RGPD

Le RGPD - Règlement général à la protection des données - est un règlement européen, résultat d'un long consensus des institutions et des États européens. Quatre ans de négociation ont été nécessaires. Adopté en avril 2016, le texte est applicable depuis le 25 mai 2018.

Le RGPD est le nouveau cadre juridique de l'Union européenne qui gouverne la collecte et le traitement des données à caractère personnel. Il a pour objectifs de :

- Donner aux citoyens de l'Union Européenne plus de visibilité et de contrôle sur leurs données à caractère personnel ;
- Permettre à « l'administration » de maîtriser le cycle de vie des données et de pouvoir les transmettre sur simple demande.

Avant de traiter du fond de cette réforme, il est utile de rappeler la hiérarchie des normes. Le RGPD étant un règlement et non pas une directive, il est d'application directe, mais il laisse certaines marges de manœuvre aux États membres et la France a fait le choix d'en utiliser certaines. Elle a donc révisé sa loi informatique et libertés pour décider ce qu'elle allait appliquer.

La loi informatique et libertés existe depuis le 6 Janvier 1978. Ses grands principes sont repris dans le RGPD. La France a été pionnière en matière de protection des données, car la loi informatique et libertés était assez visionnaire et très bien écrite se dotant en plus, d'une autorité de protection des données, la CNIL.

Néanmoins, le règlement européen apporte des nouveautés avec **trois grands axes** à retenir pour les entreprises, les associations, les collectivités locales et toutes les entités du service public.

Les services de l'éducation nationale ainsi que les écoles, collèges et lycées, les universités… doivent l'appliquer.

Avant de développer nos propos, arrêtons sur la notion de données personnelles et de traitement.

Une donnée personnelle est une donnée qui identifie ou qui rend identifiable une personne physique directement ou indirectement. (article 2 du RGPD)

Exemple : Numéro de Sécurité Social (possibilité de décomposition du NSS : sexe, année de naissance, mois, département, commune ou pays, N°ordre INSEE, clé : autant d'informations sur un individu), NUMEN ou même des caractéristiques

physiques ou une identité physique qu'elle soit psychique et/ou physiologique (comme une photo d'identité ou empreinte digitale), l'état de santé (carte vitale), les données socioéconomiques (habitudes de consommation, culturelles ex : PCS).

On parle de traitement des données lorsqu'il y a identification avec association de différentes informations (ex : cookies, journal de connexion sur un serveur pédagogique). Sur un plan plus technique, le traitement se définit comme toute opération portant sur les données à caractère personnelles, quel que soit le procédé utilisé. Par opérations, il faut comprendre : Enregistrer, Organiser, Conserver, Transmettre, Consulter, Détruire, Extraire, Modifier, Adapter.

Les EPLE doivent être capables de garantir et de prouver que leurs traitements de données à caractère personnel sont conformes et sécurisés dans une optique de renforcement du droit des personnes. **(AXE 1)**

Le RGPD simplifie les démarches et responsabilise tous les acteurs : les déclarations auprès de la CNIL disparaissent et sont remplacées par l'obligation de documenter sa conformité par la tenue d'un registre (la CNIL conserve toutefois un droit de contrôle et les sanctions sont renforcées). **(AXE 2)**

Les établissements deviennent alors pleinement responsables, ainsi que leurs prestataires et sous-traitants, du traitement et de la protection des données personnelles qu'ils utilisent et qui concernent désormais l'ensemble des ressortissants européens. **(AXE 3)**

I/ Renforcement du droit des personnes :

A/ Par une logique de consolidation des droits des membres de la communauté scolaire (parents, élèves, enseignants, administratifs etc.) :

Il renforce avant tout le droit des personnes en plaçant les personnes physiques au cœur du dispositif en leur accordant de nouveaux droits, comme le :

- Droit d'information : Toute personne a le droit de connaitre les données collectées (qui la concernent) et la finalité de leur traitement.
- Droit d'opposition : Toute personne a le droit de s'opposer au traitement de ses données à caractère personnel, ou de retirer son consentement à tout moment, pour des motifs légitimes, sauf si le traitement répond à une obligation d'intérêt public (éducation, santé…). *Le livret scolaire unique est une application nationale et il est obligatoire (arrêté du 31/12/2015 consolidé le 12/08/2018). Pas d'opposition dans le cadre général. Cependant, pour un*

motif légitime et dans une situation particulière, le droit d'opposition pourrait s'exercer. Il est à noter que dans ce cas précis, pour apprécier le bien-fondé de la demande, il est recommandé de s'adresser à son délégué à la protection des données (DPD).

- Droit de rectification : Toute personne peut demander à corriger certaines informations la concernant.
- Droit de protection des mineurs de moins de 15 ans : Lorsque le mineur est âgé de moins de 15 ans, le consentement au traitement doit être donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale, pour les traitements réalisés sur un (des) service(s) de la société de l'information (réseaux sociaux, Drives, blog, site Web…). *Ce double consentement est exigé par la Loi « Informatique et libertés » du 14 mai 2018.*
- Droit d'accès : Toute personne peut accéder à l'ensemble des informations la concernant, et en obtenir une copie. Dans le considérant 63, le responsable de traitement a obligation de communiquer au demandeur ou à son représentant l'ensemble des données à caractère personnel qui le concerne. *Le responsable de traitement est tenu de répondre à cette demande dans un délai de deux mois.*
- Droit à la portabilité (article 20 paragraphe 3 du RGPD) : le droit récupérer ses données lorsqu'elles sont sur une plateforme par exemple, soit pour soi-même, soit pour les transmettre à un autre responsable de traitement. *Ce droit ne s'applique pas au traitement nécessaire à une mission d'intérêt public (éducation, santé) ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement (traitement mis en œuvre par le ministère, un service académique, ou bien le chef d'établissement ou le DASEN dans l'exercice de leur fonction).*
- Droit de réparation du préjudice : Toute personne ayant subi des dommages matériels ou moraux du fait d'un traitement de données inadapté pourra demander réparation. *Une association de protection des données, ou bien un groupe de parents, pourra entamer un recours collectif*.
- Droit à l'oubli (article 17 paragraphe 3 alinéa C du RGPD) : Dès lors qu'une personne estime qu'une information affichée sur une plateforme ou par un moteur de recherche porte atteinte à sa réputation ou à sa vie privée, il peut demander à ce que cette information soit effacée de la plateforme ou des résultats du moteur de recherche (déréférencement).

