BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

Guide pratique pour une collectivité et un territoire numérique de confiance

AVANT-PROPOS

Quel élu ne s'est pas entendu demander si sa collectivité compte opérer une transformation numérique ? Ou, tout simplement, de quelle façon les services de sa collectivité vont s'informatiser ?

L'idée de ville numérique semble de nos jours incontournable. Comment l'appréhender toutefois ? Rendre sa collectivité numérique, l'informatiser, va de pair avec une technicité et une complexité qui peuvent rebuter de prime abord. Pourtant, la maîtrise de cette évolution est cruciale ! Les préoccupations du législateur avec les récentes réglementations en matière de données personnelles (RGPD) et d'ouverture des données (« Open Data ») le démontrent.

L'actualité quotidienne illustre la nécessité de cette maîtrise du numérique, plus particulièrement sous l'angle de la cybersécurité. On ne compte hélas plus les exemples de villes dans le monde que des cyberattaques ont momentanément paralysées. En France, c'est plus de 1200 collectivités qui ont été la cible d'attaques en 2019. Sans même parler de cybermenace, le redouté « bug », qui peut être une panne ou une simple maladresse, peut suffire à mettre à plat des services numériques à la conception parfois fragile.

Grandes, médianes ou petites, toutes les villes et intercommunalités sont concernées par cette problématique de « confiance numérique », ainsi que les départements et les régions. C'est notamment vrai au travers de services d'état civil, d'urbanisme, de gestion administrative déjà largement digitalisés. Et toutes ces collectivités le seront de plus en plus au fur et à mesure que s'informatiseront leurs infrastructures de transport, énergie, eau et télécommunications, leur signalisation routière, leur éclairage, leurs systèmes de vidéoprotection, etc. Le contexte de la crise sanitaire actuelle accélère cette transition, et rend cette question de confiance plus urgente encore.

Face à cet enjeu crucial qu'est la confiance numérique, il est de la responsabilité de l'élu d'impulser la dynamique qui seule permet à la collectivité de mettre en place un projet cohérent, maîtrisé et sûr. A cette fin, il n'est nul besoin que l'élu comprenne les rouages techniques du sujet : il doit même accepter de ne pas être un expert. Il lui faut cependant définir le cap et mobiliser ses cadres et agents territoriaux.

Répondre à cet enjeu est l'objet de ce guide, qui ambitionne de donner aux élus les clés qui permettront à leurs collectivités d'aborder cette problématique de la meilleure des manières. Synthétique (treize pages hors fiches pratiques) et destiné aux non-initiés, il vous informera et vous plongera dans différentes situations pour vous faire appréhender le sujet, ses enjeux en matière de risques et de responsabilités, et les premiers réflexes à mettre en œuvre pour offrir aux citoyens des services de confiance. Pour aller plus loin, les perspectives sur les défis à venir seront également évoquées, ainsi que trois fiches pratiques proposant des compléments pertinents.

Ce guide a été conçu par la Banque des Territoires, l'un des cinq métiers de la Caisse des dépôts, qui rassemble dans une même structure les expertises internes à destination des territoires. Il n'aurait pas pu voir le jour sans le soutien précieux de son comité stratégique que nous remercions chaleureusement, composé d'associations d'élus, d'industriels et d'administrations, dont l'ANSSI et le groupement d'intérêt public Cybermalveillance.gouv.fr.

Nous espérons qu'il trouvera auprès de vous, acteurs des territoires, sa pleine et entière utilité.

SOMMAIRE

1- Introduction 6

Un guide pour les élus des collectivités 7

Un guide pour maîtriser le risque numérique, afin d'offrir aux citoyens des services numériques de confiance 7

2- Collectivités et confiance numérique : de quoi parle-t-on ? 9

Qu'est-ce que le numérique dans les collectivités ? Qu'est-ce que la ville numérique ? 10

Qu'est-ce que la confiance numérique ? Qu'est-ce que la cybersécurité ? 10

Confiance numérique appliquée à la ville : de quoi s'agit-il ? 11

3- Quels risques et responsabilités pour les collectivités, agents et élus ? 13

Quel cadre juridique en matière de confiance numérique ? 14

Quels risques induits, pour quelles conséquences ? 14

Quelles responsabilités pour les collectivités et leurs agents ? 15

Quelle responsabilité pour les élus et les prestataires de la collectivité ? 15

4- Que faire en tant qu'élu ? Les grands principes à porter 17

Le premier rôle de l'élu : impulser l'effort collectif 18

Se forger une vision globale et définir des priorités 18

Mener des projets numériques fiables et pérennes 19

Maîtriser la ville numérique au quotidien 20

Être prêt au pire et savoir réagir 21

Projets numériques : quels points exiger ? 23

5- Collectivités et confiance numérique : les défis à venir 24

Après le RGPD et l'*Open data*, quels futurs défis réglementaires ? 25

La mutualisation des initiatives et des pratiques 25

Standardisation & interopérabilité 25

Nouvelles tendances technologiques : quel niveau de confiance ? 25

Structuration d'une offre de confiance & souveraineté numérique 26

Rôle de la Banque des Territoires 27

6- Glossaire et fiches pratiques 28

Document externe

01

Introduction

Un guide pour les élus des collectivités

La cybersécurité, la confiance numérique : des sujets trop compliqués et trop techniques qui ne peuvent être traités que par les spécialistes ? Pas du tout !

De même qu'en matière de sécurité classique, les élus échangent avec les forces de l'ordre pour définir les priorités d'action alors qu'ils ne sont pas des spécialistes de ce domaine, de même il leur appartient de s'emparer du sujet de la confiance numérique pour définir avec le soutien des experts les grandes orientations à suivre.

La Banque des Territoires est convaincue que la transition numérique des collectivités doit être impulsée et suivie par les élus, et qu'il est ainsi de leur devoir de définir des objectifs de sécurité numérique adaptés. En matière de données personnelles, le règlement général européen sur la protection des données personnelles (RGPD) ne dit pas autre chose.

Protéger les données personnelles des citoyens en premier lieu, s'assurer de moyens de secours en cas de défaillance informatique, exiger des sous-traitants une réactivité garantie en cas de crise : autant d'orientations stratégiques relevant du niveau de l'élu.

Ce n'est que dans un deuxième temps qu'interviennent les spécialistes, pour mettre en œuvre ces orientations et proposer des solutions adaptées : les équipes informatiques bien sûr, mais aussi les métiers, juristes, communicants, etc.

Ce guide s'adresse aux premiers responsables, les élus et les DGS, ceux dont l'impulsion est déterminante afin d'obtenir un numérique de confiance.

Un guide pour maîtriser le risque numérique, afin d'offrir aux citoyens des services numériques de confiance

En 2019 en France, plus de 1 200 collectivités sont directement ciblées par des cyberattaques, et on ne compte plus les erreurs involontaires de conception ou de configuration de systèmes d'information qui les affectent.

Or, cette « cyber insécurité » et ces dysfonctionnements numériques des villes et territoires ont un coût, qui croît avec le degré de numérisation des services fournis aux citoyens. Plus les services et les infrastructures sont connectés et pilotables de façon centralisée, plus les citoyens en dépendent, et plus un incident pourra provoquer de dommages et nécessiter du temps et des moyens conséquents pour y remédier.

En l'absence de mesures adaptées, le coût peut se compter en centaines de milliers voire en millions d'euros. Mais il ne saurait se réduire à cette dimension : il est aussi humain, social, politique, et souvent médiatique avec des retentissements qui peuvent s'avérer très négatifs, dans des proportions toujours difficiles à mesurer.

La confiance numérique n'est par nature pas forcément toujours « visible », mais son absence le devient fatalement. A l'inverse, la collectivité pourra utilement valoriser une démarche de confiance numérique auprès des citoyens en expliquant les choix et les mesures qui ont été opérés à leur bénéfice.

Ce guide est conçu pour répondre à cette problématique clé et donner aux élus les premiers outils leur permettant de faire face aux enjeux. S'il peut être vu comme un « guide de survie » pour les collectivités et les territoires face aux risques numériques, il représente plus encore le moyen d'offrir aux citoyens un numérique de confiance.

Ce guide s'adresse à toutes les collectivités, celles qui s'informatisent peu à peu tout autant que celles qui réalisent une transformation numérique plus ambitieuse. Les

collectivités qui s'engagent dans la *smart city* ou le *smart territoire* sont également concernées : les principes de ce guide revêtent alors pour elles une dimension capitale.

La confiance numérique, ça se prépare !

Exemples de cyberattaques et de dysfonctionnements

- Erreur humaine : on découvre un vendredi soir que le fichier des élèves de l'école primaire, données personnelles hébergées chez un prestataire réputé fiable, est devenu accessible à tous à la suite d'une mauvaise manipulation.
- Mail piégé : un agent reçoit un mail lui annonçant la livraison d'un colis. Il clique sur la pièce jointe et l'intégralité des ordinateurs de la mairie sont inaccessibles. Une rançon de 100 000 € est demandée pour les débloquer.
- Cybersabotage : les feux de signalisation s'éteignent à la suite d'un piratage informatique, provoquant des accrochages et une désorganisation de la circulation.

