT ou refusent qu'ils utilisent des tablettes. Ils estiment nécessaire de mieux délimiter les champs des données scolaires et données privées.

Ces questions qui, pour au moins une partie d'entre elles, traversent le système éducatif depuis plus d'une décennie, illustrent le manque de formation des acteurs de terrain qui n'ont pas les connaissances requises pour faire face à la problématique des données personnelles des professeurs et élèves.

Certaines académies témoignent de difficultés avec des collectivités territoriales de rattachement qui préfèrent parfois, aux ENT payants, le recours à des services gratuits. Un entretien avec un DSI a pu montrer toute l'énergie que les services académiques doivent déployer pour arriver à convaincre leurs interlocuteurs des risques encourus face à certains prestataires.

Plusieurs académies alertent les usagers à la fois sur les conditions générales d'utilisation et sur les fonctionnalités proposées par les logiciels propres à l'éducation nationale. Par exemple, les chefs d'établissement pensent souvent que l'export des données personnelles, non cryptées, et leur transmission, ne sont soumis à aucune réglementation. Ce point concerne à la fois les bases élèves et les bases des personnels de l'éducation nationale. Une académie signale ainsi le transfert de la base enseignant vers des systèmes hébergés par les collectivités territoriales de rattachement.

L'utilisation des adresses mél des personnels de l'éducation nationale mérite une vigilance particulière. Les responsables académiques constatent que nombre de courriers officiels sont transmis sur des boites aux lettres non professionnelles. Les adresses professionnelles posent par ailleurs une difficulté de gestion : créées au moment où les agents sont affectés dans une académie, elles ne sont pas supprimées de façon systématique au départ de l'agent de l'académie. Il en résulte des boites fantômes qui contiennent des données personnelles.

Dans le domaine de l'expérimentation, on relève une difficulté dans le déploiement de certains projets. Ainsi le DANE d'une académie fait état de la difficulté rencontrée à déployer une expérimentation avec un prestataire privé qui offre des services éducatifs gratuits garantissant une préservation des données à caractère personnel. Les raisons du « blocage » constaté sont principalement dues à un manque d'information et à une méconnaissance des conditions générales d'utilisation de cette plateforme dans un cadre scolaire. Alors que le projet était impulsé par la DNE et que les établissements repérés disposaient de ressources humaines adaptées, l'expérimentation est aujourd'hui au point mort.

[7] Les exemples qui sont donnés par les 22 académies qui ont répondu à l'enquête sont nombreux. Les DANE et les DSI sont confrontés à des demandes d'utilisation, ou constatent des utilisations sans aucune consultation des logiciels suivants : Google drive, Dropbox, différentes versions de la suite Microsoft en ligne, la solution CISCO, Facebook, Twiter, Linkedin, Gmail, Chrome book, Plickers, pour ne citer que les plus connus.

Un manque d'anticipation et des stratégies très différentes face à la mise en place du règlement général sur la protection des données

Alors que la loi va être prochainement modifiée[8] et que le RGPD entrera en vigueur fin mai 2018, la mission constate une préparation très hétérogène à la mise en place de ces changements.

Plusieurs académies ont anticipé la mise en place du RGPD. On constate alors une réflexion sur la communication auprès des acteurs de terrain et des établissements, la mise en œuvre de plans de formation et la mise en ligne d'outils de communication, la diffusion de vadémécums. Deux académies[9] au moins proposent ainsi des sites clairs permettant par un jeu de « questions - réponses » d'accéder à des informations explicites et de bien cerner les enjeux. Au moment de l'écriture de ce rapport, les actions en direction des parents et des élèves ne sont pas encore conduites, une seule académie envisage des actions de formation vers ce public dès cette année scolaire. Des académies font appel à des partenaires extérieurs à l'éducation nationale pour les aider à la mise en œuvre du RGPD, des audits des systèmes sont actuellement conduits dans au moins une académie, des chartes sont en cours de rédaction avec des difficultés juridiques signalées. Une académie indique des liens avec le cabinet d'avocat Lexing Alain Bensoussan sur ces questions, d'autres se rapprochent de structures associatives pour bénéficier des appuis techniques ou pour mener des audits des systèmes.

La majorité des académies attend les instructions ministérielles. Certains DANE et DSI estiment qu'ils doivent être associés aux CIL[10] et aux services juridiques pour s'emparer de la question du règlement général sur la protection des données. Le positionnement des DPD[11] dans l'organisation à l'échelle d'une académie, à l'échelle d'un département, d'une circonscription ou d'un EPLE fait l'objet de débats. Les enquêtes et entretiens réalisés montrent des hypothèses d'organisation très variées allant d'un seul DPD académique au déploiement d'un DPD par unité éducative. À l'évidence le rôle des DPD n'est pas compris de façon unique.

Quelques académies ont mis en place des cellules de réflexions sur les données personnelles des élèves. Ces comités regroupent en général les DANE, les DSI, le CIL, les doyens des corps d'inspection territoriaux, les DASEN et un représentant du secrétariat général.

Un département a mis en place un comité d'éthique sur cette question. Même si plusieurs académies font état d'un début de réflexion sans formalisation, plus de la moitié des DANE-DSI déclarent qu'aucun travail n'est entamé sur ce sujet.

À seulement trois mois de la mise en place du RGPD dans l'ensemble de l'Union européenne, les DANE et DSI sont nombreux à rapporter une grande ignorance de ce que recouvre ce texte pour une large majorité des professeurs, des chefs d'établissement et des pilotes à l'échelle académique.

La question des données personnelles est souvent envisagée de façon partielle ou sans tenir compte des trois types de données qu'elle recouvre : des données personnelles saisies par la personne (personnel administratif, professeur, élèves, parent) ; des traces d'activités scolaires : navigation,

[8] https://www.legifrance.gouv.fr/Droit-francais/Actualite/13-decembre-2017
[9] Académies de Lyon et de Strasbourg.
[10] Correspondant informatique et liberté.
[11] DPD (délégué à la protection des données) pour DPO (*digital protection officer*) en anglais.

téléchargements effectués, productions... ; des calculs effectués par un logiciel utilisé dans le cadre scolaire (temps et fréquence d'utilisation, corrélation…).

À l'échelle de la classe deux types d'utilisation des données personnelles :

- Des données exploitées dans la construction des compétences disciplinaires par des professeurs bien formés dans le cadre de l'application des programmes

Un premier ensemble concerne une exploitation des données des élèves dans le cadre de la construction des compétences disciplinaires attendues dans les programmes. Les données personnelles y sont parfois exploitées pour donner plus de sens aux apprentissages. C'est le cas effectivement en économie et gestion, en sciences de la vie et de la Terre, en sciences médicosociales, en biotechnologie ou en sciences physiques ; c'est une possibilité en enseignement des arts. Il peut s'agir de travailler sur des données biométriques, sur des performances physiques, sur des empreintes digitales par exemple. Dans certaines situations des données sensibles relatives à la santé sont utilisées (elles peuvent être issues de l'analyse des carnets de santé, d'enquêtes, de travail sous la forme de projets en première technologiques, lors des stages en entreprise, etc.). En éducation physique et sportive, une partie des données personnelles exploitées relève également de données sensibles (données de santé liées à la dispense de certaines activités, mise en place de PAI - PPS, certificats de santé pouvant révéler certaines informations personnelles, données biométriques associées à des performances sportives, …).

Les groupes disciplinaires de l'inspection générale concernés par ces utilisations font état de professeurs formés à ces questions et donc particulièrement vigilants sur le type de données et leur traitement, mais aussi sur leur caractère confidentiel. Ces enseignants y sont d'autant plus sensibles qu'ils enseignent ces notions à leurs élèves (filière ST2S ou STMG par exemple). Des formations sont mises en place qui s'appuient sur des travaux nationaux réalisés pour cadrer ces utilisations en accord avec les textes en vigueur (en particulier au travers des TraAM : les travaux académiques mutualisés), de stages de formation spécifiques, d'outils d'informations en ligne, etc.

Les informations collectées et traitées peuvent donc, dans certains cas, qu'il faut bien cerner, être liées à des données personnelles de santé et donc rentrer dans le champ des données sensibles[12]. Les règles particulières qui doivent alors s'appliquer sont aujourd'hui très contraignantes[13] et celles qui devront s'appliquer demain avec la mise en œuvre du RGPD sont largement ignorées, notamment la notion d'étude d'impact qui doit être menée à partir du moment où « le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[14]. Or, il est légitime de considérer que les traitements de données sensibles sont le plus souvent concernés par ce volet du RGPD.

La question même de l'identification d'un « *risque élevé* » qui dépasse la question des données sensibles va inévitablement poser problème. Pour autant si ce risque est avéré les responsables de traitement devront être en mesure de présenter à l'autorité de contrôle le résultat d'études d'impact

[12] Cf. Art. 9 du RGPD. L'adjectif sensible n'est pas employé mais la description recouvre ce champ.

[13] Rappelons qu'en principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes ou de leurs responsables légaux si elles sont mineures. Le RGPD rendra les conditions d'utilisation de ces données encore plus contraignantes.

[14] Paragraphe 58 de la partie introductive des articles du RGPD.

qui devront à la fois dégager les caractéristiques du traitement, les risques encourus et les mesures prises pour garantir la protection des données[15].

Il apparaît ici évident que dans le cadre scolaire des situations de traitement de données à « *risques élevés* » vont se présenter. Les exemples observés en éducation physique et sportive en témoignent.

- Des données livrées pour accéder à des services en classe par des professeurs peu ou pas formés sur les risques encourus

Le deuxième ensemble d'utilisations est lié à l'usage d'outils en ligne, de logiciels, d'équipements personnels de communication qui permettent d'enrichir les pratiques pédagogiques. Pour accéder à certains de ces outils, dont des réseaux sociaux, les élèves peuvent être amenés à s'inscrire individuellement et à livrer certaines données personnelles (il peut s'agir de leur nom, de leur adresse courriel, de leur âge, adresse, voire leur photo, etc.). Si ces outils sont utilisés, c'est qu'ils sont considérés comme efficaces et motivants pour les élèves en partie parce qu'ils sont utilisés dans leur quotidien hors la classe. Une vigilance éclairée s'impose, d'autant que l'un des objectifs du socle commun de connaissances, de compétences et de culture consiste justement à amener les élèves à une maitrise de leur identité numérique dans leur utilisation des réseaux sociaux.

Les professeurs sont peu ou pas formés aux règles et au droit qui s'appliquent dès lors que ces outils sont utilisés par les élèves. Les conditions générales d'utilisation ne font pas l'objet d'études préalables par les enseignants. Le groupe premier degré signale à ce propos que des élèves de l'école primaire utilisent des réseaux sociaux alors que l'âge légal d'inscription est fixé à treize ans. En revanche le groupe disciplinaire d'économie et gestion indique que des logiciels professionnels ont été modifiés pour permettre une utilisation en milieu scolaire sans risquer de fuite de données personnelles.

Préconisation n° 1 : Former rapidement les enseignants et les chefs d'encadrement sur l'utilisation des données scolaires numériques dans des situations pédagogiques et administratives avec une attention particulière aux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens de l'article 9 du RGPD.

Cette thématique doit s'inscrire dans les maquettes des ESPE, dans la formation initiale des chefs d'établissement, dans le plan national de formation et les plans de formation académique 2018-2019. Un parcours M@gistère est en cours de réalisation qui doit être complémentaire d'un cursus de formation proposé par l'ESENESR pour les chefs d'établissement. Par ailleurs, le ministère pourrait faire appel à des acteurs extérieurs pour l'accompagner dans ce déploiement de formation à grande échelle en particulier la CNIL ou encore l'IAPP[16].

[15] Article 27 du RGPD.

[16] L'IAPP (*International Association of Privacy Professionnals*) est la plus grande organisation réunissant les professionnels de protection de la vie privée au niveau mondial.

2. La place de l'École dans le nouvel environnement juridique sur la protection des données personnelles

2.1. Données scolaires, données sensibles ?

Il n'existe pas de définition « officielle » des données scolaires. Le terme mérite d'être précisé. On les considérera dans le présent rapport comme toutes données recueillies dans le cadre scolaire[17]. Le périmètre est donc très large : informations administratives sur les élèves, les enseignants, les personnels administratifs, les intervenants extérieurs, les parents…, les productions d'élèves ou de professeurs réalisées lors d'activités pédagogiques, des traces d'apprentissage. Ces données ont souvent un caractère personnel mais elles peuvent aussi être relatives à un groupe (classe ou établissement par exemple) ou n'être que de « simples » traces laissées par des élèves ou des professeurs dans le cadre de leurs activités scolaires.

On notera qu'aujourd'hui ni le RGPD, ni la prochaine loi informatique et liberté en préparation[18], n'abordent la question des traces et des données collectives sauf à prouver que directement ou indirectement elles permettent d'identifier une personne physique. Cependant, l'augmentation des capacités de calcul et la masse des données pouvant être traitées grâce à de nouveaux algorithmes[19] pourraient, par des croisements, permettre d'obtenir dans un futur proche des informations à caractère personnel à partir de données considérées initialement comme des données anonymes.

Si les données scolaires n'ont pas à ce jour de statut légal particulier[20], celles qui possèdent un caractère personnel doivent être traitées en respectant toutes les obligations juridiques prévues jusqu'ici par la loi informatique et libertés, la directive européenne 95-46 et prochainement par le RGPD.

Rappelons que d'après la loi informatique et liberté (article 8 de la loi du 6 janvier 1978), les données sensibles sont celles concernant :

- l'origine raciale ou ethnique ;
- les opinions politiques, philosophiques ou religieuses ;
- l'appartenance syndicale ;
- la santé ;
- la vie sexuelle.

Le consentement exprès de chaque utilisateur est alors obligatoire pour la collecte de telles données, dans les conditions prévues par le 1° du I de l'article 8 de la loi.

---

[17] Elles comportent donc aussi bien :
- des données personnelles saisies par la personne (personnel administratif, professeur, élèves, parent) ;
- des traces d'activités scolaires : navigation, téléchargements effectués…).

Des calculs effectués par un logiciel utilisé dans le cadre scolaire (temps et fréquence d'utilisation, corrélation…).

[18] https://www.legifrance.gouv.fr/Droit-francais/Actualite/13-decembre-2017

[19] Cf. le champ du *big data*.

[20] Ce qui n'est pas le cas dans d'autre pays comme par exemple les États-Unis ou la notion de « données scolaires » est définie et protégée par la loi : https://ed.gov/policy/gen/guid/fpco/ferpa/index.html, en France, la donnée scolaire n'est pas définie dans la loi informatique et liberté.

Si une donnée scolaire n'est pas sensible au sens de la loi (même si elle est perçue comme telle socialement), elle peut le devenir après certains traitements. Ainsi, par exemple, comme l'a relevé la direction des affaires juridiques du ministère de l'éducation nationale, dans le cadre du signalement d'absences coïncidant de façon répétée avec des fêtes religieuses, on peut craindre que le traitement de ces données puisse indirectement donner accès à la religion de la famille[21].

