RÉGION ACADÉMIQUE
BOURGOGNE-
FRANCHE-COMTÉ
Liberté
Égalité
Fraternité

LES DOSSIERS DE LA DRANE

DONNÉES PERSONNELLES ET BIEN-ÊTRE NUMÉRIQUE

AVRIL 2026

DONNÉES PERSONNELLES ET BIEN-ÊTRE NUMÉRIQUE

sommaire interactif

INTRODUCTION

1. Le droit à la personnalité (Code Civil) (pages 2-5)

- Le droit au respect de la vie privée
- Le droit à l'image
- Le droit à la voix
- Captation de la voix et de l'image à l'École

2. Le Règlement Général de Protection des données (RGPD, 2018) (pages 5-7)

- Les grands principes du RGPD
- Les données personnelles des élèves et des enseignants
- Les données sensibles des élèves et des enseignants
- La collecte et le traitement des données à caractère personnel
- Les responsables de traitement des données en milieu scolaire
- Le droit à l'oubli numérique (aussi appelé droit à l'effacement)

3. Les lois renforçant le protection des données personnelles des mineurs dans le cyberespace (pages 8-10)

- La loi du 7 octobre 2016 pour une République numérique
- La loi du 19 octobre 2020 encadrant l'exploitation commerciale de l'image sur les plateformes en ligne
- Le règlement sur les services numériques du 19 octobre 2022 (DSA, Digital Services Act)
- La loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne
- La loi du 6 février 2024 visant à garantir le respect du droit à l'image des mineurs
- La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique
- La résolution européenne du 26 novembre 2025 proposant de fixer à 16 ans l'âge minimum d'accès aux réseaux sociaux
- La proposition de loi du 31 mars 2026 visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux

4. Quelques études de cas spécifiques au milieu scolaire (pages 11-15)

5. Récapitulatif sur les droits et les devoirs (pages 16-17)

CONCLUSION (page 17)

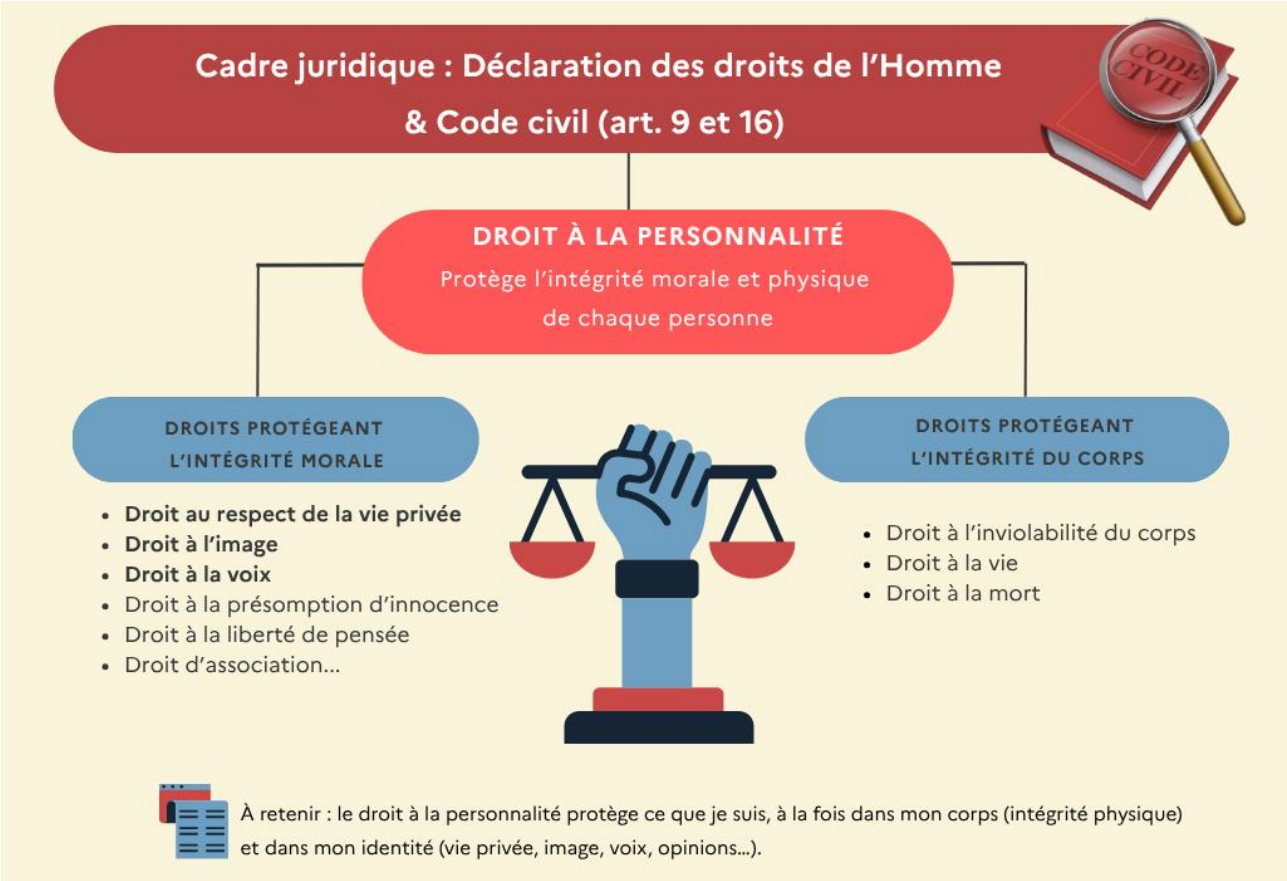
Fiche outil N°1 : Qui fait quoi dans l'établissement ?

Fiche outil N°2 : Les questions à se poser en matière de données personnelles

INTRODUCTION

Le cadre juridique touchant à la vie privée convoque plusieurs branches et sous branches du droit (droit civil, droit pénal, droit administratif, Code de la propriété intellectuelle).

L'essentiel à retenir dans toute cette complexité est que, **en France, une personne est protégée dans son individualité propre grâce à ce qu'on appelle « le droit à la personnalité »** (article 12 de la Déclaration Universelle des Droits de l'Homme de 1948, article 8-1 de la Convention Européenne des Droits de l'Homme ,articles 9 et 16 du Code civil). Ce droit est en fait un ensemble de droits fondamentaux qui se distinguent en deux grandes catégories: les droits protégeant l'intégrité physique et ceux protégeant l'intégrité morale.



Le droit à la personnalité

« *chacun a droit au respect de sa vie privée* » (article 9, Code civil)

Le droit au respect de la vie privée

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Le droit au respect de la vie privée implique notamment le respect de l'intimité, le secret médical, le droit au changement d'état civil, la protection contre les écoutes téléphoniques, la collecte d'informations à caractère privé par les services de sécurité d'un Etat et les publications portant atteinte à la vie privée.

Le droit à l'image

NB. Le droit à l'image se distingue du droit de l'image régi par le Code de la propriété intellectuelle et qui suppose, pour tout usage d'une œuvre visuelle, l'autorisation de l'auteur de cette image.

Le droit à l'image est un droit autonome découlant des dispositions de l'article 9 du code civil. Il permet à toute personne physique de s'opposer à l'utilisation (traitement, duplication, diffusion…), commerciale ou non, de son image.

