

Parcours Numérique éducatif / RGPD

Le RGPD dans les établissements scolaires

- Mahalia GALIÉ-BLANZÉ, Juriste éducation - Service des affaires régaliennes et des collectivités territoriales - CNIL

Animation : **Mylène RAMM**, Chargée de missions - AVICCA

Mylène RAMM

Mahalia Galié-Blanzé, juriste au service des affaires régaliennes et des collectivités territoriales de la CNIL va nous présenter une recontextualisation du RGPD dans l'éducation.

Mahalia GALIÉ-BLANZÉ

J'ai orienté le sujet en essayant de voir quelles étaient les responsabilités de chacun avec les nouvelles obligations du RGPD, en tenant compte de l'imbrication des acteurs relevant de la tutelle du ministère de l'Éducation nationale et des collectivités dans les traitements mis en œuvre dans l'éducation.

Le RGPD - Règlement général à la protection des données - est un règlement européen, résultat d'un long compromis des institutions et États européens. Cela a été très difficile puisque 4 ans de négociation ont été nécessaires. Adopté en avril 2016, le texte est applicable depuis le 25 mai 2018.

Avant d'en venir au fond et de voir si ce RGPD représente réellement un big bang, 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.

Il a fallu revoir toute l'organisation de la CNIL en matière de coopération européenne, puisqu'une des nouveautés est justement cette coopération entre les autorités de protection des données européennes.

La réforme de la loi informatique et libertés a par ailleurs été un peu longue et complexe. Le texte a été voté par l'Assemblée nationale le 14 mai, mais la loi n'a été promulguée que le 20 juin car elle avait été au préalable déferée au Conseil constitutionnel.

Le RGPD est-il un big bang ? Pas tant que cela en France, parce que la loi informatique et libertés existe depuis 1978 et que ses grands principes sont repris dans le RGPD. En fait, on peut dire que la France a été pionnière en matière de protection des données, car elle a été la première à se doter d'une loi qui était assez visionnaire et très bien écrite ainsi que d'une autorité de protection des données, la CNIL. Néanmoins, le règlement européen apporte des nouveautés avec trois grands axes à retenir.

Tout d'abord, il renforce le droit des personnes en plaçant les personnes physiques au cœur du dispositif et en leur accordant de nouveaux droits, comme le droit à la portabilité qui est

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.

Toujours dans cette idée de renforcement des droits et de placer les personnes au cœur du dispositif, on a aussi un champ d'application très large, beaucoup plus qu'antérieurement 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. Cela, c'est vraiment une grande nouveauté.

Le deuxième axe est la responsabilisation des acteurs. C'est notamment pour cela que le RGPD est présenté comme un big bang, car on se départi d'une logique de formalité préalable. Avant, on se posait la question de savoir quelle formalité il fallait remplir auprès de la CNIL et ensuite, une fois faite cette déclaration, on ne se posait plus la question de savoir si l'on respectait 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 qu'après. On organise d'abord en interne la gouvernance de la donnée et, si on a une question, on se tourne vers l'autorité : c'est ce que l'on appelle le principe d'*accountability* ou de responsabilisation des acteurs.

Le troisième axe à retenir est la crédibilisation renforcée des régulateurs et des autorités de protection des données, tout d'abord par des pouvoirs de sanction beaucoup plus élevés qu'auparavant. À titre d'exemple, depuis 2016 le pouvoir de sanction de la CNIL pouvait aller jusqu'à 3 millions d'euros (contre seulement 150 000 euros précédemment) ; avec le règlement européen, les sanctions peuvent s'élever jusqu'à 4% du chiffre d'affaires mondial d'une entreprise ou 20 millions d'euros. On voit que la protection des données devient un véritable enjeu, également économique.

J'ai choisi de recentrer cette présentation sous le prisme du sous-traitant, car dans le secteur de l'Éducation nationale on voit souvent une imbrication qui est liée à l'organisation prévue par les textes entre des acteurs relevant du ministère de l'Éducation nationale, le ministère lui-même, les académies, les écoles, les EPLE, mais aussi les collectivités territoriales qui ont un rôle fort à jouer et qui sont compétentes sur de nombreux champs impactant les traitements de données à caractère personnel.

Je préciserai d'abord les notions de responsable de traitement et de sous-traitant. Le responsable de traitement est celui qui détermine la finalité du traitement de données, c'est-à-dire le « pourquoi » (pourquoi il traite les données, quel est l'objectif et le résultat attendu). Il détermine également le « comment », c'est-à-dire les moyens pour parvenir à cette finalité. Choisir les moyens, cela peut être choisir un prestataire ou un sous-traitant qui lui-même a défini un outil.

