Le Rubicon de la technologie est la technologie pour la technologie.

Bénédicte Pilliet est présidente fondatrice du Cybercercle. Cet entretien a été publié le 12 novembre 2021.

1/ L'idée de souveraineté numérique territoriale a-t-elle un sens ?

Il en est de la réflexion sur la souveraineté numérique territoriale comme de la souveraineté numérique nationale : un sujet compliqué. Au niveau de l'Etat on est passé de « souveraineté » à « autonomie stratégique » à « de confiance »… Après, au niveau d'une collectivité, on pourrait poser l'idée pragmatique que la souveraineté est un concept en matière numérique qui pourrait déjà s'appuyer sur la maîtrise. Maitrise de ses données ou des usages qu'elle décide qui en seront faits, maîtrise de ses choix en matière d'outils numériques, maîtrise de ses usages, maîtrise de la possibilité de revenir sur des dispositifs qui ne conviennent plus, la fameuse réversibilité… Cela impliquerait ainsi pour les collectivités d'avoir conscience des enjeux et d'avoir les moyens de faire des choix éclairés. On est peut-être loin de la définition stricto sensu que l'on applique à la souveraineté numérique mais ce serait déjà une première étape.

2/ Les collectivités ont-elles une revanche à prendre dans l'exploitation des données collectées par les concessionnaires de service public ?

Je ne parlerais pas de revanche. Je parlerais plutôt de rééquilibrage à mettre en œuvre dans les relations avec les concessionnaires, à l'heure où les données sont considérées comme le nouvel « or noir ». Il serait juste que les collectivités – et donc les administrés – perçoivent un juste

retour de cet or noir que collectent aujourd'hui les concessionnaires de service public, ou que des mesures soient mises en place pour limiter l'exploitation de ces données par ces derniers. Les prochains contrats devraient prévoir ces éléments : les concessionnaires peuvent-ils exploiter les données collectées dans l'exercice des missions qui leur sont confiées, si oui jusqu'où et comment mettre en œuvre une rémunération pour la collectivité de l'exploitation des données qui serait faite par les concessionnaires.

3/ La cybersécurité vous paraît-elle le prochain grand chantier des collectivités et des services publics ?

Ce n'est pas le prochain. C'est celui d'aujourd'hui ! Et au-delà celui global du numérique de confiance. Nous œuvrons au CyberCercle depuis 2014 pour d'une part porter dans les territoires, auprès des collectivités, les sujets de la confiance et la sécurité numériques, et d'autre part pour faire en sorte que cette dimension soit prise en compte dans les politiques publiques portées par l'Etat.

Dans le prolongement de la Stratégie Nationale pour la Sécurité du Numérique de 2015, la création en 2017 du dispositif national Cybermalveillance.gouv.fr pour répondre aux besoins des collectivités – des PME-PMI et des particuliers – a été une très belle avancée.

La Stratégie d'accélération Cybersécurité incluse dans le Plan de Relance, et présentée par le Président de la République le 18 février dernier, dédie des actions spécifiques envers les collectivités dans le cadre d'une feuille de route "Cybersécuriser les Territoires". Là encore, c'est un signe positif de prise en compte que les collectivités sont non seulement au cœur des enjeux de sécurité numérique pour elles-mêmes et leur territoire, mais aussi qu'elles ont un rôle majeur à jouer dans ce domaine au niveau national.

Je ne peux donc que me réjouir qu'aujourd'hui ce sujet soit

devenu un sujet majeur, que les collectivités s'approprient de plus en plus, dont on parle au niveau des politiques publiques de l'Etat – quand j'ai commencé à travailler sur cette dimension en 2014 et à porter ces sujets au niveau national, j'avais souvent en retour des petits sourires en coin comme réponse – et sur lequel on met des moyens financiers. La mise en œuvre de cette feuille de route "Cybersécuriser les Territoires" devrait d'ailleurs faire l'objet d'un suivi avec des indicateurs pour mesurer l'impact des mesures mises en œuvre sur le niveau de maturité des collectivités et, le cas échéant, adapter les dispositifs pour répondre aux besoins et aux attentes afin d'être le plus efficient possible. Le chemin est encore long et de nombreuses difficultés doivent être levées pour aider et accompagner l'ensemble des collectivités dont vous connaissez l'hétérogénéité, à s'engager vers un numérique de confiance, pour assurer leurs responsabilités et leurs missions envers leurs administrés, à l'heure où la dématérialisation et le développement du e-citoyen est devenu non seulement un process sociétal naturel mais est également une obligation réglementaire.