Il appartient donc aux enseignants, avant de diffuser une vidéo ou une photo représentant leurs élèves, d'obtenir le consentement des élèves majeurs et l'autorisation des représentants légaux pour les élèves mineurs). Cet accord doit être écrit et doit préciser l'usage qui sera fait de la vidéo ou de la photo.

Le floutage des visages et la vue de dos permettent de publier une photo de personnes dont on n'a pas obtenu l'autorisation. Il faut toutefois veiller à ce que le contexte de la photo ne permette pas de déduire leur identité.

Le droit à la voix

La voix fait l'objet d'un droit de la personnalité au même titre que l'image. Les élèves ont un droit exclusif sur leur image et leur voix. **Ceci implique que les enregistrements vocaux ne peuvent être faits sans un consentement préalable et ce, même si les productions ne sont pas diffusées**.

Cet accord doit être écrit et doit préciser l'usage qui sera fait de la voix.

Captation de la voix et de l'image à l'École

Toute utilisation de la voix (podcast, radio/webradio, chorale…) ou de l'image (évènement, sortie culturelle, voyage scolaire, portes ouvertes…), suppose le consentement de l'élève (s'il est majeur) ou des représentants légaux (s'il est mineur). Par publication, on entend : publication pour un usage interne à la classe ou à l'école, diffusion restreinte aux parents via l'ENT, diffusion plus large sur un blog pédagogique ou le site Internet de l'établissement.

La demande d'autorisation doit se faire avant les enregistrements et ce, même si aucune diffusion n'est prévue. L'autorisation doit être **écrite, apposée de la signature authentique** des élèves et leurs représentants légaux (pour les mineurs). Elle droit décrire précisément l'usage qui sera fait de la voix et de l'image. Il est nécessaire de faire **une demande par projet** (c'est-à-dire, un projet avec la même classe, de même nature avec une même destination).

L'autorisation d'un seul parent suffit y compris en cas de parents séparés car c'est une situation considérée comme usuelle par la jurisprudence.

Les enseignants, eux aussi, peuvent être enregistrés ou filmés. Le cours d'un enseignant peut être capté pour des raisons de facilitation pédagogique par exemple, pour un élève qui aurait une mémoire auditive, pour un élève absent ou hospitalisé par exemple, par un élève à besoins particuliers qui aimerait réécouter la leçon etc. Ceci dit, ni les élèves ni leurs éventuels AESH, ne sont autorisés à photographier, enregistrer ou filmer un enseignant sans son consentement et encore

moins à les diffuser. Cette interdiction est d'autant plus vraie s'il s'ensuit une publication sur les réseaux sociaux.

Des modèles d'autorisation d'enregistrement de la voix et de l'image sur disponibles sur Éduscol.

2. Le Règlement général de protection des données (RGPD, 2018)

Les grands principes du RGPD

Ce texte réglementaire européen est né en 2018 de la nécessité d'adapter le droit aux évolutions des technologies et des pratiques d'enseignement-apprentissage. Il s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978.

Son article 5 énumère ses grands principes :
1 – loyauté et transparence au niveau du traitement des données
2 – limitation des finalités de ce traitement
3 – qualité des données
4 – confidentialité
5 – droit des personnes en matière d'accès, de rectification, de suppression et d'opposition à leurs données personnelles

Les données personnelles des élèves et des enseignants

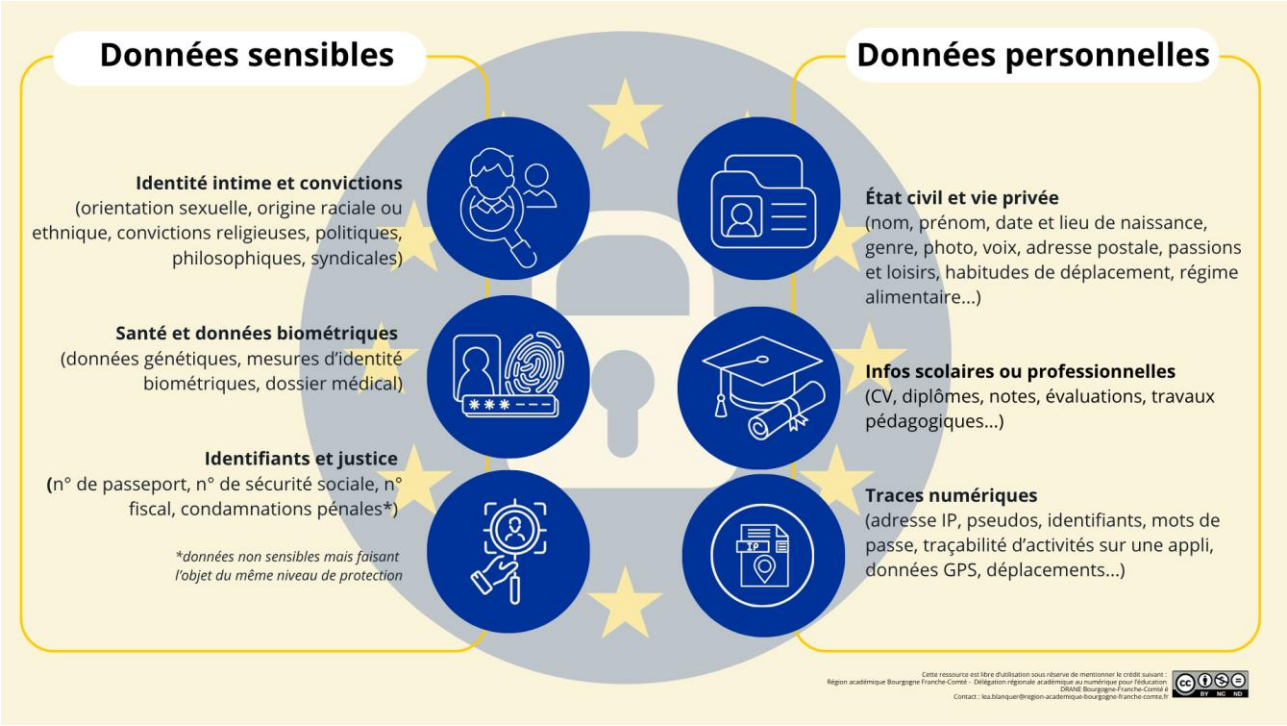
De nombreux usages pédagogiques s'appuient aujourd'hui sur l'utilisation des **données personnelles** des élèves. **Une donnée à caractère personnel est une information relevant de plusieurs domaines de la vie privée de l'élève et qui permet de l'identifier directement, indirectement ou par recoupement.**

Plus une information est sensible, plus il est indispensable de se questionner sur sa collecte et de prendre des précautions au niveau de sa sécurisation.

« *Une donnée n'est plus considérée comme personnelle lorsqu'elle est anonymisée ; c'est-à-dire lorsqu'il est impossible de reconnaître la personne concernée (en floutant le visage par exemple). Cependant, si le recoupement d'informations (même anonymisées) permet d'identifier la personne, les données sont alors toujours considérées comme à caractère personnel*. »

Les données sensibles des élèves et des enseignants

Une donnée sensible est une information qui révèle les **origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, la santé ou l'orientation sexuelle d'une personne**.



La distinction entre données personnelles et données sensibles détermine le niveau de protection et les conditions de traitement de chaque type de données.