Le sous-traitant traite les données pour le compte du responsable de traitement ; il agit sur instruction du responsable de traitement, il ne détermine pas la finalité. Le traitement de données à caractère personnel est une notion très large définie par un article dans le règlement européen : cela va de la consultation des données en passant par leur

conservation. Par exemple, un simple hébergement est un traitement de données à caractère personnel ; si on héberge pour le compte de quelqu'un, on sous-traite des données ; quand on est amené à consulter des données pour faire de la maintenance, on sous-traite les données pour le compte du responsable de traitement. Ces notions existaient dans la loi informatique et libertés et elles n'ont pas changé avec le RGPD.

En revanche, le RGPD a amené une nouvelle notion qui est la responsabilité de traitement conjointe dans laquelle il faut bien distinguer sous-traitant et responsable de traitement conjoint. Lorsque deux responsables de traitement ou plus décident ensemble, de manière conjointe, des finalités et des moyens à mettre en œuvre, ils sont responsables de traitement conjoints. Par exemple, une agence de voyage envoie des données à une compagnie aérienne et à une chaîne d'hôtels pour des réservations de voyage : chacun est responsable de son propre traitement avec des destinataires à qui on transmet les données. Si ces trois sociétés décident de se mettre ensemble pour définir un outil commun qui leur permettrait de gérer les réservations en précisant quelles données seront traitées, combien de temps seront-elles conservées, qui va s'occuper de quelle procédure... Ces sociétés auraient défini conjointement les finalités et les moyens de mise en œuvre du traitement et on pourrait considérer qu'elles sont responsables conjoints de traitement.

Comme cette notion est nouvelle, la CNIL n'aura pas tout de suite une doctrine bien établie, et il y aura forcément des cas où l'on se posera la question, des cas que l'on analysait peut-être autrement avant. Quand il y avait un responsable de traitement, et un autre acteur on le qualifiait souvent de sous-traitant parce qu'on n'avait pas vraiment le choix. Peut-être que des cas antérieurement conçus ainsi seront avec le règlement analysés différemment, à l'aune de cette notion de responsable conjoint.

C'est un point à suivre, notamment dans l'Éducation du fait de l'imbrication des rôles avec les collectivités territoriales et des différents acteurs concernés, il n'est pas impossible que sur certains cas on se retrouve sur de la responsabilité conjointe, avec son régime spécifique, alors que jusqu'à maintenant la situation n'était pas analysée de cette manière.

Pour l'instant, dans le secteur de l'Éducation nationale, on constate dans la plupart des cas que ce sont les acteurs de l'Éducation nationale (académies, ministère, EPLE, écoles) qui sont les responsables de traitement. Ils ont une finalité qui leur incombe, en application de leur mission de service public de l'Éducation (gestion scolaire, activité pédagogique, utilisation des nouvelles technologies ou des ressources numériques) pour mener à bien la mission de service public de l'Éducation. De leur côté, les collectivités territoriales vont souvent endosser le rôle de sous-traitant, notamment lorsqu'elles hébergent des données de l'Éducation nationale, de l'académie ou des établissements.

Le RGPD clarifie le cadre contractuel entre les sous-traitants et les responsables de traitement, et surtout il affirme une responsabilité propre du sous-traitant. Nous allons donc voir quelles sont les obligations des sous-traitants, puisque les collectivités seront souvent qualifiées ainsi au regard du RGPD, et ensuite quelle est leur responsabilité.

Le sous-traitant ne peut agir sans l'instruction du responsable de traitement. Il faut toujours se ménager un contrat - c'est obligatoire -, pour pouvoir justifier qu'on agit pour le compte de tel responsable de traitement et sur son instruction. Vous retrouverez à l'article 28 du

RGPD 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 vous avez déjà des contrats ou des conventions entre vos responsables de traitement et la collectivité en tant que sous-traitant, 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. La réalisation de l'inventaire de ces traitements qui doit être fait pour établir le registre peut être l'occasion de faire le point sur les différents cas où les collectivités interviennent en tant que sous-traitant, de voir s'il y a un contrat existant et de le mettre à jour ou, s'il n'y en a pas, de le mettre en place.

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. En fonction des opérations de sous-traitance effectuées, il s'agira de voir quelles mesures de sécurité, techniques et organisationnelles, seront pertinentes et à mettre en œuvre pour assurer cette sécurité des données à caractère personnel.

