La cybersécurité n'est plus une option pour nos Territoires de projet !

Josiane CORNELOUP
Présidente
Association Nationale des Pôles d'équilibre territoriaux et ruraux et des Pays (ANPP)
Députée de Saône-et-Loire

Sarrebourg, Évreux, Bayonne, La Rochelle, Angers, Houilles, Annecy, Aix-Marseille-Provence… autant de collectivités qui ont été victimes de cyberattaques ces derniers mois. La liste ne cesse de s'allonger à un rythme qui s'accélère depuis un an, notamment avec la **digitalisation accentuée de nos modes de travailler, de consommer, de produire, de vivre tout simplement**. Paralysie des services, pertes et fuites de données, rupture du lien de confiance avec les citoyens, image dégradée… autant d'impacts majeurs qu'une cyberattaque réussie entraîne pour une collectivité.

Aujourd'hui, **la question n'est donc plus de savoir "si" les collectivités seront la cible d'une cyber-malveillance, mais "quand"** : toutes sont concernées par cette menace en plein développement, quelles que soient leur taille et leur localisation géographique. Il est donc aujourd'hui indispensable de se doter d'une politique de cybersécurité cohérente et d'en faire un axe de leur culture, afin de sécuriser leurs missions au service des citoyens et habitants et des acteurs économiques présents sur leur territoire.

Alors même que le numérique devient de plus en plus omniprésent dans nos sociétés, la crise sanitaire que nous traversons actuellement a accéléré ce phénomène de transformation profonde, auquel n'échappent pas les collectivités. Nombre d'entre elles se sont engagées dans un processus de modernisation continue de leur administration et des services qu'elles délivrent. Que ce soit sous l'impulsion des citoyens ou de la réglementation, elles sont au tournant de la numérisation de la "relation citoyen" : l'e-administration (*numérisation des démarches administratives, à laquelle s'ajoute une recherche de simplification*) est un **axe important de la modernisation de l'action publique** et répond à une demande effective des citoyens dans le cadre de l'e-démocratie. Elles détiennent par ailleurs une masse importante de données, parmi lesquelles des données à caractère personnel, dont la divulgation, la suppression, l'altération, le vol, la mauvaise utilisation sont susceptibles de porter atteinte aux droits et libertés des personnes ou à leur vie privée, ou à une mauvaise gestion de l'ensemble des responsabilités sociétales dont les collectivités ont la charge : état-civil, justificatifs de domicile, données fiscales, sociales, inscriptions en établissement scolaire, résultat de vote électronique, études foncières, projets de délibérations, schémas d'aménagement, documents budgétaires… En dehors de la réglementation, notamment le RGPD, la protection de ces données est ainsi non seulement un facteur de bon fonctionnement de la société mais aussi un élément de transparence et de confiance à l'égard des citoyens.

Au-delà de cet enjeu de protection des données, la cybersécurité est également au cœur des

infrastructures que gère une collectivité : gestion de l'eau, des déchets, des systèmes de l'éclairage public, des infrastructures sportives, vidéosurveillance, mobilité intelligente, écoquartiers… autant de systèmes gérés par le numérique et le développement d'objets connectés qui se doivent d'être sécurisés, car exposés. Par exemple, la tentative récente avortée de sabotage via une attaque informatique du réseau de distribution d'eau de collectivités aux Etats-Unis en février dernier montre s'il en était besoin combien l'enjeu de la sécurisation de tels systèmes est impérieux.

Au-delà, les collectivités se sont lancées dans des plans de développement via le numérique au service des acteurs présents sur leur territoire : plan d'accompagnement à la transformation numérique des acteurs économiques, des commerçants aux industries, de développement de la e-santé ou de l'industrie 4.0, programmes d'inclusion numérique, création de tiers lieux, accompagnement au déploiement du télétravail… Autant d'actions fondamentales aujourd'hui pour l'attractivité et le développement des territoires, mais qui constituent autant d'espaces vulnérables.

Cette transformation numérique profonde des collectivités opérée pour leurs propres infrastructures, induit de fait de nouveaux risques : **face aux menaces numériques, la cybersécurité n'est plus une option.** Or, la dimension sécuritaire n'est généralement pas suffisamment prise en compte dans les démarches de transformation numérique des collectivités, qui ne sont souvent orientées que vers les usages.

L'enjeu est donc de mieux sensibiliser et surtout éclairer sur les enjeux liés à cette menace, de faire de la sécurité un pilier majeur de la transformation numérique des collectivités et de leurs plans d'actions, et d'**hisser cet enjeu comme étant un élément phare de la culture numérique** de l'ensemble des élus et des collaborateurs.
La cybersécurité souffre en effet de son image technocratique et lointaine, jusqu'au jour où l'on est concerné. Elle est souvent vue comme un sujet purement technique, réservé à des experts. Cependant ce sujet, quand il est pris en compte et anticipé par les collectivités, est souvent enfermé dans la tour d'ivoire du service informatique, qui a bien souvent du mal à mettre ses recommandations en œuvre tant cette dimension est perçue au mieux comme accessoire ou frein à la mise en œuvre du développement des projets, au pire comme un seul facteur de coût.

Or, la sécurité numérique n'est pas uniquement un sujet technique. Elle repose avant tout sur de la gouvernance, du management, de l'organisation, de la sensibilisation, de la formation, du juridique, de relations avec l'ensemble de l'écosystème d'une collectivité : prestataires, partenaires… autant de dimensions qui sont hors de la simple sphère "informatique". Elle repose sur le facteur humain et à ce titre concerne l'ensemble des collaborateurs d'une structure : en matière de cybersécurité, l'adage veut que le maillon faible se situe entre le clavier et la chaise. Plus de 80% des incidents de sécurité relèvent d'une erreur humaine. Mais ce qui montre aussi que **l'humain bien formé peut devenir le maillon fort de la cybersécurité**.

Face à ce phénomène de transformation numérique des collectivités, au recours au numérique comme facteur de développement des territoires, **la sécurité numérique doit devenir un élément clef au cœur de l'action des collectivités**, avec deux impératifs : que l'ensemble des élus s'approprient cette dimension dans leur vision stratégique de l'avenir des collectivités qu'ils dirigent, seuls capables d'insuffler l'impulsion nécessaire pour une politique de sécurité numérique transverse ; qu'elle devienne un des piliers de la culture de chaque agent, dans les missions qu'il conduit ou de ses usages des outils numériques.

Aujourd'hui, il ne peut y avoir de développement responsable et d'attractivité des territoires sans numérique, pas de numérique pérenne sans confiance numérique, et pas de confiance numérique sans sécurité numérique. C'est bien là que réside l'un des enjeux majeurs d'une transition numérique responsable.