La collecte et le traitement des données à caractère personnel

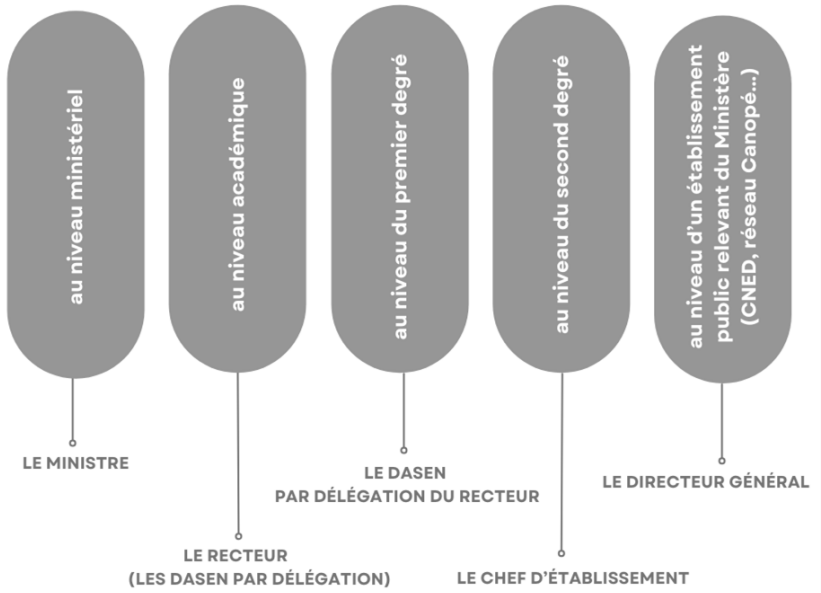
La question de la protection des données personnelles est centrale à l'Ecole en raison du suivi administratif et pédagogique de l'élève mais également de l'accès à des ressources et outils-services numériques pédagogiques.

Le RGPD n'a pas vocation à contraindre les innovations pédagogiques mais à rappeler de ne pas transiger sur les principes éthiques. Il renforce les droits des élèves, des enseignants et des chefs d'établissement et il responsabilise les acteurs traitant des données à caractère personnel en obligeant à ce que la collecte et le traitement aient un objectif utile, légitime et clairement énoncé.

On comprend ainsi qu'il n'est pas possible pour un établissement scolaire ni pour un fournisseur de services numériques de collecter les données de leurs élèves juste au cas où cela serait utile un jour.

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés.

Les responsables de traitement des données en milieu scolaire



En cas de violation de données à caractère personnel, le responsable de traitement doit prendre l'attache de la personne concernée, de la CNIL.

Le Délégué à la Protection des Données académique doit en être informé.

Le droit à l'oubli numérique (article 17)

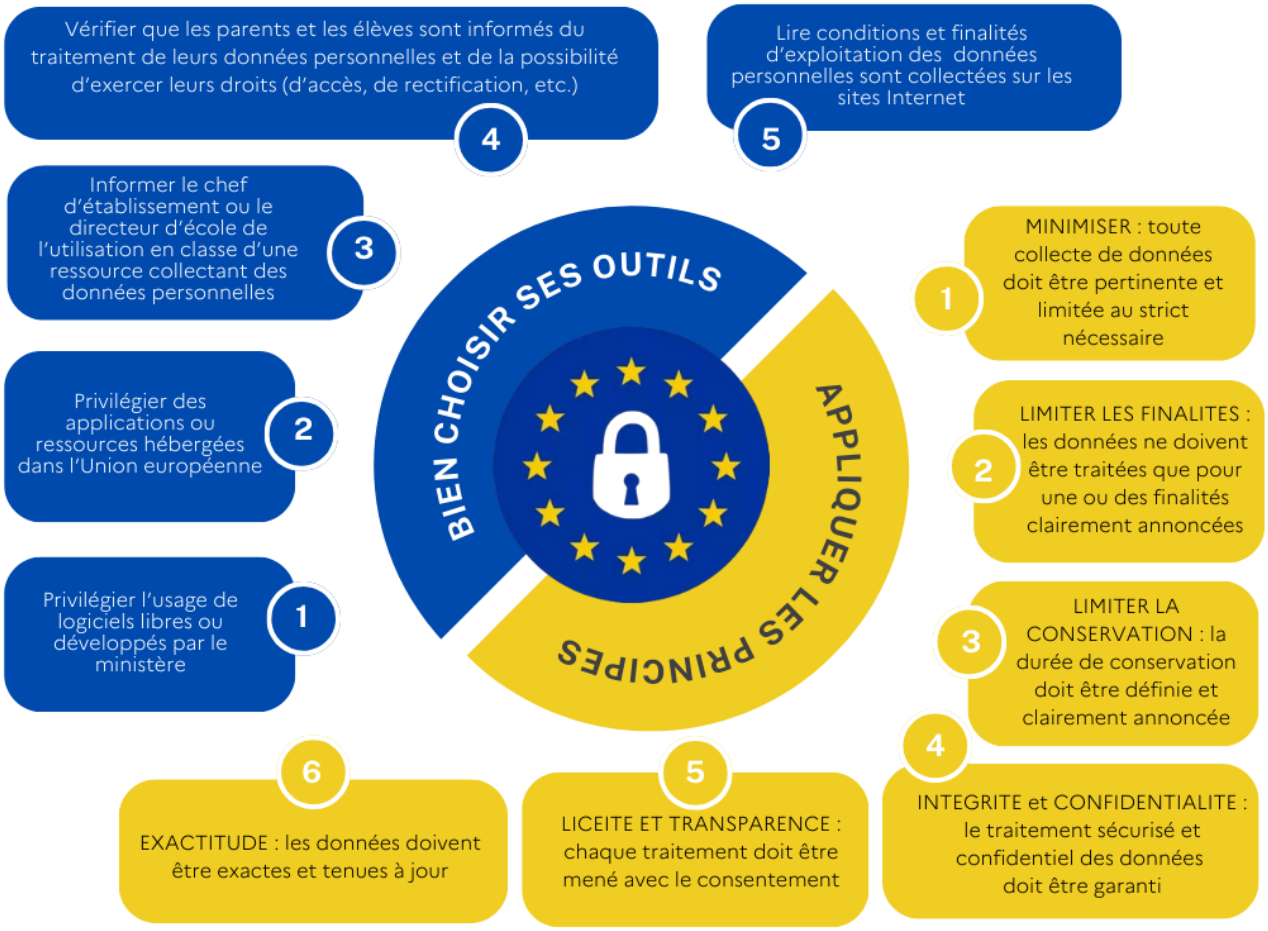
Le **droit à l'oubli numérique** a deux versants :

- le **droit au déréférencement** qui permet de demander à un moteur de recherche de déréférencer certains résultats de recherche associés à son nom et prénom (les contenus ne sont pas supprimés).

- le **droit à l'effacement**, au sens strict, qui permet de demander à l'éditeur d'un site web d'effacer ses données à caractère personnel lorsqu'il n'existe plus de raison légitime à les conserver. Ce droit peut être invoqué dans le cas d'une photo gênante publiée sur les réseaux sociaux ou d'un souhait de ne plus bénéficier des services d'un site marchand en ligne.

C'est donc bien par abus de langage que ce droit à l'oubli numérique est parfois appelé droit à l'effacement.

