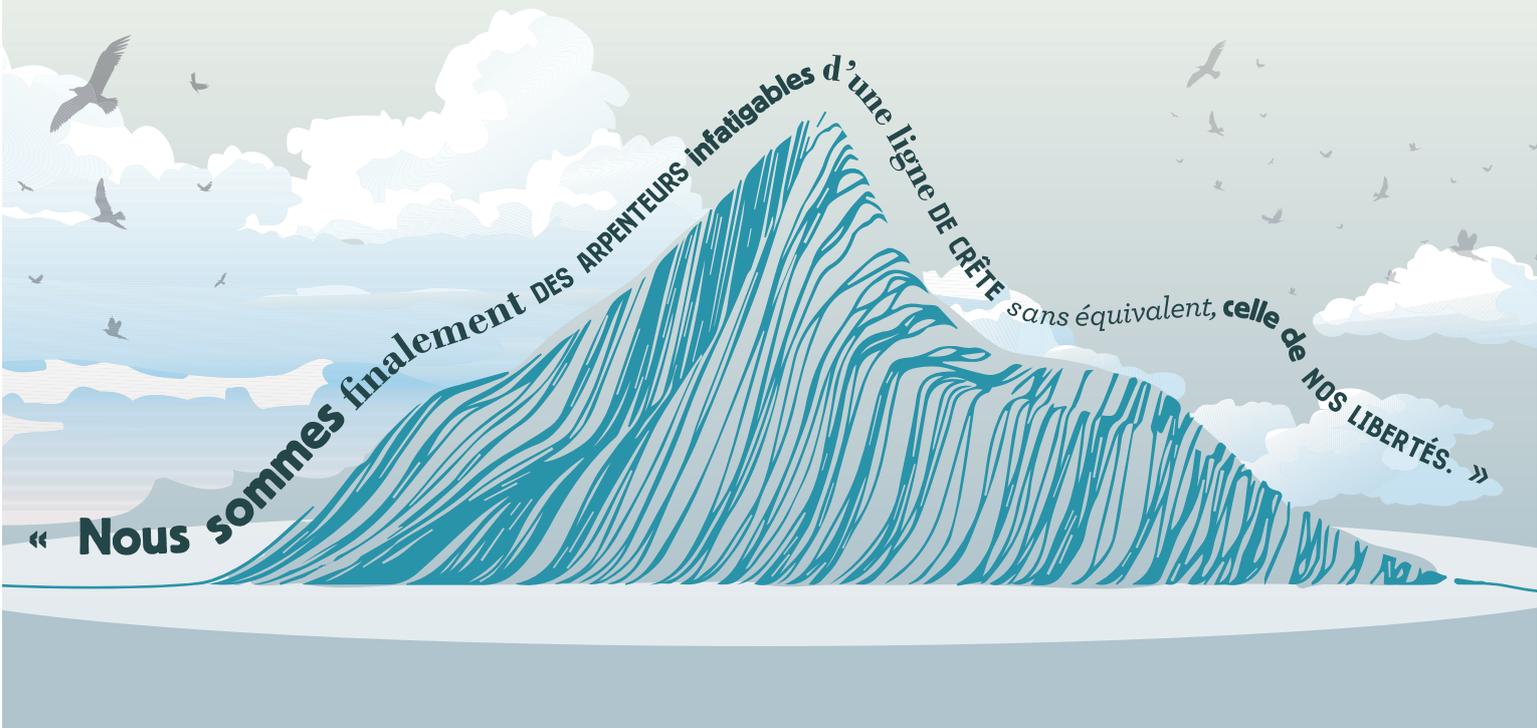


2017

Rapport d'activité

# COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Protéger les données personnelles,  
Accompagner l'innovation,  
Préserver les libertés individuelles



« Nous sommes finalement DES ARPEUTEURS infatigables d'une ligne DE CRÊTE sans équivalent, celle de NOS LIBERTÉS. »

# Numérisation de l'Éducation nationale : la CNIL appelle à l'adoption d'un socle de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur

Depuis plusieurs années, le secteur de l'Éducation nationale est marqué par une utilisation croissante du numérique à des fins administratives ou pédagogiques. Malgré les efforts du ministère de l'Éducation nationale pour développer différents cadres protecteurs des données personnelles des élèves et des enseignants, de nombreux établissements scolaires et écoles recourent à des ressources numériques ne respectant aucun de ces cadres. C'est pourquoi la CNIL s'implique largement dans cette transition numérique afin de rappeler les principes régissant la protection des données personnelles et les bonnes pratiques en la matière.