Ces exemples, tirés de l'actualité, peuvent être remédiés voire empêchés grâce à la mise en œuvre de mesures adaptées. L'élu a un rôle prépondérant : nul n'est mieux placé que lui pour donner l'impulsion, et mettre en place les conditions nécessaires à un numérique de confiance.

02

Collectivités et confiance numérique : de quoi parle-t-on ?

Qu’est-ce que le numérique dans les collectivités ? Qu’est-ce que la ville numérique ?

Les acteurs publics territoriaux sont tous engagés, à divers degrés, dans une transformation numérique. Un nombre croissant de leurs services sont gérés par des systèmes d’information, et l’immense majorité sont devenus accessibles par internet et les réseaux mobiles.

Concrètement, cela recouvre le site internet de la collectivité, la dématérialisation des échanges avec les citoyens, entreprises et acteurs publics (e-administration), la publication de données territoriales (*open data*) tout autant que la numérisation de l’espace et des services urbains : wifi public, transport, énergie, eau, systèmes de sécurité ou encore qualité de l’air.

La *smart city*, ville numérique ou territoire intelligent, c’est la transition numérique des villes et des territoires « un cran plus loin ». Le territoire recourt alors à la technologie pour améliorer la qualité des services urbains ou encore réduire leurs coûts. Les gains peuvent s’opérer en matière de chaleur, d’énergie, de flux de circulation, de réponse aux besoins des citoyens. Ce faisant, les projets *smart city* font déborder les enjeux numériques au-delà des seuls champs de l’informatique traditionnelle. Notamment grâce aux possibilités offertes par les objets connectés (*IoT*), ils s’étendent aux bâtiments, aux infrastructures, aux espaces publics, au mode de vie des citoyens et aux entreprises. Au gré de cette augmentation numérique, les problématiques de confiance numérique se multiplient et revêtent un caractère encore plus crucial encore.

Qu’est-ce que la confiance numérique ? Qu’est-ce que la cybersécurité ?

La cybersécurité, c’est un niveau de sécurité que l’on cherche à atteindre pour des systèmes et des données numériques afin de se prémunir contre les menaces cyber (cyberattaques) que l’on redoute le plus. En effet, la sécurité à 100 % n’existe pas !

Quelles sont les principaux types de cyber-attaques ?

Ci-dessous sont recensées certaines cyber-attaques parmi les plus courantes chez les collectivités. On notera que certaines d'entre elles peuvent se recouper.

- Rançongiciel/*ransomware* : virus informatique qui rend indisponible un système et des données tant qu'une rançon n'a pas été payée
- Défiguration/*defacement* : piratage d'un site Internet visant à modifier son apparence et ses messages
- Fraude au président : moyen consistant à se faire passer (de façon numérique ou non) pour un dirigeant d'une organisation afin d'en obtenir un avantage, le plus souvent obtenir le virement d'une somme conséquente
- Hameçonnage/*phishing* : cyberattaque consistant à appâter (hameçonner) une personne pour lui faire exécuter une action nuisible, comme l'ouverture d'une pièce jointe corrompue ou d'un lien pointant vers un site malveillant
- Cyber-sabotage : cyberattaque visant à rendre indisponible ou faire dysfonctionner un système, une infrastructure, un service
- Déni de service (DOS ou DDOS) : attaque contre un site ou serveur Internet, consistant à le saturer de requêtes afin de le rendre indisponible

La cybersécurité est plus précisément une démarche qui, face aux attaques que l'on risque, déploie des mesures de protection efficaces et adaptées, de quatre types :

- mesures organisationnelles : définition d'un cadre de sécurité globale, y compris pour les sous-traitants, incluant la gestion de crise d'origine cyber ;
- mesures juridiques : en premier lieu, le respect des obligations réglementaires ;
- mesures humaines : sensibilisation et formation des agents et administrés ;
- mesures techniques de protection des systèmes et de détection des cyberattaques.

La confiance numérique est un concept qui va plus loin que la seule cybersécurité. Il s'agit d'avoir confiance dans le « numérique », ce qui inclut la cybersécurité mais regroupe de façon plus large la nécessité de solutions numériques fiables et pérennes, associés à une gestion maîtrisée des systèmes, des données et des identités numériques.

Confiance numérique appliquée à la ville : de quoi s'agit-il ?

La confiance appliquée à la ville numérique, c'est d'une part diminuer le risque qu'un dysfonctionnement se produise, qu'il résulte ou non d'une cyberattaque – c'est la prévention ; et d'autre part minimiser sa gravité et faciliter la reprise, dans le cas où un dysfonctionnement se produit malgré tout.

Le sujet de la confiance numérique peut concerner l'ensemble du territoire de la collectivité, selon le degré de sa numérisation – informatique, réseaux télécoms, objets connectés, infrastructures numérisées. Les risques dont on veut se prémunir *in fine* sont variés : interruption de service, fuite de données, etc. Le chapitre 3, section 2, les détaille.

Les mises en situation proposées en encarts dans ce guide sont destinées à illustrer ce qu'est la confiance numérique d'une collectivité, et les choix que les élus sont amenés à faire en amont comme en aval.

Mise en situation n° 1 – Tirée d'un cas réel

Un agent de la collectivité reçoit un mail piégé avec un faux devis. Il ouvre la pièce jointe et l'intégralité des ordinateurs de la mairie sont bloqués. Une rançon de 20 000 € est demandée pour les débloquer. Une affaire nécessite pourtant d'accéder en urgence aux données, or il s'avère après recherche que les sauvegardes étaient accessibles à partir du réseau de la mairie, et sont devenues elles aussi inaccessibles. Que feriez-vous en tant qu'élu ?

A – déposer plainte	B – payer la rançon	C – chercher à s'offrir en urgence les services d'un expert en remédiation

Qu'auriez-vous aimé initier en amont ?

A – demander des sauvegardes régulières et stockées à part	B – sensibiliser les agents à la détection de mails suspects	C – avoir établi le contact avec un expert en remédiation

Eléments de réponse : le dépôt de plainte est indispensable. Concernant la rançon, il peut être tentant de la payer, mais il n'est pas garanti que les données seront pour autant recouvrées et, surtout, le fait de payer peut constituer une incitation à d'autres futures cyberattaques. Il vaut mieux privilégier le recours à un expert en remédiation.

La meilleure action aurait pu être menée en amont : des sauvegardes régulières et inaccessibles, la sensibilisation des agents à la reconnaissance des mails douteux, et la prise de contact avec un expert en remédiation.

03

Quelles risques et responsabilités pour les collectivités, agents et élus ?

Quel cadre juridique en matière de confiance numérique ?

La transformation numérique implique des risques nouveaux pour l'ensemble des missions portées par les collectivités. Aujourd'hui, aucune norme n'encadre explicitement la question de la confiance numérique des collectivités, mais un panel de normes trouve à s'appliquer de manière collégiale, notamment :

- en matière d'échanges d'informations avec l'administration (référentiel général de sécurité – RGS) ;
- en matière de protection des données personnelles (RGPD) ;
- en matière d'ouverture des données (loi pour une République numérique de 2016).

De nombreux textes législatifs et règlementaires doivent ainsi être appréhendés conjointement par les collectivités en matière de confiance numérique. La fiche pratique 1 recense ces principales normes.

Quels risques induits, pour quelles conséquences ?

Le risque des cyberattaques ou actes de cyber-malveillance

Les systèmes d'informations et données sur lesquels reposent les missions assurées directement ou indirectement par les collectivités sont susceptibles de faire l'objet de cyberattaques. Les cyberattaques peuvent notamment viser :

- le vol ou la divulgation de données confidentielles, comme des données personnelles (agents, citoyens) ou couvertes par le secret professionnel ;
- l'extorsion de fonds grâce à des rançongiciels ou à la fraude au président ;
- l'indisponibilité des systèmes d'information de la municipalité ;
- le sabotage d'infrastructures d'eau, de transport, d'énergie, de signalisation, etc.

Le risque des dysfonctionnements non intentionnels

Les dysfonctionnements dont peuvent être victimes les systèmes informatiques de la collectivité sont multiples. Ils peuvent découler de différentes erreurs en matière de conception, de configuration ou de maniement.

Dans une telle situation, l'origine de l'atteinte ne résulte pas d'une attaque malveillante mais d'une erreur humaine, d'un défaut de configuration ou d'un incident purement technique. Ces dysfonctionnements peuvent avoir pour conséquence notable le libre accès à des données ou des systèmes sensibles.

Le risque d'atteintes indirectes pouvant être subies par les collectivités

Des atteintes subies par des acteurs tiers à la collectivité (délégataire ou autre sous-traitant clé), tel qu'un opérateur de télécommunications, un fournisseur d'eau, un opérateur de signalisation, peuvent avoir des conséquences globales touchant l'ensemble de la collectivité et ses citoyens.

