



Covid-19 et aménagement du territoire

Appel à contributions du Cercle pour l'aménagement du territoire

Cybersécurité et aménagement du territoire : territoire bien protégé, territoire plus attractif

Martine Levy*

Juillet 2020

Au moment où la France et l'Allemagne lancent un projet de souveraineté numérique avec l'initiative Gaïa X pour se garder notamment d'envoyer leurs secrets industriels outre-Atlantique ou en Asie, et où la pandémie de Covid-19 a fait exploser le recours à Internet pour rompre l'isolement et permettre à l'économie de continuer à fonctionner, un article d'Olivier Kempf¹ met en garde contre l'oubli du Cyber par les collectivités territoriales. Un risque majeur avec les 4S², mais un enjeu "invisible" en particulier dans la campagne des municipales 2020.

Typologie des agressions en 4 catégories dites les 4 S

Espionnage avec la capture de données sensibles relatives aux informations professionnelles, économiques ou fiscales de leurs collaborateurs, administrés ou entreprises, mais aussi les données de santé ;

Sabotage soit par des agressions extérieures, soit par l'accès au système d'information ;

Subversion de l'étranger pour influencer sur l'état d'esprit du public (infox) comme dans les cas des maires de Metz³ et de Castres⁴ ;

Escroquerie avec le rançonnement en croissance et touchant des collectivités de tailles de plus en plus réduites.

* **Martine LEVY**, ancienne chargée de mission de la Datar, 1991-1999

¹ Olivier KEMPF. Cybersécurité et résilience : les grandes oubliées des territoires, in Fondation pour la Recherche Stratégique. Note n°39/20 du 14 mai 2020.

² Voir encadré

³ « Non, Dominique Gros, maire de Metz, n'a pas refusé d'enlever le porc des cantines », Rue89 Strasbourg, 20 décembre 2018.

⁴ « Le maire sortant de Castres, victime d'une fake news relayée par le candidat RN, La Dépêche, 21 février 2020.

Or, les nombreuses révolutions numériques à l'œuvre, qu'il s'agisse du stockage de données, de la valorisation de données massives, de l'utilisation à distance d'applications, ou encore des objets connectés aux protections numériques très faibles, interpellent les territoires.

Alors que les standards et la réglementation deviennent de plus en plus exigeants, l'actualité du COVID 19 vient donc interroger la capacité des collectivités territoriales à y faire face.

Leur vulnérabilité ressort de plusieurs éléments :

L'insécurité :

En France comme à l'étranger, la multiplication des incidents recensés en 2019 atteste que même les collectivités de premier niveau ne sont pas épargnées par la cybercriminalité. Dès 2015, la Gazette des Communes, lors de la première vague d'agressions cyber, recensait 6 000 communes avec des sites très vulnérables. La vague d'attaques n'a pas cessé avec la pandémie. Ainsi, dans deux petites communes du Morbihan touchées début avril, de faux messages et Intox ont circulé, en particulier, dans le secteur public hospitalier local⁵.

Le développement inégal :

Des disparités de taille et de moyens des collectivités mettent notamment en danger les perspectives pour les petites communes vis à vis des « villes intelligentes » proches ou éloignées.

À cet égard, il convient de souligner le défi posé aux collectivités pour inventer de nouvelles modalités d'organisation /protection permettant non seulement d'atténuer pour les populations les inégalités de situation mais aussi d'apporter des atouts favorables à leur développement et le souci d'atténuer les disparités de chances de leurs populations.

Faiblesses des collectivités malgré des “bonnes pratiques” :

Outre la complexité de notre organisation territoriale, « le mille-feuille territorial », les risques tiennent à l'absence de moyens techniques en la matière dans la plupart des collectivités qui ne peuvent s'offrir les services de compétences rares et coûteuses.

Quant à l'État, il ne dispose pas non plus des moyens de s'en occuper malgré la sensibilité particulière de la Gendarmerie nationale à cette question, comme en attestent les quelques paragraphes de la Revue Stratégique de Cyber défense consacrés aux collectivités locales ou la nomination par l'ANSSI en 2019 d'un chargé de mission à la sécurité des territoires.

Ainsi un sondage de 2018 révélait que 66% des fonctionnaires des collectivités interrogés ne possédaient pas de programme de sécurité et que 49% jugeaient que leur administration avait bien évalué les enjeux. Or, la reconnaissance des enjeux, de même que l'établissement de guides, comme celui de la CNIL en 2019 pour assurer une mise en conformité ne suffisent pas. Une mobilisation plus importante est nécessaire.

En particulier, les élus risquent de voir leur responsabilité mise en cause, y compris pénale en cas de cyberattaque suite à la divulgation de données d'un système non sécurisé, eu égard à

⁵ « Cyberattaques : de nouvelles mairies rançonnées à l'heure du coronavirus », L'Express, 3 avril 2020.

l'insuffisante ou inadaptée mise en œuvre de leurs obligations nationales⁶ ou européennes⁷ comme l'IGAS le signale depuis 2016.

Même si quelques Régions ont pris des initiatives, la sensibilisation des collectivités reste globalement insuffisante, notamment de la part des Départements.

Plus fréquentes sont les initiatives des agglomérations, comme Rennes et sa European Cyber Week, Lille et son Forum international annuel de cyber sécurité, mais aussi Limoges en matière de santé, Brest et son centre national de cyber sécurité maritime, Lyon et son collectif dédié à la cyber sécurité des systèmes industriels ou encore Vannes avec le cyber West challenge et sa chaire de cyber sécurité qui constituent de grands événements publics.

Les villes moyennes et petites, sans parler du monde rural, sont les grandes absentes de ce paysage, sauf exception, comme Malestroit en Bretagne avec 16 000 habitants avec son appel public en mars 2020 au renforcement des mesures de cyber sécurité⁸.

La cyber sécurité est une priorité et un investissement permettant l'organisation de la résilience générale qui va au-delà des plans communaux de sauvegarde. Il s'agit bien de l'intégrer dans une démarche générale de résilience territoriale.

En termes d'aménagement et de développement des territoires, cela signifie notamment d'associer le développement local à la résilience territoriale.

Il s'agit donc de changer le regard sur la cybersécurité en l'appréhendant, outre comme un service rendu aux administrés, d'abord en termes de développement, à savoir comme une exigence première, non seulement de l'implantation mais, aussi, du développement des entreprises sur leur territoire. La cybersécurité offre ainsi l'opportunité d'un retour collectif avec des formes de mutualisation susceptibles de réduire les fractures territoriales.

Cette situation, défi et promesse, doit mobiliser le Cercle avec son potentiel humain et ses réseaux. Au total, il ne s'agit que de reprendre et de prolonger les réflexions initiées dans les années 1990 par la DATAR.

* * *

⁶ Loi NOTRE de 2015, loi pour une République numérique de 2016.

⁷ Le RGPD encadre la gestion des données personnelles, imposant à la collectivité pour se mettre en conformité selon le Guide 2019 de la CNIL de respecter 5 principes : finalité, proportionnalité, durée limitée de conservation des informations, sécurité et confidentialité des informations, respect des droits des personnes.

⁸ « Coronavirus/COVID-19 Appel au renforcement des mesures de vigilance cybersécurité », villedemalestroit.bzh, 18 mars 2020