## LA TRANSITION NUMÉRIQUE DU MINISTÈRE DE L'ÉDUCATION NATIONALE

Le secteur de l'Éducation est, depuis plusieurs années, marqué par une véritable transition numérique. La première mutation en résultant concerne le développement, par le ministère de l'Éducation nationale lui-même, d'applications numériques à destination des élèves, de leurs familles et des personnels. Ce mouvement n'échappe pas à la CNIL qui est notamment chargée de veiller à la conformité de ces traitements aux principes de la loi Informatique et Libertés.

### Le livret scolaire unique (LSUN)

À titre d'illustration, l'année 2017 a été marquée par la création d'une application nationale de suivi de la scolarité, dans les écoles élémentaires et les établissements du second degré, dénommée **livret scolaire unique numérique (LSUN)**<sup>16</sup>. Le LSUN, qui concerne les élèves du CP à la troisième, contient le suivi des acquis des compétences ainsi que les appréciations des enseignants. Il est en outre assorti d'un service en ligne (téléservice) facultatif à l'attention des élèves et de leurs responsables légaux qui pourront ainsi accéder en ligne au livret scolaire.

L'examen du projet de texte créant le LSUN a permis à la CNIL de rappeler au ministère que l'information des personnes concernées par ce livret scolaire, prévue par la loi Informatique et Libertés, ne devait pas seulement être fournie aux utilisateurs du téléservice mais à tous les usagers concernés par le livret scolaire<sup>17</sup>.

### L'application Esculape pour la médecine scolaire

En 2017, le ministère a également mis en place l'application « Esculape », permettant aux médecins scolaires de dématérialiser les dossiers médicaux des élèves. Les dossiers médicaux des élèves étaient en effet largement gérés par les médecins scolaires sur support papier. L'utilisation du seul support papier ne répondant plus aux besoins de l'activité

des médecins scolaires, le ministère a créé un nouvel outil dont les fonctionnalités doivent permettre l'amélioration de l'organisation du travail des médecins et le suivi des élèves, notamment en cas de changement de secteur d'intervention du médecin ou de changement d'établissement de l'élève.

Dans la mesure où « Esculape » est mis à disposition de près de 2 000 médecins scolaires, qu'il concerne un grand nombre de personnes, principalement mineures (élèves des premier et second degrés d'enseignement public et privé sous contrat), et qu'il contient des données de santé, données faisant l'objet d'une protection particulière, le ministère a associé la CNIL au déploiement de ce projet. Les échanges entre la CNIL et le ministère ont, par exemple, permis d'ajuster la durée de conservation des données et de mettre en place des mesures de sécurité adaptées aux risques.

### Les services fournis par des tiers

En parallèle du développement de ces applications plutôt destinées à une gestion administrative, le ministère de l'Éducation nationale a également opé-



ré sa transition numérique en ce qui concerne les services pédagogiques offerts aux élèves. Il s'est ainsi, depuis plusieurs années, engagé dans une **ouverture encadrée de l'utilisation de services fournis par des tiers** tels que les éditeurs scolaires ou les collectivités territoriales avec les espaces numériques de travail (ENT).

L'objectif est ainsi de permettre aux fournisseurs de ces services d'intégrer l'écosystème de l'Éducation nationale tout en respectant certains référentiels nationaux. Cette stratégie à plusieurs niveaux doit permettre d'éviter l'effet dissuasif de certains cadres jugés trop contraints.

Là encore la CNIL exerce pleinement son rôle de conseil et d'accompagnement. Elle a en effet eu l'occasion d'examiner certains de ces cadres développés par le ministère pour promouvoir des solutions numériques respectueuses de la protection des données personnelles.



« Le secteur de l'Éducation nationale est marqué par la grande diversité des offres de services numériques qui bouleversent les pratiques traditionnelles. »

<sup>16</sup> Arrêté du 24 octobre 2017 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Livret scolaire unique numérique » LSUN.

<sup>17</sup> Délibération n° 2017-159 du 18 mai 2017.

## La charte de confiance des services numériques

En 2017, le ministère de l'Éducation nationale a sollicité l'avis de la CNIL sur un projet de charte de confiance des services numériques pour l'Éducation. Cette charte devait rappeler les principales dispositions du code de l'Éducation, du code des marchés publics et de la loi Informatique et Libertés applicables à ces services. Elle devait aussi prévoir des stipulations allant au-delà de ces dispositions légales afin que les conditions d'utilisation des services numériques soient adaptées aux besoins du secteur de l'Éducation, notamment en termes de protection des données personnelles.