Dans cette optique constante de renforcement des droits des personnes, on retrouve dans le RGDP un champ d'application géographique très large, beaucoup plus qu'auparavant puisque le règlement s'applique dès lors qu'un organisme même localisé en dehors de l'Union européenne traite des données de personnes se trouvant sur le territoire de l'Union européenne.

Si une société américaine offre à des résidents européens des services qui impliquent un traitement de données à caractère personnel, elle devra respecter les règles du RGPD pour ces personnes.

Il s'agit d'une véritable protection pour les citoyens européens contre les risques encourus par le traitement des données réalisé par des multinationales étrangères notamment américaines. La législation internationale s'équilibre après des années d'hégémonie et d'extra-territorialité des lois US.

B*/* Avec des obligations plus fortes à respecter dans le traitement des données à caractère personnel :

Les traitements des données à caractère personnel doivent respecter les règles suivantes :

- Le principe de Légalité – Licéité : La légalité est la conformité à la loi. La licéité est la conformité au droit, lequel puise ses sources non seulement dans la loi, mais aussi dans la constitution, les règlements, la coutume, la doctrine, la jurisprudence et les principes généraux du droit, entre autres. L'article 6 du RGPD et le chapitre II de la loi informatique et libertés fixent un ensemble de conditions à respecter pour que le traitement soit licite. *Exemple : Il est illégal de demander la nature de la pathologie d'un élève dans un formulaire d'inscription à la restauration scolaire.*
- Principe de Légitimité : Caractère de ce qui est fondé en droit ou de ce qui est conforme à l'équité, à la raison, aux règles établies, aux us et coutumes, à la tradition. Tout ce qui n'est pas illégal à la base n'est donc pas pour autant légitime. L'appréciation de la légitimité fait intervenir des critères subjectifs, appréciés de façon souveraine par les juges du fond, tel l'équité (donc les intérêts d'autrui) ou la raison. *Exemple : La collecte de la profession des parents par les enseignants (anciennes « fiches de renseignements ») n'est pas une demande légitime au regard du droit au respect de la vie privée et face au risque que cela peut représenter pour l'équité (effet Pygmalion).*
- Principe de Finalité : Les finalités sont les raisons explicites et légitimes pour lesquelles les données sont collectées et traitées. Elles sont déterminées par le responsable du traitement, seul ou conjointement avec d'autres ou bien déterminées par le droit de l'Union européenne ou d'un État membre. Les finalités conditionnent la licéité de la collecte, notamment par l'adéquation, la pertinence et le caractère strictement nécessaires des données à l'accomplissement de ces finalités (RGPD article 4). *Exemple : Les traitements opérés dans le cadre de l'emploi du temps répondent à une finalité de service public à savoir, l'organisation du temps scolaire. C'est d'ailleurs ce qu'énonce le B.O du 19 avril 2018 "Création d'un traitement automatisé de données à caractère personnel dénommé emploi du temps" (MENE1802813A)*

- Principe de minimisation des données ou de proportionnalité : Les données collectées et les traitements auxquels elles sont soumises doivent être proportionnés au but légitime poursuivi, c'est-à-dire aux finalités du traitement. Elles sont adéquates, pertinentes et limitées au strict nécessaire et il en va de même de leur durée de conservation. Autrement dit, elles ne doivent être traitées que si la finalité du traitement légitime dont elles sont l'objet ne peut être raisonnablement atteinte par d'autres moyens (sous-entendu « en s'en passant »). Il convient de noter que l'évaluation du critère de proportionnalité est à faire à l'échelon le plus fin, donnée par donnée, traitement par traitement, finalité par finalité. *Exemple : Les données des élèves qui ont quitté l'établissement sont gardées pour des durées variables selon le traitement considéré (gestion administrative et suivi de la scolarité et mise à disposition d'un ENT par exemple). On peut concevoir que les données nécessaires à la délivrance d'un certificat de scolarité puissent être conservées après le départ de l'élève pendant une certaine durée, on ne peut justifier la conservation de la PCS par cette même finalité.*
- Principe de sécurité : Dans le domaine des données à caractère personnel, la divulgation de données à des tiers non légitimes est une violation de sécurité dont les conséquences peuvent porter lourdement atteinte à la vie privée et aux libertés des personnes concernées. Il convient donc de traiter ce risque avec autant d'attention que celui de perte, d'altération ou d'inexactitude des données. En cas d'incident, il est essentiel d'avoir les traces permettant de gérer l'incident. La sécurité des données comporte principalement quatre volets qui sont la disponibilité, l'intégrité, la confidentialité et la traçabilité. *Exemple : Un chef d'établissement peut choisir librement le logiciel d'emploi du temps. En conséquence, c'est lui le responsable de traitement. Dans le cas de recours à un sous-traitant, le contrat devra donc préciser de façon expresse : les règles et mesures de sécurité et de confidentialité à mettre en œuvre, les obligations incombant au sous-traitant en matière de sécurité et de confidentialité des données et la mention du fait que ce même sous-traitant ne peut agir que sur instruction du responsable de traitement.*

II/ Responsabilisation des acteurs :

A/ Une application de la RGPD à mettre au regard du type de données :

Il s'agit d'un véritable changement de paradigme : d'une logique de formalité préalable, on passe par une logique de responsabilisation.

Jusque-là, il fallait identifier la ou les formalités à remplir auprès de la CNIL et ensuite, une fois cette déclaration réalisée, l'adresser à cette dernière pour être en conformité avec la protection des données.

Avec le RGPD, chaque acteur doit penser ses outils, penser sa protection des données, se poser des questions et documenter les raisons de ses choix, pourquoi telle mesure de sécurité et pas telle autre... Les autorités n'arrivent seulement a posteriori pour contrôle et sanction en cas de défaillance.