Dans une telle situation, le maire ou le président de la collectivité territoriale sera amené à réagir et pourrait prendre des mesures, quand bien même l'attaque ne prendrait pas directement pour cible les services sous la responsabilité de la collectivité territoriale.

Les conséquences potentielles de ces atteintes

Les conséquences directes de ces atteintes sont diverses. Elles peuvent recouvrir la perturbation du fonctionnement des collectivités, leur désorganisation voire la mise en

danger de leurs citoyens dans le cas d'une atteinte aux systèmes de signalisation routière.

En matière de conséquences indirectes, la confiance des citoyens à l'égard de leurs élus peut être altérée et l'image et la réputation de la collectivité ternies à plus ou moins long terme en cas d'atteinte à cette confiance.

De plus, la remise en état du système affecté, mais aussi la reconstitution des éventuelles données altérées ou disparues, peut entraîner un impact financier important pour la collectivité territoriale. Il pourrait être nécessaire de recourir à des prestataires externes spécialisés pour remédier à l'atteinte et limiter ses conséquences.

Enfin, des usagers ou des tiers pourraient introduire des actions en justice à l'encontre de la collectivité et/ou de ses élus/agents afin d'obtenir réparation s'ils estiment que l'atteinte concernée à causer à leur endroit un préjudice, des dommages – sous réserve que ce préjudice ou ces dommages résultent d'une faute que la collectivité aurait commise dans ses obligations en termes de confiance dans le numérique, comme évoqué ci-après.

Quelles responsabilités pour les collectivités et leurs agents ?

La responsabilité de la collectivité territoriale peut être recherchée par une action individuelle. Un usager ou un tiers doit alors démontrer l'existence d'une faute de service commise par l'administration pour être indemnisé.

On notera que la responsabilité administrative de la collectivité territoriale ne sera pas engagée en cas de faute personnelle commise par un agent, c'est-à-dire commise en dehors du service ou dans l'exercice des fonctions de l'agent mais traduisant une intention malveillante ou la poursuite d'un intérêt privé par son extrême gravité ou un excès de comportement. Un agent qui, par exemple, utiliserait de façon non autorisée des données auxquelles il aurait accès dans le cadre de ses fonctions, pour son intérêt personnel, verrait sa responsabilité personnelle engagée[1] en lieu et place de la collectivité.

De même, certains manquements à la règlementation relative à la protection des données personnelles constituent des infractions pénalement réprimées. L'engagement de la responsabilité de la collectivité pourra également faire l'objet d'une action de groupe à l'encontre de la collectivité.

Quelle responsabilité pour les élus et les prestataires de la collectivité ?

Les élus

En cas de dommage causé à un tiers, la responsabilité civile d'un élu pour faute personnelle peut également être engagée. En effet, la possibilité d'engager la responsabilité pénale de la collectivité territoriale ne fait pas obstacle à la recherche de la responsabilité d'un élu auteur des mêmes faits, sous réserve qu'il soit démontré l'existence d'une violation manifestement délibérée par celui-ci d'une obligation particulière de prudence ou de sécurité, ou d'une faute caractérisée.

- Ici encore, si le fait reproché à l'élu constitue également une infraction pénale, sa responsabilité pourrait être engagée sur ce fondement.
- Il convient de rappeler qu'un élu ne pourra être condamné, pour des faits non intentionnels, qu'à condition qu'il n'ait pas accompli « les diligences normales »

[1] Le fait de collecter des données personnelles par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et 300 000 euros d'amende par l'article 226-18 du code pénal.

attendues, au regard de ses compétences, du pouvoir et des moyens qu'il avait à sa disposition. Ces « diligences normales » peuvent être définies comme le soin que l'élu est tenu de porter à l'exercice de ses activités et fonctions. En matière de confiance numérique, cela pourrait notamment correspondre au fait d'informer, se sensibiliser ou encore de former les agents aux risques et enjeux cybersécuritaires – même s'il n'existe pas de jurisprudence en la matière à ce jour.

De plus, la collectivité territoriale est tenue d'accorder à l'élu une protection juridique, dès lors que le caractère de la faute n'est pas détachable de l'exercice de ses fonctions.

Les prestataires de services numériques

En cas de dysfonctionnement du système, de défaut de sécurité ou d'attaque malveillante d'un sous-traitant, la collectivité peut voir sa responsabilité directement engagée.

Toutefois, la collectivité conserve la possibilité d'engager la responsabilité de son prestataire. Elle pourra notamment, engager une action reconventionnelle à son encontre dans le cadre d'une instance ou encore l'appeler à la cause dans le cadre d'un litige déjà initié, si elle estime que le préjudice objet de la demande en justice résulte du fait du sous-traitant ; par exemple d'un manquement à l'une de ses obligations contractuelles en matière de sécurité numérique.

Cas des sanctions administratives de la CNIL

La CNIL peut prononcer des sanctions à l'encontre de la collectivité responsable d'un traitement de données à caractère personnel, par exemple dans le cas où une violation de données interviendrait à la suite d'une cyberattaque rendue possible par un manquement imputable à la collectivité. Elle peut prononcer les sanctions suivantes :

- rappel à l'ordre à l'encontre de la commune ;
- injonction de mise en conformité au RGPD, y compris sous forme d'astreinte ;
- sanction financière pouvant aller jusqu'à 20 millions d'euros d'amende, en fonction de la gravité du manquement et des circonstances de sa survenance.

Mise en situation n° 2 – Tirée d'un cas réel

La rentrée scolaire a lieu mardi prochain. Il est vendredi soir, et la page du site Internet dédiée à l'école municipale a été piratée : méconnaissable, elle affiche tout un lot de photographies choquantes et illégales. Le prestataire qui gère le site Internet ne répond pas, mais un canal de communication a pu être établi avec l'hébergeur.

Que feriez-vous en tant qu'élu ?

A – dépôt de plainte	B – demande à l'hébergeur de fermer le site en urgence	C – information des parents d'élèves

Qu'auriez-vous aimé initier en amont ?

A – exiger des mesures de sécurisation du site Internet	B – exiger que le prestataire mette en place un canal d'urgence

Eléments de réponse : Un dépôt de plainte est indispensable, la coupure de l'accès au site apparaît judicieuse, et l'information parents d'élèves peut s'avérer opportune. Des questions d'investigation se poseront par la suite, pour voir si des données personnelles exposant les élèves ou leurs parents ont été exfiltrées.

La meilleure action est celle à prendre en amont : exiger du prestataire un niveau de sécurité adapté, et une réactivité en cas d'incident majeur.

04

Que faire en tant qu'élu ? Les grands principes à porter

Le premier rôle de l'élu : impulser l'effort collectif

Le premier rôle de l'élu en matière de confiance numérique est de marteler son importance, afin d'impulser un effort collectif et une démarche endossée par tous.

La sécurité numérique est l'affaire de tous. Des élus décisionnaires aux concepteurs des services numériques, des agents qui les utilisent aux techniciens qui les maintiennent, des financiers qui en gèrent les coûts aux juristes qui en maîtrisent le contexte réglementaire, tous ont à s'impliquer. L'élu est alors le mieux placé pour impulser cette dynamique générale.

Tout d'abord, il s'assure de la formation des parties prenantes à la confiance numérique et à la cybersécurité. Cette formation doit être très simple et adaptée aux différents métiers – tout le monde n'a pas besoin d'être expert ! → *fiche pratique 2 qui liste quelques formations gratuites et pertinentes*

Enfin, il pousse à la mise en place d'une ville numérique de confiance, à travers quatre axes de bon sens qui font l'objet des sections suivantes :

- créer et entretenir une vision globale ;
- mener des nouveaux projets numériques fiables et pérennes ;
- maîtriser la ville numérique au quotidien ;
- être prêt au pire et savoir réagir.

Dans cette démarche, l'élu cherchera à ce que des ressources adaptées soient déployées, dans la sécurisation des projets comme, au budget, par l'affectation de moyens nécessaires au développement et au pilotage de la confiance numérique.

Se forger une vision globale et définir des priorités

L'élu d'une petite collectivité pourra parcourir rapidement cette section, qui peut concerner davantage les collectivités de taille moyenne ou grande, confrontées par nature à de nombreux sujets numériques.

Une vision globale à entretenir

Quoi de pire qu'une mosaïque de services numériques issus d'autant d'initiatives différentes, et déployés sans vision d'ensemble ? Cela donne une ville numérique impossible à maîtriser, sans cesse plus coûteuse à opérer et à maintenir, et *in fine* une proie idéale pour les cyberattaques !

Pour éviter une telle situation, l'élu doit idéalement s'assurer (→ *sections suivantes du présent chapitre*) :

- que la collectivité connaisse l'état des lieux numérique de sa ville, ce qui est nécessaire pour la maîtriser au quotidien ;
- et, lorsqu'elle vient à se doter de nouveaux services numériques, que la collectivité sache pourquoi, dans quel but, de quelle manière, et quels sont les risques numériques induits – cadrage indispensable pour mener des projets fiables et pérennes.

