LETTRE
CYBER SÉCURITÉ et Politiques Publiques

CYBER CERCLE

N°2 - 1ER TRIMESTRE 2019

Édito

LA CYBERSÉCURITÉ : UNE PRIORITÉ POUR LES COLLECTIVITÉS TERRITORIALES

Dans un rapport d'information que j'ai écrit en 2012 pour la commission des affaires étrangères, de la défense et des forces armées du Sénat, évaluant le degré de préparation de notre pays face aux attaques informatiques, je constatais l'existence de progrès significatifs tout comme la perpétuation d'importantes lacunes.

Un diagnostic équivalent pourrait être fait aujourd'hui, nuancé par le constat que de nouveaux progrès ont été réalisés dans les administrations de l'État, alors que des lacunes sensibles semblent perdurer dans les collectivités territoriales. C'est du moins ce que suggère un récent sondage effectué auprès d'un panel de fonctionnaires de l'État, des collectivités territoriales et de la fonction publique hospitalière : les deux tiers des fonctionnaires des collectivités interrogés indiquent que leur administration ne possède pas de programme de sécurité, la situation étant bien meilleure du côté des administrations de l'État.

Or la nécessité de faire de la protection des systèmes d'information une priorité à tous les niveaux est encore moins discutable aujourd'hui qu'en 2012 : le développement de l'administration électronique constitue un levier majeur de la modernisation et de l'efficacité des services publics en collectivité territoriale comme ailleurs. Ainsi, la numérisation et l'interconnexion progressent sans cesse, offrant aux actions hostiles des angles d'attaque de plus en plus ouverts. De fait, le nombre des cyberattaques ne cesse d'augmenter, quelle que soit la taille des cibles, y compris les collectivités. Le maximum doit donc être fait pour protéger les systèmes et les données transportées.

Rappelons que les collectivités territoriales traitent de nombreuses données personnelles afin d'assurer le fonctionnement des services publics dont elles ont la charge. La divulgation de ces données, qu'elles soient fiscales, sociales ou autres, leur altération, leur suppression, leur vol porteraient à la vie privée des personnes concernées une atteinte dommageable en soi. Elles auraient aussi de graves répercussions sur le déroulement du processus de modernisation de l'administration et des services des collectivités visées. À titre d'illustration, la gestion de fichiers comme ceux de l'aide sociale ou de la police municipale appelle évidemment une totale sécurisation.

À côté de la protection des données personnelles, celle des services eux-mêmes et de la collectivité qui les met en place doit être assurée. Par exemple, des incidents tels que le défaçage ou la paralysie d'un site internet, que ce soit par simple malveillance ou dans le cadre d'une opération d'extorsion conduite à l'aide d'un rançongiciel, doivent être prévenus ou rapidement résolus.

Cela dit, la prise de conscience et la connaissance des problèmes ainsi que des solutions font l'objet d'efforts soutenus depuis plusieurs années.

Ainsi un document gouvernemental élaboré à l'intention des collectivités territoriales dans le cadre du plan Vigipirate 2014 expose les objectifs de cybersécurité à viser et les recommandations à appliquer pour sécuriser leurs systèmes d'information. Ces objectifs sont regroupés en sept domaines d'activités : la gouvernance, la maîtrise des risques, la maîtrise des systèmes, la protection des systèmes, la gestion des incidents, l'évaluation et la relation avec les autorités. Chaque objectif est décliné en objectifs-relais complémentaires les uns des autres, l'ensemble constituant ainsi une synthèse pédagogique et opérante de ce qu'est la cybersécurité et de ce qu'elle implique.

Sur le plan réglementaire, un référentiel général de sécurité applicable aux collectivités territoriales comme à l'ensemble des autorités administratives a fixé en mai 2010 un cadre visant à instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Ce document a été complété et remplacé par un nouveau référentiel en juin 2014. Dans le prolongement de cette approche, un guide comprenant 42 règles d'hygiène informatique a été publié en janvier 2017.

Des outils innovants peuvent par ailleurs favoriser la montée en puissance effective de la cyberdéfense dans les collectivités territoriales, dont seules les plus importantes sont en mesure de se doter en interne des compétences nécessaires pour faire face aux attaques. Ainsi en est-il du dispositif d'assistance aux victimes, cybermalveillance.gouv.fr, qui s'adresse aux particuliers, aux entreprises et aux collectivités territoriales. Il prévoit de mettre les victimes en relation, via une plate-forme numérique, avec des prestataires techniques susceptibles de restaurer leurs systèmes ; la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique ; la création d'un observatoire du risque numérique permettant de l'anticiper. Il s'appuie sur des prestataires techniques de proximité ainsi que sur les réseaux existants au niveau territorial : administrations de l'État ou des collectivités et acteurs locaux - chambres consulaires, fédérations professionnelles, réseaux « transition numérique », etc.

En tout état de cause, un palier supplémentaire a été franchi en matière de cyberdéfense des collectivités territoriales avec l'entrée en vigueur le 25 mai 2018 du RGPD. Depuis cette date, la désignation d'un délégué à la protection des données est obligatoire pour ces dernières, en interne ou externalisé, mutualisé ou non, dans le cadre du passage à une logique de responsabilisation des acteurs impliquant de la part des collectivités un effort constant de mise en conformité et la capacité de démontrer à tout instant le niveau maximal de protection des données qu'elles traitent. En d'autres termes, ce volet essentiel de la modernisation de l'action publique qu'est le développement de l'administration électronique dans les collectivités territoriales doit désormais prendre en compte la protection des données personnelles dès la conception des services et tout au long de leur existence.

Au regard de la situation globalement insatisfaisante que je mentionne au début de ce texte, le défi n'est pas minime. Là, comme en d'autres domaines, les collectivités territoriales sauront le relever.

Jean-Marie Bockel
Sénateur du Haut-Rhin, Président de la Délégation sénatoriale aux collectivités territoriales et à la décentralisation

L'European Cyber Week de Rennes vient, pour la troisième année consécutive, de réunir plusieurs centaines de responsables économiques, politiques, universitaires, militaires autour de la question du développement de la cybersécurité. Cet événement, complémentaire du FIC de Lille ou des Assises de la sécurité à Monaco participe à la reconnaissance de la Bretagne sur ce sujet et s'inscrit dans la politique que nous menons depuis plusieurs années.