Lors des entretiens menés par la mission, certains interlocuteurs ont souhaité que les données scolaires soient intégrées dans la liste des données sensibles. **À cet égard, il convient de noter que le RGPD fait une liste explicite du périmètre des données sensibles, et que les états n'ont pas latitude de la modifier. L'extension de ce périmètre au cas des données personnelles scolaires est donc impossible.**

Même si l'extension l'était, la première difficulté résiderait dans la définition de l'étendue du concept de donnée scolaire et donc de la mise en œuvre d'une catégorie juridique de données distincte ; la seconde serait liée aux contraintes qu'engendrerait cette entrée dans le champ de la donnée sensible[22], contraintes qu'il serait impossible de respecter pour de nombreux services qui ne méritent pas un tel niveau de protection.

Une approche rationnelle de ces sujets est indispensable. Il faut disposer d'un niveau de protection adapté à l'institution scolaire, qui ne soit pas disproportionné. Cette voie nécessite probablement de s'éloigner du concept de « donnée sensible » en précisant dans la loi ce qu'on entend par « traitement sensible » de la donnée, c'est-à-dire tout traitement susceptible de transformer une donnée scolaire en donnée sensible au sens de la loi actuelle.

La piste de solutions contractuelles est alors probablement à privilégier. Des clauses contractuelles « type » précisant les traitements autorisés sur les données récoltées et leurs finalités devraient permettre de protéger les responsables de traitement (chefs d'établissement, DASEN, administration centrale).

Il convient enfin d'éviter l'utilisation, aujourd'hui très répandue, par les enseignants de services destinés au grand public qui n'offrent pas la garantie que les données scolaires transmises ne soient pas utilisées à d'autres fins que pédagogiques ou administratives.

Préconisation n° 2 : Interdire, soit par circulaire auprès des chefs d'établissement et des enseignants soit en intégrant cette interdiction dans un code de conduite, les services numériques qui opèrent des traitements sur les données scolaires autres que ceux nécessaires à des utilisations pédagogiques ou administratives.

---

[21] Par exemple : un parent indiquant que son enfant sera absent à des dates correspondant à des fêtes religieuses.

[22] Par principe, la collecte et le traitement de ces données sont interdits**.** Cependant, dans la mesure où la finalité du traitement l'exige, ne sont pas soumis à cette interdiction :

- les traitements pour lesquels la personne concernée a donné son consentement exprès ;
- les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'État.

La collecte et le traitement de ces données doivent dans ces hypothèses, être justifiés au cas par cas au regard des objectifs recherchés.

2.2. Le foisonnement des textes juridiques

Une des difficultés à laquelle le ministère de l'éducation nationale est confronté lorsqu'il aborde la question des données scolaires numériques réside dans la multitude de types de données qu'il est amené à traiter pour son fonctionnement (gestion des élèves et des personnels, relations avec les familles, mise en œuvre de pratiques pédagogiques, statistiques…) et le nombre de textes juridiques qui doivent s'appliquer à ces diverses situations. Sans viser à l'exhaustivité, citons :

1) Le règlement général sur la protection des données du 27 avril 2016[23]

Le texte, dont le titre complet est « 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) Texte présentant de l'intérêt pour l'EEE) », entrera en application le 25 mai 2018. Ce règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci (cf. chapitre 3).

2) La loi n° 78-17 du 6 janvier 1978 dite Loi informatique et liberté, modifiée le 31 janvier 2017 en cours de révision suite à la mise en œuvre prochaine du RGPD

Texte majeur qui s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles.

Projet en cours commission des lois : http://www.assemblee-nationale.fr/15/pdf/rapports/r0592-aCOMPA.pdf

3) La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

Elle vise à préparer le pays aux enjeux de la transition numérique et de l'économie de demain. Elle promeut une société numérique ouverte, fiable et protectrice des droits des citoyens.

4) Le prochain règlement européen « e-Privacy »

La directive européenne « e-Privacy » s'applique aujourd'hui aux opérateurs de télécommunications traditionnels. Elle sera remplacée par un nouveau règlement qui est en cours de discussion dans l'objectif de s'appliquer également aux nouveaux acteurs du secteur des services de communications et messageries électroniques, tels que WhatsApp, Facebook Messenger, Skype, Gmail, iMessage ou Viber. Elle devra traiter des métadonnées (par exemple, la date et l'heure d'un appel ou sa localisation), des cookies, etc.

5) Le « Privacy shield »

Mécanisme d'autocertification pour les entreprises US reconnu par l'Union européenne (UE) afin d'autoriser l'hébergement des données à caractère personnel hors UE. Ce mécanisme est en vigueur

[23] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

depuis le 1er aout 2016. Le transfert des données aux US est autorisé sous la condition que les entreprises destinataires se soient inscrites dans un registre tenu par l'administration américaine.

6) La loi relative aux droits des citoyens dans leurs relations avec les administrations[24]

Elle fixe les règles d'accès aux données administratives.

7) Des textes relatifs à l'archivage (à ne pas confondre avec le stockage) en particulier numérique

Le cadre juridique de l'archivage repose sur le code du patrimoine qui fait référence[25] à la loi informatique et liberté : « Lorsque les archives publiques comportant des données à caractère personnel collectées […], ces données font l'objet, à l'expiration de la durée prévue au 5° de l'article 6 de ladite loi, d'une sélection pour déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées. »

8) Des textes relatifs à l'obligation de confidentialité en matière de statistiques (cf. guide du secret statistique publié par l'INSEE)[26]

Le secret statistique est une forme particulière du secret professionnel qui s'applique aux statisticiens publics. Son principe général est d'apporter aux personnes qui fournissent à l'administration, ou aux personnes chargées d'une mission de service public, des informations utilisées pour l'établissement de statistiques publiques, l'assurance que ces informations ne seront pas utilisées d'une façon susceptible de leur porter tort.

9) La loi de refondation de l'école (volet formation)

Article 38 (Article 312-9 du code de l'éducation)

« La formation à l'utilisation des outils et des ressources numériques est dispensée dans les écoles et les établissements d'enseignement ainsi que dans les unités d'enseignement des établissements et services médicosociaux et des établissements de santé. Elle comporte une sensibilisation aux droits et aux devoirs liés à l'usage de l'internet et des réseaux, dont la protection de la vie privée et le respect de la propriété intellectuelle ».

10) La convention 108 du Conseil de l'Europe

Plus de 50 pays dans le monde ont déjà signé cette convention – le seul traité international dans ce domaine – qui énonce des principes essentiels sur la protection des données à caractère personnel.

La « Convention 108 » fait actuellement l'objet d'une mise à jour afin d'inclure les atteintes à la vie privée découlant de l'utilisation des nouvelles technologies de l'information et de la communication,

---

[24] **Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations** modifiée (NOR: FPPX9800029L).

[25] **Article L. 212-3.**

[26] Art. 6 et 7 bis de la loi du 7 juin 1951 relative à la coordination et le secret en matière de statistiques et de l'article 226-13 du code pénal relatif à la rupture de confidentialité.

Décret n° 86-83 du 17 janvier 1986, art. 1.1.

de renforcer son mécanisme de suivi et de veiller à ce qu'elle soit compatible avec divers cadres normatifs du monde entier, y compris le cadre juridique de l'UE.9).

2.3. Une nécessaire mobilisation du ministère aux nouveaux enjeux juridiques

Les enquêtes et auditions réalisées par la mission montrent une sensibilisation très insuffisante à la question des données personnelles chez pratiquement tous les acteurs du système éducatif : personnels de direction et d'encadrement, professeurs, élèves, parents, représentants des collectivités locales.

Même si les associations et les syndicats rencontrés sont très informés sur la question, cette préoccupation concerne surtout leurs équipes dirigeantes et beaucoup moins leurs adhérents.

Il faut s'attendre à ce que la prochaine mise en application du RGPD et les aménagements de la loi informatique et liberté qui l'accompagnent amènent la question de la protection des données personnelles au centre des débats de société de notre pays.

Il est donc urgent que le ministère de l'éducation nationale mette en place un large dispositif de sensibilisation aux enjeux de la protection des données scolaires, accompagné d'une information sur les outils que l'institution met ou va mettre en place pour la garantir.

Cette information doit être ciblée avec soin et adaptée à chaque public concerné. De plus, l'institution doit aider les chefs d'établissement et les professeurs à produire des documents destinés à l'information des élèves et de leurs parents rédigés dans une langue simple et compréhensible par un non spécialiste, comme le stipule le RGPD. Il serait utile que le ministère ou le réseau Canopé mettent en ligne les éléments qui permettront d'éviter que chacun les réinvente de son côté. À ce jour, aucun des sites institutionnels, ni education.gouv.fr, Éduscol, ou encore le site de réseau Canopé n'ont créé et mis en ligne des ressources structurées sur ce sujet (sur ce point quelques académies sont plus avancées[27]…). Une FAQ (foire aux questions) nationale serait sans doute aussi très utile pour tous les responsables de traitement. Il faut noter que l'académie de Lyon en a déjà produit une que la mission juge très pertinente et qu'il serait judicieux de porter sur un site à dimension nationale.

Certains de nos voisins sont beaucoup plus avancés que nous sur ce point. C'est particulièrement le cas du Royaume-Uni, où le *Department for Education* met d'ores et déjà en ligne de nombreux documents de communication élaborés par les établissements à destination des élèves, parents et professeurs[28]. Ces documents, de portée nationale, sont conçus pour être facilement adaptés aux spécificités locales et sont d'une clarté rédactionnelle conforme aux exigences du RGPD en termes d'accessibilité des explications au grand public.

Il convient toutefois d'éviter tout alarmisme dans la communication institutionnelle, notamment à l'intention des professeurs. Un équilibre délicat devra être trouvé entre une sensibilisation accrue aux risques posés par une utilisation non maîtrisée des données personnelles en milieu éducatif et la promotion des usages du numérique dans et hors la classe. Beaucoup d'enseignants réticents à ces usages pourraient saisir le prétexte des risques liés aux traitements et au stockage des données

[27] Voir https://dane.ac-lyon.fr/spip/FAQ-RGPD-Reglement-General-pour-la
[28] Voir par exemple https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

personnelles associées pour abandonner complètement ou limiter les contributions du numérique à leur enseignement.

Dans sa communication, il est donc essentiel que l'institution mette l'accent sur les garanties nouvelles apportées par le RGPD et dans la sécurisation juridique des acteurs.

Préconisation n° 3 : Rédiger au niveau national et diffuser largement des documents d'information sur la protection accrue apportée par le RGPD et les modifications de la loi informatique et libertés, adaptés aux différents publics : chefs d'établissement, enseignants, parents, élèves.

3. Le RGPD

3.1. L'impact du RGPD sur le traitement et le stockage des données scolaires

Le RGPD est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition législative, même s'il est fortement recommandé aux États de revoir les lois existantes pour intégrer certains principes qui leur laissent une marge d'appréciation pour la mise en œuvre[29].

L'objectif principal du RGPD est de renforcer les droits de la personne, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes[30]. Ce droit offre à chaque individu la possibilité de récupérer une partie de ses données dans un format ouvert et lisible par n'importe quel ordinateur. Les propriétaires des données peuvent ainsi les stocker ou les transmettre facilement d'un système d'information à un autre, en vue de leur réutilisation à des fins personnelles. Le RGPD cherche à conforter la responsabilité des acteurs traitant les données qu'ils en soient responsables ou sous-traitants. Il offre aussi la possibilité aux autorités en charge de la protection des données d'agir dans un cadre transnational. Cette dimension peut avoir un intérêt pour définir des politiques sur le traitement des données scolaires entre les États à l'échelle européenne.

3.1.1. La responsabilité des sous-traitants

Le droit actuel de la protection des données concerne essentiellement « les responsables de traitement ». Dans l'éducation nationale, il s'agit des DASEN pour le premier degré, et des chefs d'établissement dans le second degré. Pour l'administration centrale, il faudra définir le responsable de traitement ; Il serait logique que la secrétaire générale tienne ce rôle. Pour le ministère de l'éducation nationale, le nombre de responsables de traitement approche ainsi 11 400 personnes[31]. Leur rôle est de déterminer les finalités et les modalités de traitement des données personnelles.

---

[29] C'est la raison pour laquelle, le gouvernement français travaille actuellement sur une nouvelle loi « informatique et liberté » qui devrait être présentée devant le parlement en janvier 2018.

[30] Dans la partie 1, la nouvelle loi informatique et liberté doit intégrer les dispositifs en lien avec l'âge du consentement pour les mineurs. Le RGPD fixe à seize ans l'âge du consentement mais les États peuvent proposer que cette limite soit abaissée jusqu'à treize ans. C'est une disposition éminemment politique sur laquelle le ministère ne manquera pas d'être interpelé. Elle entrera en résonnance avec le récent débat sur l'âge légal du consentement sexuel.

[31] 11 300 chefs d'établissement, 100 DASEN et 30 recteurs.

Le RGPD élargit aux sous-traitants[32] une large partie des obligations imposées aux responsables des traitements. Cette disposition a une implication sur le tissu industriel du numérique éducatif en France, et les entreprises doivent rapidement s'organiser pour répondre à cette nouvelle exigence. La mission a pu constater que certains acteurs de la filière industrielle du numérique éducatif pouvaient être en retard dans la mise en place de ces nouvelles obligations légales. Il peut de ce fait apparaître une asymétrie entre les acteurs du numérique éducatif (en particulier avec les GAFAM[33] ou les éditeurs scolaires qui sont déjà prêts).

3.1.2. Questionnement autour du consentement

Dans l'article 6 du RGPD, le traitement n'est licite, sans consentement, que lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette disposition intègre les données personnelles demandées par le chef d'établissement pour les outils numériques liées à la scolarité, mais il sera nécessaire de mieux préciser la notion de « mission d'intérêt public » dans le champ scolaire.

En effet, tous les services numériques éducatifs relèvent-ils d'une mission d'intérêt public ? Dans le cas où l'institution sous-traite une mission, sous quelles conditions celle-ci conserve-t-elle son caractère d'intérêt public ? De nombreuses questions se posent, qui ont des conséquences très concrètes. Ainsi, on pourrait s'interroger sur la liberté pédagogique de l'enseignant quant au choix des ressources numériques qu'il entend utiliser dans le cadre de son enseignement. Par ailleurs, le responsable de traitement étant le chef d'établissement ou le DASEN, il existe un risque de tensions au sein des établissements autour de ces sujets.