Il faut alors organiser dans un premier temps en interne la gouvernance de la donnée et, en cas de doutes, se retourner vers le conseil (DPO ou DPD) voire l'autorité (la CNIL) : *c'est ce que l'on appelle le principe d'accountability ou de responsabilisation des acteurs.*

Ainsi, dans cette logique, tout traitement de données concernant les élèves (résultats scolaires, professions des parents, revenus du foyer, pays de naissance, vaccinations, allergies si elles sont conséquentes en milieu scolaire…), parents ou personnels, doit dorénavant être inscrit sur un registre interne à l'école ou à l'établissement, et maintenu à jour.

Néanmoins, les démarches déclaratives auprès de la CNIL restent obligatoires pour le traitement de données dites sensibles.

Les données sensibles par nature sont le résultat d'un traitement qui pourrait engendrer des risques importants pour les libertés et les droits fondamentaux de la personne (Considérant 51 du RGPD). Il s'agit alors de mettre en place une protection renforcée car la collecte est interdite sauf exceptions.

La Loi Informatique et libertés du 6 janvier 1978 est ainsi modifiée, dans son article 8, par les lois du 14 mai 2018 et du 20 juin 2018 : *« Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. »*

Dans le contexte de l'éducation, concrètement, on peut énumérer les données suivantes comme sensibles :

- Les données de santé : tests ou analyses génétiques ou biologiques ; maladie ou handicap ; antécédents médicaux ou traitements clinique. Par nature, elles sont non collectées mais dans le contexte scolaire, on peut retrouver ce type de données notamment dans le cas d'un état vaccinal obligatoire à jour de l'enfant ou même une fiche sanitaire (infirmerie). Pour ce dernier cas, le suivi des mineurs est interdit sous

format informatique (papier obligatoirement transmise par les représentants légaux valant consentement au directeur sous enveloppe cachetée) ;

- Handicap, PAI ou PPS : Impossibilité de collecter des données sur la nature du handicap ou la pathologie mais seulement les mesures prises en charge ;

- Les données relatives à la prise en charge sanitaire et psychologique : PPRE / PAP / PAI : Besoins éducatifs particuliers des élèves avec prise en charge sanitaire et psychologique : allergies et pathologies par exemple. Le consentement doit être éclairé, libre, écrit ;

- Le régime alimentaire sans faire apparaître de prétendus origines raciales, ethniques ou religieuses. Le chef d'établissement peut faire apparaître les mentions sans gluten, sans viande, sans sucre mais pas halal ou casher ;

- Les données biométriques (empreintes digitales pour le passage à la cantine) et les vidéos captées par des caméras dans l'enceinte de l'établissement.

B/ L'identification des responsabilités au sein de l'EPLE :

Le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». Il s'agit de la personne qui détermine la réponse aux questions suivantes : A quoi va servir le traitement ? Comment l'objectif fixé sera atteint ?

Pour les applications nationales et académiques, le responsable de traitement est :

- Au niveau ministériel : le ministre (directeurs par délégation).
- Au niveau académique : le recteur, ou les chefs de service rectoraux et DASEN par délégation.
- **Au niveau d'un EPLE : le chef d'établissement.**
- Au niveau d'une école primaire : le DASEN (ni les directeurs d'école, ni les IEN n'ont le statut de personne morale).
- Pour l'enseignement privé sous contrat avec l'état : le directeur de l'établissement.

Le chef d'établissement devient alors responsable du cycle de vie de la donnée :

- Le fait de collecter, d'enregistrer est considéré comme un traitement de données à caractère personnel. *Exemple : les données collectées au moment des inscriptions / réinscriptions des élèves.*

- Le traitement, la modification, l'extraction, le transfert également. *Exemple : le transfert vers un logiciel de vie scolaire, une extraction de la base élèves, un export entre le LSU et Affelnet lycée.*
- Le stockage correspond, par exemple, à l'hébergement du logiciel de vie scolaire chez un éditeur privé ou un ENT.
- L'archivage automatique des données, notamment les backups, en garder deux et écraser les anciennes. *L'archivage correspond, par exemple, aux attestations d'ASSR conservées sur un disque dur au secrétariat.*

Remarque : l'intérêt public peut justifier que certaines données ne fassent l'objet d'aucune destruction : c'est l'archivage définitif. Ces archives sont gérées par les services des archives territorialement compétents, c'est-à-dire les archives départementales.

En savoir plus : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

- La destruction correspond à l'effacement de la collecte de données à caractère personnel. *Par exemple, la liste nominative des emprunteurs au CDI pour l'année scolaire écoulée.*

Le responsable des traitements doit alors tenir un **registre** c'est-à-dire un recensement de l'ensemble des traitements de données à caractère personnelles. Il est structuré en deux parties :

- La liste des traitements qui permet d'identifier la finalité de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. *Par exemple, la gestion des recrutements, la gestion des clients, les enquêtes de satisfaction, la surveillance des locaux, l'organisation pédagogique de temps scolaire, la gestion de la vie scolaire des élèves etc.*
- La fiche traitement : Permettant de recenser et fixer l'objectif principal d'une application informatique de traitement des données personnelles : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles.

Donc tous les traitements réalisés sur les outils de l'école, du collège ou du lycée – ou fournis par l'établissement - (ordinateur, clé USB, ENT…), ou/et partagés dans le cadre du travail, doivent figurer sur le registre de l'établissement.

Les professeurs ne peuvent se retrancher derrière leur liberté pédagogique et doivent être transparent à l'égard du responsable des traitements de l'établissement.

Le chef d'établissement ne peut être tenu pour responsable d'un défaut de protection des données dans un traitement personnel effectué par un enseignant, s'il n'en avait pas connaissance.

Par ailleurs, le responsable de traitement est accompagné dans la mise en place de la réforme d'un DPO ou DPD (Délégué à la protection des données). Au sein de chaque académie, un (ou plusieurs) délégué est nommé par le Recteur et généralement placé sous la responsabilité directe du secrétariat général. Le DPD est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données sur l'ensemble des traitements mis en œuvre dans l'académie.