Connaître l'état des lieux numérique de sa ville, c'est savoir quels sont les services déjà numérisés, qui les opère, et c'est disposer d'une cartographie des systèmes sur lesquels ils reposent. C'est également maîtriser le coût financier récurrent pour opérer techniquement et maintenir ces services. L'audit technique reste l'un des meilleurs moyens de réaliser cet état des lieux numérique, et permet d'évaluer les risques numériques et les meilleures actions à mener pour les contenir.

Des priorités à définir

Ce n'est que sur la base d'un tel état des lieux qu'il est possible de mener une réflexion efficace sur les prochains projets numériques de la ville, et de définir des priorités parmi :

- **la consolidation et l'amélioration** : les chantiers de consolidation, de mise à niveau et d'amélioration du numérique existant. Un audit technique aidera à déterminer les actions prioritaires en la matière – chantier plus crucial encore lorsque le numérique présente des faiblesses (complexité, obsolescence, failles, etc.) ;
- **la numérisation de services municipaux existants** ;
- **la création de nouveaux services grâce au numérique**.

Cette réflexion doit prendre en compte les spécificités de la collectivité et celles de son existant numérique. Elle peut mener à différer voire abandonner des projets numériques dignes d'intérêt dans l'absolu, mais qui s'avéreraient par exemple :

- moins urgents que d'autres projets ;
- difficilement articulables avec l'organisation de la collectivité et de ses services ;
- ou susceptibles d'introduire un niveau de risque numérique trop important.

Enfin, **cette réflexion doit s'ouvrir et rechercher autant que possible des axes de mutualisation**, tant dans la phase de conception qu'en matière de moyens : intercommunalités, syndicats, services communs, associations peuvent s'avérer des alliés précieux pour faire face ensemble aux défis du numérique.

Sans cette vision globale qui seule permet la bonne maîtrise d'une ville numérique, il s'avère difficile d'instaurer la confiance numérique dans la durée.

Mener des projets numériques fiables et pérennes

Il s'agit d'une évidence : un projet de service numérique, ou, à l'échelle plus vaste, de ville ou territoire numérique, nécessite une gestion de projet maîtrisée comme tout autre projet d'une collectivité.

L'élu devrait notamment demander que l'équipe chargée de définir le projet – maîtrise d'ouvrage en premier lieu – prenne en compte les grandes considérations suivantes.

Pour un projet fiable, on veillera notamment à :

- **Définir des objectifs en matière de confiance numérique**. Au-delà de l'exigence réglementaire de conformité au RGPD, il est nécessaire de faire figurer dans le cahier des charges les principaux risques contre lesquels on souhaite se prémunir, comme la fuite de données, le sabotage, ou l'arrêt du service.
- **Exiger des mesures de cybersécurité**. La cybersécurité doit être intégrée dès la conception (« *by design* »), les mesures de cybersécurité dont les grandes catégories sont décrites en chapitre 2, section 2, doivent être abordées.
- **Définir des exigences portant sur les prestataires eux-mêmes**. Il s'agit de rechercher de garanties en matière de localisation et d'accès aux données, respects de règles de sécurité numérique, etc.

Pour un projet pérenne, on veillera notamment à ;

- **Mettre en place un suivi et une détection**. S'il apparaît indispensable de disposer d'outils de suivi opérationnel, un suivi en matière de sécurité numérique l'est tout autant afin de détecter d'éventuelles anomalies et de réagir au plus vite en cas de défaillance ou de piratage. Ces outils nécessitent des ressources et doivent être

adaptés aux moyens dont dispose la collectivité. Leur mutualisation à plus grande échelle est une voie à explorer.

- **Définir des exigences portant sur les prestataires eux-mêmes**. Il est nécessaire de s'assurer du degré de confiance numérique à moyen et long terme offert par les prestataires. On recherchera par exemple des garanties générales en matière de niveau de service, de continuité d'activité, de mises à jour de sécurité, de réversibilité (capacité à changer de prestataire), de réactivité en cas d'incident.

Pour chacun de ces axes, les équipes et prestataires doivent mettre en place des garanties. L'encadré qui clôt la présente partie détaille davantage les questions pouvant être posées à un maître d'ouvrage, une SSII (ou ESN) un prestataire du projet.

Mise en situation n° 3 – Tirée d'un cas réel

L'éclairage public est désormais intelligent : il peut être piloté et optimisé depuis un centre de commande dont la gestion est confiée à un délégataire. Depuis quelques jours, la moitié de la ville est privée d'éclairage public. Le délégataire parle d'un dysfonctionnement qu'il n'est pas encore parvenu à résoudre, mais vous n'êtes pas sûr qu'il mette suffisamment de moyens en œuvre pour remédier à la situation.

Que feriez-vous en tant qu'élu ?

A – demande de compensation au délégataire	B – information des citoyens	C – mise en place de solutions d'éclairage temporaires

Qu'auriez-vous aimé initier en amont ?

A – exiger un niveau de service minimum	B – demander des délais de réaction	C – demander un audit technique du nouveau système d'éclairage, préalable à la contractualisation

Eléments de réponse : s'il est impératif de communiquer auprès des citoyens, la mise en place de solutions de secours peut parfois s'avérer trop coûteuse, et la demande d'une compensation au prestataire ne dépend que de sa bonne volonté si rien n'a été prévu contractuellement.

En amont, quelques mesures auraient pu être exigées par l'élu : des garanties en termes de fiabilité et de délais de réaction, et plus encore un audit technique de la solution innovante retenue, pour s'assurer de sa bonne conception. Le coût correspondant à ces mesures ne doit pas être vu comme optionnel, mais comme propre au nouveau projet.

Maîtriser la ville numérique au quotidien

Sitôt que la ville devient numérique, ne serait-ce que partiellement, il est nécessaire pour la municipalité de disposer d'un suivi de l'activité numérique. On parle de supervision.

Le premier type de suivi, technique, est celui de la bonne santé du service. Les anomalies ou dysfonctionnements sont-ils détectés, et ce dans des délais permettant de réagir ? Ce sujet de la détection des incidents et menaces est clé pour instaurer la confiance dans les services numériques. Ce suivi doit être pensé pour être non pas exhaustif, mais simple et répondant aux besoins – et le cas échéant mutualisé avec d'autres partenaires.

Le deuxième type de suivi, opérationnel, est crucial pour s'assurer de l'efficacité des services numériques, est celui de la mesure de l'activité. Il consiste à disposer d'un aperçu de la façon dont le service est utilisé par les citoyens, à des fins d'amélioration du service ou de la gestion du territoire – dans l'esprit des principes qui fondent la *smart city*.

Afin que le suivi soit de qualité, il incombe au maire de s'assurer que ce suivi est pensé en amont, avant même l'intégration des nouveaux services numériques, d'une façon pragmatique qui répondent aux besoins de pilotage.

Être prêt au pire et savoir réagir

En matière de confiance numérique, la meilleure façon de faire face au pire est de s'y être préparé ! Lorsque des systèmes informatiques « tombent », tout va très vite et l'élu, qui n'est pas un expert en numérique, se retrouve vite submergé. Quelques précautions peuvent s'avérer salvatrices lorsque survient le jour J : disposer de contacts d'urgence, avoir préparé des canaux de communication de crise, connaître ses obligations juridiques, disposer au format papier de documents clés et d'un annuaire municipal, etc.

Pour se préparer, la marche à suivre est simple et peut se résumer ainsi :

1. réunir les acteurs qui auraient à gérer la crise ;
2. répondre ensemble à la question : « *Quelles sont, pour les principaux systèmes numériques de la collectivité, les conséquences de dysfonctionnements, de sabotage, de fuite de données, etc. ?* » ;
3. réfléchir alors aux principales mesures qui seraient nécessaires pour endiguer la situation lorsque la crise se produit.

Les aspects à anticiper concernent notamment le dialogue entre les acteurs (élus, agents, prestataires), l'information des citoyens, la bonne connaissance de son écosystème numérique, la réactivité des équipes et prestataires, l'opportunité de contracter au préalable un éventuel contrat d'assurance. La bonne formation des acteurs s'avère une aide précieuse dans cet exercice.

Selon les ressources dont il dispose, l'élu pourra pousser à un approfondissement de la démarche à partir de la littérature disponible[2] et le cas échéant avec une aide externe. La fiche pratique 2 présente les interlocuteurs possibles en cas de crise d'origine numérique.

[2] Guide ANSSI-CCA d'exercice à la gestion de crise cyber ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber

Mise en situation n° 4 – Tirée d'une histoire plausible

Vous venez d'être informé qu'une partie des systèmes d'information du délégataire de gestion d'eau potable viennent d'être cyberattaqués. On ne sait pas encore quelles sont les conséquences exactes, mais on craint qu'elles soient sérieuses.

Que feriez-vous en tant qu'élu ?

A – établissement d'une liaison avec le délégataire	B – information des citoyens	C – préparation à la possible commande en urgence d'eau minérale pour les citoyens

Qu'auriez-vous aimé initier en amont ?