L'article 8 du RGPD définit les « conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information ». En premier lieu cet article reconnaît qu'un individu de plus de seize ans peut de sa propre initiative « consentir au traitement de ses données à caractère personnel pour une finalité plus ou moins spécifique ». L'article 8 se réfère en cela à l'article 6, paragraphe a. En dessous de cet âge, c'est la personne légalement responsable de l'enfant qui autorise le traitement des données personnelles. Chaque état membre peut abaisser cette limite d'âge à treize ans. Dans la proposition du nouveau texte de loi informatique et liberté actuellement[34] en discussion à l'Assemblée Nationale, l'âge du consentement est fixé à quinze ans probablement par cohérence avec la discussion sur l'âge du consentement aux rapports sexuels. C'est aussi l'âge où le mineur entre généralement au lycée et où sa maturité lui permet en principe de maîtriser les usages sur internet[35].

La France va donc devoir définir dans la loi informatique et liberté l'âge à partir duquel un jeune français est reconnu pleinement responsable de ses données numériques personnelles. Les entretiens que la mission a pu avoir avec les organisations syndicales et les associations de parents d'élèves montrent une inquiétude face aux risques de captation et de traitement des données à l'insu des jeunes. Elles insistent sur les besoins de formation et d'explicitations des conditions générales d'utilisation qu'il faudra rendre accessibles à des enfants de 13, 14, 15 ou 16 ans.

---

[32] Les sous-traitants peuvent être les collectivités territoriales, les industriels du numérique éducatif, des associations etc.

[33] GAFAM, terme qui regroupe les entreprises Google, Amazon, Facebook, Apple et Microsoft.

[34] La nouvelle loi informatique et liberté a été présenté au parlement au mois de janvier 2018 en pleine rédaction du présent rapport.

[35] Propos recueillis par l'AFP auprès de la rapporteure Paula Forteza, de loi informatique et liberté en discussion au parlement en janvier 2018.

Cette nouvelle définition de l'âge du consentement aura des conséquences sur la programmation des apprentissages à conduire chez les élèves, sur les contenus d'enseignement, sur la prise de conscience par les équipes pédagogiques de nouveaux enjeux à enseigner et qui dépassent le cadre strict des disciplines. En effet :

- trois années scolaires séparent un enfant de treize ans et un enfant de seize ans. Si les enjeux autour de l'identité numérique sont bien inscrits dans le socle commun de connaissance et de culture, c'est bien à la fin de la scolarité obligatoire, donc à l'âge de seize ans, que l'on considère que l'ensemble des compétences doit être acquis. Il y a ici un paradoxe qu'il faudra prendre en compte si le législateur abaisse l'âge de consentement. À treize ans il s'agit encore d'accompagner les jeunes dans leurs apprentissages. Les programmes sont écrits de manière à ce que les enseignants puissent programmer sur l'ensemble du cycle les apprentissages à mener, soit durant trois ans. Il faudra accompagner les équipes pédagogiques pour qu'il y ait coïncidence entre l'âge légal du consentement et l'acquisition des compétences indispensables qui permettront aux élèves de prendre des décisions en toute connaissance de cause ;

- seul le programme « d'éducation aux médias et à l'information » aborde la question des données personnelles, et cela de façon très indirecte. Une seule compétence y fait référence : « comprendre ce que sont l'identité et la trace numériques ». On est bien loin de couvrir ici le champ utile à un élève pour comprendre les enjeux liés au traitement de ses données personnelles. Il faudra à la fois préciser cette compétence et former les équipes enseignantes à cette nouvelle dimension. Pour ce faire, une mobilisation du CLÉMI[36] est nécessaire ;

- le programme « d'éducation aux médias et à l'information » n'est pas affecté à une discipline, ce sont les équipes pédagogiques qui doivent s'en emparer. Chaque discipline contribue à développer les compétences inscrites dans ce curriculum. C'est à la fois une force pour permettre de montrer que les enjeux traversent l'ensemble des champs d'études, mais c'est aussi un point de fragilité, car complexe à mettre en œuvre. Les chefs d'établissements devront renforcer le pilotage de cet enseignement si l'on veut espérer former efficacement les élèves.

Quel que soit l'âge que choisira le législateur, le consentement devra s'appuyer sur une maîtrise éclairée des enjeux qui lui sont liés. Aussi, dans la loi d'orientation et de programmation de refondation de l'École, il conviendrait **de compléter l'article 38 (formation à l'utilisation des outils numériques) par** former « aux dimensions éthiques, sociales et économiques de l'utilisation des données numériques, en particulier celles à caractère personnel ».

Préconisation n° 4 : compléter par amendement à la loi informatique et liberté en révision l'article 38 de la loi d'orientation et de refondation de l'École (formation à l'utilisation des outils numériques) par former « aux dimensions éthiques, sociales et économiques de l'utilisation des données numériques, en particulier celles à caractère personnel ».

[36] CLÉMI, centre de liaison d'éducation aux médias et à l'information, service du réseau Canopé.

3.1.3. Une explicitation des finalités d'utilisation des données, une information renforcée auprès des usagers de services numériques en particulier pour les mineurs

Le RGPD renforce l'information sur les finalités d'utilisation des données. Il est demandé aux responsables de traitement de fournir une information simple, claire, et facilement compréhensible par les personnes concernées au sujet du traitement de leurs données personnelles. Par ailleurs, c'est la première fois que dans la législation européenne, des dispositions spécifiques pour les mineurs sont proposées. Outre l'âge du consentement[37], il est demandé que l'information sur le traitement des données pour les mineurs soit rédigée de manière à ce que les enjeux puissent être compréhensibles par des enfants. Ces dispositions sont très contraignantes pour les responsables de traitement au sein de l'éducation nationale, en particulier pour les chefs d'établissement et les équipes pédagogiques qui devront y apporter une attention particulière et faire preuve de pédagogie sur ce sujet sensible.

Préconisation n° 5 : Éditer au niveau national des documents précisant la nature des données collectées et des traitements effectués, destinés à être distribués aux publics concernés : chefs d'établissements, professeurs, parents, élèves. Ces documents devront être rédigés dans un langage adapté à leur public et facilement modifiables par les responsables de traitement locaux.

3.1.4. De nouveaux droits, la portabilité et le droit à réparation des dommages matériel ou moral

Plusieurs nouveaux droits sont intégrés dans le RGPD. Il convient d'insister sur deux d'entre eux, le droit à la portabilité et le droit à réparation des dommages matériels ou moraux qui renforcent la responsabilité des DASEN et des chefs d'établissement.

Le droit à la portabilité permet à une personne de récupérer les données à caractère personnel qu'elle a fournies sous une forme réutilisable et transférable. L'objectif est de redonner la maîtrise de la donnée à chaque personne, et de rappeler à l'usager qu'il est le seul propriétaire de ses données. Le responsable doit donc mettre en place les outils pour permettre cette portabilité. Il est important de souligner que ce droit à la portabilité est lié au consentement. L'article 20 du RGPD prévoit que l'exercice du droit à la portabilité ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement. Comme nous l'avons souligné, le consentement ne serait pas requis dans le cadre scolaire puisque le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

Le droit à réparation des dommages matériel et moral donne la possibilité à toute personne ayant subi un préjudice lié à la violation du RGPD de demander réparation auprès du responsable de traitement ou du sous-traitant. Les contentieux liés au traitement de données au sein de l'éducation nationale pourraient augmenter sensiblement et impliquer directement la responsabilité des chefs d'établissement et des DASEN qui n'ont pas les services juridiques actuellement adaptés pour répondre à ces litiges.

---

[37] L'expression du consentement est définie dans le RGPD : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

3.1.5. Un suivi de l'ensemble des données pour en permettre le contrôle, une gestion renforcée des données en particulier sur leurs traitements, leur stockage et leur durée de conservation

Le RGPD fait évoluer la directive de 1995. En effet, cette directive reposait sur la notion de « formalités préalables » (déclarations, autorisations…), alors que le règlement s'appuie sur une logique de conformité qui vient renforcer le rôle des responsables de traitement avec une dimension de contrôle et d'appui consolidée au niveau de la CNIL.

La protection des données devra se faire dès la conception d'un service (ce qu'on désigne dans le texte de la RGPD par *privacy by design*). Concrètement, il est notamment demandé aux responsables de traitement de limiter la quantité des données de traitement dès la création des dispositifs numériques. Cette nouvelle approche qui vise à alléger les formalités administratives et plus précisément la suppression des obligations déclaratives, passera par une responsabilisation des acteurs du traitement. Dans cette perspective, le ministère, les DASEN et les chefs d'établissement devront mettre en place les outils pour garantir cette conformité et assurer ainsi la protection optimale des données personnelles.

Les principes d'autorisation pourront être maintenus dans le cadre législatif national mais aussi remplacés par des nouvelles procédures centrées sur des études d'impact concernant la vie privée. Il est nécessaire d'analyser plus précisément la mise en place de ces études d'impact dans le champ scolaire et d'inscrire leurs spécificités dans la nouvelle loi informatique et liberté. En effet, ces études d'impact menées par les responsables de traitement ont pour objectif de faire apparaitre les caractéristiques du traitement, les risques et les mesures adoptées. Même s'il s'agit essentiellement d'études d'impact sur les données sensibles, ces procédures peuvent aussi reposer sur des traitements en lien avec « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire le profilage. Dans le cadre des nouveaux outils numériques dans le domaine pédagogique, la différentiation des apprentissages pourrait être opérée par des dispositifs de profilage en particulier avec les services dit d'*adaptive learning*[38]. Il pourrait être proposé que dans le champ scolaire le responsable de traitement diligente systématiquement des études d'impact sur le traitement des données scolaires en s'appuyant sur l'expertise des DPD.

Par ailleurs, l'article 40 du RGPD prévoit la création de codes de conduite destinés à contribuer à la bonne application du présent règlement, prenant en compte la spécificité des différents secteurs de traitement. Le code de conduite permet aussi d'en définir les modalités d'organisation. Cette disposition est particulièrement adaptée au ministère de l'éducation nationale dans le cadre de la régulation des initiatives prises par les responsables de traitement et la formalisation des relations avec les sous-traitants. La particularité de cet instrument réglementaire est de pouvoir intégrer des spécificités liées à l'environnement dans lequel il s'inscrit.

À la différence de la charte de confiance, ces codes sont contraignants juridiquement. Ils doivent être validés par les organismes de régulation nationaux. Pour le ministère de l'éducation nationale, il s'agira de définir les contours du ou des codes de conduite garantissant la mise en place du RGPD.

La question de l'utilisation des données à des fins de recherche est aussi une composante à considérer. En effet, les chercheurs ont été amenés à s'autogérer en développant leurs propres

[38] L'*adaptive learning* ou en français « apprentissage adaptatif » a pour objectif d'adapter les supports d'apprentissage en fonction des besoins et des compétences de chaque apprenant.

règles déontologiques sur l'utilisation des données personnelles, à travers la création des commissions d'éthique, de charte, ou de conventions entre laboratoires de recherche régissant l'utilisation des données. La DEPP qui agrège un nombre important de données personnelles respecte les règles de la statistique publique dont les dispositions sont à certains égards bien plus contraignantes[39] que les lois et règlements spécifiques sur les données personnelles, en particulier dans le domaine du transfert et de l'anonymisation. Par exemple, quand des chercheurs souhaitent utiliser des données de la DEPP, ils doivent se déplacer dans leurs bureaux pour limiter le transfert des données et garantir ainsi une traçabilité du traitement des données, selon les règles du CASD[40].

Dans le cadre des recherches actuelles en particulier sur les champs des neurosciences ou de l'*adaptive learning*, des laboratoires ont besoin de disposer de corpus de données d'apprenants (anonymisées sur plusieurs domaines et longitudinales[41]) pour tester et comparer leurs propositions sur ces données. Le lien entre la DEPP et le monde de la recherche pourrait être développé avec un protocole précis qui reprendrait les grandes lignes des chartes existantes[42] et s'inscrirait pleinement dans une dynamique ouverte en direction du monde de la recherche. Ces relations avec le monde de la recherche pourraient être intégrées dans le code de conduite qui pourrait être mise en place dans le domaine scolaire.

Préconisation n° 6 : Proposer que dans le champ scolaire le responsable de traitement diligente systématiquement des études d'impact sur le traitement des données scolaires en s'appuyant sur l'expertise des DPD. Il est aussi demandé dans un second temps qu'il puisse être proposé un code de conduite spécifique pour le traitement des données scolaires.

3.2. Le déploiement du RGPD

3.2.1. Une architecture incompréhensible des dispositifs numériques actuels concernant les traitements de données

Aujourd'hui, le ministère de l'éducation nationale s'est focalisé sur la création de référentiels techniques de tout genre[43], qui rendent illisible la vision globale ministérielle sur les enjeux autour des données. Si tous les acteurs reconnaissent que le schéma directeur des espaces numériques de travail (SDET)[44] a pu être structurant dans la mise en place des ENT dès le début des années 2000, certains pensent qu'il peut constituer aujourd'hui un frein pour répondre aux attentes des usagers.

Tous conviennent cependant que c'est au ministère d'assurer le cadre du contrôle et de la sécurité de la saisie, du traitement, de la transmission et du stockage des données avec un besoin fort de normalisation. *A contrario*, ils critiquent la position des directions de l'administration centrale qui privilégient avant tout des procédures techniques au détriment d'approches plus juridiques, en

[39] La loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques fixe la référence au secret comme l'une des caractéristiques majeures des enquêtes réalisées par la statistique publique.
[40] Centre d'accès sécurisé aux données.
[41] Voir sur les techniques d'anonymisation, l'avis de la Commission européenne :
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf
[42] Exemple de charte sur le projet Hubble
http://hubblelearn.imag.fr
[43] SDET, CARMO, CARMIN, GAR, projet de charte de confiance…
[44] Cf. http://eduscol.education.fr/cid56994/sdet-version-6.0.html

particulier dans la création de clauses au sein des contrats entre les établissements et les services numériques. La complexité à laquelle les acteurs sont confrontés dans la mise en place du gestionnaire d'accès aux ressources développé par le ministère (GAR) vient confirmer un sentiment d'inadaptation des outils mis en œuvre par le ministère.

En tout état de cause, il conviendrait de s'assurer que l'ensemble des référentiels soient en conformité avec les règles du RGPD.

Par ailleurs, la charte de confiance portée par la DNE, lancée au printemps 2017, n'est pas encore signée, et apparait déjà dépassée face aux questions suscitées par la polémique sur l'ouverture des annuaires académiques et surtout par la possibilité d'avoir recours à des codes de conduite contraignants (voir ci-dessus). Un sentiment d'iniquité est très présent chez les acteurs industriels français par rapport à d'autres sociétés étrangères. Le RGPD vient perturber les principes régissant la diffusion et l'accès aux ressources numériques (contenus et services). Il apparaît donc urgent d'établir un nouveau schéma de cohérence globale de ces règles, compréhensible par les usagers (et pas seulement par les spécialistes) et veiller à ce que tous les acteurs s'y conforment en particulier les GAFAM. Cette vision des principes structurant l'utilisation de ressources numériques dans un cadre éducatif ne doit pas être perçue comme une question à caractère technique, elle est de nature politique et doit être portée par les plus hauts responsables du ministère.