Il Accompagne donc les responsables de traitement dans le domaine technique, juridique et pédagogique en liaison avec le référent unique pédagogique au numérique de l'établissement. Il a un rôle d'appui, de contrôle et d'interlocuteur privilégié.

Il doit offrir aux responsables des traitements des outils. *Exemple : des études d'impacts comme l'utilisation sensible des données en amont des traitements*

En revanche, il n'a pas de responsabilité juridique.

Sa proximité avec le recteur et le secrétariat général lui confère un devoir de contrôle.

Il doit identifier les relais locaux (RUPD, IAN, Administrateurs réseaux) afin de former et sensibiliser les personnes compétentes et les enseignants dans leurs pratiques pédagogiques.

Chaque EPLE doit déclarer son DPD auprès de la CNIL.

Lien pour déclarer le DPD :

https://www.cnil.fr/fr/designation-dpo

A la fin de la procédure, le responsable de traitement recevra par courriel ainsi que le DPD, un récépissé de déclaration à conserver.

III/ Les précautions à prendre en cas de sous-traitance :

A/ La coresponsabilité du sous-traitant :

La grande nouveauté apportée par la RGPD est l'obligation pour les sous-traitants des données personnelles de tenir un registre des traitements. Cela met fin à la simple responsabilité contractuelle du sous-traitant. Dorénavant, en cas d'écart de la loi, il devient coresponsable.

Pour les sous-traitants d'un EPLE, il faut comprendre les fournisseurs « privés » des outils de vie scolaire ou de gestion de service de restauration.

Le RGPD clarifie donc le cadre contractuel entre les sous-traitants et les responsables de traitement, et surtout il affirme une responsabilité propre du sous-traitant.

Le sous-traitant ne peut agir sans l'instruction du responsable de traitement. Il faut toujours prévoir un contrat - c'est obligatoire -, pour préciser le responsable de traitement et les clauses de traitement des données. L'article 28 du RGPD précise toutes les obligations et toutes les dispositions qui doivent figurer dans le contrat, et cet article exige bien de prévoir par contrat ou par un autre acte juridique les différentes situations et les responsabilités de chacun.

Si il existe déjà des contrats ou des conventions entre le responsable de traitement et la collectivité en tant que sous-traitant ou un sous-traitant privé, il faut penser à les modifier et à les mettre à jour.

Même les contrats en cours doivent prendre en compte les nouvelles obligations de l'article 28 du RGPD.

Le sous-traitant doit prendre toutes les mesures pour assurer la sécurité et la confidentialité des données. Cela existait déjà dans la loi informatique et libertés : l'article 32 du RGPD va même préciser que le responsable de traitement et le sous-traitant mettent en œuvre les mesures de sécurité ; alors qu'avant dans la loi informatique et libertés on disait simplement que c'était le responsable de traitement qui définissait les mesures de sécurité, qu'il pouvait ensuite déléguer par contrat au sous-traitant. Maintenant, il y a bien une logique de renforcement de la responsabilité des sous-traitants.

Autre obligation : le sous-traitant qui voudrait faire appel à un autre sous-traitant doit toujours s'assurer que la bulle de protection qu'il assure lui-même est conservée. Il doit d'abord recevoir une autorisation du responsable de traitement pour recourir à un autre sous-traitant, sinon il n'est plus couvert.

Le DPD accompagnera le chef d'établissement dans ses relations avec les sous-traitants (par exemple, retravailler les clauses contractuelles) ou avec les collectivités de rattachement (travail de coopération pour vérifier les mesures existantes, adaptées si besoin).

B/ Les risques encourus par le chef d'établissement en cas de manquement éventuel au RGPD :

La CNIL se veut rassurante à ce sujet. Elle indique que « dans un souci de simplicité et d'accompagnement », elle n'exigera pas la réalisation immédiate d'une analyse d'impact des traitements qui ont régulièrement fait l'objet d'une formalité préalable avant le 25 Mai 2018. (Sous forme de récépissé, autorisation, avis de la CNIL).

Les amendes ne sont pas applicables aux traitements mis en œuvre par l'État et ses services déconcentrés, ou par les chefs d'établissement et DASEN lorsqu'ils mettent en œuvre un traitement au nom de l'État ou en qualité de représentant de l'État. La CNIL n'a pas tranché, en cas de traitement au nom de l'EPLE ou de l'école, mais les chefs d'établissements et DASEN seront protégés.

Conclusion :

Ce compte-rendu issu du parcours de formation M@gistère permet de :

- Identifier les données à caractère personnel et parmi elles, celles qui sont dites "sensibles",

- Connaître le nouveau cadre européen et faire le point sur les différentes lois en vigueur dans ce domaine,

- Faire le point sur la mise en place du RGPD dans le contexte des établissements scolaires.

- Identifier les traitements en établissement et s'approprier le registre des traitements, comprendre les missions du délégué à la protection des données.

- Définir des actions de communication à destination des équipes pédagogiques, des élèves et de leurs représentants légaux.

Vous trouverez à la fin de CR une FAQ très concrète sur l'application du RGPD dans les EPLE.

Foire aux Questions :

1/ Un enseignant peut-il ouvrir un blog hébergé par une entreprise privée pour partager ses cours, et des vidéos créées par lui, afin de permettre à ses élèves de travailler chez eux plus facilement sachant qu'aucune information liée aux élèves n'est mise en ligne ? Si oui, sous quelles conditions ?

Définitions

A titre liminaire, il convient de rappeler qu'un blog est par défaut un site internet accessible à tous. Dans le cadre d'une utilisation à des fins pédagogiques, il peut apparaître souhaitable d'en restreindre l'accès aux seules personnes autorisées, ce qui implique nécessairement dans ce cas la création de comptes utilisateurs avec identifiants et mots de passe et donc la collecte de données à caractère personnel.

Par ailleurs, si le blog est un outil interactif permettant des échanges entre les utilisateurs, notamment pour commenter les publications qui y sont faites, la qualification de traitement de données à caractère personnel n'est exclue que s'il n'y a aucune possibilité d'identification directe ou indirecte des personnes qui se connectent ou contribuent sur le blog et si aucune donnée pouvant permettre, directement ou indirectement, l'identification des élèves n'est publiée.

