Colloque de la CEPPLE du 15 au 17 mai 2019 à Paris
Cerner les enjeux éthiques et administratifs de la communication des Eglises sur le WEB

Session 4 : vendredi 17 mai à 9h00

Les Implications du Règlement général sur la protection des données (RGPD) dans la communication des Eglises

Introduction par Daniel Cassou : garantir, sécuriser, responsabiliser : une nouvelle manière de communiquer dans le cadre de la RGPD.

1. Définition de la RGPD

Le 25 mai 2018, le règlement général sur la protection des données (RGPD) est entré en vigueur en Europe. Les grands principes du règlement ont pour vocation d'harmoniser et à renforcer la protection des données personnelles pour l'ensemble des citoyens européens. Il s'applique **à toute activité survenant hors de la sphère privée, y compris donc religieuse ou bénévole.** Ce règlement concerne donc les Eglises comme toutes les organisations amenées à collecter et utiliser des « données personnelles ». Le RGPD va empêcher des abus et permettre d'assurer la protection des données des personnes. Ce règlement est considéré selon l'article 8 comme un droit fondamental pour les citoyens européens.

Définition d'une donnée personnelle

Les données « personnelles » sont par exemple : les nom et prénoms de la personne, son adresse postale, ses numéros de téléphone, adresses mail, coordonnées bancaires, date et lieu de naissance, nationalité, fonction… c'est-à-dire toute information qui permet d'identifier directement ou indirectement la personne.

2. les enjeux du RGPD sont triples : Créer la confiance, sécuriser les données, responsabiliser les acteurs

2.1. **Créer la confiance :** la confiance est le fer de lance de l'humanité. Sans confiance il n'y a pas de collaboration. C'est un point majeur. **Le RGPD n'est pas une menace,** Il peut être une opportunité d'apporter plus de rigueur dans la gestion des fichiers des Eglises, et de fonder leurs relations avec des tiers sur plus de transparence et de confiance.

2.2. **Sécuriser les données**. Tout responsable de traitement des données –qui collecte des données- doit sécuriser ses données. Les ***données personnelles*** doivent être collectées et traitées de manière ***légale, légitime*** (le collecteur a besoin de ces données pour exercer son activité statutaire, et ne les utilisera pour aucune autre finalité), **loyale et *transparente*** (la personne sait très clairement pour qui et pour quoi ses données sont collectées) ; elles doivent ensuite être conservées de manière *sûre* (protection logicielle et physique) et ***exactes*** (une donnée dont on n'est pas sûr doit être détruite).

2.3. Responsabiliser les acteurs et des sous-traitants. Ce règlement met en place une logique de responsabilisation des utilisateurs. Le ***responsable des traitements*** doit être en mesure de *prouver* le respect de ces principes. C'est le délégués à la protection des données (DPO) ou le responsable du système d'information ou informatique.

3. Trois grandes nouveautés par rapport au droit français antérieur[1]

Le RGPD reprend dans les grandes lignes les exigences françaises en matière de « *consentement* », mais il introduit par rapport au droit français trois nouveautés :

- **Les traitements manuels** sont aussi concernés, pas seulement les traitements sur des supports numériques ; un carnet d'adresses au stylo glissé dans un calepin est concerné par le RGPD ; **« consentement »,**
- L'ensemble du RGPD n'est pas centré sur la donnée elle-même, mais sur le traitement, et **surtout sur la *« légitimité »* de ce traitement** ;
- Le RGPD définit une obligation de moyens, mais il inverse la charge de la preuve : ce n'est plus à la victime d'un mauvais traitement de ses données de démontrer la faute du « *responsable de traitement* », mais à ce dernier de démontrer qu'il a pris toutes les mesures adéquates pour l'éviter ; pour cela, il doit tenir à jour une *« **documentation** ».*

4 étapes pour une mise en applications du RGPD

1. **Constituer un registre de vos fichiers**
2. **Faire le tri des données paroissiales et leur stockage** : garder une trace du consentement des personnes (membre de l'association cultuelle, effacer les mail contenant des informations à caractère personnel
3. **Respecter le droit des personnes (consentement, oubli, portabilité)** : autorisation du droit à l'image à enregistrement audio visuel, mailing avec copie à tous avec des adresses visibles, vérifier les mentions légales sur les formulaires de collectes de données, prévoir une procédure pour l'effacement définitif de données)
4. **Sécuriser vos données** : s'assurer que seules les personnes habilitées aux accès aux données, ne jamais placées des données sur des clés USB, de pas stocker de données sur des boites mail.

5. Conclusion

- Faire éventuellement un audit pour repérer les dysfonctionnements ou les points d'améliorations,
- Communiquer auprès des pasteurs et des conseils presbytéraux sur ces enjeux,
- Fournir un guide pratique pour rassurer et mettre en place de nouvelles pratiques.

L'EPUdF pourra mettre à disposition le livret pédagogique qu'elle offrira aux paroisses en septembre 2019

[1] Point de départ : Loi informatique et Liberté du 6/1/1978 qui, notamment, crée la CNIL.