PAROLE D'EXPERT

La sécurité numérique, un enjeu majeur pour la transformation numérique des collectivités territoriales et les élus

Stéphane MEYNET
Président de CERTitude NUMERIQUE

Pourquoi la sécurité numérique ?

Notre société s'est engagée depuis plusieurs années dans une transformation sans précédent. Il s'agit bien-sûr de la transformation numérique qui touche chacun de nous. Plus de services accessibles, plus rapidement, plus simplement, depuis n'importe quel endroit du globe, le numérique révolutionne nos usages et notre vie.

Les collectivités territoriales n'échappent pas à cette transformation, renforcée par la volonté au niveau de l'État de dématérialiser une majorité des services « administratifs » fournis aux citoyens.

Le numérique est souvent perçu au travers des données, que ce soit des données personnelles, des données économiques ou stratégiques manipulées par les collectivités territoriales et ses entités connexes (délégations de service public, sous-traitants, etc.). Or se focaliser sur les données uniquement serait une erreur car la transformation numérique concerne également les infrastructures comme le transport, la distribution d'eau potable, le traitement des déchets et les utilités des bâtiments publics pour les plus récents (climatisation, incendie, contrôle d'accès, etc.).

Lorsque l'on évoque la transformation numérique d'un territoire comme celui d'une collectivité territoriale, il est ainsi impératif de prendre en compte les données et les systèmes numériques en tant qu'infrastructures de service et tous les systèmes numériques s'y afférant.

Les projets de *Smart Cities*, que l'on pourrait traduire par territoires intelligents ou plutôt communicants, accélèrent cette transformation et de facto la dépendance du numérique. En pratique, tous les territoires sont aujourd'hui « Smart » à des degrés plus au moins avancés du simple fait de la dématérialisation.

Si cette transformation numérique, majeure, offre de vrais avantages, elle s'opère en créant dans le même temps une dépendance forte au numérique, sans cesse grandissante ; c'est une certitude.

Un rapide tour d'horizon (un 360°), permettra aux lecteurs de mesurer l'ampleur de cette transformation et le degré de dépendance au numérique. Sans numérique, les services de la vie courante ne fonctionnent plus ou en mode très dégradé.

Pourquoi se préoccuper de cet état de fait ?

Au-delà des aspects sociétaux que suscite le numérique, la question des risques liés au numérique se pose. Sous-estimés ou relégués en priorité basse, le risque numérique est pourtant bien réel. Certains évoqueront le business de la peur (« vous essayez de nous faire peur pour vendre vos services ») ou le motif qu' « il ne faut pas mettre la charrue avant les bœufs : on verra bien après, une fois les services en place et opérationnels, comment traiter la sécurité numérique ». Pourtant, des attaques en tout genre sont quotidiennement relatées dans la presse, avec en « top position » les rançongiciels et les fuites de données provoquant trop souvent de sévères dégâts. Seulement une minorité des incidents liés au numérique parvient dans la presse ; le business de la cybercriminalité se professionnalise et se développe rapidement.

L'objectif n'est pas d'agiter le « drapeau rouge » pour « faire peur » mais d'éclairer l'ensemble des parties prenantes (les élus, les agents territoriaux, les fournisseurs, les pouvoirs publics) des risques à prendre en compte pour, in fine, fournir aux habitants de la « Smart City » et du « Territoire Intelligent » des services numériques dans lesquels ils pourront avoir confiance.

Une réglementation à la rescousse ?

Tout le monde ou presque aura entendu parler du fameux règlement européen pour la protection des données (RGPD) dont l'échéance pour être en conformité était le 25 mai dernier. Ce que beaucoup ignorent, c'est que ce règlement, certes important, n'est qu'un élément de l'édifice réglementaire national et européen.

RGS, eIDAS, Données de santé, NIS, LPM, etc. s'appliquent potentiellement aux collectivités territoriales. Pour mémoire, l'application du RGS, visant à établir un niveau de confiance pour les échanges numériques dans la sphère publique, date de 2010. Combien de collectivités appliquent aujourd'hui ce règlement ? Combien de collectivités se préoccupent aujourd'hui de la sécurité numérique des infrastructures, comme celles de la distribution d'eau par exemple, tel que prévu dans ces règlementations ?

Comment traiter efficacement et durablement le sujet de la sécurité numérique au sein des territoires ?

Il s'agit d'un véritable défi en ce 21ème siècle pour les collectivités locales. Les outils, la technologie, aussi intelligents qu'ils puissent être ne suffiront pas. La question de la gouvernance de la sécurité numérique au sein d'une collectivité territoriale, quelles que soient sa taille et ses missions, est un vrai challenge et la condition *sine qua non* pour traiter efficacement la question. Qui porte le sujet sécurité numérique au sein de la collectivité ? Qui a les moyens, financiers et humains ? Qui porte la responsabilité en cas d'incident et encore les sanctions pénales prévues par les réglementations ?

Une gouvernance mais aussi une stratégie bien étudiées et adaptées aux enjeux de la collectivité sont un gage d'efficacité et de réussite de la démarche de sécurité numérique et une source d'économies financières importantes, soyons-en certain.

Le préalable à cela est de disposer d'une bonne visibilité des systèmes numériques nécessaires aux missions de la collectivité : la cartographie des systèmes, de ses utilisateurs et de ses responsables. Il peut être opportun lors de ce travail de cartographie d'identifier les budgets nécessaires au fonctionnement de ces systèmes. Le coût de la sécurité numérique représente généralement un faible pourcentage du coût de possession d'une installation. Le chiffre de 1% voire moins a souvent été évoqué. Cela permet de relativiser les efforts financiers à fournir, alors même que ce sont souvent ces derniers qui sont mis en avant pour ne pas agir.