Le contexte juridique

En outre, un blog constituant un site internet, il est soumis au droit applicable à tout service de communication en ligne tel qu'il est défini dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et notamment aux dispositions de l'article 6 de cette loi, qui ont été précisées par le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Ces dispositions font notamment obligation à toute personne physique ou morale assurant le stockage de signaux, d'écrits, d'images, de sons ou de messages pour mise à disposition du public de détenir et de conserver pendant un an les données de connexion des utilisateurs de nature à permettre l'identification de quiconque a contribué à la création de contenu en ligne. Par conséquent, si les élèves ou leurs responsables sont autorisés à intervenir sur le blog, leurs données de connexion devront nécessairement faire l'objet d'un traitement de données à caractère personnel.

En application du 2° de l'article R. 421-23 du code de l'éducation, qui prévoit que le conseil d'administration donne son avis sur les principes de choix des manuels scolaires, des logiciels et des outils pédagogiques, l'ouverture d'un blog à des fins pédagogiques au sein d'un EPLE nécessite l'avis préalable du conseil

d'administration avant de pouvoir être inscrit sur le registre d'activités de traitement de l'établissement scolaire.

Points de vigilance

Par conséquent, sauf dans l'hypothèse où un enseignant ouvre un blog auquel personne ne peut contribuer et sur lequel aucune donnée à caractère personnel (par exemple la photographie d'un élève) n'est mise en ligne, l'ouverture d'un blog dans le cadre scolaire constitue un traitement de données à caractère personnel auquel s'applique les dispositions du règlement général sur la protection des données (RGPD) du 27 avril 2016 et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Par ailleurs, si l'entreprise privée qui gère le service héberge des données à caractère personnel, elle doit alors être regardée comme un sous-traitant au sens du RGPD. Par conséquent, une convention de sous-traitance doit être conclue entre l'établissement et cette entreprise, selon les modalités qui sont définies à l'article 28 du règlement.

En pratique

En pratique, ce traitement de données à caractère personnel devra faire l'objet d'une inscription sur le registre de l'établissement public local d'enseignement (EPLE) qui le met en œuvre ou sur le registre tenu par les directions des services départementaux de l'éducation nationale (DSDEN) ou les rectorats d'académie (en fonction de l'organisation choisie) pour les traitements mis en œuvre dans les écoles.

2/ Un enseignant peut-il utiliser en classe un service en ligne de questionnaires ou d'évaluations nécessitant d'identifier ses « élèves » afin d'offrir des parcours et des résultats personnalisés ?

Définitions

Dans la mesure où un tel outil implique nécessairement l'identification des élèves et la collecte d'un certain nombre d'informations à caractère personnel, notamment relatives à l'évaluation des élèves, son utilisation en classe génère la mise en œuvre d'un traitement de données à caractère personnel au sens du règlement général sur la protection des données (RGPD) et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le contexte juridique

Comme tout traitement de données à caractère personnel mis en œuvre dans une école ou un établissement scolaire, il devra dès lors, préalablement à sa mise en œuvre, faire l'objet d'une analyse au regard de la réglementation applicable en

matière de protection des données personnelles avec l'appui du délégué à la protection des données (DPD) et d'une inscription sur le registre des traitements par le responsable du traitement, à savoir le directeur académique des services de l'éducation nationale (DASEN) agissant par délégation du recteur d'académie pour les traitements mis en œuvre dans les écoles et le chef d'établissement pour les traitements mis en œuvre dans les établissements publics d'enseignement du second degré.

Dans les établissements du second degré, l'utilisation d'un tel outil pédagogique sera par ailleurs soumise à l'avis préalable du conseil d'administration, en application du 2° de l'article R. 421-23 du code de l'éducation.

Points de vigilance

Dans l'hypothèse où le fournisseur du service en ligne serait amené à traiter ou à héberger des données, un contrat de sous-traitance doit en outre être établi entre le responsable du traitement et ce fournisseur, dans les conditions prévues par l'article 28 du RGPD.

Une particulière attention doit en outre être accordée dans le choix de ces outils en ligne. Beaucoup d'entre eux reposent en effet sur une analyse des traces d'apprentissage et des comportements des élèves, appelées « learning analytics », qui pourraient être qualifiés de traitements de profilage, dont la mise en œuvre est particulièrement encadrée par les dispositions du RGPD. Il convient par ailleurs de s'assurer que les données des élèves ne seront pas utilisées ultérieurement par les fournisseurs de services pour une finalité autre que celle définie par le responsable du traitement.

3/ Un enseignant peut-il utiliser une application de réseau social pour une utilisation pédagogique ? Si oui, quelles précautions doit-il prendre ? Si oui, sous quelles conditions ?

Le contexte juridique

L'utilisation d'une application de réseau social en classe entraîne nécessairement la mise en œuvre d'un traitement de données à caractère personnel au sens du règlement général sur la protection des données (RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Pour pouvoir mettre en œuvre un tel traitement, il convient donc en premier lieu que le responsable du traitement puisse justifier que ce traitement est nécessaire à l'exercice d'une mission d'intérêt public ou relève de l'exercice de l'autorité publique dont il est investi, au sens du e) du 1 de l'article 6 du RGPD. En d'autres termes, il faut pouvoir être en mesure de justifier que l'utilisation d'une telle application entre

pleinement dans le champ du service public du numérique éducatif défini à l'article L. 131-3 du code de l'éducation.

Si tel n'est pas le cas, pour que le traitement soit licite, il est nécessaire de recueillir le consentement des personnes concernées en application du a) du 1 de l'article 6 du RGPD. Conformément aux dispositions de l'article 7-1 de la loi du 6 janvier 1978 issu de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, il convient ainsi de recueillir le consentement du mineur s'il est âgé de quinze ans ou plus ou le consentement du mineur et des titulaires de l'autorité parentale s'il est âgé de moins de quinze ans.