La CNIL a estimé intéressante l'initiative prise par le ministère d'inciter les fournisseurs de ces services à s'engager dans une offre de services numériques respectueux des droits des personnes. Elle a toutefois regretté l'absence de caractère contraignant de cet instrument. À ce jour, la charte de confiance en question n'a pas été adoptée.

## Les espaces numériques de travail (ENT)

L'année 2017 a également été marquée par la refonte de l'encadrement des espaces numériques de travail (ENT). En effet, les pratiques ayant évolué depuis 2006, le cadre développé à ce moment-là par le ministère ne correspondait plus aux besoins des acteurs concernés.

Les ENT permettent à leurs utilisateurs, en renseignant une fois leurs « identifiants », d'accéder en ligne à de nombreux services ou ressources liés à la vie scolaire et à la pédagogie : cahier de texte,

outils de vie scolaire (gestion des absences, des notes, etc.), service de paiement des frais d'inscription dans l'enseignement supérieur, services collaboratifs à usage des enseignants, mais également accès à des ressources pédagogiques telles que des banques de données, des ouvrages de référence, des dictionnaires et des manuels numériques. Ces dispositifs s'inscrivent dans un projet généralement développé au niveau académique et associant de nombreux acteurs tels que les collectivités territoriales. Afin d'assurer le déploiement des ENT dans un cadre de confiance devant notamment garantir la sécurité des données traitées, le ministère a imposé le respect d'un schéma directeur des espaces numériques de travail (SDET).

L'avis de la CNIL sur ce projet de refonte a permis que plusieurs précisions utiles soient mentionnées dans l'arrêté modifiant le cadre relatif aux ENT. Par exemple :

- l'identité du responsable de traitement dans les écoles (le DASEN) est désormais expressément mentionnée,
- il est prévu que le lieu de naissance de l'élève ne soit enregistré que dans l'hypothèse où celui-ci ne disposerait pas de numéro identifiant national élève (INE) ou que ce numéro serait en conflit avec un autre,
- est fixée une durée maximale de conservation des données dans l'enseignement supérieur à l'issue de laquelle, en l'absence de retour de l'intéressé, le compte ENT doit être supprimé.

## Le gestionnaire d'accès aux ressources (GAR)

La CNIL a en outre été saisie du « gestionnaire d'accès aux ressources » dit GAR, développé par le ministère, afin de permettre l'accès, dans un cadre respectueux des règles de protection des données à caractère personnel, à des ressources pédagogiques numériques éditées par des fournisseurs privés. Ce dispositif, qui s'inscrit dans la logique du règlement européen sur la protection des données personnelles (RGPD), est assez novateur puisqu'il s'appuie sur :

- une équipe de personnels du ministère chargée en amont d'apprécier la proportionnalité des données personnelles sollicitées par un fournisseur de ressources au regard d'une ressource numérique précise,
- un portail internet à destination des fournisseurs de ressources,
- une seule et même interface de mise en relation permettant aux utilisateurs de disposer, de manière transparente, de nombreuses ressources,
- une solution technique qui agit comme un « filtre » pour ne transmettre, aux fournisseurs de ressources, que les données personnelles nécessaires,
- un contrat d'adhésion et des référentiels techniques et de sécurité imposant aux fournisseurs de ressources de respecter des principes ou obligations tels que, par exemple, la non réutilisation commerciale des données personnelles des élèves et des enseignants ou le fait pour le fournisseur de permettre la récupération aisée par les utilisateurs de leurs données.

Dans son avis sur le GAR, la CNIL a estimé qu'au-delà des garanties offertes par ce dispositif spécifique, **la situation générale de l'utilisation de services numériques dans l'Éducation nationale demeurait insatisfaisante du point de vue de la protection des données personnelles**. En effet, le caractère uniquement facultatif du recours au GAR permet que les usagers et personnels puissent accéder à des ressources et services numériques ne respectant ni le cadre de confiance imposé par le GAR, ni aucun autre cadre prévu par le ministère pour protéger les données à caractère personnel traitées dans le cadre du service public de l'Éducation, amoindrissant ainsi l'effet utile des différents cadres établis par le ministère.