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. Par ailleurs, il doit s'assurer que le sous-traitant qu'il choisit apporte des garanties suffisantes, notamment pour la sécurité des données, sinon il pourrait se voir reprocher par une autorité de contrôle d'avoir fait appel à un sous-traitant qui n'apportait pas suffisamment de garanties.

Le sous-traitant a un devoir d'accompagnement, de conseil et d'alerte du responsable de traitement. Si par exemple le responsable de traitement lui donne une consigne qui lui paraît manifestement illicite ou contraire au règlement européen sur la protection des données, le sous-traitant doit l'en informer. Il doit aussi mettre à disposition toutes les informations nécessaires pour que le responsable de traitement puisse démontrer le respect de ses obligations. Par exemple, en tant que responsable de traitement, j'ai des obligations de minimiser le traitement des données à caractère personnel, de les supprimer quand je n'en ai plus besoin, de répondre aux demandes de droit d'accès des personnes, mais parfois je ne suis pas en mesure techniquement de le faire parce que j'ai recours à un sous-traitant et que c'est lui qui va avoir soit l'information, soit la main techniquement pour procéder par exemple à la suppression des données. En tant que sous-traitant, je dois faciliter le travail du responsable de traitement qui me dirait : « j'ai besoin de supprimer ces données pour être en conformité », et c'est à moi de le faire pour qu'il puisse rester dans le respect de ses propres obligations.

Enfin, le sous-traitant doit notifier au responsable de traitement toute violation des données personnelles dans les meilleurs délais. Le responsable de traitement devra notifier la violation de données personnelles à l'autorité de protection des données, si cette faille de

sécurité est susceptible d'engendrer un risque pour la vie privée des personnes concernées. Lorsque ce risque est très important, le responsable de traitement devra aussi informer les personnes concernées. Si la faille de sécurité est du fait du sous-traitant, même non intentionnelle bien sûr, il doit en informer le responsable de traitement pour que celui-ci puisse répondre à ses obligations d'informer l'autorité voire les personnes concernées.

Il existe d'autres obligations du sous-traitant, et notamment l'obligation de mise en conformité dynamique. Comme tous les acteurs, avec le principe de responsabilisation du règlement européen, le sous-traitant doit prendre en compte les principes de protection des données personnelles dès la conception de ses produits et il doit toujours se mettre dans une posture dynamique de mise en conformité. Ce sont les principes d'*accountability* mais aussi de *privacy by design* ou *privacy by default*, qui consistent à s'assurer dès la conception et par défaut que les données personnelles sont protégées.

Par exemple, si je développe un outil au service d'un responsable de traitement, en tant que sous-traitant, pour respecter le principe de minimisation des données, je vais essayer de privilégier un menu déroulant pour qu'on ait juste à cocher des cases ou à choisir un item, plutôt que de laisser des champs libres qui risqueraient d'inciter le responsable de traitement qui va traiter les données à remplir au maximum le champs alors qu'il n'aura pas forcément besoin de toutes les données qu'il met dedans.

L'obligation de tenue d'un registre est une obligation beaucoup plus concrète. En tant que sous-traitant, vous devez tenir un registre des activités de traitement que vous effectuez pour le compte d'un responsable de traitement. Le registre doit contenir tout un tas d'informations que vous retrouverez sur le site de la CNIL, où un modèle de registre est même proposé. En tant que sous-traitant, ce registre doit être distinct du registre que vous tenez en tant que responsable de traitement. Le registre fait partie d'un ensemble qu'on appelle « la documentation » qui doit être tenue à la disposition de l'autorité de contrôle ou de protection des données. En cas de contrôle, c'est la première chose qui sera demandée. La documentation qui comprend le registre des traitements, mais aussi le registre des violations de données, les analyses que vous auriez pu mener dans le cadre de certains traitements où il est nécessaire de mener une analyse d'impact sur les risques pour la vie privée des personnes concernées, les contrats de sous-traitance, les formulaires de recueil des consentements... Il est difficile de dresser une liste exhaustive, mais cela montre qu'il y a une logique. Avec le principe de responsabilisation, il ne s'agit plus de se demander quelles formalités il faut accomplir auprès de l'autorité mais de documenter la réflexion qui a conduit à certains choix et de documenter ce qui est fait en pratique dans la structure.

Enfin dernière obligation du sous-traitant, et du responsable de traitement que vous pouvez être en tant que collectivité territoriale et donc organisme public, la désignation d'un délégué à la protection des données, également appelé DPO (*Data protection officer*). En tant que sous-traitant, vous devez obligatoirement désigner un délégué à la protection des données lorsque vous êtes un organisme public. C'est un des cas obligatoires de désignation du DPO dans le RGPD.