Au-delà, les politiques publiques de développement et d'attractivité de leur territoire, que ce soit l'aide à la transformation numérique des entreprises, la création d'éco-quartiers, le développement de systèmes de mobilité intelligents… devraient également inclure « naturellement » la dimension cybersécurité. Avec un constat de différences de maturité majeures des collectivités non seulement sur la sécurité numérique, mais également sur le numérique. Sensibilisation, formation au numérique et aux usages sécurisés du numérique, création d'outils numériques de confiance adaptés et simples d'usage (avec une sécurité « à la Disney » : la sécurité est présente mais on ne la voit pas dans les usages), culture de cybersécurité partagée au sein des collectivités, au niveau des élus et des agents, politiques publiques où la cybersécurité est un élément transverse que l'on parle de développement économique, de

sécurité globale ou de rapport au citoyen… autant de chantiers à mettre en œuvre, en prenant en compte l'existant sous peine d'être inadaptés, en allant au plus près des territoires, et sur lesquels nous devons collectivement travailler. C'est en tous cas au cœur des actions du CyberCercle depuis 2015.

4/ Quelle confiance avoir encore sur le net quand à peu près tout peut être contrefait ?

C'est effectivement aujourd'hui une tendance qui ressort dans certains sondages : la confiance dans le numérique et au-delà dans la technologie diminue depuis quelques années, notamment dans les pays développés. On peut analyser ce phénomène de façon positive : l'esprit critique des citoyens n'est plus désormais passif face aux technologies. « Le numérique c'est fantastique », et ce n'est pas car il y a des risques que nous devons « jeter le bébé avec l'eau du bain » et se passer du formidable outil que représente le numérique ! D'où à mon sens deux réponses possible.

La première, et sans ordre de priorité : des réponses technologiques pour justement aider à identifier les images, les voix, les signatures contrefaites. Cela existe déjà et l'enjeu est de développer le déploiement de tels outils au service des usages.

La seconde, et surement la plus importante : des réponses de culture-formation des citoyens. Comme je le disais, on peut voir cette baisse de la confiance « aveugle » dans le numérique comme l'éveil, le développement de l'esprit critique et d'analyse des citoyens. Face à ces risques, il est à mon sens indispensable d'apporter des réponses en termes de sensibilisation, de formation à l'ensemble des citoyens, et en termes d'éducation dès le plus jeune âge.

Nous avions travaillé avec deux députés Sereine Mauborgne et Gwendal Rouillard pour proposer un amendement dans le cadre du Projet de Loi sur l'Ecole de la Confiance visant à créer un

enseignement aux usages sécurisés du numérique dès le primaire. Cet amendement n'a pu aboutir, mais quoi de plus fondamental aujourd'hui, dans la société numérique dans laquelle nous vivons, que de permettre à nos enfants dans leurs usages numériques de se protéger, de protéger les autres et de devenir des citoyens éclairés capables notamment de gérer au mieux les risques liés au numérique, de l'usurpation d'identité aux fake news. Donner une culture de la sécurité appliquée au numérique, développer les réflexes, généraliser des outils simples pour des usages sécurisés du numérique, sont autant d'impératifs aujourd'hui pour continuer à utiliser avec plus de confiance ce que nous offre le numérique.

5/ Pensez-vous que l'esprit d'innovation doive convoquer davantage et plus souvent le civil et le militaire ?

Ce rapprochement civil-militaire dans l'innovation est déjà en marche. L'Agence de l'Innovation de Défense, la Délégation Générale de l'Armement, s'adressent aussi bien aux entreprises qui ne traitent que les sujets sous l'angle Défense qu'à celles qui créent et développent des technologies civiles mais qui pourraient également avoir une utilité pour la Défense. L'innovation, en particulier dans le numérique, est très riche dans le secteur civil et peut être dans la plupart des cas duale. Là où l'effort doit être mené c'est dans la diffusion d'une meilleure connaissance auprès des entrepreneurs de l'innovation, et en particulier ceux du numérique, de ce qu'est le milieu de la Défense, au-delà de l'image qu'il a trop souvent, connaître ses acteurs et sa culture. Et, à l'inverse, de mieux faire comprendre aux acteurs Défense ce que sont les entrepreneurs « civils » de l'innovation, leurs manières de fonctionner, leurs contraintes, leurs impératifs.