A – exiger un niveau de service et des délais de réaction minimum	B – demander un audit technique du nouveau système de gestion d'eau, préalable à la contractualisation

Eléments de réponse : s'il apparaît impératif de communiquer auprès des citoyens et de disposer d'information en temps réel de la part du délégataire, il apparaît également judicieux de se préparer à mettre en place des solutions de secours.

Quelques mesures en amont auraient pu être demandées par l'élu : des garanties en termes de fiabilité des systèmes, et plus encore un audit technique des systèmes de gestion d'eau du délégataire retenu, pour s'assurer de son niveau de cybersécurité. Le coût correspondant à ces mesures doit être vu non pas comme optionnel, mais comme propre au nouveau projet.

Projets numériques : quels points exiger ?

Il est impératif que les élus poussent des grands points d'attention lors des nouveaux projets numériques de la municipalité. Cet encadré vise à détailler ces points d'attention. Ils sont à moduler selon le degré de criticité du service, du système ou du prestataire considéré.

Ces points d'attention sont également des axes d'analyse de la Banque des Territoires lorsqu'elle étudie les opportunités d'investissement en matière d'innovation numérique.

Maîtrise d'ouvrage

acteurs : municipalité (niveau décisionnel), conseil, etc.

- ☐ exiger le respect des réglementations (RGPD, eIDAS, RGS, etc.) → *fiche pratique 1*
- ☐ s'assurer de la propriété industrielle des prestations intellectuelles – notamment des développements informatiques réalisés pour le compte de la collectivité
- ☐ définir les besoins ou priorités en matière de sécurité du numérique, sur la base d'une analyse globale pilotée par la maîtrise d'ouvrage, et refléter ces besoins sous forme d'exigences dans les cahiers des charges
- ☐ exiger une cartographie des systèmes et processus en jeu
- ☐ exiger des principes :
  - de sécurité *by design* (i.e. conception intégrant la cybersécurité) respectant des guides de référence comme le guide d'hygiène informatique de l'ANSSI
  - de respect des bonnes pratiques en matière de conception et de développement de systèmes numériques : pérennité, maintenabilité, documentation, etc.
- ☐ exiger un soin particulier en matière de confiance numérique :
  - en cas de connexion des nouveaux services à des systèmes existants
  - sur tout point névralgique (service critique, brique centrale, etc.)
- ☐ exiger un outillage de suivi (*reporting*) permettant de détecter les anomalies métier et de cybersécurité
- ☐ exiger des principes de reprise d'activité (sauvegardes, modes dégradés, clauses de réactivité des sous-traitants, etc.)

Maîtrise d'œuvre

acteurs : municipalité (niveau technique / DSI), SSII/ESN, etc.

- ☐ s'assurer de la bonne prise en compte des exigences de confiance numérique définies au niveau de la maîtrise d'ouvrage – le cas échéant en recourant à un audit technique
- ☐ rendre compte sur cette prise en compte

Prestataire informatique ou sous-traitant industriel

acteurs : hébergeurs, informatique en nuage, solutions as a service*, objets connectés, etc.*

- ☐ rechercher le respect des réglementations et demander une clause d'auditabilité
- ☐ rechercher la maîtrise des données de la collectivité, territoriales et personnelles (localisation, accès, réversibilité)
- ☐ rechercher l'indépendance par rapport aux sous-traitants (interopérabilité, standards, réversibilité)
- ☐ exiger des garanties en matière de niveau de service, adaptées aux besoins de sécurité des services numériques concernés
- ☐ s'assurer autant que possible de la compétence et de la pérennité du prestataire

05

Collectivités et confiance numérique : les défis à venir

Après le RGPD et l'*Open data*, quels futurs défis réglementaires ?

Au-delà de la réglementation RGS, l'*Open Data* et le RGPD (→ fiche pratique 1) ont été les grandes innovations réglementaires de ces dernières années qui ont poussé les collectivités à se pencher sur le sujet de la confiance numérique.

Or, le champ de la confiance numérique est encore récent, et les menaces en constante évolution : il y a fort à parier que de nouvelles réglementations et des projets de changements des réglementations existantes interviendront dans ce domaine.

Les bonnes pratiques actuelles risquent-elles d'être un jour gravées dans le marbre de la réglementation ? On pourrait notamment imaginer les principes de formation des agents et de bonne conception numérique (« *security by design* ») rejoindre le champ législatif. Les collectivités ont un rôle à tenir pour définir les évolutions réglementaires, afin qu'elles s'adaptent à leurs enjeux concrets et permettent d'offrir un numérique de confiance.

La mutualisation des initiatives et des pratiques

Chaque territoire est doté d'une organisation et d'une histoire propres qui nécessitent un projet numérique adapté à ses spécificités. Pour autant, d'une ville, d'un territoire à l'autre, de nombreux défis en matière de numérique et de confiance numérique gagnent à être relevés de manière collective, et ce tant pour une question de coût des chantiers que de rareté des profils experts. Partager les pratiques, fédérer les initiatives, mutualiser les coûts sont autant de façon de s'emparer du sujet de manière efficace.

Les possibilités sont variées : entre municipalités, *via* l'intercommunalité, le département, la région, des services communs, ou en recourant à des structures d'accompagnement. Tout l'enjeu est de faciliter, faire connaître et systématiser les moyens qu'ont les collectivités d'avancer collectivement sur le sujet de la confiance numérique. Une initiative comme le réseau DECLIC s'inscrit dans cette recherche de mutualisation.

Standardisation & interopérabilité

Une offre de confiance pour les projets de ville numérique ne pourra se développer sans une logique de standardisation et d'interopérabilité au service des territoires.

Pour que les villes ne dépendent pas de technologies exclusives, pour qu'elles puissent opérer librement des choix nouveaux, pour qu'elles ne risquent pas de se faire déposséder de leurs données, il est nécessaire qu'émergent des principes et normes harmonisés dans ce sens. Différents acteurs commencent à travailler sur ce sujet, au premier rang desquels l'AFNOR pour la France. On citera également le chantier européen Fiware, une initiative « *open source* » de définition de composants universels de *smart cities*.

La confiance numérique elle-même relève de ce besoin : la standardisation et l'interopérabilité permettent une meilleure rationalisation de l'ensemble de la ville numérique, dont la maîtrise et la protection deviennent plus aisées.

Nouvelles tendances technologiques : quel niveau de confiance ?

Toute nouvelle technologie pose un nouveau défi en matière de confiance. Les exemples ici abordés, non exhaustifs, l'illustrent pour quelques-unes des grandes tendances actuelles.

Le déploiement du wifi territorial

Depuis quelques années, les wifi publics se multiplient dans les lieux publics, offices de tourisme, campings municipaux, bibliothèques et transports collectifs. Ces wifi territoriaux

ne doivent pas être déployés sans un soin particulier pour leur sécurisation. La loi y pousse elle-même : il incombe à l'opérateur du wifi territorial, collectivité ou délégataire, des obligations de confiance numérique comme le respect du secret des correspondances, le respect de la vie privée, la sécurisation et continuité de service du réseau[3].

L'accélération du déploiement de l'internet des objets (IoT)

Les dernières années ont vu la multiplication des projets reposant sur des objets connectés. Ils permettent, par exemple, la remonté des alarmes de feux tricolores, la modulation de l'éclairage public ou le pilotage du chauffage dans les bâtiments publics.

Ces projets IoT sont à considérer avec une grande attention. Souvent complexes, ils mêlent les dimensions suivantes : sécurisation des objets connectés déployés sur le terrain, sécurisation des données et des services issus de ces objets, et sécurisation de leurs infrastructures de communication. Ces enjeux se retrouvent, à un degré d'intensité supérieur, dans la problématique du déploiement de la technologie 5G sur les territoires.

L'automatisation et l'Intelligence Artificielle

Plus un service numérique est automatisé et plus la main est laissée à la machine, plus les conséquences d'une défaillance ou d'un piratage seront importantes :

- L'automatisation suppose le plus souvent un moindre contrôle humain, rendant plus difficile la détection de cyberattaques ou de dysfonctionnements ;
- Les modules d'intelligence artificielle auto-apprenante (IA) prennent des décisions difficiles à comprendre rétrospectivement. On parle d'effet « boîte noire », qui rend d'autant plus difficile la détection d'un mauvais réglage ou d'un piratage de l'IA.

De façon générale, l'intégration de l'IA et de l'automatisation doit faire l'objet d'un soin tout particulier, selon des principes de sécurité *by design*. → *encadré de fin du chapitre 4 sur les recommandations concernant les nouveaux projets numériques*

Dans le cas de l'IA, il est de plus nécessaire de comprendre et expliquer les décisions de l'algorithme. Autrement, la responsabilité de la collectivité pourrait être engagée sur une décision – inintelligible – prise par une IA dont elle ne maîtrise pas les ressorts.