À la question de savoir si le délégué désigné pour vos activités menées en tant que responsable de traitement peut être le même que le délégué qui doit se prononcer sur vos activités de sous-traitant. À la CNIL, nous préconisons d'avoir le même DPO afin de faciliter le point de contact pour les personnes qui voudraient exercer leurs droits, et de faciliter

aussi les contacts avec l'autorité de contrôle. Pour l'instant, vous pouvez désigner un délégué qui aura la double casquette.

Ce délégué peut être mutualisé, il peut être interne ou externe, mais il faut toujours qu'il puisse bénéficier de moyens matériels et organisationnels, et de ressources qui lui permettent de mener à bien ses missions. Donc, désigner un délégué externe qui n'est jamais joignable, ce n'est pas une bonne chose ; désigner un seul délégué sur une région académique pour tous les établissements, toutes les écoles plus l'académie elle-même ne paraît pas répondre aux nécessités de disposer des moyens suffisants pour mener à bien ces missions. Par contre, si le délégué s'entoure d'une équipe avec des référents et des relais, pourquoi pas ? Les situations seront appréciées au cas par cas.

Quelles sont les conséquences en cas de manquement à toutes ces obligations ? Il existe maintenant une responsabilité directe en propre et en tant que sous-traitant qui n'existait pas du tout dans la loi informatique et libertés. Vous pouvez être sanctionnés pour le non-respect de toutes les obligations : par exemple ne pas avoir désigné un DPO, ne pas avoir tenu un registre, ne pas avoir agi conformément aux instructions du responsable de traitement, ne pas l'avoir aidé ou informé pour qu'il puisse respecter ses propres obligations, ne pas l'avoir informé d'une violation de données... Si le manquement au RGPD cause un dommage à une personne et que le responsable de traitement et le sous-traitant sont impliqués dans ce dommage, la personne pourra demander réparation de l'intégralité de son préjudice au sous-traitant ou au responsable de traitement. C'est le principe classique d'obligation à la dette, donc responsable de traitement et sous-traitant sont solidaires. Après, il y a bien sûr des principes de contribution à la dette : le sous-traitant ou le responsable de traitement condamné à la réparation de l'entier préjudice peut se retourner contre les autres pour récupérer la part du dommage qu'il a indemnisé et dont il n'était pas tenu *in fine*.

Un guide sous-traitant est disponible sur le site de la CNIL¹ ; je vous invite à le consulter notamment parce qu'il contient de nombreux exemples de clauses. Ce ne sont pas des modèles mais des exemples qui peuvent être inspirants. Il pourrait être mis à jour d'ici la fin de l'année civile.

Dernier point, l'idée de responsabilisation des acteurs implique une organisation en réseau. La CNIL ne pourra plus accompagner individuellement les acteurs. Il faut saisir l'opportunité du délégué pour avoir des réseaux d'échanges, comme on peut le voir dans l'enseignement supérieur où les anciens correspondants « informatique et libertés » s'étaient organisés en réseau pour échanger. Lorsque le réseau a une difficulté il la fait remonter à l'autorité, ce qui permet ainsi de répondre de manière efficace et de diffuser l'information. Merci.

Les réponses* aux questions ci-dessous apportées par Mme GALIÉ-BLANZÉ constituent des indications générales, une analyse au cas par cas pourrait contenir des spécificités entraînant une analyse différente. [...]

(* Les réponses aux questions sont réservées aux adhérents de l'AVICCA)

¹ https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Collectivités et numérique éducatif : les actes de la journée

Lycées

- [La reprise de la maintenance de l'informatique des lycées en région Centre-Val de Loire par le GIP RECIA](#)
- [Le lycée 4.0 dans la région Grand Est](#)

Collèges

- [La maintenance et la centralisation informatique dans les collèges de l'Ain](#)
- [Le projet de centralisation de la maintenance informatique des collèges en Dordogne](#)
- [Le réseau et la centralisation de la maintenance informatique des collèges dans la Manche](#)

Le raccordement des établissements scolaire

- [Monter un GFU pour apporter du débit internet à ses établissements publics](#)

Changer la forme scolaire

- [L'expérience de la « classe mutuelle »](#)
- [Soutenir l'innovation pédagogique pour une collectivité, l'appel à projets du Val-d'Oise](#)

RGPD

- [Le RGPD dans les établissements scolaires et réponses à vos questions \(actes réservés adhérents\)](#)
- [Le RGPD dans les établissements scolaires \(Verbatim Grand Public\)](#)