Attention toutefois : ce droit n'est pas systématique. Il s'étudie au cas par cas, en fonction de certains critères (notoriété de la personne concernée, conditions de mise en ligne, nature du contenu…) et à condition de ne pas aller à l'encontre des différentes branches du droit à l'information (intérêt public, liberté d'expression…). **Il faut donc bien réfléchir car il est plus facile de ne pas mettre en ligne un contenu que de le faire retirer plus tard.**



3. Les lois renforçant le protection des données personnelles dans le cyberespace

La loi du 7 octobre 2016 pour une République numérique

(Legifrance)

Cette loi a devancé certains aspects du RGPD applicable au 25 mai 2018.

Le droit à l'oubli numérique pour les mineurs

Les mineurs bénéficient d'un « droit à l'oubli » (article 63) et cela concerne en particulier les cas de cyberharcèlement sur les réseaux sociaux. **Au moment de la collecte des données, ils peuvent obtenir auprès des plateformes en ligne l'effacement des données problématiques « dans les meilleurs délais ».** En l'absence de réponse ou en cas de réponse négative de la plateforme dans un délai d'un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de 3 semaines pour y répondre. Sur demande directe des enfants, les plateformes de vidéos doivent retirer leurs vidéos. Le consentement des parents n'est pas exigé.

Le droit à la mort numérique

Après un décès, tous les comptes et données du défunt restent disponibles sur internet (immortalité numérique). Actuellement, en l'absence d'une demande de la part des héritiers ou des proches, le profil de la personne décédée continue d'exister. Ce sont aux réseaux sociaux d'organiser le devenir de ces profils.

La loi Barrot modifie la loi du 6 janvier 1978 (article 85) et **veut que chacun puisse de son vivant exprimer ses volontés sur la conservation et la communication de ses données après son décès ou demander leur effacement**. Ce droit peut s'exercer depuis le 1er juin 2019, en vertu du décret du 29 mai 2019 d'application de la loi "Informatique et libertés".

Le droit au respect de la vie privée fait que ces données étant, par nature, strictement personnelles, les membres de la famille ou amis ne peuvent y avoir accès. Ainsi, la loi apporte de la souplesse et autorise les héritiers à disposer d'un droit d'accès et un droit de suppression aux données *post-mortem* du défunt.

La loi du 19 octobre 2020 encadrant l'exploitation commerciale de l'image d'enfants de moins de 16 ans sur les plateformes de vidéos en ligne

(Légifrance)

Le « *sharenting* » ou surpartage parental désigne la publication de contenus concernant des enfants, par leurs propres parents, sur des plateformes en ligne. En quête de profit et de popularité, ces parents mettent en scène leurs enfants contre des contrats publicitaires, des placements de produits, une rémunération au nombre de vues. Cette pratique s'est massifiée ces dernières années et présente des risques cybermalveillants : les images et vidéos d'enfants peuvent être détournées par des réseaux pédo-criminels ou encore peuvent donner lieu à du chantage ou du cyberharcèlement.

La loi du 19 octobre 2020, entrée en vigueur en avril 2021, vise à encadrer le travail des enfants influenceurs de moins de 16 ans, sur les plateformes de vidéos type *volg*s ou Youtube. **Elle instaure un double contrôle réglementaire : d'une part, elle oblige les parents à respecter la vie privée de leur enfant, y compris son droit à l'image, au titre de leurs prérogatives liées à l'exercice de l'autorité parentale et d'autre part elle enjoint les plateformes en ligne à adopter des chartes de bonnes conduite**.

Le règlement sur les services numériques du 19 octobre 2022 (plus communément appelé le DSA (en anglais : *Digital Services Act*)

(Union européenne)

Ce qui est illégal hors ligne doit aussi l'être en ligne : voici le principe de ce règlement européen.

Il vise à permettre plus de transparence impose de nouvelles règles à respecter et de nouvelles mesures à mettre en place pour lutter contre les contenus illicites et désinformation en ligne, interdire la publicité ciblée envers les mineurs, endiguer le cyberharcèlement, favoriser les services

numériques innovants, préserver les droits fondamentaux (liberté d'expression et d'information, principe de non-discrimination, respect du niveau élevé de protection des consommateurs..).

L'application du DSA s'est faite en deux vagues :

- Depuis le 25 août 2023, le DSA doit être respecté par 'géants du web' comme Aliexpress, Amazon Store, AppStore, Facebook, Google Maps, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X, Twitch YouTube, etc.
  * *Cette liste a été complétée en décembre de la même année par trois sites pornographiques.*

- Dès le 17 février 2024, le règlement s'applique aux fournisseurs d'accès à Internet, *marketplaces*, *cloud,* réseaux sociaux, plateformes de voyage et d'hébergement en ligne, etc.

La Commission européenne a franchi une étape majeure dans la protection des mineurs en ligne. Elle a annoncé, le 15 avril 2026, lancement prochain d'une nouvelle application de vérification d'âge et qui sera bientôt accessible à tous les citoyens de l'UE. Objectif : empêcher les enfants d'être exposés à des contenus nuisibles, à des jeux d'argent ou à des contenus pornographiques.

La France fait partie des sept pays qui ont testé l'application européenne en profondeur et l'intégreront cette année à leurs portefeuilles numériques nationaux.

Ce nouvel outil vient compléter la stricte application du Règlement sur les services numériques.

La Loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne

(Légifrance)

Une loi qui définit les caractéristiques des réseaux sociaux

L'exposition abusive à Internet et aux réseaux sociaux des plus jeunes peut avoir plusieurs conséquences : addiction aux écrans, problèmes de sommeil, risque de cyberharcèlement, de désinformation, d'exposition à la pornographie... Devant ces risques, le projet de loi Sécuriser et réguler l'espace numérique (SREN) viendrait compléter la loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique (LCEN) en donnant une définition de ce qu'est un réseau social (Wikipédia et les répertoires éducatifs et scientifiques à but non lucratif ont été exclus des nouvelles mesures sur la 'majorité numérique').

Les réseaux sociaux numériques partagent trois traits communs :

- la mobilisation des données personnelles afin de créer des « profils »
- la création d'un espace personnel paramétré de présentation et de représentation de l'utilisateur
- la mise à disposition d'outils d'interaction et de partage entre les contacts

De nouvelles obligations pour les réseaux sociaux

La loi oblige les plateformes en ligne telles que Snapchat, TikTok, Instagram, à respecter certaines obligations :

- refuser l'inscription des mineurs de moins de 15 ans, sauf si un des parents a donné son accord
- permettre aux parents de demander la suspension du compte de leur enfant de moins de 15 ans
- informer, lors de l'inscription, des conditions d'utilisation de leurs données personnelles
- informer des risques liés aux usages numériques et des moyens de les prévenir
- activer, lors de l'inscription d'un mineur, un dispositif de contrôle du temps passé en ligne sur la plateforme

La « majorité numérique à 15 ans » (l'âge pour s'inscrire seul sur les réseaux sociaux)

Actuellement, la collecte de données personnelles sur des jeunes de moins de 13 ans n'est pas autorisée. Au sens du RGPD, les réseaux sociaux sont donc interdits aux enfants de moins de 13 ans. Pour les 13-14 ans le consentement des parents, en plus de celui du mineur, est requis.

La loi instaure la majorité numérique à 15 ans : autrement dit, les mineurs devraient avoir au moins 15 ans pour pouvoir s'inscrire seul (sans autorisation de leurs parents) sur les réseaux sociaux. Pour vérifier l'âge de leurs utilisateurs et l'autorisation parentale, les plateformes en ligne ont l'obligation de mettre en place une solution technique, conforme à un référentiel élaboré par l'ARCOM après consultation de la CNIL.

