

Conduite à tenir dans le choix des outils numériques

Dans la crise que nous traversons actuellement, il est conseillé de **privilégier des outils numériques déjà à disposition dans l'établissement, ils sont maintenant opérationnels (ENT premier et second degré (ATRIUM, ENT 04, One, Beneylu, ...), Chamillo, Pronote, classe virtuelle du CNED) et permettent d'assurer la continuité pédagogique.**

Nous constatons une explosion de nouveaux outils pour faire face aux difficultés de connexion, mais ils ne sont souvent pas maîtrisés et posent d'importants problèmes de diffusion de données personnelles (non-conformité au Règlement Général à la Protection des Données (RGPD)).

Il est donc impératif de revenir à des pratiques raisonnées et encadrées.

1. Risques spécifiques à évaluer

Des risques spécifiques existent dans l'utilisation de certains outils qu'il convient d'évaluer en prenant en compte :

- la nature des informations échangées :
 - données à caractère personnel ;
 - informations de nature confidentielle pour l'établissement (exemple : informations stratégiques).
- la vulnérabilité des utilisateurs (ex : élèves ou enseignants pouvant se retrouver en situation de harcèlement) ;
- l'existence ou non de cadrage réglementaire avec les participants ; l'absence de ce cadre peut avoir des impacts lourds sur la vie des personnes et l'institution (impact juridique, impact en termes d'image ...) ;
- l'exposition de données.

2. Les vulnérabilités

Les vulnérabilités des solutions retenues peuvent provenir :

- d'une impossibilité à identifier les personnes accédant au service ;
- d'un défaut de sécurité de la plateforme - faille de sécurité ;
- d'une récupération des informations par la plateforme elle-même (exemple commercialisation des données à caractère personnel recueillies par la plateforme).

La vigilance est d'autant plus importante que le public est vulnérable.

Le réseau des Délégués à la Protection des Données (DPD) a relevé de nombreux incidents sur des plateformes utilisées en dehors de tout cadre réglementaire (exemple: Discord, Whatsapp, ...).

Il s'interroge aussi quant à l'utilisation de plateformes non maîtrisées (exemple ZOOM pour les conseils de classe) et à la protection apportée aux informations échangées avec les représentants des parents d'élèves ou des élèves délégués dans ce cadre-là.

Focus DISCORD

Discord est une application très utilisée par les élèves pour communiquer entre eux lorsqu'ils pratiquent des jeux en ligne. Elle permet de disposer d'un salon de chat textuel et audio, avec différents canaux de discussion. Nous avons constaté son utilisation à des fins pédagogiques comme outil de classe virtuelle.

En effet sa performance, son ergonomie et son intuitivité ont pu séduire certains enseignants pour communiquer facilement avec les élèves qui disposent déjà d'un compte sur la plateforme.

L'utilisation de cet outil est à proscrire pour les raisons suivantes :

- la solution n'est pas prévue pour être utilisée autrement qu'à titre "personnel", il n'existe pas de lien sous-traitant (Discord) et responsable du traitement (chef d'établissement, DASEN) ;
- le traitement ne peut pas être opéré sur la base d'une mission de service public, mais uniquement sur la base du consentement. Celui-ci doit être libre, ce qui n'est pas le cas quand il y a prescription de l'enseignant pour s'inscrire sur un serveur « classe ». De plus, **une preuve du consentement des représentants légaux des mineurs de moins de 16 ans est indispensable !**
- le modèle économique de cette solution pose question. Avec 250 millions de comptes gratuits et sans publicité, l'entreprise est néanmoins valorisée à 2 milliards de dollars. Les conditions générales d'utilisation (CGU) précisent : « *Divulgarion de données personnelles : Conformément à la section « NOTRE DIVULGATION DE VOS INFORMATIONS » ci-dessus, nous pouvons être amenés à partager vos données personnelles avec des parties tierces. Nous divulguons les catégories de données personnelles mentionnées plus haut à des fins commerciales.* » (Sources : <https://discordapp.com/privacy>)

La société trouve donc son financement dans la commercialisation des données de leurs usagers.

Focus sur ZOOM

Zoom recouvre les principaux cas d'usage de la web conférence, du chat et la réunion en ligne. Zoom permet de créer une salle virtuelle dans laquelle les participants peuvent interagir aussi bien depuis leur ordinateur que depuis leur tablette ou leur smartphone.

L'utilisation nécessite la création d'un compte sur <https://zoom.us/signup> par l'animateur de la réunion qui crée ensuite une réunion et y invite les participants.

Par son ergonomie et sa facilité d'utilisation, ZOOM est en phase de devenir, avec la crise du COVID19, l'application de visioconférence la plus utilisée au monde.

L'utilisation de cet outil est à proscrire pour les raisons suivantes :

- La version gratuite à laquelle ont recours les établissements ne permet pas de bénéficier d'un contrat comme l'impose l'article 28 du RGPD liant le responsable de traitements (chef d'établissement) et le sous-traitant (Zoom). Les CGU de Zoom précisent : « *Zoom Video Communications, Inc. sera le responsable du traitement des données personnelles...* » ;
- Les données sont collectées dès lors qu'il y a interaction avec les services ZOOM et sont stockées aux Etats-Unis ou dans le monde entier, comme le précisent les CGU. **Il s'agit donc d'un transfert de Données à Caractères Personnels hors de l'UE, ce qui est par défaut interdit.**
- « *les données personnelles peuvent être transférées aux États-Unis, à une société affiliée à Zoom dans le monde entier ou à des tiers agissant [au nom de Zoom] aux fins de traitement ou de stockage* ». CGU ;
- soumis aux règlements de l'U.S. Federal Trade Commission « *Zoom peut être forcé de divulguer des données personnelles à la suite de requêtes légales par les autorités publiques et pour répondre aux exigences de la sécurité nationale ou des autorités.* »
- de nombreuses interrogations sur la sécurisation de cet outils sont soulevées.