Structuration d'une offre de confiance & souveraineté numérique

Afin de mener une transition numérique offrant un vrai niveau de confiance, les collectivités, comme les entreprises, ont besoin d'une offre industrielle intégrant cet enjeu. Cette offre doit intégrer des solutions spécialisées en confiance numérique d'une part, et des solutions métier conçues dans un souci de confiance numérique d'autre part. Enfin, pour ce qui est de l'élaboration des projets numériques, une offre en matière d'assistance à maîtrise d'ouvrage compétente en confiance numérique est également nécessaire.

Cette structuration est à mettre en regard avec une problématique plus générale de souveraineté numérique : l'Etat a-t-il les moyens d'agir et de décider dans le cyberespace, ainsi que la capacité à maîtriser les réseaux, les communications électroniques et les données numériques ? Cette question cruciale nécessite non seulement de recourir à des solutions technologiques de qualité, mais également que les missions et métiers les plus critiques dépendent avant tout d'infrastructures ou de services français, sinon européens. Elle entraîne une réflexion sur notre dépendance aux grandes entreprises américaines du numérique, les « GAFAM ».

[3] Cf. guide « *Wifi territorial, une solution pour votre collectivité* » de la Banque des Territoires

Rôle de la Banque des Territoires

L'Etat, l'Union européenne et les investisseurs en matière de solutions numériques ont vocation à financer cette double ambition d'une structuration de l'offre et d'une souveraineté numérique.

La Banque des Territoires s'y inscrit pleinement : dans son métier d'investisseur, elle cherche à investir dans des solutions innovantes permettant aux collectivités de suivre une transition numérique de confiance. Elle recherche en premier lieu les opportunités permettant de sécuriser de façon simple les briques les plus sensibles de la ville numérique, celles qui aident à gérer les risques numériques portés par la ville, et celles qui aident à gérer la crise numérique lorsqu'elle vient à se produire.

De façon plus générale dans son rôle d'investisseur, la Banque des Territoires porte une attention particulière au respect des principes abordés dans ce guide (→ encadré final du chapitre 4).

06

Glossaire et fiches pratiques

GLOSSAIRE

Le présent glossaire reprend les grandes notions qu'un élu devrait utilement connaître en matière de confiance numérique et de cybersécurité.

ANSSI : agence nationale de la sécurité des systèmes d'information, autorité nationale en matière de sécurité et de défense des systèmes d'information

audit technique [de sécurité] : un audit technique d'un système numérique est réalisé par des auditeurs experts en informatique et en cybersécurité, à même d'éprouver la fiabilité, la robustesse et le niveau de cybersécurité du système → *partie 4*

CNIL : commission nationale de l'informatique et des libertés, autorité administrative indépendante compétente notamment en matière de protection des données personnelles

confiance numérique : domaine regroupant tout ce sur quoi se fonde la confiance dans le « numérique » – inclut la cybersécurité mais également de façon plus large la nécessité de solutions numériques fiables et pérennes, associés à une gestion maîtrisée des systèmes, des données et des identités numériques

cybersécurité : niveau de sécurité que l'on cherche à atteindre pour des systèmes et des données numériques afin de se prémunir contre les menaces cyber le plus redoutées

ESN / SSII : entreprise de services numériques, équivalent du terme SSII

eIDAS : règlement européen sur l'identification électronique et les services de confiance → *fiche pratique n° 1 dédiée à la réglementation*

fraude au président : moyen consistant à se faire passer, de façon numérique ou non, pour un haut responsable d'une organisation afin d'en obtenir illégalement un avantage, le plus souvent obtenir le virement d'une somme conséquente

hameçonnage / phishing : cyberattaque consistant à appâter (hameçonner) une personne pour lui faire exécuter une action nuisible, comme l'ouverture d'une pièce jointe corrompue ou d'un lien pointant vers un site malveillant

IoT / Internet of Things / Internet des Objets : désigne l'ensemble des objets ou machines connectés à Internet : caméra de surveillance, compteurs intelligents, signalisation connectée, etc.

Open Data : principe d'ouverture par défaut des données publiques aux citoyens → *fiche pratique n° 1 dédiée à la réglementation*

NIS : directive européenne sur la sécurité des réseaux et systèmes d'information, qui définit notamment le statut des opérateurs de services essentiels (→ *glossaire, terme OSE*) – pour ce qui est des collectivités, seules les grandes métropoles et leurs délégataires de services sont susceptibles d'être concernées

OSE : opérateurs de services essentiels, désignés par l'Etat et devant appliquer des mesures de cybersécurité renforcées → *fiche pratique n° 1 dédiée à la réglementation*

OIV : opérateurs d'importance vitale, désignés par l'Etat et devant appliquer des mesures de cybersécurité renforcées → *fiche pratique n° 1 dédiée à la réglementation*

pourriel / *spam* : les pourriels, ou courriels indésirables, sont les e-mails non sollicités et non pertinents que l'on est susceptible de recevoir en grande quantité

réversibilité : capacité d'un client à récupérer tous les actifs et informations nécessaires à la transmission du service à un autre prestaire → *encadré en fin de chapitre 4, dédié aux grandes recommandations à mettre en œuvre*

rançongiciel / *ransomware* : virus informatique qui rend indisponible un système et des données tant qu'une rançon n'a pas été payée

RGPD : règlement européen sur la protection des données personnelles

RGS : référentiel général de sécurité relatif aux échanges informatiques avec l'administration → *fiche pratique n° 1 dédiée à la réglementation*

***smart city* / ville numérique** : la *smart city*, ville numérique ou territoire intelligent, désigne un état de développement numérique avancé des villes et des territoires. La technologie est utilisée pour améliorer la qualité des services urbains ou encore réduire leurs coûts. Les gains peuvent s'opérer en matière de chaleur, d'énergie, de flux de circulation, de réponse aux besoins des citoyens. Ce faisant, les projets *smart city* font déborder les enjeux numériques au-delà des seuls champs de l'informatique traditionnelle en les étendant aux bâtiments, aux infrastructures, aux espaces publics, au mode de vie des citoyens et aux entreprises.

souveraineté numérique : désigne, pour l'État, la capacité autonome d'appréciation, de décision et d'action dans le cyberespace ainsi que la capacité à maîtriser les réseaux, les communications électroniques et les données numériques

FICHE PRATIQUE 1 : REGLEMENTATION

La présente fiche introduit de façon succincte le cadre réglementaire intervenant en matière de confiance numérique des collectivités. Pour aller plus loin, on pourra utilement se tourner vers le guide de l'ANSSI sur l'essentiel de la réglementation en matière de sécurité numérique des collectivités territoriales.

1) Le cadre spécifique en matière de sécurité des systèmes d'information

Référentiel général de sécurité (RGS)[4] *: les échanges impliquant une autorité administrative*

En leur qualité d'autorités administratives, les collectivités territoriales sont soumises au référentiel général de sécurité. Ce texte, qui vise à sécuriser les échanges numériques entre les autorités administratives et les usagers des services publics, a donc pour objet de participer à la confiance numérique des administrés envers les collectivités territoriales lors de l'utilisation des services électroniques mis à leur disposition par elles.

Le RGS définit concrètement des exigences de sécurité numérique pour les systèmes de déclaration d'imposition, de règlement de contravention, de transmission de demandes de renouvellement de papiers d'identité, etc. Le RGS instaure également un processus de qualification des prestataires de services de confiance auxquels les collectivités territoriales peuvent avoir recours dans le cadre de la mise en place de leurs téléservices.

Règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (règlement eIDAS)[5]

Ce texte européen vise à améliorer la confiance dans les transactions électroniques et à créer une base commune pour les interactions sécurisées entre les citoyens, les entreprises et les autorités publiques dans l'Union européenne.

Il s'applique ainsi aux collectivités territoriales qui échangent avec le public par voie électronique. Le règlement s'intéresse à la fois à l'identification électronique aux services de confiance et à l'effet juridique donné aux documents électroniques.

Loi du 18 décembre 2013 de programmation militaire 2014-2019[6] *(ci-après « LPM ») : l'encadrement des opérateurs d'importance vitale*

La LPM impose des mesures de sécurité numérique renforcée aux opérateurs d'importance vitale (OIV), opérateurs dont les services pourraient, en cas d'incident, porter gravement atteinte au potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation, ou mettre gravement en cause la santé ou la vie de la population.

La liste des OIV est confidentielle. Ils peuvent être désignés notamment parmi les secteurs de la gestion de l'eau, de l'énergie et des transports : les plus grandes collectivités sont ainsi susceptibles d'être concernés.

Directive « Network and Information Systems »[7] *(directive NIS) et sa loi de transposition du 26 février 2018*[8] *: l'encadrement des opérateurs de services essentiels*

La directive NIS comporte des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union européenne. Elle régit notamment les opérateurs de services essentiels (OSE), pendant européen des OIV,

[4] Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité.
[5] Règlement (UE) n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.
[6] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[7] Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
[8] Loi n°2018-133 du 26 février 2018 « portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ».

opérateurs de services dits essentiels au fonctionnement de la société ou de l'économie et dont la continuité impérative pourrait être gravement perturbée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture de ces services.

