La cybersécurité des collectivités : un enjeu majeur qui nécessite un accompagnement de l'Etat

Ludovic HAYE
Sénateur du Haut-Rhin

Cette Parole d'Expert est particulière : elle présente l'intégralité de l'interview du Sénateur que le CyberCercle a réalisé en juin 2024 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, selon vous, l'Etat doit-il accompagner les collectivités vers plus de cybersécurité ?

Pendant longtemps, lorsqu'on parlait cybersécurité, l'on pensait plutôt entreprises que collectivités, notamment car ces dernières ne visaient pas de profit, donc n'étaient pas considérées comme des cibles. Pourtant, d'ici à 2031, une attaque cyber est attendue toutes les deux secondes contre les administrations, les collectivités et les entreprises.

Aujourd'hui, les collectivités, de par la quantité de données qu'elles gèrent et des compétences qu'elles ont pour assurer le bon fonctionnement de la société, sont exposées au même risque que les entreprises, sans avoir les mêmes protections, ni la même organisation. Et, plus les collectivités sont petites, moins elles ont de moyens pour se protéger. Ajoutons également le constat d'un véritable « nœud gordien » : les collectivités ont de plus en plus de données à gérer, elles sont soumises à des contraintes de dématérialisation et d'ouverture de leurs données avec l'open data, ce qui crée de fait des faiblesses en termes de sécurité, elles doivent donc renforcer la protection de ces données, et ce dans un contexte budgétaire restreint… L'Etat se doit donc d'accompagner les collectivités vers plus de cybersécurité en mettant à leur disposition son expertise, ses moyens et son expérience.

Quand vous échangez avec des élus locaux de votre territoire, la cybersécurité est-elle un sujet qui les préoccupe ?

La cybersécurité devient un sujet pour les collectivités. Avec les attaques sur les hôpitaux, les élus ont pris conscience de ce sujet, non seulement par la perte financière qu'une cyberattaque peut induire, mais aussi et surtout par la perte de service aux citoyens qu'elle peut générer. Les élus se sentent aussi garants des données de leurs citoyens et ont compris qu'il y avait là un vecteur de risque de perte de confiance avec leurs administrés.

Quels effets avez-vous vu sur votre territoire de la dimension "Cybersécuriser les territoires" du Plan de Relance France 2030 ? Comment selon vous l'Etat pourrait-il accompagner davantage les collectivités vers plus de cybersécurité ?

Suite à l'adoption du Plan France Relance, plusieurs actions ont été mises en place dans le Grand Est, pilotées par la Région notamment. J'ai deux exemples qui me viennent en tête : un appel à projet lancé par la Région pour soutenir les projets collectifs

de développement de la cybersécurité sur le territoire et un plan régional de cybersécurité adopté en 2023. Le financement est le nerf de la guerre. Encore faut-il que ce budget soit bien fléché sur les actions cyber et qu'il soit cohérent. Pour cela, la compréhension du sujet cybersécurité et l'impulsion par les élus locaux sont fondamentales pour conduire des projets adaptés. Aujourd'hui aucune collectivité n'a la prétention de dire qu'elle est imprenable.

L'objectif est donc de mettre en oeuvre à moindre coût un kit minimaliste cyber pour se protéger : l'Etat pourrait ainsi engager une démarche en ce sens : celle du "premier kilomètre du numérique sécurisé". Il faut aller au-delà de la sensibilisation : avoir une sorte de domaines curatifs ciblés en fonction de son exposition. Il faut pouvoir passer à l'action.

Par ailleurs, on se rend compte que des lacunes existent dans les dispositifs lorsqu'une attaque est avérée. Il n'est pas rare d'ailleurs que je sois appelé dans ces cas-là ! Les CSIRTs régionaux sont là pour répondre à ces enjeux, mais plus de visibilité et de lisibilité entre les différents dispositifs de réponse à incident seraient souhaitables. Les acteurs sur ce sujet sont aujourd'hui nombreux (services de l'Etat, Gendarmerie, CCI, Association d'élus, etc.) et nous ne pouvons que nous en réjouir. Il est cependant primordial de ne parler que d'une seule voix aux collectivités qui parfois se sentent perdues.

Comme vous le savez, les principales associations d'élus locaux ont écrit en avril dernier à Marina Ferrari, Secrétaire d'Etat au Numérique, pour lui faire part de leurs réserves face aux exigences de la directive NIS 2 pouvant s'appliquer aux collectivités, et qui doit être transposée dans le droit français d'ici le 17 octobre. Que pensez-vous d'une telle règlementation pour les collectivités ?

La directive NIS 2 est une illustration des grandes réglementations que peut adopter l'Union Européenne pour protéger ses citoyens.

Néanmoins, attention à la surinterprétation des textes et à la superposition des couches d'obligations : il est de la responsabilité du législateur de mettre les garde-fous nécessaires pour éviter les dérives. La loi a cette finalité : ne pas apporter de complexité mais répondre à un besoin.

Je comprends parfaitement les inquiétudes des élus locaux quant à cette transposition. Les dispositions du texte, bien qu'efficaces, demandent du temps, des moyens et de l'énergie pour leur mise mettre en place. Elles nécessitent de la part de l'Etat un accompagnement au changement et de laisser aux collectivités le temps de s'adapter.

Au Sénat, je travaillerai sur ce texte et j'appelle de mes voeux une réelle discussion avec les collectivités locales afin de déterminer un calendrier progressif et cohérent afin de laisser aux collectivités et à l'Etat le temps d'installer les nouvelles règles. Le chemin est tracé et les sanctions potentielles ne doivent pas être une épée de Damoclès au-dessus des collectivités.