La cybersécurité : un socle pour les territoires intelligents

Denis HAMEAU
Adjoint à la maire de Dijon, délégué Qualité du service public Relation aux usagers et innovation
Conseiller de Dijon Métropole, délégué Smart City, On Dijon, enseignement supérieur, université

Comment est né ON DIJON, cette initiative pionnière dans le pilotage de l'espace public ?

Le projet ON DIJON est né il y a une décennie d'une double nécessité : assurer le pilotage intelligent de l'espace public, et répondre à un enjeu économique autour de la filière numérique dont on souhaitait qu'elle se structure sur le territoire, développer des compétences, et ce dans une logique d'attractivité du territoire. Au-delà du projet centré sur la ville, nous avons souhaité intégrer les 23 collectivités de la Métropole qui faisaient face aux mêmes enjeux, sans disposer ni des ressources humaines ni des compétences pour adresser les sujets en lien avec le numérique, la cybersécurité pour y répondre efficacement. D'où l'idée d'un projet mutualisé à l'échelle métropolitaine.

En parallèle s'est opérée une mutualisation progressive des services numériques dans les collectivités au niveau de la Métropole avec une logique d'acquisition et de développement des compétences y compris sur le domaine de la cybersécurité.

L'objectif de notre démarche était clair : mutualiser les compétences et rationaliser les coûts pour offrir des services adaptés aux citoyens et optimiser la gestion de l'espace public.

Quelle a été la méthode mise en place pour structurer ce projet aussi ambitieux ?

Pour construire ce type de projets les process sont fondamentaux. Un accompagnement politique et administratif doit être conduit en parallèle et se rejoindre. ON DIJON est un projet transversal, porté par la direction générale des services (DGS).

Dès le départ, les agents ont été associés. Un groupe projet a réuni RH, direction du numérique, agents de terrain, DGST, élus référents – notamment en voirie – et le président de la Métropole. Nous avons mis en place un dialogue compétitif autour d'un appel d'offre spécifique car ce que nous inventions n'existait pas encore sur le marché. L'enjeu était aussi de soutenabilité financière sur le long terme – 105 millions d'euros sur douze ans via un contrat CREM. Quatre grands groupes ont répondu, avec des expertises variées en infrastructure, cybersécurité, IA, et déploiement applicatif. Le volet cybersécurité a été déterminant dans l'évaluation des offres.

Quels résultats concrets ont été obtenus depuis 2018 ?

Aujourd'hui, nous pilotons l'éclairage public, la vidéoprotection, la voirie, en lien étroit avec les agents de terrain. Côté RH, un travail a été mené

pour diagnostiquer les compétences numériques service par service, dans une logique de conduite du changement. La période du COVID a été un véritable crash test pour le dispositif qui a montré toute sa capacité à favoriser le dialogue en cas de crise.

Nous avons également développé une application métropolitaine qui offre plusieurs services aux citoyens – comme le paiement de la cantine, la réservation de livres ou de films à la médiathèque… - et qui lui permet aussi de signaler en temps réel les problèmes dans l'espace public. Ils deviennent acteurs de la gestion de la ville. Et cette interaction doit aussi se faire dans un cadre sécurisé.

ON DIJON a également permis de structurer un partenariat étroit avec l'Université de Bourgogne, devenue établissement public expérimental avec 12 établissements associés. L'IA y est un axe fort avec un pôle dédié, et nous avons insisté pour y intégrer également la cybersécurité.

Vous avez aussi ouvert la voie à l'open innovation. Comment cela s'est-il concrétisé ?

L'open innovation est au cœur de notre approche. Dès 2018, nous avons lancé des « data challenges » avec VivaTech pour valoriser nos données et favoriser le développement de start-up à travers nos cas d'usages. Premier champ d'application : la mobilité, pour améliorer le commerce de centre-ville ou l'expérience touristique. Nous avons ainsi travaillé avec des start-up après sélection pour développer un "coach mobilité" qui propose des parcours optimisés, permettant aussi de mesurer l'impact carbone et l'impact sur la santé de vos déplacements. D'autres ont permis de mieux flécher nos investissements dans l'espace public, via l'identification des zones de départementales les plus dangereuses par l'analyse des données.

Et l'intelligence artificielle dans tout cela ?

L'IA était déjà présente dans le projet initial mais le contrat a été pensé pour permettre l'introduction progressive de nouvelles technologies, dont l'IA générative. Elle ouvre des perspectives, mais elle doit s'inscrire dans un cadre éthique, transparent et compréhensible. Nous avons porté une attention particulière autour de l'éthique de la gestion de la donnée. Un comité métropolitain de la donnée a été créé en 2019-2020. Il vient de voter cette année une charte métropolitaine de la donnée qui s'impose à tous les délégataires.

L'objectif : créer de la valeur sans générer de défiance par les citoyens. D'où la nécessité d'expliquer pour favoriser l'adhésion. Et bien sûr de gérer les risques de tels développements. L'éthique, la transparence et l'explication sont essentielles pour maintenir la confiance des citoyens.

Comment la cybersécurité est-elle gérée au quotidien aujourd'hui ?

C'est notre socle depuis le départ. On se ne lance pas dans le monde des territoires intelligents sans cybersécurité. Notre système subit plus de 1000 attaques par jour. Un tableau de bord nous permet d'y faire face. Nous collaborons aussi avec des start-up, comme celle identifiée via la French Tech Réunion, qui propose des tests pédagogiques de résistance de nos systèmes : un exemple de la coopération qui peut se faire avec nos territoires d'outre-mer. La cybersécurité est vivante : elle évolue avec les menaces.

La direction du numérique travaille également à développer une culture cyber chez les agents, pour ne pas laisser de maillon faible. On ne peut pas protéger un système sans embarquer ses utilisateurs.

Demain, avec une potentielle relocalisation des industries, ou une évolution vers plus d'industries, il va falloir avoir être attractif et donc avoir les compétences localement. On n'est pas dans le prospectif, on est dans un élément d'attractivité

fondamental du territoire : la cybersécurité est un socle et il faut qu'elle irrigue dans les différents systèmes parce qu'elle est une condition de pérennité de nos systèmes et de notre capacité à agir.

Aujourd'hui, le numérique et la cybersécurité ne sont pas encore intégrés dans les logiques économiques classiques. Il est urgent de changer cette vision. C'est aussi une question de souveraineté. D'où le projet sur lequel je travaille au niveau de la Région d'un véritable Campus Cyber construit autour des filières industrielles du territoire. Mais le modèle économique reste à trouver.

Quel regard portez-vous sur la directive européenne NIS 2 ?

Les collectivités doivent monter en maturité mais la cybersécurité ne se décrète pas. Elle se construit par l'adhésion. Il ne suffit pas d'imposer des normes : il faut accompagner les collectivités dans leur montée en compétences. On pourrait imaginer un horizon de trois ans pour les grandes collectivités, pour atteindre un niveau permettant ensuite de mutualiser leur expertise et de favoriser leur environnement. Mais il faut donner les moyens.

Un dernier mot sur la résilience ?

C'est un enjeu central. Nos territoires doivent apprendre à gérer les crises de toutes sortes, y compris cyber. A l'image des territoires ultramarins, il nous faut développer une véritable culture de la résilience. Et donc de la cybersécurité.