Les OIV peuvent être désignés notamment parmi les secteurs de l'eau, de l'énergie et des transports : les plus grandes collectivités sont ainsi susceptibles d'être concernés.

2) Le cadre spécifique de la protection des données personnelles

Point d'intérêt majeur de ces dernières années, la protection des données personnelles constitue l'une des clés de voûte de la confiance numérique et fait l'objet d'une règlementation abondante.

Règlement général sur la protection des données personnelles (RGPD)

Le RGPD, applicable depuis le 25 mai 2018, constitue le texte de référence en matière de protection des données à caractère personnel au niveau européen[9]. Il unifie le régime juridique de la protection des données à caractère personnel au sein de l'Union européenne, et met en place une responsabilisation des acteurs du traitement, en faisant notamment peser sur les personnes morales une obligation de sécurité des données.

Dans la mesure où la collectivité territoriale est amenée à collecter, utiliser et transférer des données à caractère personnel, quelle qu'en soit la finalité, elle se doit de le faire en conformité avec le RGPD. Entre autres mesures, les collectivités territoriales doivent désigner un délégué à la protection des données personnelles (DPO), qui peut le cas échéant être partagé avec d'autres collectivités territoriales dans un esprit de mutualisation.

Directive Police-Justice : un cadre européen sur le traitement de données personnelles par les autorités compétentes

Les dispositions de la directive Police-Justice, transposées dans la loi informatique et liberté (cf. ci-dessous) s'appliquent aux traitements de données à caractère personnel lorsqu'ils sont opérés à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites[10].

Le champ d'application de la directive, restreint, est susceptible de s'appliquer à la sécurisation des espaces publics ou en matière de police municipale. Les communes sont soumises à ces dispositions lorsqu'elles exercent dans cette perspective leur mission de prévention de la délinquance.

Loi informatique et libertés (LIL)[11] : encadrement des données personnelles à l'échelle nationale

La LIL contient des dispositions relatives aux « *marges de manœuvre nationales* » autorisées par le RGPD que le législateur a choisi d'exercer ainsi que les mesures de transposition en droit français de la directive Police-Justice. Lorsque les données à caractère personnel des citoyens, des agents de la collectivité territoriale ou des partenaires et prestataires tiers font l'objet d'un traitement, la LIL a vocation à s'appliquer.

Recommandations et bonnes pratiques de la CNIL

La CNIL, régulateur des données à caractère personnel français, accompagne notamment les personnes morales de droit public dans leur mise en conformité avec les normes relatives à la protection des données personnelles.

---

[9] Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[10] Directive (UE) 2016/680 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[11] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les recommandations et bonnes pratiques de cette autorité administrative contribuent à renforcer le cadre juridique existant et à préciser la portée d'une règlementation récente (ex : page de la CNIL dédiée à la mise en conformité au RGPD des collectivités territoriales).

Le Cloud Act[12] *américain et sa potentielle application extraterritoriale*

La loi fédérale *Cloud Act* permet aux autorités américaines de requérir d'un fournisseur de services établis sur le territoire des Etats-Unis la transmission de données dans le cadre de procédures pénales (et non pour les seules activités de renseignement), quand bien même ces données seraient stockées dans un pays étranger.

Concrètement, le recours d'un procureur à une telle réquisition doit s'appuyer sur un faisceau d'indices concordants. En pratique, les grandes entreprises américaines du numérique hébergeant de nombreuses plateformes en ligne (notamment les services *cloud* de Google, Microsoft et Amazon) sont particulièrement concernées par ce texte : les données qui leur sont confiées sont susceptibles d'être accessibles aux autorités américaines.

3) Les obligations applicables aux collectivités territoriales en matière de confiance numérique

Cette section ne se veut pas exhaustive : elle vise à fournir des exemples d'obligations en matière de confiance numérique incombant aux collectivités du fait de textes n'ayant pas la confiance numérique pour objet premier.

Les obligations générales des collectivités territoriales en matière de confiance numérique

Si les textes généraux précités sont pour parties applicables aux collectivités en matière de confiance numérique, aucun texte dédié les visant spécifiquement n'est à relever. Pourtant, il est évident que cette question devient de plus en plus centrale pour les collectivités, et ce dans l'exercice de l'ensemble de leurs missions. Toutes les « grandes » missions historiquement attachées aux collectivités telles que les services administratifs, la distribution d'eau potable, la gestion des établissements scolaire ou encore de police sont nécessairement concernées par la transformation numérique et les enjeux de confiance que celle-ci induit.

Il revient à chaque collectivité d'appliquer les obligations relatives aux missions qui lui sont confiées, et, en l'absence de spécifications relatives à la confiance numérique, d'assurer la qualité qui lui est demandée dans l'exercice de ses missions sur le terrain du numérique.

Les obligations nées du Code des relations entre le public et l'administrations doivent également de manière générale être prises en compte dans les outils numériques mis en place ou utilisés par les collectivités.

Les obligations spécifiques des collectivités territoriales en matière de confiance numérique

Article 47-2 de la Constitution : le respect du principe de sincérité des comptes publics

En vertu du principe de sincérité des comptes publics prévu par l'article 47-2 de la Constitution, les collectivités territoriales doivent présenter des comptes conformes à la réalité de leur exercice comptable annuel. La transmission des dépenses faite par l'ordonnateur des collectivités territoriales au comptable public peut se faire par voie ou support électronique dans certaines conditions précises[13], et le comptable doit pouvoir notamment s'assurer de la fiabilité de l'identification de l'ordonnateur émetteur[14].

Toutefois, il existe un risque de piratage des comptes lors du transfert des données comptables. L'attaquant est susceptible de modifier les bordereaux de dépenses, ce qui aura

[12] H.R.4943 – Clarifying Lawful Overseas Use of Data Act (CLOUD Act), promulgué le 6 février 2018.

[13] Article D. 1617-23 du Code général des collectivités territoriales.

[14] Article 84 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

pour effet de modifier les comptes de la collectivité territoriale. Les collectivités territoriales doivent donc redoubler de prudence et se conformer à la lettre à ces prescriptions.

Loi pour une République numérique : l'obligation pour les collectivités d'ouvrir leurs données

La loi pour une République numérique du 7 octobre 2016 introduit pour les collectivités territoriales de plus de 3 500 habitants une obligation en matière d'ouverture des données (« *open data* » en anglais) de rendre accessibles au public certaines données administratives, notamment :

- Les principaux documents administratifs ;
- Les données, mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental.

Les collectivités territoriales de plus de 3 500 habitants disposant d'au moins 50 agents municipaux doivent mettre en ligne toutes les bases de données dont elles disposent, dans un format ouvert et exploitable, à l'exception des données à caractère personnel et de sécurité. Cela concerne plus de 4 400 collectivités (villes, métropoles, départements et régions).

Les outils informatiques déployés par les collectivités pour respecter cette obligation de l'open data doivent répondre à des exigences de confiance numérique afin que l'intégrité de ces données soit garantie ; et que le moyen de leur mise à disposition ne permette pas l'accès vers d'autres informations ou systèmes n'ayant pas vocation à être ouverts au public.

Le code du patrimoine : les obligations des collectivités en matière d'archivage électronique

Le code du patrimoine dispose que la conservation des archives[15] doit être organisée dans l'intérêt public afin de permettre la documentation historique, mais aussi la gestion des besoins quotidiens des collectivités territoriales et la justification des droits des personnes physiques et morales[16].

De façon générale, on applique le système de la Durée d'Utilité Administrative (DUA), durée légale ou pratique durant laquelle l'archive doit être conservée afin d'obéir aux obligations légales ou règlementaires lorsqu'elles existent, pour prévenir les risques de non-disponibilité de l'archive et pour répondre aux besoins de mémoire de l'administration. Au terme de la DUA, une décision concernant le traitement final du document est prise par le service concerné[17].

L'archivage, lorsqu'il est opéré électroniquement, répond à des enjeux critiques de confiance numérique en matière d'intégrité et de disponibilité de l'archive.

Réforme territoriale engagée par la loi NOTRe : l'obligation pour les collectivités de transférer des données en cas de transfert de compétences

La loi « NOTRe » du 7 août 2015 portant nouvelle organisation du territoire de la République[18] concerne notamment la gestion des données des collectivités territoriales.

Ainsi, dans le cadre d'un transfert de compétences, la collectivité territoriale anciennement compétente doit (i) identifier les données collectées en lien avec la compétence transférée et (ii) assurer leur transfert à la nouvelle collectivité territoriale compétente de façon sécurisée. La nouvelle collectivité territoriale compétente doit ainsi garantir la sécurité de ces données transférées[19].

---

[15] L'article L. 211-1 du code du patrimoine définit les archives comme « *l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité* ».

[16] Article L. 211-2 du code du patrimoine, voir également article L212-3 du code du patrimoine.

[17] Note d'information relative à la durée d'utilité administrative des pièces justificatives des comptes et des dossiers de marchés publics, DGP/SIAF/2018/003.