Parler de cybersécurité, c'est parler de souveraineté. La puissance d'un pays, d'un territoire, son développement économique et sa capacité à décider de son avenir passe aujourd'hui par la maîtrise de la cybersécurité. Cette question de souveraineté raisonne avec l'histoire de la Bretagne. Notre région a toujours été engagée dans la souveraineté de notre pays et donc de l'Europe : militaire avec une présence historique de l'armée, de la DGA-MI, de la force sous-marine, de l'électronique de Défense, ou encore dans la navale. Mais aussi économique avec la souveraineté alimentaire dont la Bretagne a et est un acteur majeur en Europe et demain énergétique avec ce que nous faisons sur les énergies marines renouvelables et les smart-grid, le secteur de l'énergie étant d'ailleurs un domaine d'application stratégique pour la cyber. L'engagement dans la cyber est donc naturel et s'inscrit dans le temps long, c'est une singularité très forte que nous avons, notre sujet n'est pas juste de développer l'économie mais aussi de participer à la construction d'une souveraineté nationale et européenne. Cet engagement nourrit notre volonté de devenir un territoire producteur de confiance numérique, ô combien nécessaire pour réussir notre transition numérique.

Le positionnement de la Bretagne sur la cybersécurité s'appuie sur trois liens forts que nous cultivons. D'abord, le lien puissant de confiance entre le monde militaire et le monde civil : c'est la force de cette relation qui nous a permis de créer le pôle d'excellence cyber avec le Ministère de la Défense. Cette alliance étonnante entre une région et un Ministère de la Défense a permis de réunir les leaders de la cyber en France, le monde académique les entreprises de toutes tailles. Il permet de combiner des engagements nationaux avec la mise en œuvre concrète sur le terrain. Le Pôle d'excellence cyber est aujourd'hui un lieu de confiance propice pour accélérer l'innovation duale. Il travaille sur les problématiques concrètes de ses membres et en particulier dans le champ de la formation, de la recherche et du développement économique.

LA BRETAGNE RÉSOLUMENT ENGAGÉE DANS LE DÉVELOPPEMENT DE LA CYBERSÉCURITÉ

Ensuite, nous travaillons depuis longtemps le lien formation – recherche – innovation – développement économique : le temps des silos est terminé et il faut penser les projets de manière systémique. Faire travailler ensemble différents univers constitués est une des illustrations du savoir-faire collectif que nous défendons. Ce lien est au cœur de l'ensemble des outils de notre écosystème qui contribue à la dynamique cyber.

Enfin, nous avons toujours la volonté de combiner l'échelon territorial avec l'échelon national et l'échelon européen. Notre contribution régionale à la souveraineté, à la cybersécurité est aussi dans cette capacité à construire un écosystème territorial puissant, à s'appuyer et à renforcer l'échelon national et à porter nos savoir-faire et nos convictions à l'échelle européenne. Nous considérons qu'il faut penser les trois échelons en même temps. Nous sommes présents dans des programmes INTEREG avec notre agence de développement Bretagne Développement Innovation, et directement dans le PPP Cyber, dans le pilotage de l'action de coordination des stratégies des régions européennes spécialisées en Cyber, au sein d'ECSO (European cyber security organisation). Notre engagement européen sur la cyber est du même niveau que celui sur la PAC, sur la pêche ou sur les énergies.

Pour conclure, nous avons deux sujets de nature différentes mais d'importance égale pour les semaines et les mois qui viennent.

Le premier c'est l'intelligence artificielle. Travailler sur la cybersécurité aujourd'hui, c'est aussi travailler sur l'intelligence artificielle. L'ensemble des emplois, et contrairement à ce que l'on croit souvent les emplois de cadre, vont être impactés. Il nous faut donc l'anticiper et investir ce sujet. C'est un champ pour l'avenir de la cybersécurité et nous nous investirons sur cette question.

Le deuxième c'est l'appel de Paris. Nous devons le faire réussir. Le Président de la République a eu raison de faire cet appel et de le faire maintenant. Nous vivons dans un monde imprédictible et nous devons tout faire pour que l'espace numérique ne se réduise pas à un espace de guerre, de manipulations, de fake News, il faut donc le protéger, il faut donc défendre nos valeurs démocratiques. C'est le sens de cet appel. La Bretagne le soutient et je pense que les régions européennes ont un rôle majeur à jouer pour le faire réussir.

Loïg Chesnais-Girard
Président de la Région Bretagne

Les collectivités territoriales collectent depuis toujours de très nombreuses données. Cette collecte leur permet d'assurer les services au public et leurs compétences après de leur population.

Leurs pratiques sur la gestion de la donnée, de la collecte à la suppression, sont variées et ne suivent pas de règles établies, appliquées par toutes de manière uniforme. Ceci n'est pas sans poser un certains nombres de problèmes, notamment ces dernières années, face à la recrudescence des attaques cyber et aux ransomware en particulier.

Si les pratiques en matière de data sont propres à chaque communes ou EPCI, il n'empêche que jusqu'à l'arrivée du RGPD la déontologie professionnelle applicable par tous agents territoriaux, la loi informatique et liberté de 1978 et le sens des responsabilités des élus et DGS vis à vis des informations collectées ont assuré un bon cadre de protection.

Plusieurs facteurs récents sont cependant en train de modifier considérablement la philosophie de traitement de la donnée dans les collectivités territoriales.

Les attaques cyber et les vols de données depuis 2014 ont provoqué une véritable prise de conscience des élus sur le fait qu'ils puissent être des cibles financières juteuses pour leurs auteurs. Les demandes de rançon se sont multipliées sans que souvent les maires n'osent porter plainte ou même en parler. Ces faits récents ont permis la mise en place de nouvelles pratiques de protection du patrimoine informationnel des collectivités, tant au niveau des données des citoyens que celles des communes.