Il parait toutefois difficile de recueillir le consentement des mineurs, quel que soit leur âge, dans le cadre scolaire. En effet, le 11) de l'article 4 du RGPD précise que le consentement consiste en une « manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Or, il est permis de s'interroger sur la question de savoir si, dans le cadre scolaire, l'élève peut être regardé comme donnant valablement son consentement compte tenu de l'autorité qu'exerce sur lui l'enseignant qui propose l'utilisation d'une application numérique en classe.

Points de vigilance

Le fait qu'un ou plusieurs élèves ou les titulaires de l'autorité parentale pour les mineurs de moins de quinze ans ne consentent pas à la collecte de leurs données personnelles conduit nécessairement à ce que les élèves ne puissent pas suivre l'enseignement et interagir dans le cours dans les mêmes conditions que les autres élèves, ce qui présente le risque d'une rupture d'égalité entre les élèves.

Conformément aux dispositions de l'article 4 du RGPD, le responsable de traitement doit être en capacité de déterminer les finalités et les moyens du traitement (article 4 du RGPD). Cependant, les conditions d'utilisation (CGU) des réseaux sociaux sont le plus souvent élaborées unilatéralement par le fournisseur de services et ne permettent pas au DASEN ou au chef d'établissement d'exercer le moindre contrôle sur le traitement de données qu'il met en œuvre dans son établissement, ce qui n'est pas conforme à la réglementation applicable.

En pratique

En tout état de cause, qu'il soit mis en œuvre sur le fondement du consentement de la personne concernée ou de l'exercice d'une mission d'intérêt public, tout traitement de données à caractère personnel mis en œuvre au sein d'une école ou d'un établissement public du second degré doit être regardé comme étant sous la

responsabilité du DASEN agissant par délégation du recteur d'académie dans le premier degré et du chef d'établissement dans le second degré.

Aussi, pour pouvoir utiliser un réseau social dans le cadre scolaire, ou tout autre service numérique en ligne, il est nécessaire que les conditions générales d'utilisation (CGU) du service fassent l'objet d'un contrôle par les services du ministère ou du rectorat d'académie et présentent des garanties suffisantes, notamment en termes de sécurité des données. Il convient notamment que les fournisseurs de services acceptent d'avoir la qualité de sous-traitants et de ne pouvoir traiter ou héberger les données que sur instruction du responsable de traitement. En dehors d'un tel cadre, qui implique donc des CGU spécifiques négociées par les services du ministère, dites « CGU éducation », il ne paraît pas possible pour le chef d'établissement ou le DASEN de garantir aux élèves et à leurs responsables que les services qu'il mettent en œuvre au sein de l'établissement scolaire respectent les conditions de sécurité adéquates en matière de protection des données à caractère personnel et les droits des personnes concernées.

Comme tout traitement de données à caractère personnel, l'utilisation d'un réseau social en classe doit en outre faire l'objet d'une inscription sur le registre du responsable du traitement et d'une information des personnes concernées conformément aux dispositions des articles 13 et 14 du RGPD.

Les personnes concernées par le traitement (les élèves et leurs responsables s'ils sont mineurs) devront en outre être dûment informées par le responsable du traitement des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

4/ Un enseignant peut-il ouvrir un compte nominatif pour ses élèves sur un service de messagerie, une plateforme de travail coopératif ou de stockage et d'échange de documents développés par une entreprise privée et, si oui, quelles sont les règles à respecter dans ce domaine ?

Dès lors qu'un enseignant ouvre un compte nominatif permettant ainsi d'identifier les élèves avec leurs noms et prénoms, il met en œuvre un traitement de données à caractère personnel. L'utilisation de ces services entraîne d'ailleurs la collecte et le traitement d'autres données à caractère personnel telles que des photos ou des productions scolaires.

Par conséquent, les mêmes considérations que celles qui ont été décrites précédemment s'appliquent à ces traitements, à savoir : pouvoir justifier que le traitement est nécessaire à l'exécution d'une mission de service public ou recueillir le consentement des personnes concernées, avec toutes les réserves déjà rappelées précédemment ; s'assurer que les conditions générales d'utilisation permettent au responsable du traitement (DASEN ou chef d'établissement) de garder la maîtrise

des données à caractère personnel collectées ; s'assurer que le service ou la plateforme présente les garanties suffisantes notamment en termes de sécurité.

Le traitement fait par ailleurs l'objet des mêmes obligations d'inscription sur le registre des activités de traitement et des modalités d'information prévues aux articles 13 et 14 du RGPD.

5/ Dans le cadre du RGPD qui est responsable du traitement des données à caractère personnel pour une école, un collège, un lycée, public ou privé ?

Le 7° de l'article 4 du règlement général sur la protection des données (RGPD) définit le responsable de traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Sauf dans l'hypothèse où le traitement fait l'objet d'un paramétrage local, qui est susceptible de justifier une responsabilité conjointe, les traitements mis en œuvre par le ministère de l'éducation nationale dans les établissements scolaires relèvent uniquement de la responsabilité du ministre chargé de l'éducation nationale.

Ce principe s'applique aux traitements mis en œuvre dans les établissements publics mais également dans les établissements privés sous contrat dès lors que les traitements mis en œuvre relèvent de la compétence du ministre chargé de l'éducation nationale (par exemple, la gestion des personnels). Pour les traitements mis en œuvre dans les écoles ou les établissements scolaires à l'initiative d'un personnel (par exemple, un enseignant), la responsabilité incombe à la personne ayant la capacité juridique de représenter l'établissement, notamment en justice dans l'éventualité d'un recours. Dans les établissements du second degré publics, qui ont la personnalité morale, c'est le chef d'établissement qui, en sa qualité d'organe exécutif de l'établissement conformément à l'article R. 421-9 du code de l'éducation, doit être regardé comme le responsable des traitements mis en œuvre dans son établissement.

En revanche, dans les écoles publiques, les directeurs n'ayant pas la capacité juridique de représenter l'école (cf. les articles 2 à 4 du décret n° 89-122 du 24 février 1989 relatif aux directeurs d'école) ce sont les directeurs académiques des services de l'éducation nationale (DASEN), agissant sur délégation des recteurs d'académie qui, en application de l'article R. 222-19-3 du code de l'éducation, doivent être regardés comme responsables des traitements mis en œuvre. S'agissant enfin des traitements mis en œuvre dans les écoles, collèges et lycées privés, il ne peut y avoir de réponse de principe dans la mesure où la qualité de responsable de l'établissement dépend du mode de constitution et de fonctionnement de ces établissements.

