

## Grand Chambéry, un exemple réussi de mutualisation des services numériques et de cybersécurité



### **Martin NOBLECOURT**

*Conseiller délégué chargé du numérique et de la mutualisation de Grand Chambéry  
1er adjoint de Chambéry chargé des ressources humaines, des finances et de l'appui au pilotage*

*Cette Parole d'Expert est particulière : elle présente l'intégralité de l'interview que le CyberCercle a réalisé dans le cadre de la Note de Conjoncture 2024 « Data-IA et Cybersécurité dans les territoires » du Groupe La Poste et de la Banque des Territoires.*

### **Pourquoi avoir lancé une démarche de mutualisation des services numériques et de cybersécurité au niveau de l'agglomération ?**

Le processus de mutualisation des services numériques, comprenant la cybersécurité, a été enclenché dès 2010 entre la ville centre et son agglomération avec un objectif d'optimisation des ressources humaines et pour aller vers un socle d'infrastructures et d'outils communs. Cet engagement s'est fait dans le cadre d'une réflexion globale sur l'organisation de la fonction informatique, et est apparu comme d'autant plus

pertinent que plusieurs collectivités faisaient face à des départs de personnels dans leur service dédié.

Cinq organisations ont ainsi mutualisé leurs moyens dans un service commun DSIN : Grand Chambéry, Chambéry, le CCAS de Chambéry, La Motte Servolex et La Ravoire.

Les trente-cinq autres collectivités de Grand Chambéry qui n'ont pas exprimé le besoin aujourd'hui s'appuient sur des prestataires locaux et sont également accompagnées par l'OPSN Agate qui a notamment développé une offre de service dans l'utilisation de leurs logiciels de gestion communale et autour de la cybersécurité avec la fourniture d'outils, de prestations d'accompagnement, allant de la sensibilisation à la conduite de projets. Nous travaillons d'ailleurs en coopération avec ce dispositif. Ces communes sont en revanche pleinement intégrées dans le volet de mutualisation de Grand Chambéry relatif à la protection des données personnelles opérée en 2018 pour répondre aux obligations du RGPD.

### **Quel modèle avez-vous adopté pour proposer des services numériques et de cybersécurité mutualisés aux communes de l'agglomération ?**

Nous avons défini un schéma directeur numérique, concernant à la fois un socle technique adapté aux usages mais aussi aux projets que souhaitent conduire les collectivités membres. D'où une structure de socle commun avec des ajouts métiers par collectivité.

Quand on travaille en mutualisation, il est

fondamental que les collectivités montent en puissance ensemble et qu'elles aient chacune une visibilité sur le plan de charge de la DSI, avec l'organisation de la charge de travail DSIN/métiers, la mutualisation des plans projets et des moyens associés. D'où la nécessité d'un dialogue continu entre la DSI et les élus, qui ont d'ailleurs bénéficié d'un programme de sensibilisation à la cybersécurité.

Concernant l'avenir, il apparaît que le socle des critères d'exigence lié au numérique s'élargit de plus en plus : responsable, durable, inclusif, éthique, souverain... autant d'impératifs qui s'adressent aujourd'hui au numérique, et qui s'intègrent aussi à notre réflexion sur les équipements à venir en matière de cybersécurité et de protection des données.

### **Quel bilan tirez-vous de cette mutualisation ?**

Les points positifs sont clairs : une capacité à faire mieux et plus que si chacun était seul, grâce à des économies d'échelle et un gain en termes de politiques d'achat, un travail en commun sur des outils optimisés et de plus grande performance. La mutualisation a également permis un échange entre acteurs, une montée en compétences commune, tout en favorisant des spécialisations entre collectivités qui bénéficient à tous. Sans mutualisation on ne peut être en excellence nulle part.

Les freins intrinsèques à une telle démarche de mutualisation résident à la fois dans le fait de tenir le collectif et l'équilibre indispensable à trouver sur le développement d'axes communs à toutes les collectivités sans freiner ou favoriser les projets de certaines d'entre elles, et dans la complexité de répondre à des organisations métiers différentes d'une collectivité à l'autre. J'ajouterais aujourd'hui un frein plus global qui peut limiter le développement de la mutualisation sur ce sujet, à

savoir les contraintes financières et réglementaires qui touchent de plus en plus les collectivités et qui font que la cybersécurité, comme d'autres démarches structurantes, sont difficiles à prioriser comparé aux services directs aux usagers.

« Commodité, nécessité et opportunité » : trois phases qui caractérisent pour nous en tous cas le process de mutualisation en matière de numérique et de cybersécurité.

### **Quel est dans cette démarche l'impact de la réglementation ?**

Quand on prend l'exemple du service commun de protection des données personnelles à trente-huit communes mis en place à l'occasion du RGPD, on voit l'impact positif qu'une réglementation peut avoir. Néanmoins, une réglementation à elle seule ne suffit pas. C'est le niveau d'ambition que se donnent les collectivités, la clarté et la transparence de l'offre et de la démarche de l'agglomération qui favoriseront l'adhésion à la mutualisation.

Au-delà de la réglementation, l'accompagnement de l'Etat des collectivités en matière de cybersécurité, sur des financements de projets notamment, devrait passer d'« une logique de concours » à « une logique d'examens », autour d'une transparence renforcée sur les critères d'éligibilité.