Julie-Charlotte FERREIRA

Quels sont les impacts de la fracture numérique des agents des collectivités territoriales face à la cybercriminalité?

Université BORDEAUX MONTAIGNE
Cyber criminalités

Promotion 2024-2025

Abstract :
Cet article traite des conséquences de la fracture numérique sur les agents des collectivités territoriale et des causes de leur vulnérabilité face à la cybercriminalité. Nous avons choisi de centrer notre étude sur la dimension de la collectivité territoriale car elle nous semble être la plus représentative mais aussi la plus présente sur les territoires français. De plus, cette collectivité a l'avantage de donner à voir une mixité de profils sociaux-professionnels d'une grande richesse.
Nous posons le postulat qu'il semble urgent pour les collectivités locales de tenter de réduire coûte que coûte cette fracture numérique en en faisant une priorité politique et budgétaire, et ce afin de faire monter en compétences et capabilité les agents afin de se prémunir au mieux face au risque de cyber malveillance, tant au niveau individuel que sur le plan collectif.

La fracture numérique au sein des collectivités territoriales se définit par une inégalité d'accès, de compétences et d'usages, un clivage entre des services « connectés » et « déconnectés », des inégalités d'investissements ainsi que par une résistance au changement numérique. La sociologie des usages, le TAM et le concept de capabilité nous éclaire sur les mécanismes de cette fracture.

Cependant, les différentes menaces touchant les collectivités comme le hameçonnage (phising), le rançonnage (ransonware), l'arnaque au président et l'ingénierie sociale ont des répercussions financières, juridiques et réputationnelles directes sur les collectivités. Pour autant, ces pratiques récentes sont encore trop peu prises en compte pour permettre la mise en place d'une base de données performantes, faute d'études, d'analyses, d'indicateurs, de retours d'expériences. Le facteur humain, pourtant central dans les attaques cyber n'est quant à lui pas assez exploité.

Dans les faits, la fracture numérique des agents se manifeste par des inégalités d'accès aux outils ainsi que par des inégalités d'accès structurelles aux ressources, qui engendrent à leur tour des inégalités suivant les profils et les catégories des agents. Cela a pour conséquences un sentiment de déclassement, d'isolement et de stress numérique tout en freinant possiblement leur évolution professionnelle.

La fracture numérique impacte directement les collectivités dans leur gestion du risque cyber, notamment sur les plans opérationnels et financiers, mais aussi psychologiques. La faible culture numérique et le manque de formation des agents à ces bonnes pratiques d'hygiène numérique limitent les capacités de prévention et de réaction des collectivités.

Au final, des leviers d'action existent mais ils restent encore sous-exploités par les collectivités. Des initiatives de formation et d'accompagnement aux évolutions technologiques et à la réduction des risques cyber, l'adaptation des outils numériques et la possibilité d'une gouvernance numérique inclusive semblent incontournables pour réduire du même coup la fracture numérique des agents et la vulnérabilité des collectivités face à la menace cyber.

Introduction

Nous sommes à un tournant de notre société ou la technologie prend le pas sur l'humain et le dépasse. Nos politiques ont également cette volonté de dématérialiser le plus de services publics pour permettre une meilleure gestion des coûts par l'automatisation de certaines tâches. Par exemple, quand dans un passé pas si lointain un agent de l'état civil remplissait avec nous le dossier, aujourd'hui nous devons le préremplir par internet et prendre rendez-vous en ligne pour la validation des pièces du dit dossier avec un agent. Cette fracture numérique est basée sur 3 axes : l'accès (géographique et matériel), les compétences et son usage.

Cette fracture numérique augmente considérablement le risque de cyber attaque. Le facteur humain a la plus grande place car il sera le point d'entrée privilégié du fait d'un manque de formation ou de sensibilisation aux intrusions possibles.

Dans un premier temps, nous définirons le concept de fracture numérique et proposerons un tour d'horizon des différents outils issus des sciences humaines permettant de mieux l'appréhender au sein des collectivités territoriales.

Nous développerons dans un second temps les différentes attaques que peut subir une collectivité et comment celles-ci se matérialisent.

Puis nous verrons comment la fracture numérique affecte les agents des collectivités territoriales face aux cyberattaques.

Ce qui nous amènera à tirer les leçons des impacts directs et indirects de la fracture numérique des agents sur les collectivités qui les emploient.

Enfin nous mettrons en avant des projets qui portent ou porteront leurs fruits dans les prochaines années sur le territoire métropolitain.

Tout au long de cet article, nous décrirons au travers de divers rapports, enquêtes, articles de presse ou d'instituts l'impact du biais qui est l'un des facteurs fondamentaux souvent négligé dans la cybercriminalité : l'humain.

I) Cadre théorique et état de l'art

Le concept de fracture numérique apparu dans les années 1990 renvoie initialement à une inégalité d'accès aux technologies de l'information, en particulier à Internet. Toutefois, les chercheurs ont rapidement souligné que cette fracture ne se limitait pas à un simple accès matériel, mais qu'elle recouvrait aussi des inégalités de compétences et d'usages.