L'arrivée du Règlement Européen sur la Protection des Données à caractère Personnel (RGPD) en avril 2018 est également une autre étape importante dans la modification de la culture de la gestion de la donnée dans les Collectivités territoriales. Les responsabilités pénales et financières du Maire et du DGS/Secrétaire de mairie sont fortement accrues et le citoyen est remis au cœur de ses droits sur ses données. Au-delà de la simple règlementation, la notion de confiance est davantage introduite entre élus et citoyens. Confiance qu'il faut conserver et protéger...

Un autre facteur modifie fortement les politiques publiques des collectivités, et ce, quelle qu'en soit leur taille : la dématérialisation. Qu'elle soit poussée et voulue par l'Etat - dématérialisation de la chaîne comptable ou des marchés publics, par exemple – ou initiée par les propres services de la commune pour des usages simplifiés et directs depuis le domicile des personnes, elle provoque une arrivée massive de données personnelles. Des données qu'il faut traiter, sauvegarder, protéger et voire supprimer, le cas échéant.

Se pose désormais la question des bonnes pratiques en matière d'optimisation de la gestion de la donnée dans les collectivités locales. Les sujets prioritaires aujourd'hui portent à la fois sur la sauvegarde et la protection des données, souvent confiées à des prestataires extérieurs. Les communes vont devoir se montrer plus exigeantes sur le niveau de qualité des prestations avec leur partenaire informatique : la durée de conservation, le lieu de sauvegarde, les accès, etc...

Un autre sujet d'action est la gouvernance de la donnée. Protéger les données est une chose, les exploiter dans l'intérêt général est mieux. Les collectivités territoriales se doivent d'y réfléchir déjà. Elles ne sont pas équipées ni ne possèdent les ressources pour mener chacune, individuellement, une politique de la donnée. La ville intelligente est un enjeu majeur et la mutualisation de la data sera au cœur des futures politiques publiques. L'EPCI semble être l'échelon adapté avec les syndicats mixtes départementaux du numérique ou de l'énergie à mener ce portage collectif.

L'Etat travaille sur plusieurs programmes en lien avec la modernisation de l'administration et de la transformation digitale. Les collectivités locales doivent prendre part à ces chantiers et s'organiser pour être proactives et moteur. La data est source de richesses à moyen et long-terme. En attendant, les communes et les EPCI, les Métropoles devront faire le choix d'investir pour anticiper ce virage culturel dans leurs pratiques. Humainement avec le recrutement de profils transverses capables d'accompagner les métiers, mais aussi financièrement pour installer des infrastructures performantes et sécurisées de gestion de la donnée.

Les données des citoyens sont notre patrimoine national. Il faut les protéger mais aussi les considérer comme une ressource infinie au service de nos territoires, de nos administrations publiques et de notre population. Ce sujet sera, me semble-t-il, l'un des sujets prioritaires du prochain mandat local.

Anne le Henanff
Adjointe au Maire de Vannes en charge de la communication et du numérique, Vice-présidente de l'association nationale Villes Internet

LE RGPD, PHASE 2

Pour ceux qui en douteraient encore, la toute récente décision de sanction de Google LLC (soit la société américaine et non sa filiale française) par la CNIL en raison du non-respect des règles posées par le RGPD démontre bien que nous sommes aujourd'hui passés dans la phase 2 de l'ère « RGPD ».

Rappelons que ce texte européen, le Règlement Général sur la Protection des Données est entré en application le 25 mai 2018, deux ans après son adoption. Il renforce fortement le cadre européen applicable à la protection des données à caractère personnel, dont la loi du 6 janvier 1978 en France (pour plus de détails, voir notamment l'article du cabinet ATIPIC Avocat). Notons à cet égard que la loi française a été modifiée par l'ordonnance du 12 décembre 2018 après une première modification pendant l'été 2018, notamment à des fins de lisibilité afin que le totem que représente la loi du 6 janvier 1978 regroupe dorénavant dans un seul texte les règles issues du RGPD mais également les règles d'adaptation en droit français nécessaires, ainsi que les spécificités que le législateur français avait tenu à y apporter[1].

La définition de ces données étant très large, le texte concerne la majorité des bases de données que les entreprises ou les entités du secteur public sont amenées à constituer. Si les fortes sanctions pouvaient inciter à une mise en conformité rapide, certains auguraient qu'elles ne seraient jamais appliquées à ce niveau (jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, ou 20 millions d'euros pour les entités étant dépourvus de CA tels que les associations et les collectivités territoriales). Le niveau de sanction inédit de Google (50 millions d'euros) et le fait que la sanction ne porte que sur une toute petite partie des sujets de la plainte originelle (l'instruction des autres sujets perdurant) incitent maintenant à penser le contraire et à s'inscrire volontairement dans la conformité.

Certes, les sénateurs avaient tenté, pendant l'été 2018 et la modification de la loi du 6 janvier 1978, non seulement d'exclure toute sanction financière pour les collectivités territoriales, mais également de les faire bénéficier d'une taxe payée par les opérateurs de communication électronique pour les aides à se mettre en conformité. Mais l'initiative n'a pas été suivie d'effet et les collectivités territoriales qui n'auraient pas déjà été sur le chemin de la conformité par rapport à une loi existant depuis 1978 doivent aujourd'hui, 40 ans après, consentir de nombreux efforts pour rattraper leur retard et se mettre au niveau d'exigence de conformité actuelle.

Surtout que la conformité au RGPD n'est pas que juridique, elle nécessite l'apport coordonné de plusieurs expertises pour agir sur trois piliers essentiels : organisationnel, technique et juridique.

Seule une approche intégrant ces trois aspects permet de mettre en œuvre de façon efficace les principes découlant du RGPD, étant entendu que la plupart des collectivités territoriales ont déjà, heureusement, un acquis sur le sujet sur lequel s'appuyer :

- cartographie des traitements existants ;
- identification des données traitées ;
- détermination des fondements juridiques permettant leur traitement ;
- création / mise à jour d'un registre des traitements ;
- transparence des informations à communiquer ;
- construction et sécurisation de traitements orientés « privacy by design » ;
- documentation de l'ensemble de la chaîne de traitement et des décisions prises ;
- nomination obligatoire de Délégués à la Protection des Données (DPD/DPO) pour les entités du secteur public ;
- réalisation d'études d'impact sur la vie privée dans les cas où les traitements ont les conséquences les plus graves pour les personnes ;
- création des processus de notification des violations de données personnelles ;
- développement de solutions de portabilité des données dans les cas qui le nécessitent ;
- etc.