3.2.2. Des flux de données au sein d'un ensemble applicatif dense dans l'éducation nationale

Dans le premier degré le stockage des données scolaires et leur gestion opérationnelle sont effectués au travers de la base élève 1er degré (BEI1). Elle permet de recenser au niveau de chaque école les élèves inscrits, d'affecter les élèves aux classes, de suivre la scolarité, les passages, les radiations, etc. À partir de cette base, et cela depuis janvier 2015, des fiches de liaison normalisées peuvent être éditées pour des échanges avec les représentants légaux des élèves. Au moment de sa première inscription, l'élève se voit attribuer un numéro national d'identification (INE) qui le suit durant toute sa scolarité. C'est la base nationale des identifiants des élèves (BNIE) qui l'attribue. BE1D est relié à l'application AFFELNET 6e qui permet l'affectation des élèves en classe de 6ème.[45]

Dans le second degré, c'est le **système SIECLE** (Système d'information pour les élèves en collège et lycée et pour les établissements) qui contient les données des différents domaines de la scolarité. Le système est subdivisé en dix applicatifs principaux, spécialisés chacun dans un domaine :

- SIECLE base élèves établissements qui gère le dossier administratif des élèves avec des données sur l'identité et les coordonnées des élèves et de leurs responsables ; l'affectation de l'élève depuis l'établissement jusqu'aux groupes auxquels il appartient ; le redoublement éventuel, l'hébergement, les bourses, les circuits de transport ; la scolarité antérieure ; les attestations et diplômes obtenus. C'est à partir de cette base qu'à des fins de pilotage, des listes peuvent être générées avec des données sélectionnées ;
- SIECLE vie scolaire qui permet la gestion de l'ensemble des évènements de la vie scolaire ;

[45] À partir du rapport n° 2015-054 de l'IGAENR, *Adoption des systèmes d'information à la gouvernance du premier degré et au pilotage des écoles*.

- SIECLE notes qui permet la saisie des évaluations ;
- SIECLE décrochage ;
- SIECLE orientation qui permet des échanges avec des systèmes d'information d'autres ministères ;
- SIECLE SIPA pour suivre les inscriptions et les places vacantes ;
- SIECLE LSU qui permet de suivre l'acquisition des compétences du socle et de valider les niveaux de maitrise ;
- SIECLE LSL qui permet de renseigner le livret scolaire en lycée ;
- SIECLE Bourses pour la gestion des bourses en collège
- SIECLE GFE pour la gestion des frais liés à l'hébergement des élèves.

Les personnes habilitées peuvent mener des requêtes et obtenir des listes d'élèves associés aux données sélectionnées. Les chefs d'établissements rencontrés par la mission soulignent l'efficacité de ces outils et le recours régulier à des extractions, mais ils reconnaissent ne pas s'interroger sur les éventuelles conséquences des traitements réalisés.

Le système SIECLE est relié à d'autres applications de l'éducation nationale qui permettent de gérer d'autres données scolaires : les affectations après orientation des élèves[46], la gestion de l'École ouverte[47], la gestion des examens depuis l'inscription jusqu'à la délibération des jurys[48], les données médicales[49], etc.

Pour l'enseignement privé sous contrat, deux bases de données stockent les informations scolaires : ANGE 1D et ANGE 2D respectivement pour le premier et le second degré au sein du système GABRIEL. Des interfaçages et des échanges de données se font avec le logiciel FNOGEC qui permet de gérer les aspects financiers, dont les payes.

Un deuxième ensemble d'applications permet de gérer la structure et les services des enseignants[50]. Par exemple des échanges de données se font entre la base de données élèves hébergée dans SIECLE et l'application STS-Web. Les services des enseignants sont associés entre autres aux élèves au travers des groupes et des classes.

Des flux de données scolaires vers les collectivités territoriales et vers des prestataires privés

Les collectivités territoriales sont destinataires de flux de données scolaires. Les mairies peuvent être reliées à la base élève du premier degré BEI1. Elles peuvent accéder à BE1D avec des droits d'accès spécifiques pour réaliser les inscriptions et gérer les activités périscolaires. Ces flux d'informations

[46] Deux applications permettent de gérer les affectations : AFFLENET pour l'entrée en 6ème, le post 3ème et l'affection en première ; PARCOURS SUP qui va permettre à partir de 2018 de gérer l'affection des élèves dans le supérieur.

[47] Application « École ouverte »

[48] Le portail OCEAN est interconnecté à SIECLE. Les différents modules permettent l'inscription des élèves et le suivi par le chef d'établissement, la saisie des contrôles continue, la gestion des salles et des listes pour les examens, la saisie des notes des épreuves, etc.

[49] Le logiciel SAGESSE (Système automatisé gestion santé établissement) destiné aux personnels infirmiers des établissements scolaires du second degré.

[50] Application STS Web.

entre écoles et mairie via des réseaux numériques sont encore peu développés du fait de la diversité des systèmes utilisés dans les communes[51]. Les conseils départementaux ou les régions peuvent recevoir certaines informations extraites de la base SIECLE. Il peut s'agir d'informations aussi variées que la scolarité des élèves, le niveau de revenu des responsables légaux, le niveau d'attribution des bourses, etc. Une région centralise ces données via la carte jeune associée spécifiquement aux lycéens pour gérer l'attribution de matériel informatique par exemple.[52]

Des entreprises privées sont également destinataires de flux de données scolaires. C'est surtout le cas des entreprises qui gèrent les ENT ou les données de la vie scolaire de façon à ce que les élèves, quand ils se connectent, puissent être associés à la bonne classe, au bon groupe, etc. C'est le cas aussi, et pour les mêmes raisons, des logiciels offrant des ressources pédagogiques comme les BRNE. Cette interconnexion permet lors d'un changement de classe ou d'établissement d'associer immédiatement l'élève aux ressources et aux services auxquels il peut accéder.

Des flux de données sur des réseaux protégés, mais en général non cryptés

Au sein de l'éducation nationale, l'accès complet aux bases de données et leur modification ne peuvent se faire qu'à partir du réseau administratif[53] et pas sur les réseaux pédagogiques. Néanmoins une partie des données personnelles des élèves est accessible à partir du réseau pédagogique via les applications de vie scolaire ou de suivi des évaluations par exemple. Il n'y a donc pas d'étanchéité entre les deux réseaux. Entre les applications d'un établissement, les données sont transmises sur des réseaux protégés et les données sont transmises « en clair » sans être cryptées.

Les mêmes protocoles de transmission sont utilisés quand des flux de données sont échangés entre les serveurs de l'Éducation nationale et les collectivités territoriales de rattachement ou entre l'Éducation nationale et les entreprises privées impliquées dans les ENT ou les ressources pédagogiques mises à disposition des élèves.

Enfin l'une des sociétés qui produit des applicatifs de gestion de la vie scolaire et des emplois du temps utilise les mêmes protocoles de transfert de données. Les fichiers qui sont reçus des établissements sont dans des formats très facilement lisibles du type « CSV ».

Un exemple de société qui met en place un cryptage... mais qui a un coût

L'une des sociétés privées qui propose une suite logicielle de gestion de la vie scolaire et des emplois du temps a mis en place un système de cryptage de haut niveau des données. Ici toutes les étapes des transferts sont concernées par ce cryptage : de la base élèves SIECLE vers les serveurs de la société, des serveurs de la société vers les établissements ou vers d'autres acteurs comme les collectivités territoriales ou les sociétés qui produisent des ressources pédagogiques ou encore celles qui gèrent les ENT.

---

[51] Cf. note 45.

[52] Expérimentation dans la région Occitanie.

[53] Dans les établissements scolaires il existe deux types de réseaux, le réseau administratif et le réseau pédagogique. Les machines connectées au réseau administratif accèdent aux logiciels de gestion (système SIECLE et autre). Seuls les chefs d'établissement, les gestionnaires et des personnels habilités y accèdent avec des identifiants propres. Les élèves et les professeurs accèdent au réseau pédagogique où sont disponibles les applications de vie scolaire, les logiciels pédagogiques, l'ENT, les services éducatifs, etc.

La « clé de cryptage » est facturée à toutes les structures qui souhaitent pouvoir exploiter les informations détenues par la société y compris celles qui ne peuvent plus, en théorie, être directement rattachées à un individu (nombre d'élèves quittant l'établissement aux différentes heures pour gérer les transports scolaires, nombre d'élèves demi-pensionnaires, etc.). Cette rémunération supplémentaire sur des données qui n'appartiennent en réalité pas à la société a posé question à la mission.

D'autres interlocuteurs expriment une réticence à mettre en place de façon systématique un cryptage des données et estiment que les transferts sur des réseaux protégés est suffisant dans le cadre scolaire. Les solutions techniques existent, mais sont complexes à mettre en œuvre et seraient un frein au développement des systèmes. Ils font également remarquer que ce type de procédure alourdit les procédures de connexion des familles et des professeurs qui sont déjà peu enclins à utiliser des mots de passe hautement sécurisés.

Préconisation n° 7 : Faire spécifier dans les contrats passés entre les établissements scolaires et les éditeurs de logiciels de vie scolaire, d'emploi du temps ou d'ENT, que les données doivent être stockées par les hébergeurs sous forme cryptée, les responsables de traitement étant seuls habilités à posséder la clef de décryptage.

La figure 1 (voir page suivante) schématise les échanges de données au sein de l'institution et avec les opérateurs privés fournissant des services numériques.

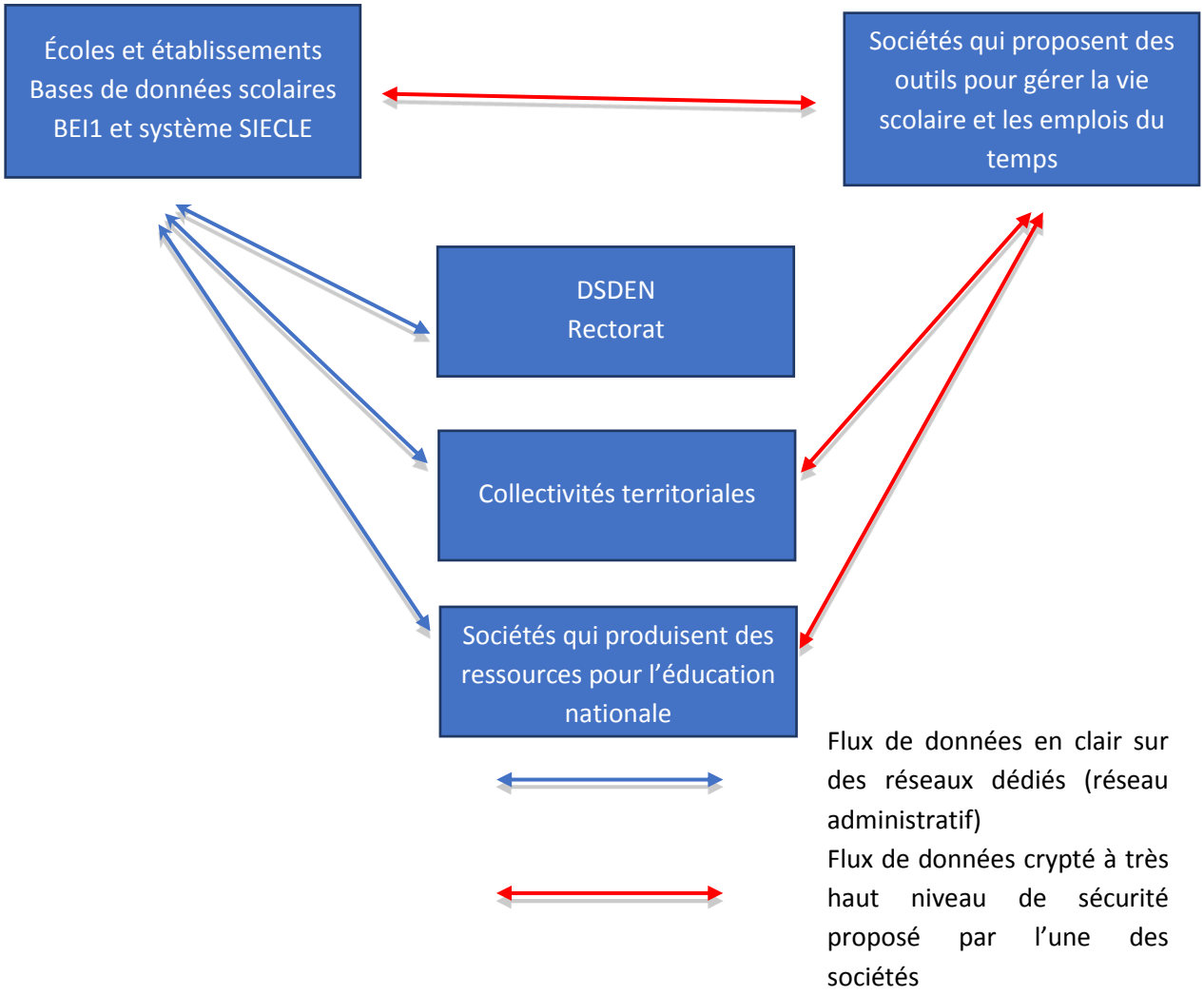
Si l'on peut admettre que des données scolaires puissent être transmises sans cryptage au sein des réseaux dédiés de l'éducation nationale, il apparaît plus surprenant qu'elles puissent être transmises « en clair » vers des prestataires extérieurs. L'un des interlocuteurs de la mission a fait part de son étonnement et regrette que le projet initié par l'éducation nationale et ayant pour objectif de crypter de façon sécurisée toutes les données issues des bases élèves n'ait jamais pu être mené à bien.

Des données transmises qui ne sont pas toujours nécessaires pour les traitements visés

La mission a pu observer que bien souvent des données inutiles étaient transmises à des tiers. Ainsi, la présence des photos des élèves ou des informations sur la profession de leurs parents n'ont guère de justification pour mettre en œuvre des logiciels de vie scolaire (absences, notes, etc.).

Il convient que toutes les personnes ayant à mettre à disposition un fichier de données à caractère personnel pour un traitement particulier adopte un principe de sobriété qui consiste à ne transmettre que les champs de ce fichier utiles et justifiés pour le traitement envisagé.

Figure 1 : Schéma des flux de données associées au niveau de sécurisation



Préconisation n° 8 : Établir une cartographie détaillée de l'ensemble des flux de données scolaires circulant dans l'éducation nationale, dans les collectivités territoriales, les entreprises privées et les associations en précisant leurs relations, la nature des données transmises et leur cryptage éventuel. Il s'agira en particulier de veiller à ce que les données personnelles issues de bases de données gérées par le ministère transmises à des tiers soient systématiquement cryptées.

