Afterwork du CyberCercle – 23 janvier 2018 – LILLE

COMPTE RENDU

Cybersécurité et collectivités territoriales

avec

Rémy FEVRIER

Président du Pôle 4CN

&

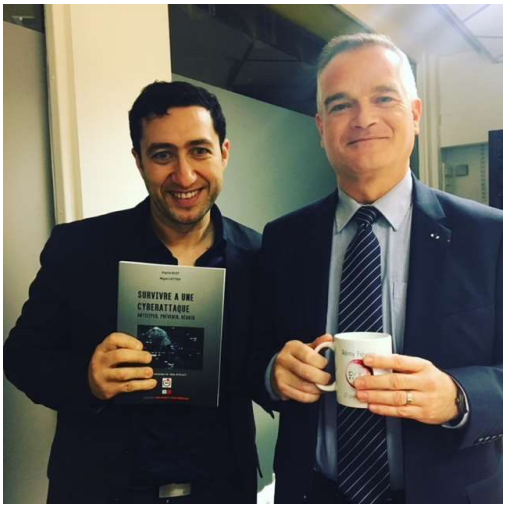
Garance MATHIAS

Avocat à la Cour de Paris

&

Akim OURAL

Adjoint au maire de Lille, Conseiller métropolitain délégué à l'économie numérique



Le CyberCercle travaille depuis plusieurs années avec les collectivités territoriales sur les enjeux de cybersécurité auxquels ces dernières sont confrontées.

Les collectivités territoriales gèrent 17 types de fichiers différents, et à travers ces derniers traitent des données personnelles et sensibles de leurs administrés : état civil, différents services publics... Une collectivité est, de ce fait, une cible de choix et doit donc être protégée. L'un des défis de la « e-démocratie » sera la « e-administration » et la dématérialisation des appels d'offre : dans ce cadre, une collectivité DOIT s'intéresser à la cybersécurité. Mais, pour réussir à instaurer une culture de sécurité numérique, il est nécessaire de donner les clefs aux collectivités pour qu'elles puissent comprendre les enjeux et agir en conséquence.

Dans le cadre des discussions, la question de remettre à plat le Code des collectivités territoriales, en particulier au sujet du recrutement, a été évoquée. Il y a en effet une nécessité de faire évoluer les habitudes et les codes. En matière de cybersécurité, la formation est particulièrement indispensable. La cybersécurité est une chaîne, et une chaîne n'est qu'aussi forte et résistante que le plus faible de ses maillons. La sensibilisation et la formation sont donc deux notions fondamentales qu'il faut appliquer à tous les secteurs.

> ***« La véritable difficulté est de faire de la culture numérique à un public qui n'y est pas sensible. Voilà qui pose de vraies questions. La cybersécurité ne doit plus être vue comme un frein, mais comme un véritable facteur de compétitivité. »***
> **Garance MATHIAS**, *Avocat à la Cour de Paris*

Il y a une énorme différence entre « *utilisation* » et « *maîtrise* » : on ne maîtrise pas obligatoirement un outil quand on l'utilise, a fortiori l'outil numérique. Le risque réside dans l'agir, et il est nécessaire d'accepter le fait suivant : un humain est et sera toujours plus facile à « hacker » qu'un ordinateur. C'est la raison pour laquelle il existe une véritable nécessité de la formation à la cybersécurité pour tous. Il faut travailler à former dès l'école et tout au long de leur cursus les citoyens à la cybersécurité et aux bonnes pratiques. Le numérique évoluant très rapidement, il est nécessaire de mettre en place une formation continue à la cybersécurité, pour tous, tout au long de la vie.
Quels sont les impacts du RGPD pour une collectivité territoriale ? La nomination d'un Délégué à la Protection des Données (DPO), qui pourra être externalisé ou mutualisé ; un travail de mise en conformité est et sera obligatoire ; sensibiliser les acteurs aux enjeux de la protection des données.

> ***« Il faut aider les collectivités sur la cybersécurité, car il ne faut pas se leurrer : nous [les collectivités] sommes mauvais en matière de cybersécurité, et nous avons besoin de travailler avec vous. »***
> **Akim OURAL**, *Adjoint au maire de Lille, Conseiller métropolitain délégué à l'économie numérique*

Les citoyens et leurs données sont au cœur du RGPD, c'est la raison pour laquelle les enjeux de cybersécurité sont si prégnantes pour les collectivités territoriales, qui doivent donc protéger les données qu'elles traitent. Le champ de la cybersécurité est large et les ressources nécessaires sont conséquentes pour certaines collectivités. C'est la raison pour laquelle ce règlement peut effrayer, mais ce travail est nécessaire.

En matière de cybersécurité, il est préférable de parler des territoires plutôt que des collectivités. En effet, c'est avec tout le territoire que les acteurs doivent travailler, pour implanter la cybersécurité partout en France. Il est nécessaire d'impulser une stratégie de territoires, car il ne s'agit pas uniquement des collectivités territoriales, mais aussi de l'ensemble des acteurs présents. De même, il faut sensibiliser au-delà des enjeux relatifs à la réglementation. Il faut aider les territoires et les collectivités à bâtir et mettre en place une véritable stratégie de cybersécurité, et passer outre la problématique des moyens conséquents mais nécessaires, notamment pour les collectivités

modestes. Sans sécurité, il n'y a pas de ville sûre ; sans ville sûre, il n'y aura pas de ville connectée ; et sans ville connectée, il n'y aura jamais de ville intelligente.

« La menace terroriste de demain sera 2.0. Les SCADA sont omniprésents : si la cible devient un avion long-courrier en vol, il n'y aura pas 20 ou 30 morts, mais des centaines. Un 11 septembre 2.0 est possible, plusieurs chercheurs ont déjà montré la faisabilité d'un tel scénario. »

Rémy FEVRIER, *Président du Pôle 4C*