Les relations avec les sous-traitants doivent également, dans la plupart des cas, être revues, notamment au niveau des processus achat : en effet, le RGPD impose de ne sous-traiter le traitement des données qu'à des opérateurs économiques eux-mêmes conformes au RGPD.

Par ailleurs, si cette conformité est un chantier d'importance, le RGPD ne doit pas être l'arbre cachant la forêt des autres textes récents ou à venir en matière de protection des données ou de sécurisation du système d'information : Code de la défense pour les Opérateurs d'Importance Vitale (via la Loi de Programmation Militaire 2013), loi du 26 février 2018 pour les Opérateurs de Services Essentiels et les Fournisseurs de Service Numérique (transposition de la directive NIS), projet de règlement européen ePrivacy en cours de discussion, obligations spécifiques aux secteurs de la santé, des paiements électroniques ou encore des opérateurs de service de confiance, etc.

Face à cette vague de fond réglementaire, il est indispensable d'anticiper la mise en conformité afin d'éviter de multiplier les budgets et de diluer l'efficacité. L'anticipation est d'autant plus nécessaire que les mécanismes imposés (directement ou indirectement) par le RGPD sont appelés à s'inscrire dans la durée.

Et si l'on connaît l'objectif, les nombreux retours d'expérience permettent d'être attentif sur les points pouvant apparaître comme bloquants ou à anticiper : les contraintes budgétaires, la nécessaire sensibilisation des élus, le soutien indispensable de la Direction Générale des Services dans la promotion de la conformité RGPD, la chantier du partage de responsabilité dans les écosystèmes d'échanges de données (INSSE, préfecture, police, trésor public), le croisement avec les autres impératifs réglementaires (CADA, etc.), la multiplicité des autres sujets d'intervention au quotidien, etc.

Heureusement, conformité ne rime plus forcément avec budgets très importants : les collectivités territoriales peuvent ainsi s'appuyer sur des solutions permettant de mutualiser les organisations ou les travaux à mettre à œuvre (DPD externe mutualisé, clauses contractuelles, sécurisation technique, etc.). Et surtout, la conformité RGPD, si elle est souvent vue comme une contrainte, recèle d'importantes opportunités : quand les données sont mieux maîtrisées et les citoyens mieux informés sur les traitements, l'optimisation et la meilleure connaissance des citoyens permet l'optimisation des services qui leur sont proposés, au bénéfice de tous.

François Coupez
Avocat-fondateur
d'Atipic Avocat

[1] *Enfin, sur les 99 articles de ce texte, 56 peuvent donner lieu à des règles spécifiques en droit local.*

LA RÉGION **AUVERGNE-RHÔNE-ALPES,** UNE RÉGION PLEINEMENT **IMPLIQUÉE DANS LA CYBERSÉCURITÉ**

Face à la diversification et à l'intensification des usages numériques, la cybersécurité est devenue un enjeu majeur. Aujourd'hui, plus de 75%[1] des Français possèdent un smartphone et se rendent quotidiennement sur Internet. Les relations avec les acteurs publics n'échappent pas à cette évolution puisque près de 70% des citoyens s'adressent aux administrations par le biais de sites ou d'applications. Il est en effet désormais possible de déposer un dossier d'allocations, de recherche d'emploi, une demande d'autorisation ou de subventions de manière dématérialisée. Si elles permettent notamment des gains de temps, ces procédures exposent les organismes publics et privés, tout comme les individus, à de nouveaux risques. Or la sécurité et l'intégrité des données échangées est indispensable pour instaurer et maintenir un haut niveau de confiance numérique. Elles nécessitent donc une vigilance accrue.

De par le large éventail de ses missions (transports, lycées, formation, économie ...), la Région Auvergne Rhône-Alpes est pleinement concernée par cette question. Elle a ainsi souhaité élaborer une stratégie globale intégrant à la fois ses enjeux internes en tant que collectivité territoriale, mais aussi une diffusion en externe sur l'ensemble de son territoire.

Pour répondre aux problématiques d'e-administration et de confiance numérique, la Région a intégré la notion des usages aux prérogatives « techniques » de sa Direction des Systèmes d'Information. Cela s'est traduit également par la nomination d'un Délégué à la Protection des Données et par la mise en place d'une cellule pour la Sécurité des Systèmes d'Information et la refonte de sa politique de sécurité. Certaines des actions engagées s'inscrivent dans un contexte de réponse à de nouvelles contraintes et de nouvelles réglementations telles que le RGPD[2] ou la directive SRI[3] qui se sont imposées aux administrations. D'autres relèvent d'une politique volontariste, comme les initiatives à destination des acteurs économiques par exemple.

En effet, si la Région s'appuie sur de nombreux partenaires locaux et nationaux et peut compter sur le soutien d'agences spécialisées (CNIL[4] , ANSSI[5]), elle a bien identifié la nécessité que le monde économique, comme les citoyens, s'approprient plus largement ces thématiques. C'est pourquoi, le Conseil régional accompagne une politique de développement numérique ambitieuse à l'échelle des territoires. Plusieurs initiatives ont été lancées comme la mise en œuvre d'un plan de transformation numérique, mais aussi le soutien de structures de formation et d'accompagnement.

La plateforme Ma-solution-numérique.fr fait partie des outils qui ont été mis en œuvre pour favoriser la prise de conscience autour des enjeux de transformation numérique dans les TPE-PME. Elle intègre des ressources variées provenant de différents partenaires[6] et notamment des fiches, des témoignages, des documents types ou des guides sur la cybersécurité. Le programme d'aide Ambition PME est un autre volet de cet accompagnement. Il a permis à plus de 150 entreprises d'accéder à un soutien au développement numérique et à la cyber protection, par des financements allant de 4 000€ à 9 000€ par entreprise pour un retour sur investissement de respectivement 15 000€ (ratio 1 pour 3) et de 40 000€ (ratio 1 pour 4). La Région prend en charge jusqu'à 80% de l'accompagnement des entreprises.