Dans le cadre du Tour de France de la Cybersécurité que nous avons lancé en 2018, nous avions organisé des rendez-vous one to one avec la DGA au profit des starts up ou PME-PMI innovantes en cybersécurité présents sur les territoires afin qu'elles puissent voir si elles pouvaient bénéficier des

dispositifs de financement RAPID. Or nous nous sommes rendu compte que non seulement beaucoup d'entrepreneurs ne connaissaient pas le dispositif, mais également qu'ils ne connaissaient pas la DGA – voire étaient réticents à rencontrer des représentants du ministère de la Défense – je ne parle pas bien sûr de la Bretagne ! L'ensemble des acteurs, qu'ils relèvent de la Défense ou du monde civil, a intérêt sur l'innovation à mieux se connaître, à échanger et à se rencontrer. L'enjeu là encore est également de comprendre la culture et les contraintes de l'autre, de briser les silos traditionnels afin de pouvoir avancer ensemble.

6/ Quel est à vos yeux le Rubicon de la technologie ?

Pour moi, le Rubicon de la technologie est la technologie pour la technologie. Aujourd'hui la technologie va de plus en plus vite, dans ce qui semble être une course effrénée. L'enjeu pour moi est aujourd'hui de déterminer vers quelle société nous souhaitons aller et la place de l'humain dans celle-ci face au développement des technologies. Au CyberCercle, on dit souvent que la cybersécurité ne sert que si elle est au service des métiers ou des missions. Quels sont aujourd'hui les objectifs sociétaux auxquels répond la technologie ? Quelle est la société, la « cybersociété » pour reprendre le titre d'un livre de Myriam Quéméner, dans laquelle nous souhaitons vivre ? Comment ce développement technologique se concilie t-il avec nos valeurs ? Comment l'humain reste t-il au cœur des enjeux et de la maîtrise ? Il me semble que cette réflexion est trop souvent absente aujourd'hui.

7/ La souveraineté repose sur les technologies mais également sur la dimension Ressources humaines. Comment voyez-vous ce sujet ?

La cybersécurité manque de ressources humaines formées et qualifiées. C'est un enjeu majeur aujourd'hui pour l'ensemble des acteurs publics et privés. L'un des axes d'action est donc de développer des formations ad hoc qui répondent à ces

besoins, et de les faire connaître.

Dans le cadre du Tour de France de la Cybersécurité nous avons à cœur de valoriser les formations qui existent sur les territoires où nous faisons étape – et elles sont de plus en plus nombreuses -, mais aussi de mieux faire connaître les métiers. Car il ne suffit pas de créer des formations, encore faut-il qu'elles soient remplies. Il est donc fondamental de montrer la diversité et la richesse des métiers de la cybersécurité, et ce dès le collège, et au-delà de l'image du « geek à capuche » qui est véhiculée, ou du profil « ingénieur bac + 5 ».

J'ajouterais également que l'un des enjeux en matière de ressources humaines dans notre secteur est d'attirer les profils féminins : les femmes ont toute leur place dans la cybersécurité. Des actions envers les jeunes filles pendant leurs études – ou auprès des femmes en reconversion – sont donc là encore indispensables pour susciter des vocations. Et je tiens à saluer sur ce sujet le travail de terrain qui est fait par les bénévoles du Cercle des Femmes de la Cybersécurité, dont je suis membre du conseil d'administration, qui s'engagent dans les collèges, les lycées… pour présenter les métiers, qui ont mis en place des programmes de mentorat pour accompagner les jeunes femmes dans leur parcours professionnels, et développent des outils adaptés comme cet ouvrage sur les métiers et les formations « Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité ».

Il est indispensable si l'on souhaite disposer de ressources humaines formées en cybersécurité, de mener des actions sur le terrain au plus près des acteurs, de présenter toute la richesse de nos métiers à travers la diffusion de paroles d'experts et de rôle modèles, et de développer sur les territoires des réseaux associant écoles, organismes de formation, entreprises et collectivités.