La loi impose également aux réseaux sociaux des contraintes afin de mieux prévenir et poursuivre le cyberharcèlement.

▶ Le gouvernement a réuni un groupe d'experts pour que soit rédigé un rapport sur la santé des enfants surexposés en ligne *Enfants et écrans : à la recherche du temps perdu*. Ce rapport sera remis au Parlement en avril 2024.

La loi du 19 février 2024 visant à garantir le respect du droit à l'image des mineurs

(legifrance)

Tout ce qui est publié en ligne peut avoir des répercussions sur le futur d'un mineur ou sur sa réputation, c'est pourquoi chaque publication doit faire l'objet d'une attention accrue, *a fortiori* en raison des capacités évolutives de l'intelligence artificielle.

La loi adoptée à l'unanimité en 2024 est une réponse aux potentielles dérives. Elle vise plus largement à rappeler que **les parents ne disposent pas d'un droit absolu sur l'image de leurs enfants et elle introduit la notion de vie privée de l'enfant dans la définition de l'autorité parentale du code civil.** En d'autres mots, en matière de droit à l'image, « les enfants ne sont pas des sous-citoyens » ; leur avis doit être pris en compte.

La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique

(legifrance)

« *Filtre anti-arnaque, blocage rapide des sites pornographiques accessibles aux mineurs, peine de bannissement des réseaux sociaux pour les cyber-harceleurs… Voici quelques-unes des mesures de loi dite SREN pour mieux réguler l'espace numérique et protéger les internautes, notamment les plus jeunes*. »

La loi confie, entre autres, à l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) le soin d'établir un référentiel fixant les exigences techniques minimales auxquelles devront se conformer les systèmes de vérification d'âge des sites pornographiques, sous peine de lourdes amendes.

Résolution européenne du 26 novembre 2025 proposant de fixer à 16 ans l'âge minimum d'accès aux réseaux sociaux

Au sein de l'Union européenne, les États restent divisés sur ce sujet, même si l'idée progresse nettement. Elle a franchi une étape symbolique le 26 novembre 2025, lorsque le Parlement européen a adopté une résolution (sans portée obligatoire) proposant de fixer à 16 ans l'âge minimum d'accès aux réseaux sociaux, aux plateformes de partage de vidéos et aux compagnons d'IA, tout en autorisant les 13-16 ans à y accéder avec l'accord de leurs parents.

La France est le premier pays européen à avoir instauré la « majorité numérique » (âge minimum pour accéder aux réseaux sociaux). Alors qu'elle s'apprête à limiter l'accès aux réseaux sociaux pour les moins de 15 ans et que plusieurs pays engagent à leur tour des réformes pour mieux protéger les mineurs, le Conseil de l'IA et du numérique (CIANum) publie une note qui analyse les dispositifs en vigueur et avance des pistes pour les renforcer : *Protection des mineurs en ligne par le contrôle de l'âge : comment aller plus loin ?* (CIANum, mars 2026).

Proposition de loi du 31 mars 2026 visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux

(Sénat)

Le 31 mars 2026, le Sénat a adopté, avec modifications, la proposition de loi en première lecture. Elle veut encadrer plus strictement l'accès des mineurs aux réseaux sociaux en interdisant certains services aux moins de 15 ans jugés dangereux, en conditionnant l'accès aux autres à un accord parental explicite et en imposant aux plateformes des obligations techniques de vérification de l'âge et de protection renforcée des jeunes.

Le texte a été élaboré dans la continuité du règlement européen sur les services numériques (DSA) de 2022, de la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite "SREN" et des lignes directrices de la Commission européenne sur la protection des mineurs en ligne, publiées en juillet 2025.


1
2016
LA LOI DU 7 OCTOBRE 2016 POUR UNE RÉPUBLIQUE NUMÉRIQUE
• LE DROIT À L'OUBLI NUMÉRIQUE POUR LES MINEURS
• LE DROIT À LA MORT NUMÉRIQUE
2
2020
LA LOI DU 19 OCTOBRE 2020 ENCADRANT L'EXPLOITATION COMMERCIALE DE L'IMAGE D'ENFANTS DE MOINS DE 16 ANS SUR LES PLATEFORMES DE VIDÉOS EN LIGNE
3
2022
LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES DU 19 OCTOBRE 2022 (DSA)
• NOUVELLES OBLIGATIONS AUX GRANDES PLATEFORMES EN LIGNE POUR QU'ELLES RETIRENT PLUS EFFICACEMENT LES CONTENUS ILLÉGAUX ET SOIENT PLUS TRANSPARENTES
Ce qui est illégal hors ligne doit aussi l'être en ligne
4
2023
LA LOI DU 7 JUILLET 2023 VISANT À INSTAURER UNE MAJORITÉ NUMÉRIQUE ET À LUTTER CONTRE LA HAINE EN LIGNE
• CONTRAINTES RENFORCÉES POUR LES RÉSEAUX SOCIAUX
• ACCÈS AUTORISÉ AUX RÉSEAUX SOCIAUX À PARTIR DE 15 ANS
5
2024
LA LOI DU 19 FÉVRIER 2024 VISANT À GARANTIR LE RESPECT DU DROIT À L'IMAGE DES MINEURS
• INTRODUCTION DE LA NOTION DE VIE PRIVÉE DE L'ENFANT DANS LA DÉFINITION DE L'AUTORITÉ PARENTALE
« les enfants ne sont pas des sous-citoyens »
6
2024
LA LOI DU 21 MAI 2024 (LOI SREN) VISANT À SÉCURISER ET À RÉGULER L'ESPACE NUMÉRIQUE
• PROTECTION DES ENFANTS CONTRE LES CONTENUS EN LIGNE PORNOGRAPHIQUES
7
2026
PROPOSITION DE LOI DU 31 MARS 2026 VISANT À PROTÉGER LES MINEURS DES RISQUES AUXQUELS LES EXPOSE L'UTILISATION DES RÉSEAUX SOCIAUX
• INTERDICTION DE CERTAINS SERVICES AUX MOINS DE 15 ANS JUGÉS DANGEREUX
• ACCORD PARENTAL OBLIGATOIRE
• OBLIGATIONS TECHNIQUES DE VÉRIFICATION DE L'ÂGE ET DE PROTECTION RENFORCÉE POUR LES GRANDES PLATEFORMES

n (DRANE)

4. Quelques études de cas spécifiques au milieu scolaire

La vidéoprotection ou vidéosurveillance

Seule une nécessité de sécurité exceptionnelle en raison d'actes de malveillance répétés et d'une implantation dans un lieu particulièrement exposé à des risques d'agression, de vol ou de trafic de stupéfiants, justifie l'installation d'un système de vidéosurveillance dans un établissement scolaire.

Pour installer un dispositif de surveillance à partir de caméras enregistrant et transmettant des images prises aux entrées/sorties ou aux abords des collèges et lycées, **les chefs d'établissement doivent obtenir une délibération du conseil d'administration ainsi qu'une demande préalable d'autorisation auprès du préfet du département**. L'autorisation, s'il y a lieu, relève du droit au respect de la vie privée et est délivrée pour une durée de 5 ans renouvelable et la durée de leur conservation ne peut excéder un mois, sauf enquête pénale.