L'engagement de la Région Auvergne-Rhône-Alpes sur la cybersécurité et la souveraineté numérique se concrétise également dans les démarches de relocalisation des moyens, des compétences et des savoirs. L'accompagnement de la collectivité sur les mises en services des Data-centers XSalto (Seyssinet-Pariset, 2016) et Rock (Lyon, 2019) contribuent à doter la Région d'infrastructures de qualité, garantissant la conservation des données sensibles au niveau local, pour mieux se protéger des cybermenaces.

Alors que la majorité du trafic Internet du pays dépend des GIX parisiens, Auvergne-Rhône-Alpes a décidé de privilégier l'échange au niveau local. La Région est ainsi un partenaire historique des deux GIX (nœuds d'échange Internet), Rezopole et MassifIX auxquels elle a attribué près de 3 millions d'euros. Cette offre permet la mise en concurrence des opérateurs, et donc la baisse des coûts pour les communications Internet, mais aussi une diversité dans les propositions des opérateurs. La volonté de développer des compétences sur ces sujets en proximité contribue également au renforcement de la cybersécurité. Disposer de plusieurs nœuds d'interconnexions Internet permet en effet d'apporter résilience et indépendance techniques et offre une capacité naturelle à limiter les menaces qui peuvent peser sur ces infrastructures essentielles.

Enfin, une politique publique de cybersécurité efficace consiste aussi (et avant tout) à prévoir les besoins à venir en matière d'emploi et de formation. La Région Auvergne-Rhône-Alpes a pour ambition de devenir une Région leader et un accélérateur du numérique en Europe. Pour répondre à ces objectifs, la Région s'est dotée d'un outil unique : le Campus Région du Numérique. Installé sur un terrain de plus 10 hectares à Charbonnières-les-Bains courant 2020, ce « navire amiral » permettra de passer à l'échelle l'initiative du King Charles lancé à Lyon en 2017, et constituera une plateforme d'échange entre les écoles et les entreprises du territoire. Le Campus s'articule autour de trois grands axes : la formation, l'accompagnement et le conseil aux entreprises dans leur transformation numérique et la mise en place d'une usine de recherche et d'innovation. Tout cela repose sur l'articulation et la démarche partenariale entre la Région et tous les acteurs du territoire : CCI, CMA, MEDEF, CPME, etc. Le Campus du Numérique ne se réduit pas à un seul lieu : il s'étend sur tout le territoire d'Auvergne-Rhône-Alpes. Les futurs talents pourront en effet collaborer directement avec les employeurs locaux, notamment par le biais de plus de 35 formations labellisées « hors-les-murs ». Ces formations opèrent un maillage fin du territoire, proposent un large panel de formations aux métiers de la filière numérique et font du Campus Région un projet unique de diffusion de la culture numérique et d'accélération de la transformation numérique des entreprises. On compte parmi celles-ci notamment le Certificat Préventeur Cybersécurité des Systèmes d'Information de l'INP de Grenoble ou encore le master MISTRE (Microélectronique Intégration des Systèmes Temps Réel Embarqués). Les collaborations qui ne manqueront pas d'émerger favoriseront l'innovation, l'accompagnement et l'émergence de pôles d'excellence sur la cybersécurité industrielle en Auvergne-Rhône-Alpes.

A travers ces actions, la Région entend consolider son rôle, sa volonté de leadership et son rayonnement à l'échelle locale et européenne. Cela passera nécessairement par l'émergence et le renforcement d'acteurs d'excellence autour des problématiques de cybersécurité et par la consolidation des collaborations et partenariats public-privé. Par ailleurs, la sécurité et la souveraineté numériques ne peuvent être envisagées que dans le cadre d'une approche systémique, raison pour laquelle des actions d'acculturation et d'accompagnement des populations et des entreprises doivent aussi être mises en œuvre. Au-delà des outils et des techniques, les question d'« hygiène numérique » sont primordiales. Pour prendre un exemple très concret, le meilleur antivirus ne protège pas des risques liés à l'absence ou au trop faible niveau de protection d'un mot de passe à l'ouverture de la session d'un ordinateur. La vulnérabilité d'un système peut se situer à des niveaux très divers et un des maillons du système peut provoquer la défaillance de l'ensemble par manque de précautions et de cloisonnement. Ce sont donc les usages quotidiens et l'adhésion de l'ensemble des utilisateurs à ces bonnes pratiques qui doivent être pensés en parallèle de la mise en place des outils. Avec l'apparition d'environnements de plus en plus interconnectés (développement de capteurs pour la « *smart cities* » ou territoires intelligents, véhicules autonomes, industrie 4.0 ...), le couple « outils et usages » devient de plus en plus impérieux à mettre en place. De ce fait, il devient

indispensable de diffuser largement une culture numérique dans la société française, une meilleure compréhension des enjeux qui entourent les évolutions en cours. Le numérique n'est pas seulement une révolution technique et technologique. C'est avant tout une transformation culturelle et sociétale. Les usages doivent donc être éclairés et discutés au plus tôt. C'est notamment pour cette raison que le Conseil régional a initié une exposition itinérante dans les lycées pour sensibiliser aux nouveaux métiers et nouvelles compétences, mettre en lumière la question de l'identité numérique et des enjeux de mixité dans ces métiers. 4 000 lycéens et lycéennes ont d'ores et déjà été sensibilisés. L'objectif est de parvenir à 6 000 cette année.