6/ Chaque responsable de traitement doit-il nommer un délégué à la protection des données (DPD) ?

En application du 1 de l'article 37 du règlement général sur la protection des données (RGPD), les responsables de traitement et les sous-traitants sont tenus de désigner un DPD lorsque le traitement est effectué par une autorité publique ou un organisme public ou lorsque l'activité de base de l'organisme consiste en un suivi systématique à grande échelle de personnes ou en un traitement à grande échelle de catégories particulières de données à caractère personnel.

Les responsables des traitements mis en œuvre dans les écoles, les collèges et les lycées publics sont donc tenus de désigner un DPD.

Toutefois, le 3 du même article prévoit que : « 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 ».

Une mutualisation du DPD au niveau académique ou infra-académique est donc tout à fait possible.

En revanche, les établissements d'enseignement privés sous contrat, qui ne relèvent d'aucune des dispositions du 1 de l'article 37 du RGPD, ne sont pas soumis à l'obligation de désignation d'un DPD.

La désignation d'un DPD dans les établissements d'enseignement privés sous contrat n'est donc qu'une faculté prévue par le 4 de l'article 37 du RGPD.

Si les lignes directrices concernant les délégués à la protection des données adoptées le 13 décembre 2016 par le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dénommé « G29 », recommandent aux organismes privés chargés d'une mission de service public de désigner un DPD, il ne s'agit néanmoins que d'une recommandation et non pas d'une obligation.

7/ Une école primaire peut-elle créer un fichier sur un tableur recensant les nom et prénom des élèves, leur classe et leurs demi-journées de présence/absence. Ce fichier a vocation à être soit diffusé sur le réseau local de l'école (première possibilité) afin d'être complété par les enseignants pour leurs classes respectives, soit conservé uniquement sur le poste informatique de direction (et complété par la directrice). Est- ce autorisé ? Et si oui quelles sont les démarches à effectuer ?

Dans la mesure où il implique la collecte de données relatives à la l'identité et à la vie scolaire des élèves, un tel fichier, qu'il soit ou non diffusé sur le réseau local de l'établissement, constitue un traitement de données à caractère personnel au sens du règlement général sur la protection des données (RGPD) et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Comme tout traitement de données à caractère personnel mis en œuvre dans une école, il doit donc faire l'objet d'une inscription sur le registre des activités de traitement tenu par le responsable du traitement, à savoir le directeur académique des services de l'éducation nationale (DASEN), agissant sur délégation du recteur d'académie.

Les personnes concernées par le traitement doivent être informées des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

Elles doivent ainsi être informées : de l'identité et des coordonnées du responsable du traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture des données, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la CNIL.

Le cas échéant, les personnes concernées doivent également être informées : de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des conséquences pour la personne concernée, du droit de retirer son consentement à tout moment, du fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (exemples : clauses contractuelles types de la Commission européenne).

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

8/ L'échange de courrier électronique entre les membres de la communauté éducative (élève/élève, professeur/parents etc.) via une messagerie mise en œuvre par une école est-il considéré comme privé ?

Il résulte d'une jurisprudence constante de la cour de cassation que les fichiers et courriers échangés par un salarié à l'aide d'un outil informatique mis à sa disposition

par l'employeur pour les besoins de son travail sont présumés revêtir un caractère professionnel, sauf si le salarié les a expressément identifiés comme revêtant un caractère personnel (par ex, Cass soc, 16 mai 2013, n° 12-11866).

Le Conseil d'Etat n'a jusqu'alors pas eu l'occasion de prendre position sur cette question.

La cour d'appel de Rennes, statuant en matière pénale, a quant à elle considéré que les courriels échangés par un agent public par le biais d'une messagerie professionnelle sont présumés revêtir un caractère professionnel sauf à ce que leur contenu intéresse de manière évidente la vie privée de leur auteur (CA Rennes, 14 janvier 2010, n° 972010).

Le caractère professionnel d'un message peut autoriser l'employeur, dans certaines conditions – et notamment dans le respect de la réglementation en matière de protection des données à caractère personnel – à exercer un contrôle sur la messagerie de l'agent.

En revanche, dès lors que l'objet du courriel échangé par un enseignant avec un parent d'élève mentionne son caractère privé, il doit être regardé comme une correspondance privée couverte par le secret des correspondances prévu par l'article L. 32-3 du code des postes et des communications électroniques et par le droit au respect de la vie privée reconnu par l'article 8 de la convention européenne des droits de l'homme (CEDH).

Les échanges de courriels entre élèves ont quant à eux par nature un caractère privé. Ce principe de protection des correspondances des enfants ressort de l'article 16 la convention relative aux droits de l'enfant. Il n'est donc pas possible de contrôler leurs courriels, y compris lorsqu'ils utilisent la messagerie qui a été mise à disposition par l'école.

A toutes fins utiles, il convient de rappeler que les messageries électroniques et les dispositifs de contrôle de l'utilisation de ces dernières constituent des traitements de données à caractère personnel au sens de l'article 4 du RGPD et doivent, par conséquent, être inscrits sur le registre des activités du traitement.

9/ Quelles démarches sont à entreprendre pour être conforme à la loi en cas de mise en œuvre d'une plate-forme de e-learning sur laquelle sont enregistrés les élèves ou les stagiaires de la formation continue(nom, prénom, adresse e-mail et les dates et durées de connexions aux cours pour des raisons d'obligation au titre du financement de la formation et/ou pour le conseil régional afin de bien prouver la réalité de l'action de formation) ?

Dès lors qu'elles collectent des données relatives à l'identité des élèves, les plateformes de e-learning constituent des traitements de données à caractère personnel.

Ces traitements doivent par conséquent faire l'objet d'un enregistrement sur le registre des activités du traitement par le responsable de traitement, conformément à l'article 30 du RGPD.