En ce qui concerne l'intérieur de l'enceinte scolaire, l'autorisation relève de la loi informatique et libertés, les EPLE n'étant pas considérés comme des lieux ouverts au public. Ni l'autorisation préfectorale ni la demande préalable auprès de la CNIL ne sont requises. Deux conditions doivent être remplies : les images ont vocation à être enregistrées et conservées et non pas seulement visionnées ; les agents responsables du traitement des images doivent être clairement identifiés. Les personnels, élèves, parents et toute autre personne concernée doivent être informés de la finalité du système et des conditions de traitement des images (durée de conservation, sécurisation des données…).

Dans tous les cas, les caméras ne doivent pas être intrusives et doivent être complémentaires à d'autres mesures de sécurité. Ainsi, des caméras de sécurité ne peuvent être installées qu'aux entrées et sorties des établissements scolaires et dans les espaces de circulation (foyer, cantine, CDI, cour de récréation, préau et salle de classe sont exclus).

La photographie scolaire

(Bulletin officiel)

La photographie est régie par le BO n°24 du 12 juin 2003 qui précise que :

- l'autorisation des titulaires de l'autorité parentale est obligatoire (cette autorisation ne vaut pas engagement d'achat)
- la diffusion électronique de ces photos d'élèves est soumise à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Par ailleurs, le droit à l'image impose de demander une autorisation pour pouvoir afficher les photos d'un voyage ou d'une sortie dans un média scolaire ou encore dans le hall de l'établissement, *a fortiori* lors de journées portes ouvertes.

Le trombinoscope scolaire

La création d'un trombinoscope de classe suppose la création d'un fichier de données personnelles (la photo, le nom, le prénom, la classe permettent d'identifier l'élève). Il faut donc obtenir, des élèves majeurs ou des responsables légaux pour les élèves mineurs, une autorisation écrite pour les prises de vue et pour la diffusion. Ces photos individuelles doivent montrer l'élève en situation scolaire.

Ni les photos d'identité ni les portraits sur fond peint ne peuvent pas être proposées pour ne pas concurrencer les photographes professionnels locaux.

L'utilisation et la diffusion du trombinoscope doivent faire l'objet d'une déclaration préalable à la CNIL et la finalité du trombinoscope devra être précisée (l'établissement devra prouver la pertinence des données collectées par rapport aux objectifs du trombinoscope).

Dès lors que les élèves sont identifiables, il faut s'interdire la mise en ligne de toute photo (trombinoscope, photo de classe, photos prises dans le cadre d'activités d'enseignement) sur un site accessible au grand public. Il faut préférer les réseaux internes sécurisés, comme par exemple un ENT avec accès par authentification personnalisée ou un site web d'école hébergé sur un serveur du rectorat.

Quel que soit le support de diffusion envisagé (photos numériques, vidéos, tirages papiers), il ne doit pas y avoir d'archivage. Tous les supports doivent être détruits après leur utilisation.

Il faut enfin savoir que le droit de retrait permet aux parents de demander à tout moment à retirer certaines photos qui ont été publiées de leur enfant même s'ils ont signé une autorisation en début d'année.

Le livret scolaire unique numérisé (LSUN)

Les livrets personnels de compétences de l'école élémentaire et du collège ont évolué pour ne plus former plus qu'un livret scolaire commun : le Livret Scolaire Unique Numérisé (LSUN). C'est un outil numérique de suivi pour la scolarité obligatoire du CP à la troisième.

Ce livret, accessible en ligne, contient les notes des élèves, les bilans périodiques et de fin de cycle, les appréciations des professeurs et le suivi de l'acquis des compétences. Ces données constituent des données personnelles. Elles sont conservées pendant 4 ans (3 ans de durée d'un cycle scolaire à laquelle on ajoute une année.

Le LSUN est obligatoire (arrêté du 31 décembre 2015) en revanche le téléservice associé est facultatif ; une version papier est transmise aux parents qui ne souhaitent pas utiliser le téléservice.

La gestion des inscriptions et abonnements à des 'ressources numériques éducatives'

Les ressources numériques éducatives (RNE) désignent tout contenu, service associé outil-services au format numérique, présentant un bénéfice pour des activités d'enseignement-apprentissage et en lien direct avec les programmes scolaires. Elles s'adressent aux enseignants et aux élèves, pour un

usage en classe et/ou hors la classe. Elles répondent aux orientations pédagogiques ainsi qu'aux standards juridiques et techniques du Ministère.

- Les RNE non conventionnées

L'inscription d'élèves à des services numériques non conventionnés avec le Ministère n'est pas recommandée (manuels numériques hors ENT, Doodle, outils Google Docs…) en raison d'une différence de législation du droit américain, d'un éventuel changement unilatéral des conditions d'utilisation, de la cession de certaines données ou de la violation du droit d'auteur. S'il veut, malgré la contre-indication, inscrire ses élèves à des outils hors du cadre officiel, il doit obtenir l'accord -des parents et de la CNIL- pour chaque ressource utilisée. Un accord global n'est pas valable. **S'il abonne un établissement ou des élèves hors du champ conventionnel et sans prévenir son institution, l'enseignant est susceptible d'une plainte devant un tribunal.**

- Les RNE relevant d'une politique ministérielle

L'accord parental n'est en revanche pas nécessaire pour l'inscription à l'ENT car celui-ci relève d'une politique ministérielle et intègre les élèves à partir d'une base de données de l'Éducation nationale avec un droit d'opposition nul. Le développement de l'usage des ENT répond en grande partie à des soucis légaux. S'il reste encore incomplet, il présente l'avantage de mobiliser différents acteurs dans un cadre juridique sécurisé et simplifié (échange de fichiers avec les élèves dans un but pédagogique, service de messagerie sécurisé, accès à des ressources via le Médiacentre…).

Il convient de privilégier l'abonnement à des ressources institutionnelles ou soutenues par le MENJ (ex : le dispositif ÉduUp) ou encore des ressources fournies par des partenaires associés GAR/Médiacentre car elles répondent aux normes du RGPD.

Les blogs pédagogiques d'enseignants

Un blog pédagogique est un site internet. Si les élèves ou leurs parents sont autorisés à intervenir sur le blog, leurs données de connexion devront faire l'objet d'une inscription sur le registre de l'EPLE qui le met en œuvre ou sur le registre des activités de traitement tenu par les DSDEN ou les rectorats d'académie.

Par ailleurs, l'ouverture d'un blog à des fins pédagogiques nécessite l'avis préalable du conseil d'administration qui pose les principes de choix des manuels scolaires, des logiciels et des outils pédagogiques.

La création d'une adresse e-mail pour un élève

Aujourd'hui, aucune réglementation ne consacre de majorité numérique globale à 15 ans.

En principe, conformément à l'article 45 de la Loi Informatique et Libertés et sous réserve de l'appréciation souveraine des tribunaux, les titulaires de l'autorité parentale doivent donner leur accord conjointement avec celui de leur enfant si celui-ci a moins de 15 ans.

Les mineurs de plus de 15 ans, eux, sont juridiquement considérés comme capables de conclure des contrats ayant pour objet le traitement de leurs données dans le cadre de services en ligne, telle qu'une messagerie électronique, si et seulement si :

- ces services sont adaptés aux publics mineurs qu'ils accueillent ;
- ces traitements respectent strictement les règles de protection des données personnelles telles que fixées par le RGPD et la Loi Informatique et Libertés (minimisation des données collectées, pour une finalité bien déterminée, une durée limitée et de manière sécurisée…) ;
- le mineur est informé de façon claire et adaptée des conditions d'utilisation de ses données et de ses droits informatiques et libertés, afin qu'il puisse comprendre le sens et la portée de son engagement ;
- les parents disposent d'une voie de recours pour demander la suppression du compte de leur enfant s'ils l'estiment nécessaire afin de protéger son intérêt supérieur.