Parmi les pistes de réflexion pour une gouvernance et une stratégie cohérentes, nous pouvons évoquer les pistes suivantes :

- traiter de manière cohérente et homogène les différents types de systèmes numériques, que ce soient des « systèmes de gestion » ou des « systèmes industriels » par exemple et surtout de ne pas cloisonner la gestion de la sécurité numérique ;
- intégrer progressivement mais sûrement la sécurité numérique dans les métiers, comme cela a été fait dans le passé avec la qualité ;
- associer le sujet sécurité numérique au projet de transformation numérique et de Smart City – Territoire Intelligent et cela, dès l'origine du projet. Encore une fois, la sécurité ne vient pas « après » comme il est fréquent de l'entendre. Plus la sécurité est prise tard, plus les efforts, humains et financiers, à fournir seront importants et inversement. Le « security by design » tant au niveau technique que de la gouvernance devrait être ainsi un impératif pour tout projet de Smart City - Territoire Intelligent qui se veut pérenne ;
- se recentrer sur les métiers et les services rendus par la collectivité pour ses habitants. La sécurité numérique n'est pas une fin en soi mais contribue à construire la confiance dans le numérique. Se recentrer sur les métiers suppose de partager, d'échanger sur les besoins métiers et, collectivement, d'identifier des solutions pour renforcer le niveau de sécurité ;
- former les élus, les DGS, les DG métiers et l'ensemble des personnels pour que, très simplement, chacun à son niveau, puisse acquérir les clés de compréhension lui permettant de mener à bien ses missions avec le bon niveau de sécurité ;
- identifier les réglementations s'appliquant à la collectivité ;
- mener une analyse de risques, même macro, concernant les systèmes essentiels aux missions de la collectivité. L'analyse de risque, souvent perçue comme un monstre effrayant engloutissant des ressources n'est pourtant pas nécessairement quelque chose de complexe.

Enfin, rappelons que la sécurité numérique s'articule sur trois axes : « Anticiper, Prévenir et Réagir » (cf. les Mémos CERTitude NUMERIQUE[1]).

Prévenir un incident au moyen de dispositifs de protection est bien évidement absolument indispensable. Mais se préparer à subir un incident et à le traiter pour en limiter les effet, l'est tout autant. La transformation numérique à parfois complètement délaissé les modes de secours et modes dégradés permettant de fonctionner, a minima, en cas d'incidents. Combien de collectivités territoriales auraient évité de gros problèmes et auraient affronté sereinement les rançongiciels dont elles ont été victimes si elles avaient « simplement » sauvegardé leurs données ?

Une question de ressources ?

La problématique, régulièrement évoquée par les collectivités, est celle des ressources dont elles devraient disposer pour traiter la sécurité numérique. Le coût RH, les difficultés pour recruter des personnels, liées à la rareté des profils ayant les bonnes compétences, ou le coût des prestations de la sous-traitance conduisent des collectivités à renoncer. Personne ne leur jettera la pierre. Réglementation ou pas, l'absence de solutions simples et de ressources à

[1]https://www.certitudenumerique.net/memo.html

des tarifs raisonnables relèguera malheureusement la sécurité numérique « à plus tard ».

Peu de collectivités possèdent la capacité à constituer une équipe sécurité numérique capable de traiter efficacement toutes les composantes de ce domaine. Mêmes les plus importantes éprouvent des difficultés à recruter des RSSI ou des DPO.

La mutualisation des ressources entre plusieurs collectivités devient ainsi une nécessité vitale. La création de « centres de ressources cyber », offrant, au sein d'un territoire, des services dans le domaine de la sécurité numérique que ne peuvent s'offrir des collectivités individuellement, semble désormais incontournable.

Le GIP cybermalvaillance.gouv.fr, issu de la stratégie nationale de sécurité numérique de 2015, a ouvert la voie dans le domaine puisque ce dispositif apporte un premier niveau de réponse aux victimes d'actes de cybercriminalité. Des centres de ressources de sécurité numérique pourraient utilement compléter ce dispositif national et être des relais territoriaux efficaces.

En parallèle, développer des infrastructures numériques de confiance partagées entre plusieurs collectivités (des clouds régionaux par exemple) ainsi que des outils conformes aux réglementations serait également une aide éminemment précieuse et une source notable de gains financiers.

En conclusion, l'objectif de cet article n'est pas de faire un procès ni de pointer du doigt d'éventuelles défaillances au sein des collectivités territoriales dans le domaine de la sécurité numérique mais d'insister encore une fois sur le nécessité d'engager une démarche, même modeste, pour renforcer la sécurité des systèmes numériques importants pour leurs activités, et que la feuille de route n'est pas infranchissable.

La sécurité numérique est l'école de l'humilité comme aime à la rappeler Guillaume Poupard, le directeur général de l'ANSSI. Tous, même les plus aguerris, seront victimes demain d'incident cyber plus ou moins grave, c'est une certitude.

La sécurité numérique est donc aujourd'hui une nécessité pour construire la confiance dans les usages numériques au service de la collectivité et de ses habitants.

La confiance numérique, une garantie de pérennité, de succès et un facteur d'attractivité devrait ainsi être un sujet majeur pour les politiques.

« Agissons efficacement ensemble »[2] pour construire les territoires du futur, résilients face aux menaces numériques et offrant un niveau de confiance élevé dans les services qu'ils proposent.

[2]citation de Bénédicte Pilliet, Présidente du CyberCercle, lors de la journée Sécurité Numérique, Sécurité Portuaire 2018 au Havre