En matière de cybersécurité, le rôle des collectivités locales, et plus particulièrement de la Région, est varié : penser ses propres pratiques, accélérer le déploiement d'infrastructures structurantes comme le très haut débit, favoriser la prise de conscience des entreprises en matière de transformation numérique, accompagner les citoyens dans la compréhension des enjeux sociétaux ... Les collectivités locales doivent être capables d'intégrer de la prospective dans leurs politiques, de se doter des compétences en interne pour analyser et comprendre les mutations en cours. Elles doivent - en fonction de leurs compétences respectives - être des tiers de confiance, proposer des lieux de médiation et d'apprentissage numériques, impulser la création de filière de formation... C'est à ces conditions qu'elles pourront être protectrices (des données et plus généralement des libertés) et forces de proposition dans les années qui viennent.

Juliette Jarry
Vice-Présidente de la Région Auvergne-Rhône-Alpes, déléguée aux infrastructures, à l'économie et aux usages numériques

[1] *Source : Baromètre du numérique 2017, Arcep (https://www.arcep.fr/uploads/tx_gspublication/barometre_du_numerique-2017-271117.pdf)*
[2] *Texte européen : Règlement Général pour la Protection des Données*
[3] *Directive européenne sur la Sécurité des Réseaux et de l'Information*
[4] *Commission Nationale Informatique et Libertés*
[5] *Agence Nationale pour la Sécurité des Systèmes d'Information*
[6] *Les partenaires de la Région Auvergne-Rhône-Alpes pour la plateforme Ma Solution Numérique sont : Auvergne-Rhône-Alpes Entreprises, la CCIR Auvergne-Rhône-Alpes, la CRMA Auvergne-Rhône-Alpes, la CPME Auvergne-Rhône-Alpes, le cluster Digital League, l'ENE (Entreprises & Numérique), le Medef Auvergne-Rhône-Alpes et Minalogic*

LES COLLECTIVITÉS SONT UN DES PILIERS CLÉ DE LA SÉCURITÉ NUMÉRIQUE SUR LES TERRITOIRES

Du plus près du citoyen à la mairie jusqu'aux échelons régionaux, les collectivités tiennent une place importante et sont un enjeu de sécurité à la fois comme victimes potentielles de cyberattaques et de cybermalveillance, et comme premier interlocuteur et référence quotidienne des citoyens en demande de confiance et d'accompagnement aux usages numériques.

Les collectivités territoriales rassemblent un nombre important d'informations et de données sensibles pour la vie privée des citoyens et la marche de la Cité. État-civil, données sociales, applications liées à l'urbanisme et aux services publics : les données collectées, traitées et conservées par les collectivités quel que soit leur niveau de maturité numérique ont besoin d'être protégées et sont susceptibles d'être convoitées par des attaquants. La sécurisation des systèmes d'information des collectivités, soit de façon autonome soit par mutualisation locale, est cruciale. L'ANSSI produit à cette fin des guides et recommandations qui sont essentiels à suivre.

Mais la sécurité du numérique n'est rien sans la montée en compétences de l'ensemble des utilisateurs et notamment de ceux qui, dans les collectivités, vont manipuler ces données sensibles au quotidien ou qui, de par leurs fonctions, sont en situation de vulnérabilité car ils ont accès à de nombreuses données sensibles.

Ces personnels, élus ou agents des collectivités, sont donc un public à sensibiliser de façon prioritaire, en prenant en compte leurs spécificités, leurs métiers, leur hétérogénéité. Maires, directeurs généraux de services, secrétaires de mairies, ils ne sont pas et n'ont pas à devenir des experts en cybersécurité. Mais il faut prendre conscience que la résilience des collectivités territoriales en matière de sécurité numérique passe largement par eux.

Le dispositif Cybermalveillance.gouv.fr, qui porte dans ses missions la sensibilisation des utilisateurs, particuliers comme professionnels, travaille avec les associations d'élus et de collectivités pour produire des contenus de sensibilisation en prenant en compte les problématiques des collectivités territoriales.

Les collectivités sont également le lieu où le citoyen, confronté à la rapide transition numérique et à la dématérialisation massive des processus administratifs, va chercher conseil et aide.

Les agents et élus ont un rôle de médiation crucial à l'heure où l'inclusion numérique est une problématique d'importance nationale. Si les citoyens ne maîtrisent pas les fondamentaux de la sécurité numérique, ils ne peuvent avoir confiance et s'approprier la transition numérique et les démarches dématérialisées.

La plateforme Cybermalveillance.gouv.fr est là pour outiller dans la sensibilisation et l'accompagnement des élus, des agents et des citoyens. Veille, assistance, alertes, bonnes pratiques, elle est un outil au service de ses publics et utile au quotidien à l'écosystème d'accompagnement des collectivités territoriales vers davantage de sécurité du numérique , et donc de confiance.

Adrienne Charmet
Chargée de Mission Relations institutionnelles à Cybermalveillance.gouv.fr

SÉCURITÉ NUMÉRIQUE DES TERRITOIRES : CONTRAINTE OU OPPORTUNITÉ ?

Difficile de parler de sécurité numérique pour les territoires sans paraphraser les nombreuses publications sur ce sujet, à commencer par les miennes.

Au travers de cet article, volontairement court, j'ai souhaité aborder le sujet de la sécurité numérique sous l'angle « positif » et non sous celui trop souvent mis en avant, celui des enjeux, des risques et des réglementations uniquement.

Bien évidemment, nous ne le répéterons jamais assez, la sécurité numérique est une nécessité pour le bon fonctionnement des territoires, la sécurité et la confiance que ses habitants, ses entreprises et associations leur accorderont. Les efforts à fournir en matière de sécurité numérique sont incontournables, c'est une certitude. Certains l'ont malheureusement appris à leurs dépends, suite à un incident, d'autres sous l'impulsion de la réglementation.

Contrainte ou opportunité ?

La première approche de la sécurité numérique soulève généralement la question des obligations : que faut-il faire pour être conforme à la réglementation ? Le volet opportunité n'est malheureusement que très rarement évoqué.

Saisissons cette chance formidable de (re)valoriser et (re)dynamiser les territoires au travers, entre autre, du numérique et de ses nombreux services.

Un des facteurs de succès pour cela réside dans l'acceptation, par les habitants des territoires, des nouveaux usages que confère le numérique. La sécurité numérique contribue fortement à cette acceptation puisqu'elle est une condition indispensable pour construire la confiance, élément fondamental de tout développement numérique, toute transformation numérique, que tous, nous vivons quotidiennement.