3.2.3. L'audit en amont des acteurs privés intervenant dans le champ scolaire et utilisant des données personnelles

Aujourd'hui, une difficulté à laquelle est aussi confronté le ministère de l'éducation nationale réside dans sa capacité à contrôler les acteurs privés quant à leur respect des règles en vigueur sur la protection et la sécurisation des données personnelles. Ces entreprises qui proposent des ressources ou services numériques déclarent quand ils répondent à des appels d'offre ou des appels à projet qu'ils sont conformes à législation. Comme il n'existe pas d'audit de ces structures, l'institution n'a aucune visibilité quant à ce qui est réellement fait par ces partenaires de l'école dans le domaine des données personnelles. Il en est de même pour les acteurs publics comme les opérateurs ou les

collectivités territoriales qui gèrent de nombreuses données personnelles en lien avec le champ scolaire. Pour ce qui concerne le stockage des données scolaires par les logiciels de vie scolaire et les ENT, un audit de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) devrait être obligatoire.

Le RGPD prévoit que la responsabilité de ces contrôles revient à la CNIL et qu'elle est la seule autorité à disposer de l'ensemble des outils coercitifs. La mission pense qu'il pourrait être proposé d'effectuer un audit a priori par le ministère (administration centrale, ou inspections générales) quand une entreprise souhaite pénétrer le marché scolaire numérique. Ces audits n'auraient pas vocation à être une barrière à l'entrée, mais ils permettraient d'effectuer des préconisations d'amélioration à partir du moment où ces acteurs ne seraient pas en conformité avec l'ensemble des textes législatifs.

Pour le contrôle des responsables de traitement au-delà des sous-traitants, qui est aussi une autre composante du RGPD, le ministère pourrait accompagner le travail de la CNIL dans ses fonctions de contrôle en s'appuyant sur les inspections générales et plus précisément sur une organisation proche de celle existante pour l'audit interne au ministère de l'éducation nationale et de l'enseignement supérieur et de la recherche[54].

3.2.4. Proposition d'organisation au sein de l'administration centrale et dans les services déconcentrés

3.2.4.1 La place et le rôle d'un DPD

Le ministère de l'éducation nationale devra, dans des délais très courts, nommer des DPD, à la protection des données (en anglais, DPO, *data protection officer*) qui accompagneront les responsables de traitement. Cette mesure majeure du RGPD est une obligation pour l'ensemble des personnes publiques[55]. Les sous-traitants devront aussi répondre à cette obligation lorsque les activités de base […] du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.[56]

Le DPD joue le rôle de « chef d'orchestre » de la conformité en matière de protection des données au sein des organisations. Il est chargé :

- d'informer et d'accompagner les responsables de traitement, ainsi que l'ensemble des agents du ministère ;
- de contrôler la conformité au RGPD et plus généralement au droit en matière de protection des données ;
- de conseiller les responsables de traitement sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ;
- de coopérer avec la CNIL et d'être le point de contrôle avec celle-ci.

[54] Il s'agit d'une mission ministérielle qui s'appuie sur des IGAENR et les services de l'audit interne du ministère. Ce sont les IGAENR qui effectuent les missions d'audit auprès des directions, services déconcentré, …

[55] Art. 37 à 39 du RGPD.

[56] Art. 39 du RGPD.

La place de cette nouvelle fonction au sein de l'éducation nationale nécessite d'être interrogée. Elle est stratégique et justifie la création d'un emploi fonctionnel. Il ne s'agit pas d'un simple glissement linguistique entre CIL et DPD, mais d'un réel changement de périmètre d'intervention, de nature des dossiers à traiter et de responsabilités. Il semble que le ministère n'a pas encore pris la pleine mesure de ces enjeux organisationnels en particulier dans les services déconcentrés. En effectuant un comparatif avec d'autres pays, la mission a pu observer que certains avaient déjà proposé un accompagnement spécifique[57], pour les chefs d'établissements, les parents… Il est essentiel de préciser le positionnement institutionnel de ces DPD. La montée en compétence des personnels qui assumeront ces responsabilités est urgente au sein des académies. Cette nouvelle fonction nécessite une triple compétence : juridique (il convient de bien connaitre l'environnement juridique relatif aux données à caractère personnel), technique (un minimum de compréhension des techniques de captation, de traitement et de stockage des informations est indispensable) mais une bonne connaissance du contexte particulier de l'éducation nationale (pédagogique et administratif) est indispensable afin de pouvoir analyser les pratiques des personnels de l'éducation nationale au niveau des écoles, des établissements scolaires et des services administratifs en lien avec les enjeux de la protection des données personnelles.

3.2.4.2 Organisation au sein de l'administration centrale

Le positionnement du DPD est stratégique. La DAJ et la DNE étant sous la responsabilité hiérarchique directe du secrétariat général (partagée en ce qui concerne la DNE avec la DGESCO), la mission pense que le DPD doit être positionné auprès de la secrétaire générale. Cette place lui permettra en effet d'une part d'avoir l'autorité indispensable et une vision transversale sur l'ensemble des champs concernés que sa mission nécessite, d'autre part de répondre aux nombreuses questions auxquelles il sera confronté en conjuguant volet juridique et pratiques de terrain. Il convient ainsi d'éviter la situation qui préside actuellement dans l'organisation de l'administration centrale où des informations vers les académies sur le RGPD émanent soit de la DAJ (qui n'a pas obligatoirement toutes les connaissances techniques nécessaires dans le domaine du numérique) soit de la DNE (qui dispose d'un spécialiste juridique en interne sans pour autant être l'interlocuteur officiel de la CNIL). Par ailleurs, l'importance de la formation des chefs d'établissement dans le déploiement du RGPD pendant quelques années nécessitera un accompagnement spécifique de l'ESENESR par le DPD.

Pour la mission, il semble essentiel que ce DPD soit positionné sur un emploi à temps complet et dans l'organigramme du ministère de façon pérenne. Cependant, dans un premier temps, il pourrait être envisagé de nommer rapidement un directeur de projet « *préfigurateur de la mise en œuvre du RGPD au sein de l'éducation nationale* » afin d'accompagner la secrétaire générale dans le déploiement du RGPD. Ce directeur de projet pourrait être opérationnel au début du mois de mai prochain (la nomination nécessite un certain délai : publication de la fiche de poste, sélection des candidats, etc.). Ce directeur de projet, préfigurateur du déploiement du RGPD, pourra participer aux choix des DPD dans les services déconcentrés et les accompagner dans leurs nouvelles fonctions, concevoir les formations nécessaires de ces personnes et plus largement des personnels de l'éducation nationale voire de ceux de l'enseignement supérieur et de la recherche, en relation avec l'ESENESR.

[57] https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Préconisation n° 9 : Positionner auprès de la secrétaire générale du ministère de l'éducation nationale un poste de DPD à temps complet. Dans l'attente de cette nomination, mettre en place dès aujourd'hui, un groupe projet chargé de la mise en œuvre du RGPD.

3.2.4.3 Organisation au sein des services déconcentrés

Trois options sont possibles, au niveau des régions académiques, dans les rectorats ou dans les départements auprès des DASEN. La fonction de DPD, élément central dans la capacité du ministère à effectuer un contrôle efficace des données personnelles, devra s'accompagner des moyens pour mener à bien sa mission. Dans une première phase de mise en place, un temps complet dans chaque région académique semble un minimum. Un niveau départemental permettrait une plus grande proximité avec les écoles et les établissements même si ce choix engendre des coûts budgétaires plus importants (postes fonctionnels supplémentaires, formation, etc.) d'autant qu'on peut penser que la question des données scolaires numériques dans les années à venir prendra une autre dimension dans les pratiques pédagogiques et administratives.

D'après le RGPD, ce sont les responsables de traitement qui doivent nommer un DPD. Ainsi, il pourrait y avoir un DPD par établissement scolaire, ce qui parait difficilement opérationnel. Aussi il serait nécessaire de recueillir leur accord pour pouvoir les mutualiser par département ou par académie (disposition prévue dans le RGPD[58]).

Il faut aussi rappeler que le rôle du DPD peut être assumé par une organisation tierce, et que, si les académies n'ont pas tout de suite identifié les personnes-ressources, elles pourront faire appel à des sociétés spécialisées. Pour garantir son indépendance, il semble nécessaire que le DPD soit placé directement auprès du recteur de la région académique (ou de l'académie suivant le choix opéré) ou du secrétaire général de la région académique ou de l'académie et se concentrer sur cette seule mission. Un emploi fonctionnel semble indispensable.

Préconisation n° 10 : Demander aux recteurs de nommer à leur côté un DPD sur emploi fonctionnel d'ici la prochaine rentrée scolaire pour au moins les douze régions académiques.

3.2.4.4 Le positionnement du DPD par rapport au projet de Chief Data officer dans chaque ministère

La DINSIC travaille actuellement sur un arrêté ou une circulaire pour demander à chaque administration de mettre en place un *chief data officer*.

Le *chief data officer* aurait pour fonction de développer, promouvoir et valoriser l'exploitation des données. L'idée est de créer ainsi une personnalisation de la tension plusieurs fois signalée dans ce rapport entre les avantages liés à l'utilisation des données et la nécessité de contrôler leur usage, rôle assuré par le DPD. La DINSIC pense qu'il doit exister un cercle vertueux dans les relations entre ces deux acteurs et qu'une même personne ne peut être en charge de ces deux missions.

---

[58] Article 37 : « *Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.* »

Sans juger de l'opportunité de créer un nouveau poste en même temps qu'un DPD (ce qui risque d'engendrer de la confusion sur le terrain), il y a un réel enjeu à ne pas freiner le développement de services, d'outils pédagogiques ou administratifs qui utilisent des données et à ne pas contrevenir à la stratégie d'open data portée par l'État.

3.2.5. Gouvernance, chaine de responsabilité, dispositif pour accompagner le déploiement du RGPD dans un cadre national…

C'est à l'État que revient la responsabilité d'assurer la sécurisation des données numériques à caractère personnel ; le ministère de l'éducation nationale doit prendre la pleine mesure de cette responsabilité. La question de la sécurisation des données numériques à caractère personnel à travers le RGPD est une occasion de remise en ordre. Il peut revenir à l'État en effet, au-delà du cadre légal et contractuel, de fixer une stratégie de prévention des risques, de formation des différents niveaux d'interlocuteurs et de gestion aux enjeux des nouvelles dispositions législatives. Parmi les obligations que la mission a repérées, se trouve la nécessité d'établir une chaîne de responsabilité claire. En l'état, mieux vaut s'armer pour affronter de futurs contentieux et accompagner dans un sens protecteur élèves familles et enseignants, plutôt que de prétendre au risque zéro.

Cependant l'établir s'apparente très vite à une quadrature du cercle.

En première analyse, la situation laisse aujourd'hui apparaître des responsabilités très éclatées.

D'une part, une politique ministérielle prescriptrice mais ne disposant pas des moyens nécessaires à sa mise en œuvre (matériels pour les enseignants et les élèves, abonnements, débit, maintenance, etc.) que vient corroborer la loi de refondation dans ses articles 21 et 23 ; d'autre part des collectivités territoriales de libre administration peu enclines à dépenser pour satisfaire aux demandes du ministère (le choix de certains applicatifs – moteur de recherche , réseaux sociaux… – a été présenté à la mission comme effectué sur la base de la gratuité) ; enfin, des EPLE agissant en autonomie et se retrouvant les véritables décisionnaires par le fait de passer commande d'applicatifs, d'autoriser par exemple des pratiques pédagogiques à partir des moyens personnels de l'enseignant ou de l'élève. L'innovation pédagogique doit s'assurer que les outils sur lesquels elle s'appuie sont conformes à l'esprit du RGPD.

La difficulté principale à la mise en place d'une politique visant à protéger les données, les personnes, et apporter des garanties réside dans l'absence d'un levier performant pour le ministère.

Reprendre la main signifierait y consacrer une enveloppe financière sans précédent et l'exemple des ENT, dont la mise en place reste inaboutie, montre la faible pertinence d'une telle approche. Dans tous les cas les délais semblent irréalistes.

Contraindre les collectivités ne parait guère plus satisfaisant sans moyens correspondants ; il s'agirait d'aller à rebours de plusieurs décennies de décentralisation. La mission préconise plutôt de confirmer la confiance placée dans chaque interlocuteur. Le RGPD s'imposera en effet à tous, le ministère prenant la main et fixant à chaque niveau d'intervenants dans la chaine ses droits et devoirs, sans pour autant se substituer aux responsabilités respectives. Dans la future loi informatique et libertés, la transcription en droit français du RGPD pourra donner le cadre qui

permette au MEN pour les décisions d'utilisation, d'achat, de location d'outils numériques pédagogiques ou administratifs, de fixer les références pour chaque acteur.

Et il pourrait le faire à partir d'une triple exigence : souveraineté / sécurité / responsabilité.

L'administration centrale du ministère de l'éducation nationale devra se doter d'une instance ou commission en capacité de pouvoir structurer le déploiement du RGPD, de faire le lien avec les instances de régulation sur les enjeux politiques, d'animer la communauté des DPD, et d'accompagner la création des codes de conduite. À très court terme, il semble urgent de nommer un chef de projet auprès du secrétariat général avec un groupe projet mobilisant l'ensemble des acteurs du ministère : administration centrale et services déconcentrés.

3.2.6. Création d'un comité d'éthique et d'expertise sur l'intérêt public de l'utilisation de données scolaires

Plusieurs interlocuteurs ont montré leur intérêt pour la constitution d'un comité d'éthique des usages du numérique dans l'éducation. Organe consultatif, il pourrait en particulier se prononcer sur les questions éthiques éventuellement posées et l'intérêt public de l'utilisation de données récoltées ou traitées dans le cadre scolaire. Pour nos interlocuteurs, l'indépendance d'un tel comité ne pourrait être garantie s'il était hébergé par la CNIL qui est un organisme de régulation et de contrôle (mission renforcée par le RGPD). Il est opportun de rappeler que la CNIL a cependant, ces dernières années, été missionnée sur des questions d'éthique et non seulement sur des enjeux de régulation. Certains chercheurs s'étaient élevés contre cette extension des missions de la CNIL. D'un autre point de vue, certains soulignent qu'un comité d'éthique spécifique aux données scolaires présenterait un risque de déresponsabilisation des acteurs ; en effet, les responsables de traitement au lieu de prendre les décisions qui leurs incombent, pourraient être tentés de les remonter systématiquement à cette instance.

Quelques exemples des questions éthiques en lien avec des usages numériques spécifiques

Certains usages peuvent, même lorsqu'ils respectent le cadre juridique, soulever des interrogations quant à leur caractère acceptable ou souhaitable d'un point de vue social ou éthique. Cela pourrait être le cas, notamment s'agissant d'une expérimentation menée actuellement dans l'Oise (académie d'Amiens) depuis novembre 2017. Des élèves sont équipés de bracelets connectés entre leur domicile et l'école puis, à l'heure du déjeuner, entre l'école et la cantine. À la montée et à la descente du bus, chaque bracelet est détecté par un smartphone qui envoie automatiquement un SMS et/ou un courriel aux parents, afin de les informer que leur enfant est bien arrivé.