Les réseaux sociaux comme outils pédagogiques

Les enseignants mobilisent parfois les réseaux sociaux pour des projets pédagogiques parce que ce sont des outils du quotidien des élèves et parce qu'ils proposent des espaces collaboratifs intuitifs et ergonomiques. Or, ces réseaux sociaux sont mis à disposition par d'opérateurs privés et conçus pour des usages privés. L'utilisation des réseaux sociaux à des fins pédagogiques pose donc la question de la responsabilité de l'enseignant et des risques qu'il encourt en matière de données personnelles: pour créer un compte. Doit-il utiliser un pseudonyme ? Doit-il utiliser son adresse courriel ou celle de l'ENT ? Quelle est sa marge de manœuvre au regard de la modération des comptes « classes » ?

L'exploitation des réseaux sociaux dans une intention pédagogique, nécessite, comme tout autre service numérique en ligne, que les conditions générales d'utilisation du service fassent l'objet d'un contrôle par les services du ministère ou du rectorat d'académie. Ils doivent présenter des garanties suffisantes au niveau de la sécurité des données. Les opérateurs de ces réseaux sociaux devraient normalement accepter de faire un traitement des données des élèves seulement sur demande ou instruction du responsable de traitement (chef d'établissement ou IA-DASEN). En dehors d'un tel cadre, qui implique donc des CGU spécifiques négociées par les services du ministère, dites « CGU éducation », il faut considérer que les conditions de sécurité adéquates en matière de protection des données personnelles ne sont pas réunies. **Par conséquent, il est fortement recommandé aux enseignants de s'abstenir d'utiliser les réseaux sociaux avec des élèves de moins de 13 ans (l'accès étant interdit par le RGPD avant cet âge).**

Les enregistrements sonores des élèves comme activités d'apprentissage

Il est de plus en plus fréquent d'enregistrer les voix d'élèves pour des raisons pédagogiques (cela diffère des activités de communication qui consistent à valoriser le travail des élèves), par exemple :

- Tout au long de l'année, à la demande de l'enseignant de langue, les élèves utilisent l'enregistreur de l'ENT pour enregistrer leur voix puis échanger ces enregistrements avec l'enseignant en question (l'échange se fait donc à l'attention exclusive de l'enseignant sur le serveur de l'établissement).

- Dans le cadre d'un projet EMI, les élèves du Club WebTV/Webradio, sous la houlette d'un binôme d'enseignants, enregistrent des JT ou des podcasts qui sont hébergés sur PodEduc et seront publiées sur le blog de l'établissement.
- Un professeur de français conseille à ses élèves de s'entrainer à l'oral pour préparer une épreuve, de s'enregistrer à l'aide de leur smartphone et de lui transmettre ces enregistrements via la messagerie ENT.

Dans tous les cas, **la demande d'autorisation doit se faire avant les enregistrements et ce, même si aucune diffusion n'est prévue.**

Rentrée scolaire et affichage des listes des classes

La publication des listes scolaires est une pratique usuelle et utile. Néanmoins, un affichage l'extérieur de l'établissement peut engendrer, dans certains cas spécifiques, des risques pour la vie privée des élèves concernés. La CNIL recommande 3 bonnes pratiques à adopter :

- Limiter le nombre de personnes ayant accès à l'affectation de l'élève dans sa classe
- Informer les parents en amont de l'affichage
- N'afficher que les informations strictement nécessaires sur la liste scolaire

Cinq réflexes à adopter pour protéger les élèves

1. Toujours privilégier ENT, GAR et ressources institutionnelles
2. Ne pas créer de comptes élèves sur des services non conventionnés sans validation du chef d'établissement
3. Ne jamais publier de photo ou de vidéo d'élève identifiable sur un site Intrernet public ; utiliser des espaces sécurisés ou flouter.
4. Limiter la collecte de données au strict nécessaire et définir une durée de conservation.
5. En cas de doute, demander conseil (RUPN, chef, DPD via la voie académique).

5. Récapitulatif sur les droits et les devoirs

Chacun bénéficie de droits forts liés à sa personne (vie privée, image, voix, données personnelles) et que l'école doit les respecter strictement.

Droits et devoirs des enseignants

Les enseignants ont le droit d'utiliser des outils et ressources numériques pour enseigner à condition de respecter le droit à l'image et à la voix des élèves : toute captation (photo, vidéo, enregistrement sonore) suppose une autorisation écrite, datée et explicite des représentants légaux (ou de l'élève majeur), même sans diffusion publique, avec description précise de l'usage prévu.

Ils doivent protéger les données personnelles qu'ils manipulent (notes, productions d'élèves, données de connexion, etc.), ne collecter que ce qui est utile au projet pédagogique, et utiliser en priorité les services institutionnels (ENT, ressources conventionnées / GAR) qui répondent au RGPD. L'inscription d'élèves sur des

services non conventionnés (plateformes privées, outils collaboratifs grand public, réseaux sociaux) n'est pas recommandée ; si un enseignant passe outre, il doit obtenir un accord spécifique des parents pour chaque service, et il engage sa responsabilité en cas de problème (plainte possible devant un tribunal).

Les enseignants ont aussi le droit au respect de leur propre image et de leur voix : les élèves ne peuvent pas les filmer ou les enregistrer ni diffuser ces contenus sans leur accord.

Lorsqu'ils utilisent des blogs, des enregistrements audio, des vidéos, des trombinoscopes ou des listes de classe, ils doivent limiter les données publiées, privilégier les espaces sécurisés (ENT, hébergement rectoral) et respecter les durées de conservation (pas d'archivage illimité, possibilité de retrait sur demande des familles).

Droits et devoirs des chefs d'établissement

Le chef d'établissement (ou l'IA-DASEN pour le 1er degré) est « responsable de traitement » pour de nombreuses données scolaires : il doit garantir la conformité au RGPD, tenir un registre des traitements, informer le Délégué à la protection des données (DPD) en cas de violation et dialoguer avec la CNIL si nécessaire.

Il lui appartient de cadrer l'usage des outils numériques (ENT, ressources numériques éducatives, blogs, messageries, vidéosurveillance) via les instances de l'EPLE, en veillant au respect des textes (Loi Informatique et Libertés, RGPD, lois récentes sur les mineurs en ligne, SREN, etc.).

Pour la vidéosurveillance, il ne peut la mettre en place qu'en cas de nécessité de sécurité exceptionnelle, avec délibération du conseil d'administration et, pour les abords, autorisation préfectorale ; les caméras doivent rester non intrusives, limitées aux zones de circulation, avec information claire des usagers et durée de conservation des images encadrée.

Il doit encadrer la photographie scolaire, les trombinoscopes, le Livret scolaire unique numérisé (LSUN) et la gestion des inscriptions à des ressources numériques (choix des services, respect des règles de diffusion et de conservation, information des familles).

Enfin, il doit privilégier les ressources institutionnelles ou partenaires du GAR/Médiacentre, et s'assurer que tout projet impliquant des réseaux sociaux ou des services privés a été examiné au regard de la protection des données et du statut des mineurs (interdiction / autorisation parentale selon l'âge).