Mais la sécurité numérique souffre d'un manque cruel de ressources. Peu de formations préparent à ces nouveaux usages et à ces nouveaux métiers, absolument essentiels au développement d'un numérique de confiance. Toutes les études consacrées à ce sujet annoncent des chiffres vertigineux quant au besoin de « main d'oeuvre » et de « matière grise » dans le domaine de la sécurité numérique et plus largement celui du numérique.

Cette situation de pénurie et de marché en tension est une véritable opportunité de développer des formations portant sur la sécurité numérique et plus largement sur la confiance numérique, procurant ainsi un véritable facteur d'attractivité pour les entreprises et les étudiants d'un territoire.

Première opportunité : un investissement pour l'avenir qui adresse les problématiques fortes des compétences.

Les formations peuvent se présenter sous différents formats : longues ou courtes, initiales ou continues, diplômantes ou non, etc. Elles peuvent s'ouvrir à de multiples profils tels que des étudiants ou des employés. Mais les besoins de formation, d'information ou de sensibilisation comme cela est parfois évoqué, concernent tous les habitants d'un territoire sans exception. Tous utilisent volontairement ou non le numérique, ne serait-ce que pour les démarches administratives aujourd'hui dématérialisées.

De ce fait, il serait nécessaire d'impliquer les habitants, les entreprises et organisations, dans les réflexions sur la transformation numérique et les besoins en « formation » pour qu'ils deviennent acteurs et non plus de simples utilisateurs. Aider ces acteurs à opérer leur propre transformation numérique au travers de conseils, de séances d'informations et de kit sur la sécurité numérique profitera à tous et renforcera l'acceptation de cette transformation sans précédent qu'est le numérique.

Deuxième opportunité : reconnecté les habitants à leur territoire en les impliquant dans les questions de numérique et de sécurité numérique.

Mais, ne nous voilons pas la face, le coût annoncé de la sécurité numérique freine trop souvent les initiatives voire empêche la prise d'initiative et l'engagement de projet au niveau des territoires. Pourtant, comme la qualité, ou comme les 35h (certains s'en souviendront), la sécurité numérique est une opportunité de repenser les usages et de se concentrer sur les vrais besoins pour un territoire. C'est aussi une opportunité de repenser les organisations et la manière de traiter la question du numérique et ceci, afin de ne pas tomber dans le travers de développement de solutions numériques coûteuses ou inadaptées.

Repenser la manière de traiter la question du numérique est fondamental car pour reprendre un slogan des années 70, « on n'a pas de pétrole, mais on a des idées ». Pour cela, opter pour une approche unifiée, mutualisée et cohérente de la sécurité numérique englobant l'ensemble des systèmes numériques et des données d'un territoire est nécessaire. Cette approche oblige à une meilleure identification des besoins, une meilleure connaissance de ses systèmes et une meilleure maîtrise de ses fournisseurs. Par conséquent, cette approche « maîtrisée » au juste besoin contribuera à une meilleure maîtrise des coûts liés au numérique et de fait, libère des budgets pour la sécurité numérique.

S'il est difficile d'avancer un chiffre en termes de retour sur investissement de la sécurité numérique, une approche « maîtrisée » limite les coûts à 1 % du budget d'une installation voire moins, que ce soit en fonctionnement ou en investissement. C'est en cela aussi que la sécurité numérique est une opportunité.

Troisième opportunité : « La sécurité numérique abordée comme une source d'économie ». Qui oserait un tel slogan ? Et pourtant… La sécurité numérique est aussi un outil au service de l'efficacité.

Traiter le numérique en intégrant dès le départ la dimension sécurité facilitera la mise en conformité des territoires aux différentes réglementations portant sur la confiance et la sécurité numérique. Mais, là encore, l'enjeu est bien au-delà de la réglementation. Renforcer la sécurité et la résilience numérique d'un territoire par quelques efforts (les fameux 1 % du budget évoqués précédemment) favorisera l'arrivée de nouvelles entreprises, de nouveaux investisseurs, de nouveaux habitants. Personne n'envisagerait aujourd'hui de s'installer dans une zone n'offrant pas un minimum de sécurité (dans le sens sûreté) où des vols et agressions sont nombreux. Demain, il en sera de même pour la sécurité numérique. Personnes ne voudra investir dans un territoire peu sûr. Oui au SmartTerritoire si ce SmartTerritoire est un SafeTerritoire.

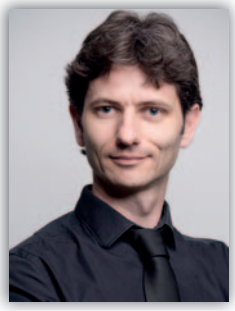
Quatrième opportunité : développer l'attractivité d'un territoire en créant des territoires de confiance sur le plan numérique, des safeTerritoires.

Si les « grands » territoires appliquent ou peuvent appliquer ces quelques propositions, la question se pose pour les plus petits. En particulier pour challenger intelligemment ses fournisseurs en s'appuyant sur des exigences de sécurité numérique, il faut être suffisamment important en terme de chiffre d'affaire pour ces derniers.

Se parler entre territoires, partager les expériences, mutualiser les ressources et regrouper les efforts constituent sans nul doute une première réponse efficace. « Agir efficacement ensemble ! ».

L'objectif de ce court article était d'aborder la sécurité numérique sous un autre angle, celui des opportunités qu'elle génère au travers du développement de formations attractives et bénéfiques à tous, des sources d'économies potentielles et surtout du repositionnement de l'humain au cœur de la problématique numérique et sécurité numérique. Reconnecter les habitants aux territoires dans un monde sans cesse toujours plus virtuel. Au delà des questions de confiance et de toutes les problématiques de sécurité, parfois effrayantes, ne le cachons pas, le numérique suscite une réflexion sociale et sociétale, quant à la place de l'humain. Soyons persuadé que l'humain demeure un maillon fort également sur les questions de sécurité numérique.