À Toulouse l'utilisation du logiciel de gestion de cantine ALISE Arc en Self, logiciel privé permettant de gérer les exigences alimentaires des élèves, peut aussi interroger. En début d'année, les élèves renseignent obligatoirement leurs exigences alimentaires. Il s'agit d'organiser au mieux la demi-pension et donc en fonction des différents jours de savoir combien il faut prévoir de repas spécifiques. Il est dès lors possible, d'après la proviseure, d'éditer la liste des élèves et leur exigence alimentaire et d'en déterminer des appartenances religieuses.

Face à ces interrogations, la mission estime que les multiples décisions auxquelles vont être confrontés les DPD nécessiteront sans doute dans certains cas de pouvoir disposer d'un avis éclairé qui dépasse le cadre purement juridique. Par ailleurs, la création d'un comité d'éthique peut s'avérer

être un signal politique fort destiné aux acteurs (syndicats, parents d'élèves, associations) qui insistent pour que soit reconnu le caractère spécifique des données scolaires. Cette création pourrait accompagner, en se plaçant au niveau des principes, les mesures de nature administrative occasionnées par la mise en place du RGPD (notamment la création de la fonction de DPD).

Si la décision était prise de mettre en place un tel comité, trois possibilités se présenteraient :

- l'intégration de la thématique « éducation » dans un comité interministériel « éthique et numérique » souhaité par de nombreux responsables d'organismes d'enseignement supérieur et de recherche (cf. tribune du journal le Monde du 14 décembre2017[59]). On peut penser légitimement que la place de l'éducation serait marginale dans une telle configuration comme elle l'est dans les autres organismes de ce type (par exemple le CNNUM) ;
- l'extension du périmètre d'intervention du comité d'éthique CERNA (Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene[60]) déjà mis en place par des chercheurs en informatique issus de différents organismes (INRIA, CNRS, CEA, ONERA). Ce choix permettrait d'éviter la redondance de participation de chercheurs et réciproquement d'intégrer des personnalités du scolaire quand il s'agit de recherche dans le champ de l'éducation ;
- la création d'un comité spécifique à l'éducation nationale auprès du ministre et en appui des actions portées par le DPD ministériel.

Sur ce point l'exemple du ministère des solidarités et de la santé suggère une alternative intéressante. Ce ministère a en effet été confronté aux mêmes questions. Afin d'y répondre, il a créé en son sein l'institut national des données de santé (INDS)[61] par arrêté du 23 avril 2017. Cet institut a mis en place un comité d'expertise sur l'intérêt public, instance consultative formée de personnalités venant d'horizons très variés, qui formule des avis sur l'intérêt public de la finalité de l'utilisation des données de santé et qui conditionne l'autorisation ou l'interdiction de ces utilisations.

La mission préconise qu'un comité analogue avec les mêmes objectifs soit mis en place au sein du ministère de l'éducation nationale. Ce comité d'éthique et d'expertise sur l'intérêt public sur l'utilisation des données scolaires intègrerait des membres de la communauté éducative : administration centrale et déconcentrée, représentants des collectivités territoriales, chefs d'établissement et enseignants, parents d'élèves, représentants des élèves, entreprises privées, associations.

Cette organisation pallierait l'absence d'une législation spécifique pour les données scolaires et pourrait contribuer à construire une doctrine sur les questions relatives à la finalité d'« intérêt public » (cf. RGPD) dans le domaine de l'enseignement.

Préconisation n° 11 : Créer au sein du ministère de l'éducation nationale, un comité d'éthique et d'expertise sur l'intérêt public de l'utilisation de données scolaires qui serait composé de membre de la communauté éducative d'horizons très divers.

---

[59] http://www.lemonde.fr/idees/article/2017/12/14/il-faut-creer-un-comite-national-d-ethique-du-numerique_5229661_3232.html
[60] http://cerna-ethics-allistene.org/
[61] http://www.indsante.fr/

4. De l'anonymat, à l'hébergement, où en sommes-nous sur la sécurité des données personnelles ?

4.1. L'anonymat n'apparaît plus comme étant le seul élément qui garantit la sécurité sur l'utilisation des données personnelles

Les protocoles liés à l'anonymat des données personnelles sont aujourd'hui intégrés par l'ensemble des acteurs, et le transfert de ces données entre des tiers s'effectue selon des techniques de cryptage ou de chiffrement. La question qui se pose réside dans la nécessité d'interroger cette notion d'anonymat à l'aune des puissances de calculs déployés par les outils numériques qui accèdent, même si la donnée est anonyme, à l'identité d'un individu. Ces évolutions technologiques risquent de bouleverser les modèles de réglementation qui ne reposent que sur les données personnelles et intègrent difficilement toutes les autres données indirectes. C'est bien l'analyse matricielle et la compilation de l'ensemble des données produites par les usagers qui n'ont pas a priori de caractère personnel (production de ressources, présences sur les réseaux sociaux, navigation de site web…) qui sont utilisées pour créer des stratégies de profilage. La question du traitement devient alors centrale. C'est bien à ce niveau qu'il faut établir un certain nombre de règles. L'enjeu des traces numériques peut être considérable pour l'éducation nationale. Dans le cadre des services numériques proposés, le profilage est la brique principale des nouveaux services dont les données autres que les données personnelles sont essentielles pour mettre en place des outils qui intègrent la différentiation dans les apprentissages, la prévision des résultats, etc. La directive *e-privacy* (sur les traces, cookies, log…) devrait être remplacée par un règlement dans les prochains mois. L'institution doit anticiper cette évolution pour l'intégrer pleinement selon les spécificités de l'éducation nationale. Il sera difficile d'apporter une réglementation qui offrira toutes les garanties de sécurité : l'information et la formation de l'ensemble des acteurs du ministère doivent devenir une priorité.

4.2. La problématique de l'hébergement des données sur le territoire national

L'hébergement des données sur le territoire peut continuer à être un point de crispation pour certains acteurs qui estiment que l'hébergement constitue un des éléments de souveraineté pédagogique. Cette dimension est essentiellement portée par des associations ou certains industriels. Les associations revendiquent la nécessité de privilégier le recours à un cloud souverain pour l'éducation. Même si cette idée peut apparaitre séduisante, les tentatives sur la création de cloud souverain ont échoué. Certains industriels voient en l'hébergement des données sur le territoire national un avantage concurrentiel par rapport à des acteurs étrangers et en particulier aux GAFAM. Ils mettent en avant les critiques sur le *Privacy Shield*. Cet accord, qui régit les échanges de données entre l'Europe et les États-Unis et qui doit garantir une protection uniforme des deux côtés de l'Atlantique aux citoyens de l'Union, fait l'objet de critiques acerbes. Les CNIL européennes ont livré un premier rapport sévère sur son application et demandent des améliorations rapides[62], un an et demi après sa mise en place.

Pour une majorité des acteurs du numérique éducatif, la question de l'hébergement national ne se pose pas à partir du moment où les données sont stockées en Europe. Pour les usagers, il existe une dimension symbolique forte de savoir leurs données hébergées sur le territoire national.

[62] *Le « Privacy Shield » sous le feu des critiques*, Les Échos, 6 décembre 2017.

La mission estime que les articles du RGPD en lien avec la coopération renforcée entre autorités pour les traitements transnationaux suffiront à garantir la sécurité du stockage des données sur l'ensemble du territoire européen. Par ailleurs, les traitements de données s'effectuent aujourd'hui en flux, l'hébergement peut apparaitre comme une question moins prégnante. Sur ce point, il est important de faire le lien avec les questions soulevées par les traces numériques et les implications sur la protection de la vie privée des usagers.

4.3. Le *e-privacy* ou règlement sur la « vie privée et les communications électroniques »

La directive 2002/58/CE aussi appelé la directive *e-privacy* n'est plus adaptée ni aux nouveaux moyens de communication à partir de l'internet ni en adéquation avec le règlement sur la protection des données personnelles, le RGPD. La Commission européenne fait en particulier état « d'importantes évolutions technologiques et économiques qui se sont produites sur le marché » ; de l'importance de plus en plus grande de « recours aux moyens de communication via le web en lieu et place des moyens de communication traditionnels par exemple : la voix sur IP, la messagerie instantanée ; le courrier électronique web ; etc. ». Ces moyens de communication ne sont pas tous soumis aujourd'hui au cadre réglementaire de l'Union. Elle a décidé de remplacer cette directive par un règlement qui comme pour le RGPD s'impose aux états.

Le nouveau règlement « vie privée et communication électronique » devait prendre effet le 25 mai 2018 c'est-à-dire à la même date que le règlement « général sur la protection des données ». Il est aujourd'hui repoussé à une date ultérieure, tant les compromis sont difficiles à trouver. Ces deux règlements sont complémentaires : « tandis que le RGPD garantit la protection des données à caractère personnel, la directive "vie privée et communications électroniques" préserve la confidentialité des communications, lesquelles peuvent aussi contenir des données à caractère non personnel et des données relatives à une personne morale ».[63]

Cette nouvelle directive « vie privée et communication électronique », souvent dénommée *e-privacy*, s'inscrit dans une série de textes qui permettent de réguler les communications électroniques sur le territoire de l'Union. Ainsi le règlement s'inscrit dans la directive des communications électroniques déjà adoptée en 2016 et dans celle des équipements radioélectriques adoptés en 2014. L'ensemble visant à une plus grande protection des données à la fois dans la conception des matériels, des logiciels, et des pratiques mise en œuvre ; y compris les pratiques commerciales. Juridiquement, elle s'appuie entre autres sur l'article 7 de la charte des « Droits fondamentaux de l'Union européenne » qui concerne le « Respect de la vie privée et familiale » : **« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »**[64].

Le nouveau règlement[65] dans l'état actuel des discussions vise à renforcer :

- le niveau de protection de la vie privée des utilisateurs de moyens de communication ;

[63] Paragraphe 3.1 du texte du 10 janvier 2017, proposition de règlement du parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communication électronique »).

[64] Charte des « Droits fondamentaux dans l'Union européenne », article 7.

[65] Texte du 10 janvier 2017, proposition de règlement du parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communication électronique »).

– les règles de concurrence rendues plus équitables entre les différents acteurs économiques.

Les entreprises vont devoir proposer des solutions matérielles et logicielles permettant d'« assurer efficacement le respect de la vie privée et des communications » des utilisateurs « de moyens de communication par contournement[66] ».

La précédente directive n'a pas permis de « responsabiliser » les utilisateurs. Pour atteindre cet objectif, le nouveau règlement installe le « consentement » lors de l'utilisation des solutions. Il s'agira donc d'avoir une action volontaire de la part des utilisateurs pour accepter certaines conditions d'utilisation. Elles devront rendre transparents les paramètres de confidentialité.

À plusieurs reprises le règlement fait état des risques dans l'exploitation des données des communications électroniques qui, si elles sont traitées, peuvent révéler des informations concernant les personnes physiques ou morales. Les objets connectés[67], les points d'accès WIFI ouverts[68], les logiciels et services de communication électronique, les fournisseurs d'annuaires accessibles au public, les logiciels permettant l'accès à l'Internet sont particulièrement ciblés.

Ce nouveau règlement aura des implications importantes au sein de l'éducation nationale tant le recours à des outils de communication électronique est important au sein des établissements. Il s'agira à la différence de ce qui a pu être constaté dans le déploiement du RGPD d'anticiper sa mise en place et d'effectuer toutes les actions de formation à destination des enseignants qui à la différence des chefs d'établissement, responsable de traitement dans le cadre du RGPD, sont les premiers concernés par ce nouveau règlement qui est en lien direct avec les pratiques pédagogiques innovantes.

4.4. Les recherches dans le domaine de la traçabilité des données

L'exemple de la traçabilité dans le domaine de l'alimentation a été cité par plusieurs interlocuteurs comme étant une voie qui pourrait s'avérer intéressante pour les données scolaires sous forme numérique. Les chercheurs interrogés ont toutefois soulevé les difficultés actuelles concernant le « taggage » de données alphanumériques contrairement aux données audiovisuelles. Une seconde difficulté réside dans la position d'émetteur et non de destinataire du ministère.

Il convient de suivre les travaux en cours dans le domaine du marquage des données voire d'inciter des recherches qui permettraient au ministère et ses administrés de savoir quand les données scolaires sortent du périmètre pour lequel elles ont été transmises.

[66] Les moyens de communication par contournement sont tous les nouveaux moyens de communication utilisant des technologies innovantes : voix IP, Chat, forum, mèl, etc.
[67] Paragraphe (12) du règlement.
[68] Paragraphe (13) du règlement.

5. De l'ouverture des algorithmes à la souveraineté pédagogique des données scolaires

5.1. La transparence des algorithmes, une différence entre le privée et le public

Dans la mouvance de la stratégie *open data* portée par l'État, la loi du 7 octobre 2016 pour une République numérique intègre des dispositions réglementaires sur la nécessité pour les services de l'État de rendre accessibles les algorithmes développés par ses services. Ce nouvel outillage législatif vient renforcer la protection de la vie privée, et renforce le sentiment que chaque usager est bien informé sur le traitement de ses données personnelles. La nécessité pour l'éducation nationale de respecter ces dispositions surtout quand les algorithmes sont utilisés à des fins de profilage ou de recommandations personnalisées est essentielle pour éviter toutes les polémiques comme celles qui se sont produites à propos de l'entrée dans l'enseignement supérieur avec APB. Cette transparence est un outil de souveraineté pédagogique. Il est essentiel de réaliser que la souveraineté en matière de numérique ne repose pas uniquement sur le contrôle mais bien sur un enjeu de transparence et de partage. Cependant, l'ouverture des algorithmes mis en œuvre dans les applications développées par des entreprises privées qui sont utilisées dans le cadre des missions du service public d'éducation n'ont pas un caractère obligatoire. Sans modifier la loi, le ministère pourrait exiger par voie contractuelle d'exiger de ces entreprises la transparence sur leurs algorithmes.

Préconisation n° 12 : Inclure une clause d'explicitation des principes sur lesquels reposent les algorithmes utilisés dans les traitements de données à caractère personnel dans les contrats passés avec les développeurs privés.

5.2. Le traitement des données scolaires par les logiciels de vie scolaire

5.2.1. Une gestion de la vie scolaire des lycées et des collèges publics hors du contrôle de l'État

La grande majorité des établissements scolaires français a choisi des logiciels de vie scolaire[69] développés par des entreprises privées. Une des sociétés occupe une part de marché nettement supérieure aux autres[70] (voisine de 80 %) ce qui lui donne une position de quasi-monopole. Afin d'exploiter leurs services, un certain nombre de données personnelles des élèves et des enseignants sont transmises à ces sociétés. Les établissements ont parfois le choix entre un stockage des données dans l'établissement ou sur les serveurs des entreprises (en général mieux sécurisés que ceux des établissements).