« La CNIL appelle à l'adoption, par le ministère, d'un socle commun de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur de l'Éducation nationale, à respecter quel que soit le mode d'accès aux ressources pédagogiques. »

## LES ENJEUX SOULEVÉS PAR LA TRANSITION NUMÉRIQUE DU SECTEUR DE L'ÉDUCATION DU POINT DE VUE DE LA PROTECTION DES DONNÉES

Tout d'abord, le fait que les données scolaires concernent essentiellement des personnes mineures et qu'elles contiennent des appréciations, des évaluations sur la « valeur », les compétences, les « performances » et même le comportement des élèves leur confère un caractère hautement personnel qui requiert dès lors une approche adaptée. Le règlement européen sur la protection des données personnelles, qui renforce les droits des personnes et porte une attention particulière aux mineurs, devrait permettre d'affermir cette démarche.

En outre, le secteur de l'Éducation nationale est marqué par la grande diversité des offres de services numériques qui bouleversent les pratiques traditionnelles : déploiement d'équipements informatiques mobiles facilitant l'accès aux ressources en ligne, services de stockage dans le *cloud*, outils collaboratifs avancés, réseaux sociaux pédagogiques, applications pour faciliter la communication entre les enseignants et les familles.

Bon nombre de ces usages du numérique ne répondent à aucun des cadres proposés par le ministère mais séduisent néanmoins par leur efficacité, leur simplicité d'utilisation voire même parfois par leur gratuité. Sans remettre en cause l'utilité de ces services numériques, la CNIL relève que leur utilisation est susceptible de soulever des interrogations quant au respect des principes régissant la protection des données personnelles.

Cette situation a également suscité de la part d'associations de parents d'élèves comme de syndicats d'enseignants, plusieurs saisines auprès de la CNIL. Ces organisations s'inquiètent notamment des conditions dans lesquelles certains acteurs clés du numérique lorsqu'ils offrent leurs services auprès du monde éducatif sont susceptibles d'utiliser,

pour leur propre compte, les données scolaires.

Le recours à des solutions numériques « grand public », dont les conditions générales d'utilisation (CGU) ne prennent pas en compte les spécificités d'une utilisation à des fins administratives ou pédagogiques, dans le cadre du service public de l'Éducation, est fréquent alors même que leurs CGU n'interdisent généralement pas la publicité, la réutilisation à des fins commerciales des données personnelles ou encore le profilage.

Même les solutions numériques dédiées au secteur de l'Éducation, avec des conditions d'utilisation spécifiques, ne sont pas toujours conçues selon le principe du *privacy by design* destiné à garantir que la protection de la vie privée est intégrée dès leur conception. Il est ainsi souvent difficile pour le responsable de traitement de savoir où exactement sont hébergées les données personnelles des élèves et des personnels dont il a la charge, de s'assurer que celles-ci ne sont pas conservées

indéfiniment ou qu'elles font l'objet de mesure de sécurité satisfaisantes.

C'est pourquoi la CNIL estime qu'il est essentiel que le travail amorcé par le ministère pour encadrer de tels usages soit poursuivi et approfondi afin d'assurer d'une protection effective des données personnelles des élèves. Elle appelle ainsi à l'adoption, par le ministère, d'un socle commun de principes généraux protecteurs des données personnelles, adaptés aux spécificités du secteur de l'Éducation nationale, à respecter quel que soit le mode d'accès aux ressources pédagogiques.

Ces principes pourraient notamment inclure des exigences allant au-delà du simple rappel des obligations légales telles que notamment l'interdiction de réutiliser, à des fins commerciales, les données des élèves, l'hébergement des données personnelles au sein de l'Union européenne, ou encore le fait de permettre la récupération aisée des données personnelles des élèves et des personnels.



INFOSPLUS

### Learning analytics ou analyse de l'apprentissage

- Il s'agit de l'analyse des traces numériques d'apprentissage afin de mieux comprendre et optimiser celui-ci.
- Ces analyses portent aussi bien sur les traces d'utilisation des services telles que le nombre de clics par lien dans un e-module donné, la fréquence et le temps d'utilisation d'un service que sur les performances des personnes concernées, les traces d'interactions, ou encore des données sociodémographiques telles que l'âge, le sexe, le niveau d'Éducation.
- L'analyse de ces données doit notamment permettre d'améliorer les formations, en personnalisant l'apprentissage.