Stéphane Meynet
Président
de CERTitude NUMERIQUE



CYBERCERCLE FORMATION : UN CADRE DE CONFIANCE POUR FORMER À LA SÉCURITÉ NUMÉRIQUE

Dans le prolongement de l'action qu'il mène depuis 2011 pour rendre plus appréhendables la sécurité numérique, ses enjeux, son cadre institutionnel et réglementaire, et ainsi participer à la diffusion d'**une culture de sécurité numérique**, le CyberCercle a créé des **modules de formation** qui permettent d'approfondir ces champs dans un cadre privilégié.

CyberCercleFormation aborde les sujets de cybersécurité dans toutes leurs dimensions et en particulier **stratégiques, juridiques et réglementaires, de gouvernance et organisationnels.**

CyberCercleFormation s'adresse à trois types de publics :

- les **dirigeants de PME-PMI et les cadres dirigeants non spécialistes de la cybersécurité** – directions générales, directions marketing, digital, conformité, service juridique ou ressources humaines – qui souhaitent mieux maîtriser cette nouvelle dimension indispensable aujourd'hui dans leur champ de compétences ;
- les **RSSI** et **DSI** qui désirent mieux maîtriser les **enjeux juridiques et réglementaires** liés à leurs champ d'action et responsabilités ;
- les **élus et cadres territoriaux** qui sont aujourd'hui confrontés à la transformation numérique des territoires et des usages, et qui doivent mieux appréhender la sécurité numérique pour assurer un développement pérenne de leurs actions, notamment pour garantir **la confiance dans les services numériques qu'ils mettent en œuvre au service des citoyens.**

Les modules de formation ont volontairement des **formats courts**, d'une ou de deux journées, afin d'éviter de peser trop lourdement sur les agendas.

CyberCercleFormation propose quatre modules de formations :

- **La cybersécurité au cœur de la transformation numérique des entreprises** pour les Top managers de PME/ETI, professions libérales et activités de conseil
- **La cybersécurité au cœur de la transformation numérique des collectivités** pour les élus, directions des services généraux, directions métiers
- **La cybersécurité des systèmes industriels** pour les Top managers de PME/ETI, directions générales de service de collectivités, directions métiers, acheteurs et juristes
- **Réglementation, juridique et cybersécurité** pour les risques managers, directions de la conformité, Top managers, directions des services généraux

Les formateurs de CyberCercleFormation sont tous des **professionnels** spécialistes de la cybersécurité et dotés de qualités de pédagogue qui leur permettent de transmettre leurs savoirs de façon efficiente, en adéquation avec leur auditoire. Des **représentants des institutions publiques** viennent apporter un éclairage sur des sujets définis, permettant aux participants un accès à une expertise institutionnelle et un échange personnalisé avec les représentants de l'État en charge de ces questions.

En parallèle des **sessions inter-entreprises** qui seront mises en place à partir de janvier 2019 à Paris et en région, notamment en Auvergne-Rhône-Alpes, le CyberCercle peut **définir et mettre en œuvre des formations et séminaires au sein de votre organisation**, en les adaptant aux besoins et aux profils de vos collaborateurs.

cybercercle.com

LE CYBERCERCLE : UN CADRE DE CONFIANCE POUR DÉCRYPTER LES ENJEUX STRATÉGIQUES DE LA SÉCURITÉ NUMÉRIQUE

Réalisation impression : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

Créé en 2011, le CyberCercle est un cercle de **réflexion, d'expertise et d'échanges** sur les questions de la confiance et de la sécurité numérique, placé sous la dynamique de parlementaires et d'élus locaux, avec le soutien des institutions de l'Etat en charge de ces questions.

Plate-forme favorisant le **dialogue public-privé**, il est un **cadre de confiance** à destination de l'ensemble des acteurs aujourd'hui **concernés par le numérique** et de ceux qui s'engagent **dans des programmes de transformation numérique** - entreprises, organismes publics ou collectivités. Il leur permet ainsi de mieux appréhender les dimensions de sécurité numérique indispensable à leurs activités, de décrypter les politiques publiques, françaises et européennes qui les concernent, tout en leur permettant de se créer un réseau de confiance sur ces sujets.

Dans cet objectif, le CyberCercle organise depuis 2012 **des petits-déjeuners-débats mensuels** à Paris et à partir du second semestre 2019 en région Auvergne-Rhône-Alpes.

Il a également créé depuis 2013 des **journées de rencontres à Paris ou en région**, événements fédérateurs qui rassemblent les acteurs institutionnels et privés de la cybersécurité et l'écosystème sectoriel ou local concerné :

- les Rencontres Parlementaires de la Cybersécurité **#RPCyber dont la 7ème édition se déroulera en novembre 2019 à Paris** ;
- des Rencontres territoriales dans le cadre du **Tour de France de la Cybersécurité** lancé en janvier 2018. En 2019, le #TDFCyber fera ainsi étape à **Bourges, Pau, Toulon, Lannion, Dijon, Lyon et Nantes** ;
- des Rencontres sectorielles, et notamment celles sur le maritime avec les Rencontres Parlementaires Cybersécurité & Milieu Maritime et les Rencontres Sécurité Numérique - Sécurité Portuaire (SNSP). Prochain RDV : la 5ème édition des #RPCyberMaritime le 28 juin 2019 à Lannion.

Le CyberCercle édite également une lettre d'information **« Cybersécurité et Politiques Publiques »** qui traite à chaque numéro d'un sujet déterminé, à travers des articles courts rédigés par des experts et accessibles à tous. Après les numéros sur le **maritime** et les **collectivités territoriales**, les deux prochains seront dédiés aux **objets connectés** (2ème trimestre 2019), à la **santé** (3ème trimestre 2019) et à l'**Europe** (4ème trimestre). Un numéro spécial **dédié au TDFCyber2019** viendra clôturer cette année.

La Lettre Cybersécurité & Politiques Publiques est éditée par le CyberCercle.
Directrice de la Publication : Bénédicte Pilliet

20 rue Tronchet - 69006 Lyon • contact@cybercercle.com • cybercercle.com • @CyberCercle