Il convient de préciser que les traitements ayant pour objet de permettre aux élèves ou aux enseignants d'effectuer des formations en ligne (e-learning) entrent sans aucun doute dans le champ du service public du numérique éducatif défini à l'article L. 131-3 du code de l'éducation.

Leur mise en œuvre dans les établissements scolaires relève par conséquent de l'exécution d'une mission de service public au sens du e de l'article 6 du RGPD. Le responsable du traitement (DASEN ou chef d'établissement) n'est donc pas tenu de recueillir le consentement des personnes concernées pour pouvoir mettre en œuvre un tel traitement de données à caractère personnel.

Il convient de préciser que dans le cas où la plateforme est gérée par un prestataire de service, celui-ci doit être regardé comme sous-traitant au sens de l'article 28 du RGPD.

Un contrat doit donc être conclu entre le responsable de traitement et ce prestataire dans les conditions prévues par l'article 28 du RGPD.

Le responsable du traitement doit en effet être en mesure de s'assurer que le sous-traitant présente des garanties suffisantes de manière à ce que le traitement réponde aux exigences du RGPD, notamment en termes de sécurité.

Par ailleurs, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, aux termes des articles 13 et 14 du RGPD.

Elles doivent ainsi être informées : de l'identité et des coordonnées du responsable du traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture des données, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la CNIL.

Le cas échéant, les personnes concernées doivent également être informées : de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des

conséquences pour la personne concernée, du droit de retirer son consentement à tout moment, du fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (exemples : clauses contractuelles types de la Commission européenne).

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

10/ Un enseignant peut-il refuser de transmettre au responsable de traitement, au nom de la liberté pédagogique, les applications numériques effectuant des traitements de données à caractère personnel de ses élèves ?

Un traitement de données à caractère personnel ne peut pas être mis en œuvre sans que les dispositions du règlement général sur la protection des données (RGPD) du 27 avril 2016 et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés aient été respectées, notamment l'inscription du traitement sur le registre des activités de traitement prévu à l'article 30 du RGPD. Dans ces conditions, le responsable du traitement (le DASEN sur délégation du recteur dans le premier degré et le chef d'établissement dans le second degré) doit être informé des applications numériques utilisées en classe avec les élèves si celles-ci génèrent la mise en œuvre d'un traitement de données à caractère personnel. Il convient de rappeler qu'en application du 1 de l'article 24 du RGPD, le responsable du traitement « met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au (…) règlement ».

La liberté pédagogique de l'enseignant est encadrée : comme le rappelle l'article L. 912-1-1 du code de l'éducation, elle s'exerce « dans le respect des programmes et des instructions du ministre chargé de l'éducation nationale et dans le cadre du projet d'école ou d'établissement avec le conseil et sous le contrôle des membres des corps d'inspection ».

Dans le second degré, l'article R. 421-23 du code de l'éducation précise d'ailleurs que le conseil d'administration, sur saisine du chef d'établissement, donne son avis notamment « sur les principes de choix des logiciels et des outils pédagogiques ».

L'enseignant est donc libre de choisir les outils pédagogiques qu'il souhaite utiliser dans le cadre de sa mission éducative, mais le conseil d'administration de l'établissement public local d'enseignement (EPLE) est appelé à émettre un avis sur les principes qui guident ses choix.

De même, dans le premier degré, l'article D. 411-2 du code de l'éducation prévoit qu'une information doit être donnée au conseil d'école sur les principes de choix des manuels scolaires ou de matériels pédagogiques divers.

11/ Pour les enseignements professionnels, les professeurs ont à choisir des solutions numériques liées au métier auquel prépare la formation. La plupart de ces solutions sont aujourd'hui proposées en ligne par les éditeurs. Les élèves (ou étudiants) sont susceptibles de les utiliser sous leur propre identité. Quels sont les points de vigilance auxquels sensibiliser les professeurs pour les aider dans leur choix ?

Le contexte juridique

Dans la mesure où les élèves utilisent leur nom, un identifiant ou encore une adresse mail pour accéder au service proposé, ces solutions numériques constituent des traitements de données à caractère personnel au sens du règlement général sur la protection des données (RGPD) du 27 avril 2016 entré en vigueur le 25 mai 2018 et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Par conséquent, comme tout traitement de données à caractère personnel mis en œuvre dans un établissement scolaire, il doit faire l'objet d'une analyse au regard de la règlementation applicable en matière de protection des données personnelles avec l'appui du délégué à la protection des données (DPD) et d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le chef d'établissement dans les établissements du second degré.

Dans le cas où les solutions numériques sont gérées par un prestataire de service, celui-ci doit être regardé comme un sous-traitant au sens de l'article 28 du RGPD.

Un contrat doit donc être conclu entre le responsable du traitement et ce prestataire dans les conditions prévues par l'article 28 du RGPD.

Le responsable du traitement doit en effet être en mesure de s'assurer que le sous-traitant présente des garanties suffisantes de manière à ce que le traitement réponde aux exigences du RGPD.

En pratique

Il est donc impératif de sensibiliser les professeurs sur la nécessité de choisir une solution numérique proposée par un éditeur qui, notamment :

- s'engage à respecter les règles instaurées par le RGPD. Par exemple, certains éditeurs peuvent appliquer un code de conduite approuvé ou un mécanisme

de certification approuvé, ce qui constitue un élément pour démontrer l'existence de garanties suffisantes (cf point 5 de article 28) ;

- s’engage à respecter les mesures de sécurité instaurées par le RGPD (article 32). Il s’agit par exemple de la pseudonymisation et du chiffrement des données à caractère personnel ;

- s'engage à informer le responsable de traitement en cas de violation de données à caractère personnel (cf point 2 de l’article 33) ;

- s'engage à n’avoir recours qu’à des sous-traitants soumis aux mêmes obligations que celles prévues dans le contrat de sous-traitance initial.

Par ailleurs, dans la mesure où ces solutions numériques entrent dans le champ du service public du numérique éducatif défini à l’article L. 131-3 du code de l’éducation, le traitement est nécessaire à l’exercice d’une mission d’intérêt public au sens du e) du 1. de l’article 6 du RGPD. Le consentement des personnes concernées n’a donc pas à être préalablement recueilli.