[18] Loi NOTRe n°2015-991 du 7 août 2015 portant nouvelle organisation du territoire de la République.

[19] A titre d'exemple, la loi NOTRe impose un transfert de compétence du département à la région dans le domaine des transports. A cet effet, les départements doivent identifier les données qui devront faire l'objet d'un transfert à la région afin qu'elle puisse exercer cette nouvelle mission. Ces données qui pourront naturellement inclure des données à caractère personnel devront donc faire l'objet de mesures de sécurité particulières.

FICHE PRATIQUE 2 : REFERENCES ET CONTACTS POUR ALLER PLUS LOIN

Les références et contacts listés par la présente fiche, s'ils brossent un périmètre assez large, ne prétendent pas à l'exhaustivité.

Lectures de référence

Sur le sujet de la cybersécurité et des collectivités, les livrables suivants approfondissent la matière du présent guide :

- guide « *Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation* » de l'ANSSI
- guide « *Cybersécurité : toutes les communes et intercommunalités sont concernées* » produit par l'AMF et l'ANSSI, à paraître fin 2020
- publications de la FNCCR à paraître en 2021 sur trois sujets : législation en matière de cybersécurité, état des lieux des différents systèmes d'information des collectivités, principes techniques et juridiques de cybersécurité des collectivités ;
- guide « *Construire un territoire de confiance et de sécurité* » de la Smart Buildings Alliance

Concernant le sujet clé de la formation des agents, on recommandera :

- les 12 bonnes pratiques de l'ANSSI et de la CPME *ssi.gouv.fr/bonnes-pratiques*
- le cours de sensibilisation de l'ANSSI (« MOOC »), en ligne, simple et gratuit, acessible sur *secnumacademie.gouv.fr*
- le kit de sensibilisation de Cybermalveillance.gouv.fr, accessible à l'adresse *cybermalveillance.gouv.fr/contenus-de-sensibilisation*

Sur les autres aspects abordés dans ce guide, des livrables plus spécialisés existent. Certains d'entre eux peuvent cibler avant tout des organisations dotées de moyens humains et techniques conséquents, mais leurs principes restent valables à toutes les échelles :

- généraliste : guide d'hygiène informatique de l'ANSSI ssi.gouv.fr/hygiene-informatique
- analyse du risque numérique : guide de maîtrise du risque numérique de l'ANSSI et de l'AMRAE *ssi.gouv.fr/guide-maitrise-du-risque-numerique-latout-confiance*
- sous-traitance : guide de l'ANSSI sur la maîtrise des risques en matière d'externalisation *ssi.gouv.fr/externalisation*

Enfin, notamment sur les sujets techniques, on recommandera les nombreuses publications disponibles sur le site de l'ANSSI (*ssi.gouv.fr/administration/bonnes-pratiques*).

Interlocuteurs ou lieux de réflexion sur le sujet de la cybersécurité

ANSSI : L'Agence nationale de la sécurité des systèmes d'information s'est dotée d'un dispositif de contact et d'action visant à soutenir le tissu économique et les institutions à l'échelle régionale. Les coordonnées des référents de l'ANSSI en région sont accessibles sur le site de l'ANSSI : *ssi.gouv.fr/agence/cybersecurite/action-territoriale*.

Réseau DECLIC : Exclusivement dévoué à l'intérêt général des collectivités servies par les structures associées, le réseau DECLIC vise à mutualiser l'information, les expériences, la veille technologique et réglementaire, par une mise en commun d'outils et de moyens. Il rassemble plus de 17 000 collectivités locales. *asso-declic.fr/*

Les fédérations d'élus, comme la FNCCR et l'AdCF, ont également vocation à mener des réflexions et des actions sur le sujet de la sécurité numérique des collectivités et territoires.

La fiche pratique 3 de ce guide aborde le sujet plus spécifique des interlocuteurs en cas de cyberattaques et crises numériques.

FICHE PRATIQUE 3 : INTERLOCUTEURS EN CAS DE CYBERATTAQUES ET AUTRES CRISES NUMERIQUES

La présente fiche recense les principaux points d'accès aux interlocuteurs utiles en cas de cyberattaques et de crises d'origine numérique : prestataire, autorités judiciaires, etc.

Le guichet unique pour les victimes d'actes de cybermalveillance

Le dispositif national d'assistance Cybermalveillance.gouv.fr assure un service d'assistance, de conseils en ligne et une mise en relation avec des professionnels en sécurité numérique référencés sur l'ensemble du territoire.

Dépôt de plainte

Le site de l'ANSSI recense les différents guichets auprès desquels il est possible de déposer plainte en cas de cyberattaque ssi.gouv.fr/en-cas-dincident

Assistance technique

Prestataires de réponse à des incidents de sécurité (PRIS) : si la qualification par l'ANSSI de tels prestataires n'a pas été lancée, le référentiel d'exigences associé a été publié et les prestataires aidant à la remédiation d'incident de sécurité peuvent être questionnés quant à leur respect de ces exigences. Les candidats sont d'ores et déjà référencés sur le site de l'ANSSI : ssi.gouv.fr/pris/

Deux initiatives peuvent par ailleurs être mentionnées en matière d'expertise cyber adaptée à des petits et moyens acteurs :

- le label ExpertCyber porté par Cybermalveillance.gouv.fr et qui couvrent l'expertise en matière de systèmes d'information professionnels, de téléphonie et de sites Internet (cybermalveillance.gouv.fr/tous-nos-contenus/actualites/label-expertcyber) ;
- l'exemple de l'association GACyb portée par la CCI Bretagne Ouest, qui rassemble des entreprises du secteur numérique domiciliées dans le Finistère et signataires d'une charte « cybersécurité des prestataires de services informatiques et numériques ».

A PROPOS DE CE GUIDE

■ Equipe projet

Ce projet de guide a été porté par le département transition numérique, au sein de la direction de l'investissement de la Banque des Territoires :

- François CHARBONNIER, investisseur confiance numérique et chef de projet ;
- Didier CELISSE, responsable marketing & animation territoriale transition numérique ;
- Aymeric BUTHION, chargé de marketing transition numérique ;
- Lucas GRIFFATON-SONNET, investisseur villes et territoires intelligents ;
- Cédric CLEMENT, responsable du pôle confiance numérique.

■ Comité stratégique

Nous remercions chaleureusement les membres du comité stratégique pour leurs nombreux apports en séance et par écrit, tant sur la structure du guide que sur son contenu, et sur les supports associés :

- CNNum – Conseil national du numérique ;
- Commission supérieure du numérique et des postes ;
- Assemblée des communautés de France ;
- Association des maires de France et des présidents d'intercommunalités ;
- Fédération nationale des collectivités concédantes et régies ;
- France Urbaine ;
- Les Interconnectés ;
- Réseau DECLIC ;
- Alliance pour la confiance numérique ;
- Hexatrust ;
- Syntec Numérique ;
- ANSSI ;
- Cybermalveillance.gouv.fr.

■ Interviews

Nous remercions vivement ceux qui ont accepté de répondre à nos nombreuses questions pour alimenter le guide :

- Assemblée des communautés de France : Erwan LE BOT (conseiller enseignement supérieur, recherche et innovation)
- Association des maires de France et des présidents d'intercommunalités : Véronique Picard (conseillère)
- Réseau DECLIC : Emmanuel VIVE (président)

- Insee / Secrétariat d'Etat au numérique : Benoît LOUTREL (mission Régulation des réseaux sociaux)
- ANSSI : Eric HAZANE (chargé de mission stratégie des territoires)
- AFNOR :
    - Stéphane MOULIERE (responsable du département Transport, Energies et Communication)
    - Nicolas MARCQ (chef de projet)
- Smart Building Alliance :
    - Emmanuel FRANÇOIS (président)
    - Patrice DE CARNE (délégué général)
- Capgemini :
    - Thomas PERPERE (responsable de l'offre *Connected Territories*)
    - Alexandre RYCKMAN (chef des projets *Smart City OnDijon* et *CCPHVA*)
    - Jean-Nicolas LOPEZ (*sales public account manager*)
- Suez :
    - Nicolas PREGO (directeur technique et marketing – *Smart & Sustainable Cities*)
    - Sabrina ARCHAMBAULT ALABERGÈRE (*project manager for smart and resourceful cities*)
- Thales :
    - Olivier KERMAGORET (directeur *Segment Critical IT Outsourcing*)
    - Richard KALCZUGA (responsable du *Business development* communication et sécurité)
- Wavestone :
    - Patrick MARACHE (*senior manager*)
    - Guillaume MATTHIEU (*manager*)

■ Coopération

Nous remercions enfin nos prestataires :

- Cepheïd Consulting, pour leur expertise en matière de sécurité numérique, ses idées et ses nombreuses relectures ;
- Bird & Bird, pour leurs travaux sur les risques et responsabilités juridiques.

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE

banquedesterritoires.fr

@BanqueDesTerr

Direction de la communication du groupe Caisse des Dépôts - Octobre 2020 - 20-174-BDT - Imprimerie Caisse des Dépôts