Il ne s'agit pas d'une externalisation ordinaire d'un service, mais d'une véritable délégation de service public qui ne dit pas son nom, sans aucune interaction avec l'administration centrale du ministère, chaque établissement contractualisant directement avec ces sociétés, conséquence de trente ans d'histoire qu'il sera maintenant difficile de faire évoluer.

[69] Création d'emploi du temps, gestion des retards et des absences, saisie des notes, communication avec les familles, etc.).

[70] Cette entreprise couvre 7 000 établissements scolaires français (6 000 publics et 1 000 privés) ; 4 000 établissements ont leurs données scolaires hébergés sur le serveur de la société.

La question se pose de la requalification éventuelle des marchés passés avec chaque EPLE pour ces logiciels de vie scolaire : chacun est certes sous le seuil des marchés publics nécessitant une mise en concurrence, mais de très nombreux établissements publics étant concernés, on peut s'interroger sur le fait que la qualification de marché fractionné ne s'applique pas. De plus, ces marchés sont reconduits annuellement sur une très longue période (éventualité du dépassement dans ce cas du seuil des marchés publics). Les montants annuels globaux représentant l'acquisition de ces produits (de l'ordre d 25 M€) nécessitent une expertise juridique approfondie au regard du droit européen et national de la commande publique. Il convient probablement d'interroger sur ces sujets, au-delà de la mission des achats du ministère, les services de Bercy.

Cette situation pose par ailleurs de nombreux problèmes de sécurité et de pérennité des données, d'encadrement des traitements et de continuité du service public en particulier lors de la mise en œuvre d'une réforme qui nécessite une évolution des fonctionnalités de ces logiciels[71].

Préconisation n° 13 : Confier au ministère de l'économie une expertise approfondie, au regard du droit national et européen, sur la passation des marchés entre les EPLE et les sociétés éditant les logiciels de vie scolaire les plus utilisés.

5.2.2. Le stockage des données des élèves et des professeurs sans aucun regard de l'État sur la sécurité des serveurs les accueillant

La mission a pu constater qu'aucun audit des conditions de stockage des données transmises par les établissements à ces sociétés (quand ils choisissent cette option) n'est conduit par un service de l'État (en particulier l'ANSSI). Il serait nécessaire que ces entreprises soient homologuées au sens du RGS (référentiel général de sécurité). Eu égard aux cyberattaques de plus en plus nombreuses et à la sensibilité du type de données traitées, la mission considère qu'il est nécessaire de remédier rapidement à ce point et de diligenter des audits sur les serveurs des entreprises accueillant des données scolaires. L'ANSSI devrait pouvoir être mobilisée sur ce point.

Il convient ici de rappeler que ce n'est pas le seul cas concernant des services de l'éducation nationale externalisés ; ainsi la mission IGEN / IGAENR, conduite en 2016-2017 sur les processus qualité et sécurisation des examens, avait alerté le ministère sur le stockage des copies de baccalauréat dans le cadre de l'expérimentation sur la dématérialisation de leur correction. Suite à cette alerte, la société concernée vient d'engager un processus de certification de sécurité de 1er niveau auprès de l'ANSSI. Cette démarche pourrait être exemplaire pour les autres services numériques portés par l'institution et les acteurs privés.

Préconisation n° 14 : Exiger une certification ANSSI de premier niveau au moins pour tous les contractants hébergeant des données scolaires à caractère personnel.

[71] Par exemple la récente réforme du collège n'aurait pu se mettre en place sans une évolution des logiciels de création d'emplois du temps, évolution sur laquelle le ministère n'avait aucune prise.

5.2.3. Le cryptage et la portabilité des données d'apprentissage

5.2.3.1 Le cryptage

Depuis le passage en mode hébergé de certains logiciels, la mission a eu connaissance que, dans le cas le plus répandu, les données scolaires exportées à partir de ces logiciels sont cryptées, officiellement pour sécuriser les échanges.

Pour pouvoir exploiter les données scolaires dans le cadre des projets d'ENT, par exemple, il est nécessaire de payer une clé de décryptage annuelle en plus de la licence sur un des logiciels. Le financement du décryptage est pris en charge par les collectivités ou les éditeurs ENT.

Rappelons que les chefs d'établissement, en tant que responsables du traitement, sont tenus de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (article 34 de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978).

Par ailleurs, l'accès aux ressources numériques, au LSU et à d'autres contenus ou services transite souvent par ces outils qui se substituent en ce sens aux ENT. Ce passage est parfois accompagné d'un octroi perçu par la société éditrice de logiciels de vie scolaire qui crypte les données scolaires qui lui sont transmises. Il est à noter que cette clé n'est pas accessible aux établissements qui souhaiteraient mettre en œuvre leur propre solution : ceux qui l'ont demandé à l'éditeur ont essuyé un refus de vente.

Préconisation n° 15 : Demander aux entreprises contractant avec des établissements de l'éducation nationale la liste des prestataires auxquels elles font appel pour la mise en œuvre de leurs services. Clarifier les engagements contractuels vis-à-vis de l'utilisation des données scolaires par ces sous-traitants.

5.2.3.2 La portabilité des données d'apprentissage, le déploiement des LRS (learning record store)

Il semble important pour la mission de rappeler les évolutions technologiques actuelles en matière de norme dans le domaine de la portabilité et du transfert des données en particulier dans le champ du numérique éducatif (ou *Digital learning*). Il s'agira pour le ministère d'être particulièrement attentif à ces évolutions avec le déploiement, par exemple de solution comme les LRS. Le LRS est une base de données dont le rôle est de stocker des traces d'apprentissage. Ces données, une fois stockées, sont accessibles par d'autres applications. L'enregistrement des données dans le LRS, ainsi que leur récupération par des applications tierces, se fait par un mécanisme standardisé qui s'appuie sur une interface de programmation applicative[72]. La norme LRS est un changement majeur et va être amenée à remplacer les spécifications SCORM[73] qui n'utilisent pas la technologie API freinant les

[72] Ou API (*application programming interface*) qui est un ensemble normalisé de classes, de méthodes, ou de fonctions qui permet à un logiciel d'offrir des services à d'autres logiciels.

[73] SCORM (*Sharable Content Object Reference Model*) est un ensemble de spécifications et de recommandations techniques permettant la communication entre un fournisseur d'activité *e-learning* et un *Learning Management System* (LMS). SCORM est capable de tracer la complétion d'une activité ainsi que le succès, le temps passé, et le score.

usages et le transfert des données d'apprentissages. La nouvelle norme LRS facilitera les échanges d'information numérique en particulier pour tout ce qui concernera les traces d'apprentissage.

5.2.4. Des traitements, en particulier statistiques, qui devraient interroger le ministère

Les traitements que ces entreprises peuvent opérer sur les données à caractère personnel ne sont pas connus de l'administration. Ils sont très puissants, par exemple statistiques par académie et par type d'établissement sur le nombre d'élèves et de professeurs absents, le nombre d'élèves ayant été exclus de cours, le nombre d'heures professeurs par élèves…

Même si ces statistiques – qui ne sont pas issues du traitement de données en *open data* – n'ont pas un caractère personnel, il n'en demeure pas moins qu'elles sont de nature stratégique. Elles pourraient donner à ces sociétés des avantages concurrentiels dans le développement futur de services pour l'éducation, renforçant par la même la dépendance de l'institution à leur égard. Elles pourraient par ailleurs constituer un élément de pilotage dont l'institution pourrait bénéficier.

5.2.5. Continuité et adaptabilité du service public d'éducation

Les questions soulevées dans les paragraphes précédents interrogent le service public d'éducation quant à sa capacité à assurer :

- une continuité dans la gestion des établissements scolaires en cas par exemple d'arrêt des activités des sociétés éditrices de logiciels de vie scolaire (impossibilité par exemple d'assurer une rentrée scolaire normale faute de pouvoir disposer à temps des emplois du temps) ;
- une mutabilité de ces services afin qu'ils puissent suivre certaines évolutions souhaitées par le ministère (mise en place de réforme ayant des conséquences sur la gestion d'emploi du temps, des absences, etc.) ou permettre l'accès à de nouveaux services pour lesquels les chefs d'établissement demandent un accès via leurs outils quotidiens.

Continuité et mutabilité sont deux principes du service public.

Sur l'ensemble de ces sujets, la mission a eu le sentiment d'avoir fait découvrir à nombre de ses interlocuteurs des problèmes dont ils n'avaient pas pris toute la mesure et il lui est apparu que l'administration centrale prenait connaissance à l'occasion des entretiens menés de l'ampleur des difficultés rencontrées par les acteurs de terrain.

5.2.6. La protection des données rejoint l'objectif stratégique de souveraineté éducative et l'articule à celui de la sécurisation des *process*

Consacrer le caractère stratégique d'actifs dans le secteur de l'éducation mais aussi considérer que les données collectées par les établissements (notations, appréciations, suivis des parcours des élèves, services des enseignants, etc.) constituent un élément de patrimoine susceptible d'être mieux protégé par un contrôle effectif de l'État peuvent apparaitre comme un message fort au moment où nos administrations se préparent à la mise en œuvre du RGPD.

L'État dispose principalement de deux moyens pour protéger les secteurs stratégiques ou sensibles français : la régulation et la participation au capital et aux organes d'administration des sociétés

concernées. En fonction, l'État agit en tant que régulateur ou actionnaire. Les réflexions sur l'efficacité de ces outils se sont multipliées ces derniers temps.

Une des pistes de travail envisagée par la mission consiste en une entrée directe de l'État au capital des sociétés qui présenteraient un caractère hautement sensible pour la protection des données personnelles des enseignants, des élèves, et de leurs familles. Selon les formules choisies, en direct ou via la banque publique d'investissement, Bpi France, avec ou non une minorité de blocage, selon les différents mécanismes de son association ou non à la gouvernance, il consacrerait le caractère d'« actif stratégique » de certaines sociétés françaises.

Il montrerait de plus qu'existent dans le secteur de l'éducation des « pépites numériques » pour lesquelles l'État jouerait un rôle d'accompagnement en lien avec des perspectives de développement international fortes. Elles viendraient prendre une place importante dans une stratégie de positionnement de la France sur le marché mondial de l'ed'tech.

Cette approche équilibrerait celle qui consiste actuellement à ce que l'État cède des participations détenues (par exemple dans le secteur de l'énergie) pour financer son plan de soutien à l'innovation dans le domaine du numérique. On peut considérer en effet que, dans le domaine du numérique aussi, existent des secteurs qui relèvent d'une forme de souveraineté et entrainent *de facto* un contrôle de l'État, ici en l'occurrence la souveraineté pédagogique.

Pour s'approcher des critères actuels définis par l'État actionnaire, ces entreprises doivent répondre à trois critères cumulatifs : produire des services considérés comme publics, être l'objet d'interventions permanentes du politique affectant leur gestion ou leurs équilibres financiers, avoir des ressources importantes provenant du contribuable.

Ces critères pourraient être revus ou affinés dans un cadre législatif afin que cette notion de souveraineté éducative ou encore que le soutien au développement de « champions numériques français », soient effectivement pris en compte.

Diverses approches techniques et financières s'offriraient au gouvernement :

- Une prise de participation de l'APE[74]. Devant les grands enjeux de transitions économiques, technologiques et industrielles, l'État affirmerait que son intervention en fonds propres est justifiée et nécessaire. Il s'assurerait ainsi d'un niveau de contrôle suffisant dans des entreprises intervenant dans des secteurs particulièrement sensibles en matière de souveraineté.

- Une prise de participation de la Bpi. Souhaitant accompagner l'évolution de ces entreprises mais sans participer directement à la gouvernance, l'État pourrait demander à la Bpi une entrée au capital conformément à son rôle d'accompagnement de l'innovation et du développement international ; toutefois les objectifs de souveraineté et de sécurité seraient moins clairement assurés avec cette formule.

[74] L'agence propose au ministre chargé de l'économie la position de l'État actionnaire en ce qui concerne la stratégie des entreprises et organismes figurant sur la liste annexée au présent décret, dans le respect des attributions des autres administrations intéressées. À ce titre, elle analyse la situation économique et financière de ces entreprises et organismes et sollicite les compétences des administrations intéressées. Elle met en œuvre les décisions et orientations de l'État actionnaire. En tant que de besoin, l'agence participe, en liaison avec les administrations compétentes, à l'élaboration des contrats qui lient ces entreprises.

- Un contrat-cadre national avec l'éducation nationale. Devant le constat que les sociétés éditrices de logiciels et de solutions d'hébergements mettant en jeu des données personnelles de la communauté éducative, contractent commercialement en direct avec les EPLE, les collectivités locales ou même des sociétés technologiques qui développent elles-mêmes d'autres applicatifs, il peut être envisagé la conclusion au niveau national d'un cadre global listant une série d'obligations ayant trait à la sécurité, aux protocoles de travail et au respect de la protection des données personnelles. Cela ne peut pour autant contourner les règles en vigueur en matière de commande publique, notamment la mise en concurrence. Une autre direction consisterait alors à faire appel à des groupements d'achats, par exemple à l'échelle d'une académie avec rédaction de cahiers des charges communs, permettant d'envisager des formules proches de la délégation de service public.

Préconisation n° 16 : Faire en sorte que l'État se repositionne vis-à-vis des prestataires de certains services numériques clés, administratifs et pédagogiques, afin de pouvoir exercer sa souveraineté en matière d'éducation.

Sur la question de la souveraineté éducative vis-à-vis de l'international, il pourrait aussi être envisagé d'étendre le décret de 2005 revu en 2011 sur les investissements stratégiques au domaine de l'éducation, réduisant ainsi le risque de prise de contrôle de la gestion de pan entier du secteur éducatif français par des acteurs étrangers.

Préconisation n° 17 : Intégrer l'éducation nationale dans le domaine des secteurs d'activité industriels stratégiques soumis à une autorisation préalable du gouvernement français en cas d'investissements étrangers.

Toutes ces pistes montrent la possibilité d'une gradation dans la réponse publique, à articuler avec le message envoyé en direction des acteurs de la chaine de responsabilité en académie et les objectifs généraux de sécurité et souveraineté.

Conclusion

Aujourd'hui des plateformes[75], publiques ou privées, transforment le fonctionnement du système éducatif français. Comme dans d'autres domaines (Spotify ou Deezer en musique, Uber dans les transports, Airbnb pour la location de logement et bien d'autres), certains services numériques modifient profondément de nombreux processus administratifs (conception d'emploi du temps, gestion des absences, affectation des élèves…) et pédagogiques (accès à l'information, évaluation, individualisation des parcours de formation, organisation des enseignements dans et hors la classe…).

[75] Juridiquement, une plateforme en ligne constitue un système de traitement automatisé de données défini dans les travaux du Sénat comme « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* ».