Enfin, le secteur de l'Éducation nationale est également marqué par le fait que **le développement du numérique peut conduire à la constitution de gisements de données massifs et par là même à des possibilités infinies d'exploitation de celles-ci notamment à des fins de meilleure connaissance des élèves ou d'amélioration des pratiques pédagogiques.**

Il en va ainsi des *learning analytics* ou « analyses de l'apprentissage ». S'ils peuvent être légitimes dans leur principe, de tels usages requièrent une certaine prudence au regard des modèles prédictifs de comportements qu'ils peuvent être amenés à bâtir. Les *learning analytics* peuvent en effet être utilisés pour « prédire » des situations d'échecs, des abandons dans certaines formations en ligne, pour détecter des élèves à risque, pour les affecter dans une filière « adaptée à leur profil ». Or, comme l'a souligné la CNIL dans son rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, **les *learning analytics* ne sont pas sans soulever la question de l'enfermement algorithmique alors que de telles analyses des données d'apprentissage ne devraient pas avoir pour objet ni pour effet un déterminisme sur les parcours scolaires les élèves.**

Pour toutes ces raisons, la CNIL considère qu'il est indispensable de définir des règles claires pour de tels usages des données des élèves.

Ainsi, un travail doit être mené pour :

- **déterminer** les finalités pouvant légitimement être poursuivies au titre de ces analyses ;
- **délimiter** les conséquences que de telles analyses peuvent emporter sur les personnes concernées ;
- **définir** les mesures concrètes permettant de s'assurer du respect des deux points précédents ;
- **garantir** la nécessaire transparence sur une telle utilisation des données personnelles des élèves.

Compte tenu de ces différents enjeux, la protection des données personnelles des élèves demeure une priorité pour la CNIL et l'arrivée du règlement européen permettra de renforcer cette protection.





## Mise en demeure d'APB (Admission post-bac)

Le rôle de la CNIL ne se limite pas à un contrôle a priori de la conformité du projet de traitement à la loi Informatique et Libertés. Elle veille aussi au respect a posteriori de ces principes destinés à protéger la vie privée des personnes.

En mars 2017, elle a ainsi contrôlé le traitement admission post-bac (APB) permettant l'affectation des lycéens à une formation dans l'enseignement supérieur. Les constatations opérées lors de ces contrôles ont révélé plusieurs manquements aux règles gouvernant la protection des données personnelles, conduisant ainsi la Présidente de la CNIL à mettre en demeure publiquement le ministère de l'enseignement supérieur, de la recherche et de l'innovation, le 28 septembre 2017.

Outre une information insuffisante des personnes concernées, il a été constaté que, s'agissant des formations non sélectives, un algorithme déterminait automatiquement, sans intervention humaine, les propositions d'affectation faites aux candidats, à partir des trois critères prévus par le code de l'Éducation : le domicile du candidat, sa situation de famille et l'ordre de préférence des vœux qu'il a formulés. Or, l'article 10 de la loi Informatique et Libertés interdit une telle prise de décision purement automatisée.

La procédure de droit d'accès ne permettait pas aux personnes d'obtenir des informations précises relatives à l'algorithme et à son fonctionnement, notamment la logique qui sous-tend le traitement APB ou le score obtenu par le candidat. En effet, l'article 39 de la loi Informatique et Libertés dispose que les personnes qui exercent leur droit d'accès doivent pouvoir obtenir

« Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé ».

La CNIL n'a pas remis en cause le principe même de l'utilisation des algorithmes dans la prise de décision, notamment par les administrations. Cependant elle a rappelé les principes prévus par la loi : compte tenu des enjeux éthiques que soulèvent les algorithmes utilisés pour prendre une décision produisant des effets juridiques à l'égard d'une personne, leur utilisation des algorithmes ne peut exclure toute intervention humaine et doit s'accompagner d'une information transparente des personnes.

La réponse du ministère à cette mise en demeure a permis à la Présidente de la CNIL de considérer que les divers manquements avaient cessé et de clôturer la mise en demeure. Le ministère a, en effet, informé la Présidente de la fermeture de la plateforme APB et de la mise en place d'un nouveau dispositif dénommé « Parcoursup ».

Parallèlement la Commission a été saisie, pour avis, du projet d'arrêté autorisant la mise en œuvre de la première phase du nouveau traitement « Parcoursup », dédiée à la collecte des vœux des candidats pour l'entrée dans une formation de l'enseignement supérieur. La Commission sera en outre prochainement saisie pour avis sur le projet d'arrêté portant autorisation du dispositif permettant l'affectation des étudiants, sur la base des vœux ainsi recueillis.