Le numérique à l'école n'est pas « hors droit » : enseignants et chefs d'établissement partagent un droit à la protection de leurs propres données, mais aussi un devoir de vigilance et de conformité lorsqu'ils conçoivent des activités, choisissent des outils ou diffusent des contenus impliquant les élèves.

CONCLUSION

La protection des données n'est pas seulement une question juridique ou technique.

Les données personnelles des élèves, tout comme celles des enseignants, ne sont pas libres de droit ! Elles leur appartiennent exclusivement et inaliénablement.

Le traitement licite et éthique des données est un facteur de confiance.
Le numérique facilite et multiplie les occasions de copier et diffuser des voix et des images d'individus mais il faut garder en tête que toutes ces données sont des objets juridiques protégés à plusieurs titres. En effet, parallèlement au droit civil et pénal, le droit de la protection des données à caractère personnel a aussi pleinement vocation à s'appliquer via le RGPD.

Toute personne qui souhaite exploiter des données est tenue de se conformer aux règles contractuelles et celles régissant les traitements de données personnelles. En plaçant les données personnelles et le respect de la vie privée au cœur de ses pratiques, l'école devient un lieu clé de bien-être numérique pour les élèves comme pour les adultes. Elle offre un cadre sécurisé où les usages du numérique sont pensés pour limiter les risques (surexposition, traçage excessif, atteintes à l'image) et préserver l'équilibre entre innovation pédagogique et protection de chacun.

Ce bien-être numérique repose sur des choix d'outils responsables, une collecte de données strictement nécessaire et des projets qui respectent l'intégrité physique et morale des personnes. En privilégiant les services institutionnels, en encadrant les captations d'images et de voix et en sensibilisant les communautés éducatives, l'école construit un environnement où les élèves peuvent apprendre, créer et collaborer sans être transformés en simples « profils » exploités par des plateformes.

Enfin, l'école a la mission d'apprendre aux élèves à prendre soin d'eux dans le monde numérique : comprendre leurs droits, maîtriser leurs traces, développer un rapport apaisé aux écrans et aux réseaux sociaux. En articulant éducation aux médias, éducation à la citoyenneté et éthique du numérique, elle contribue à former des citoyens capables de concilier usages numériques, respect des autres et santé mentale.

Traitement des données personnelles

QUI FAIT QUOI dans l'établissement ?

CHEF D'ÉTABLISSEMENT

- [ ] Valide les traitements principaux (ENT, vidéosurveillance, blogs pédagogiques, RNE, LSUN, etc.).
- [ ] S'assure que le registre des traitements est tenu à jour, avec l'appui du délégué à la protection des données (DPD).
- [ ] Organiser l'information à l'attention des usagers (affichages, mentions d'information, réunions parents, règlement intérieur, charte informatique...).

RÉFÉRENT RGPD/ ADMINISTRATIF

(secrétaire, gestionnaire, éventuellement RUPN en appui)

- [ ] Tient au contribue au registre des activités de traitement (modèle type).
- [ ] Centralise les demande d'exercice de droit (accès, rectification, effacement, opposition) et les transmet au DPD.
- [ ] Suit les conventions ou contrats des services numériques utilisés (durée, finalité, hébergement).

RÉFÉRENT NUMÉRIQUE (ERUN OU RUPN)

- [ ] Conseille les collègues sur le choix d'outils conformes (ENT, GAR, ressources numériques conventionnées...)
- [ ] Alerte sur les risques liés aux services non conventionnés et accompagne la recherche d'alternatives

ENSEIGNANTS

- [ ] Verifient la conformité de leurs projets (captattions audio et vidéo, utilisation pédagogique des réseaux sociaux, RNE....)
- [ ] Font remontrer au chef d'établissement ou au RUPN tout nouveau service numérique qu'ils souhaitent utiliser

Région académique Bourgogne Franche-Comté, Délégation régionale académique au numérique pour l'éducation (DRANE)

Check list

LES QUESTIONS À SE POSER en matière de données

AVANT DE LANCER UNE NOUVELLE RESSOURCES NUMÉRIQUES AVEC DES ÉLÈVES

- [ ] Ai-je vérifié s'il existe une version libre ou institutionnelle ?
- [ ] Quelles données sont collectées ? Sont-elles minimales et justifiées ?
- [ ] Ai-je une base juridique claire (mission d'enseignement, intérêt public, consentement nécessaire...) ?
- [ ] L'information à l'attention des familles est-elle prévue ?

AVANT DE FILMER / PHOTOGRAPHIER / ENREGISTRER

- [ ] Les autorisations sont-elles écrite, datées et signées par projet (et non globale à l'année) ?
- [ ] L'utilisation est-elle précisée ? (durée, périmètre de diffusion°
- [ ] Le stockage est-il sécurisé et à durée déterminée ? Une destruction est-elle prévue à la fin du projet ?

EN CAS D'INCIDENT OU FUITE DE DONNÉES

- [ ] Qui prévenir au sein de l'établissement (chef d'établissement, référent RGPD, RUPN, ERUN...)
- [ ] Quel est le délai pour informer le DPD académqiue ? Et quels sont les éléments à transmettre (type de données, nombre de personnes, mesures prises...) ?

ENSEIGNANTS

- [ ] Verifient la conformité de leurs projets (captattions audio et vidéo, utilisation pédagogique des réseaux sociaux, RNE....)
- [ ] Font remontrer au chef d'établissement ou au RUPN tout nouveau service numérique qu'ils souhaitent utiliser

Région académique Bourgogne Franche-Comté, Délégation régionale académique au numérique pour l'éducation (DRANE)

SOURCES

RGPD : Quels sont les principes de protection des données personnelles (Emmanuel Pernot-Leplay)
CNIL - Commission Nationale de l'Informatique et des Libertés
La protection de la vie privée face aux médias (Sénat)
Le livret scolaire unique du CP à la troisième (ÉducationGouvFr, 2020)
Droit au respect de la vie privée et familiale (Conseil de l'Europe)
Quelques notions juridiques liées à l'utilisation pédagogiques de ressources numériques (Académie d'Amiens, 2026)
Les données à caractère personnel – Comprendre et appliquer les nouvelles réglementations dans les établissements scolaires (Réseau Canopé, 2018)
Déontologie et utilisation des réseaux sociaux numériques dans l'éducation nationale - Avis n° 2021-002 du 8 juillet 2021 (Collège de déontologie de l'éducation nationale, 2021)
Les enjeux juridiques contemporains du numérique et de l'éducation : état des lieux (IH2EF, 2023)
Rentrée scolaire et affichage des listes des classes : quelles sont les bonnes pratiques (CNIL, 2025)
Le règlement sur les services numériques (DSA) en bref (Union européenne, 2026)
Numérique : le règlement sur les services numériques entre en vigueur (Ministère de l'économie2024)
Le "Digital Services Act" : mode d'emploi (Commission européenne, 2025)
La majorité numérique en 6 questions (Vie publique, 2026)
L'application européenne pour vérifier l'âge des utilisateurs est prête (toutel'europe.eu)
Une application européenne de vérification de l'âge pour assurer la sécurité des enfants en ligne (Commission européenne)
Protection des mineurs en ligne par le contrôle de l'âge : comment aller plus loin ? (CIANum, mars 2026).

Dernière mise à jour : 22.04.2026
Contact : lea.blanquer@region-academique-bourgogne-franche-comte.fr