Les données scolaires, sous toutes leurs formes, sont au cœur de ces évolutions. Pour que le système éducatif conserve la maitrise de son fonctionnement administratif, de sa spécificité pédagogique, pour qu'il puisse mettre en œuvre les orientations souhaitées et éviter qu'il subisse des évolutions imposées par des agents extérieurs, l'institution doit faire preuve d'une grande vigilance.

Afin de préserver les principes d'égalité, de neutralité et de continuité définissant le service public d'éducation, l'État doit se doter de dispositifs contraignants lui permettant de s'assurer la maitrise des échanges et des traitements de données scolaires. Il y a, dans ce domaine, urgence à sensibiliser, informer et former la communauté éducative – dont la marge d'autonomie est grande dans le choix et l'utilisation de services numériques – sur les enjeux de la protection des données – sans pour autant remettre en question les avantages de l'usage du numérique.

À cette fin l'administration du ministère doit mieux s'organiser en centrale et en académie ; il est indispensable qu'une politique claire, partagée, s'appuyant sur les principes de souveraineté, de sécurité et de responsabilité, soit définie afin que les messages émis en direction de ses administrés et ses partenaires soient cohérents, que les informations transmises aux collectivités territoriales soient homogènes et qu'une relation de confiance entre l'ensemble des membres de la communauté éducative, parents compris, soit établie. Une prise de parole sur ces questions au plus haut niveau du ministère de l'éducation nationale est très attendue.

De leur côté, certaines entreprises dont les produits sont utilisés par les établissements scolaires estiment ne pas être traitées par l'institution sur le même plan que les groupes de dimension internationale. Pour remédier à ce sentiment d'inégalité et mobiliser ces acteurs, il convient que l'administration centrale mette en place une structure d'échange d'informations dans laquelle l'ensemble des représentants du numérique éducatif soient représentés.

La loi du 7 octobre 2016 pour une République numérique et la loi informatique et libertés permettent déjà aux citoyens de contrôler l'usage de leurs données personnelles par les administrations utilisant des algorithmes pour prendre des décisions individuelles. Il est aujourd'hui nécessaire de s'assurer que ce contrôle s'applique également aux algorithmes des applications développées par des entreprises privées qui sont utilisées dans le cadre des missions du service public d'éducation.

La mise en œuvre du règlement européen sur la protection des données et la nouvelle loi informatique et liberté offre une opportunité d'action même si leur champ d'application, à ce jour, se limite aux données à caractère personnel et ne couvre pas l'ensemble des données scolaires (traces, données collectives, travaux anonymes d'élèves) qui sont potentiellement source de recherche et d'innovation.

La création de la fonction de DPD au sein de l'administration centrale et des services déconcentrés doit être une priorité pour le ministère. Des outils spécifiques du RGPD comme les codes de conduite sont particulièrement adaptés aux spécificités du monde éducatif. Il est fort probable que la spécificité de l'École sera questionnée dans les débats parlementaires qui se dérouleront à l'occasion de l'examen de la nouvelle loi informatique et liberté. Les principes retenus auront un impact durable sur le fonctionnement du système éducatif.

L’institution doit aussi anticiper la question des traces numériques qui constituent aujourd’hui un enjeu majeur pour l’éducation nationale puisque les services numériques innovants proposant des outils de profilage utiliseront probablement massivement ce type de données.

Si l’éducation nationale doit mettre la puissance des développements numériques actuels et à venir au service de la pédagogie et de la gestion de son administration, elle doit se porter garante du respect de la vie privée de l’ensemble des membres de la communauté éducative et de la souveraineté de la France sur son système éducatif et ainsi garantir sa mission de service public.

Gilles BRAUN

Jean-Marc MERRIAUX

Jean Aristide CAVAILLÈS

François PAQUIS

Jean-Marc MOULLET

Stéphane PELLET

Rappel des préconisations

Préconisation n° 1 : Former rapidement les enseignants et les chefs d'encadrement sur l'utilisation des données scolaires numériques dans des situations pédagogiques et administratives avec une attention particulière aux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens de l'article 9 du RGPD.

Préconisation n° 2 : Interdire, soit par circulaire auprès des chefs d'établissement et des enseignants soit en intégrant cette interdiction dans un code de conduite, les services numériques qui opèrent des traitements sur les données scolaires autres que ceux nécessaires à des utilisations pédagogiques ou administratives.

Préconisation n° 3 : Rédiger au niveau national et diffuser largement des documents d'information sur la protection accrue apportée par le RGPD et les modifications de la loi informatique et libertés, adaptés aux différents publics : chefs d'établissement, enseignants, parents, élèves.

Préconisation n° 4 : compléter par amendement à la loi informatique et liberté en révision l'article 38 de la loi d'orientation et de refondation de l'École (formation à l'utilisation des outils numériques) par former « aux dimensions éthiques, sociales et économiques de l'utilisation des données numériques, en particulier celles à caractère personnel ».

Préconisation n° 5 : Éditer au niveau national des documents précisant la nature des données collectées et des traitements effectués, qui seraient distribués aux publics concernés : professeurs, parents, élèves. Ces documents devront être rédigés dans un langage adapté à leur public et facilement modifiables par les responsables de traitement locaux.

Préconisation n° 6 : Proposer que dans le champ scolaire, le responsable de traitement diligente systématiquement des études d'impact sur le traitement des données scolaires qui pourraient être portées par les DPD présents dans les administrations déconcentrées. Il est aussi demandé dans un second temps qu'il puisse être proposé un code de conduite pour le traitement des données scolaires.

Préconisation n° 7 : Faire spécifier dans les contrats passés entre les établissements scolaires et les éditeurs de logiciels de vie scolaire, d'emploi du temps ou d'ENT, que les données doivent être stockées par les hébergeurs sous forme cryptée, les responsables de traitement étant seuls habilités à posséder la clef de décryptage.

Préconisation n° 8 : Établir une cartographie détaillée de l'ensemble des flux de données scolaires circulant dans l'éducation nationale, dans les collectivités territoriales, les entreprises privées et les associations en précisant leurs relations, la nature des données transmises et leur cryptage éventuel. Il s'agira en particulier de veiller à ce que les données personnelles issues de bases de données gérées par le ministère transmises à des tiers soient systématiquement cryptées.

Préconisation n° 9 : Positionner auprès de la secrétaire générale du ministère de l'éducation nationale un poste de DPD à temps complet. Dans l'attente de cette nomination, mettre en place dès aujourd'hui, un groupe projet chargé de la mise en œuvre du RGPD.

Préconisation n° 10 : Demander aux recteurs de nommer à leur côté un DPD sur emploi fonctionnel d'ici la prochaine rentrée scolaire, pour au moins les 12 régions académiques.

Préconisation n° 11 : Créer au sein du ministère de l'éducation nationale, un comité d'éthique et d'expertise sur l'intérêt public de l'utilisation de données scolaires qui serait composé de membre de la communauté éducative d'horizons très divers.

Préconisation n° 12 : Inclure une clause d'explicitation des principes sur lesquels reposent les algorithmes utilisés dans les traitements de données à caractère personnel dans les contrats passés avec les développeurs privés.

Préconisation n° 13 : Confier au ministère de l'économie une expertise approfondie, au regard du droit national et européen, sur la passation des marchés entre les EPLE et les sociétés éditant les logiciels de vie scolaire les plus utilisés.

Préconisation n° 14 : Exiger une certification ANSSI de premier niveau au moins pour tous les contractants hébergeant des données scolaires à caractère personnel.

Préconisation n° 15 : Demander aux entreprises contractant avec des établissements de l'éducation nationale la liste des prestataires auxquels elles font appel pour la mise en œuvre de leurs services. Clarifier les engagements contractuels vis-à-vis de l'utilisation des données scolaires par ces sous-traitants.

Préconisation n° 16 : Faire en sorte que l'État se repositionne vis-à-vis des prestataires de certains services numériques clés, administratifs et pédagogiques, afin de pouvoir exercer sa souveraineté en matière d'éducation.

Préconisation n° 17 : Intégrer l'éducation nationale dans le domaine des secteurs d'activité industriels **stratégiques** soumis à une autorisation préalable du gouvernement français en cas d'investissements étrangers.

Annexes

Annexe 1 : Lettre de saisine 47

Annexe 2 : Organisations et administrations rencontrées 49

Annexe 1

Lettre de saisine

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Éducation nationale

Le directeur du cabinet *Paris, le* 13 NOV. 2017

Note à l'attention de

Madame Anne ARMAND
Doyenne de l'Inspection générale de l'Éducation nationale
Monsieur Jean-Richard CYTERMANN
Chef de service de l'Inspection générale de l'administration, de l'Éducation nationale et de la recherche

Objet : Mission sur les données numériques à caractère personnel au sein de l'Éducation nationale.

Le développement des technologies numériques constitue un levier majeur de transformation du système éducatif français. Cette dynamique doit toutefois respecter un certain nombre de principes fondamentaux, dont la stricte garantie, au bénéfice de tous les acteurs concernés, de la protection des données à caractère personnel.

Si ce principe guide d'ores et déjà l'action des pouvoirs publics, des interrogations légitimes existent à ce jour quant aux risques de pratiques susceptibles de s'écarter des règles fixées dans ce domaine. Ces préoccupations concernent notamment l'utilisation qui pourrait être faite de ces données par des acteurs privés intervenant dans le champ éducatif.

Or, la confiance indispensable de l'ensemble des acteurs requiert transparence, traçabilité et régulation des différents outils utilisés par les usagers et personnels de l'Éducation nationale, afin notamment que l'éventuel recours à des services fournis par des tiers soit autorisé avec discernement. A cet égard, si les différentes données recueillies constituent des ressources précieuses pour le développement de méthodes pédagogiques innovantes, le développement souhaitable d'acteurs privés performants dans le secteur de la « *EdTech* » devra intervenir dans un cadre juridique et opérationnel clair et partagé en matière de gestion des données.

.../...

110 rue de Grenelle - 75357 Paris SP 07 - Téléphone : 01 55 55 10 10

Dans le cadre de la présente mission, vous dresserez un état des lieux de la gestion actuelle des données personnelles et une analyse des différentes problématiques qu'elle soulève. Ces travaux devront notamment porter sur :

- les règles et pratiques actuelles aux niveaux central, déconcentré et des écoles et établissements de l'Éducation nationale, dans et hors les espaces numériques de travail (ENT) ; vous interrogerez dans ce cadre la pertinence des documents contractuels (« CGU éducation ») et schémas directeurs (SDET) appliqués aux différents partenariats noués en matière de numérique éducatif ; vous étudierez la spécificité du dispositif des ENT et du gestionnaire d'accès aux ressources (GAR) et l'impact en matière de gestion des données personnelles des expérimentations et pratiques spontanées des acteurs en matière de services tiers ;
- la conformité de l'ensemble de ces règles et pratiques avec le droit de l'informatique et des libertés (actuelles ou à venir dans les prochains mois en application du droit européen) ainsi que les évolutions juridiques, organisationnelles et opérationnelles à mettre en œuvre à court et moyen termes afin de garantir la protection des données à caractère personnel ;
- les recommandations utiles à une sensibilisation accrue des élèves et de leurs familles et à la formation des personnels d'enseignement et d'encadrement sur ces sujets ;
- les potentialités pédagogiques qu'offrent les technologies du « *big data* » dans le domaine de l'éducation et leur articulation pertinente avec la gestion des données personnelles par le système éducatif.

Sur ces sujets, un éclairage international permettrait de mettre en perspective vos constats et préconisations.

Votre mission mènera une large concertation auprès des différents interlocuteurs concernés, dont notamment les organisations syndicales, les associations de parents d'élèves, les opérateurs de l'État, les fédérations de prestataires commerciaux et associatifs de services numériques (infrastructures, équipements, ressources, etc.), les associations de défense des libertés publiques.

Vous interrogerez également les services centraux et déconcentrés de l'administration de l'Éducation nationale (DGESCO, SG, DAJ, DNE, DEPP, DREIC réseaux des DSI et des DAN, etc.) ainsi que les différents services gouvernementaux en charge de ces problématiques (secrétariat d'État au numérique, CNIL, SGDSN, etc.).

La mission rendra ses conclusions à la fin du mois de janvier 2018. Au cours de la seconde moitié du mois de décembre 2017, un rapport d'étape synthétique permettra de disposer des premiers constats ainsi que des principaux axes d'action et de communication identifiés par votre mission.

Christophe KERRERO

Annexe 2

Administrations, organisations, entreprises et personnalités rencontrées

Direction interministérielle des systèmes d'information et de communication de l'État

Ministère de l'éducation nationale :

- Secrétariat général du ministère de l'éducation nationale
- Direction générale de l'enseignement scolaire
- Direction des affaires juridiques
- Direction pour le numérique éducatif
- Direction générale des ressources humaines
- Direction de l'évaluation, de la prospective et de la performance
- DAN et DSI de l'académie d'Aix Marseille
- DAN et DSI de l'académie de Guadeloupe
- DAN, DSI et CIL de l'académie de Lyon

Secrétariat d'État au numérique

CNIL

CNCDH

Secrétariat général de l'enseignement catholique

Entreprises :

- AFINEF
- Association Savoir Livre
- Index éducation (éditeur de logiciels de vie scolaire)
- Axess éducation (éditeur de logiciels de vie scolaire)
- Apple
- Google
- Qwant
- Microsoft

Fédérations de parents d'élèves :

- PEEP
- FCPE

Syndicats :

- SNES
- CGT
- SNPDEN
- IDEFO
- UNSA

Ligue des droits de l'homme

Ligue de l'enseignement

Personnalités rencontrées

- Anne Boyer, professeure d'informatique au laboratoire lorrain de recherche en informatique et ses applications (LORIA)
- Gilles Dowek, chercheur à l'INRIA
- Jean Gabriel Ganascia, professeur à l'université Pierre et Marie Curie (UMPC),
- Guillaume Piolle, enseignant chercheur en informatique à Centrale Supélec, Rennes
- Laurent Cytermann, maitre des requêtes au Conseil d'État
- Jean Gaeremynck, conseiller d'État, président de la section des finances et Michel Isnard, inspecteur général de l'INSEE, membres du comité du secret statistique
- Yann Padova, Partner, Cabinet Baker McKenzie, ancien secrétaire général de la CNIL (2006-2012)

Académies et vice rectorats qui ont répondu aux questionnaires DAN / DSI

Aix-Marseille
Amiens
Besançon
Bordeaux
Caen
Clermont-Ferrand
Corse
Créteil
Dijon
Grenoble

Guadeloupe
Guyane
Lille
Limoges
Lyon
Martinique
Mayotte
Montpellier
Nancy-Metz
Nantes
Nice
Nouvelle Calédonie
Orléans-tours
Paris
Poitiers
Polynésie
Reims
Rennes
Réunion
Rouen
Saint Pierre et Miquelon
Strasbourg
Toulouse
Versailles
Wallis et Futuna