1) Trois niveaux de fracture numérique aujourd'hui couramment reconnus

a) La fracture d'accès :

Celle-ci est liée à la disponibilité des équipements. Cette fracture est d'abord d'ordre économique, ce malgré la démocratisation croissante des appareils permettant un accès au numérique. La connectivité est également une des problématiques, puisque nous ne vivons pas tous dans des zones où l'accès aux réseaux numériques (4G, 5G, fibre…) est accessible, du fait d'un retard de déploiement ou du jeux de différentes politiques publiques.

b) La fracture des compétences :

Cette fracture porte essentiellement sur la formation et la capacité à utiliser les outils numériques. En effet, au-delà de la possibilité d'y avoir accès, encore faut-il avoir des connaissances acquises de façon autodidacte ou par le biais de formation. Encore une fois, une personne ne vivant pas dans un environnement dans lequel elle serait habituée à côtoyer des outils numériques aura plus de difficulté à y développer les compétences requises.

c) La fracture d'usage :

Même si nous pouvons très bien savoir manier les réseaux sociaux et autres applications mobiles au quotidien, la difficulté peut apparaitre lorsque nous passons sur un ordinateur avec des applications dédiées à un métier ou à un but précis. Cette fracture englobe les deux précédentes et pose la question de quoi faire une fois que l'on a l'accès et les compétences.

Ces fractures se cumulent souvent et reflètent des inégalités sociales, générationnelles, territoriales et professionnelles. Dans le monde du travail, elles peuvent engendrer des dynamiques d'exclusion ou de marginalisation, notamment dans les secteurs les moins préparés à la transition numérique.

2) La fracture numérique dans la fonction publique et les collectivités territoriales

La numérisation des services publics a débuté à la fin des années 90 avec la création du programme d'action gouvernemental pour la société de l'information (PAGSI). C'est en 2000 que ce projet se concrétise avec la création du ministère de programmes pluriannuels de modernisation (PPM) et l'avènement du site service-public.fr. Il permet la mise en place d'une administration à accès pluriel pour les usagers. De nombreux projets voient le jour les années suivantes, tel que ADELE, France numérique 2012, France connect… Tous ces plans mis en place par l'état visent à améliorer, moderniser l'accès aux services publics mais également aux agents de pouvoir répondre de façon efficace aux usagers. Toutefois, cette transformation suppose un accompagnement conséquent des agents publics qui en sont les premiers exécutants.

Dans les collectivités territoriales, la diversité des métiers, des niveaux de compétences et des ressources créent un terrain propice aux inégalités numériques internes. Plusieurs travaux ont mis en lumière :

a) Un clivage entre services "connectés" et "déconnectés".

Par "services connectés" on entend ceux dédiés à l'urbanisme, les finances, les RH, dans lesquels les agents ont l'habitude de l'outil numérique car ils l'utilisent tous les

jours dans leur pratique professionnelle et également à titre privée (réseaux sociaux, courriels personnels…). Ils en connaissent les codes. Par “services déconnectés”, on pense aux services techniques, de la petite enfance, de nettoyage, dans lesquels les agents utilisent souvent exclusivement l’outil pour des actions de ressources humaines : e-mails de leur supérieur ou informations de la collectivité, entretien annuel etc. Sur le plan personnel, cette population n’aura peut-être pas accès aux mêmes outils qu’une personne dite “connectée”. Ces outils peuvent prendre la forme d'un accès à un smartphone ou à un ordinateur qui nécessite une connexion en 4G ou fibre de bonne qualité. Au-delà de la question de l’utilisation même se matérialise d’abord le barrage de l'accès à la technique.

La petite collectivité n’a souvent pas les moyens de fournir à tous ses agents des outils et des connexions adéquats, contrairement à d’autres administrations mieux dotées, dans lesquelles les agents bénéficiant du télétravail peuvent avoir accès à un ordinateur et pour certains, selon leurs missions, à un smartphone professionnel.

b) Des inégalités d’investissement dans la formation numérique :

Elles prennent leur source dans l’obligation de gestion des petites collectivités sur des sujets plus tendus ou perçus comme plus prioritaires que la cybersécurité. Il est tout à fait entendable que les priorités ne soient pas portées sur le numérique et la formation des agents. En ce sens, l’entretien et l'administration des écoles ou de la voirie sont souvent les préoccupations premières pour une ville et aussi une partie importante de son budget. Des choix sont à faire et malheureusement nous constatons que le cyber passe toujours au second plan. Une mairie de 300 habitants n’aura pas les mêmes apports financiers qu’une région ou un département et ne pourra mettre en place qu’un service minimum pour un risque équivalent.

c) Une résistance au changement numérique :

Cette résistance met en exergue l’obsolescence du matériel et peut “faire peur” car ce sont de nouveaux investissements parfois très coûteux. C'est en quelque sorte le fameux « ça fonctionne très bien, ne changeons rien ». Cette résistance prend également ses racines dans le sentiment d’incompétence lié à l’évolution rapide des différentes techniques de cyber malveillance. Il s'agit donc bien à la fois de choix en termes d’investissements tant humain que technique.

L’OCDE en 2020 a insisté sur le fait que la fracture numérique au sein du service public ralentit la modernisation de l’administration et accentue les inégalités professionnelles. Dans ce contexte, les agents territoriaux deviennent à la fois vecteurs et victimes de la transformation numérique et de sa sécurité.
Pour expliquer cela nous bénéficions de l'éclairage de plusieurs outils pour tâcher de comprendre un peu mieux les mécanismes de la fracture numérique.

3) Les outils de compréhension en sciences humaines :

a) **La sociologie des usages** :
   Cette approche considère que les technologies ne sont jamais neutres et que leur appropriation dépend des contextes sociaux, culturels et organisationnels. Elle permet de comprendre comment les agents s'approprient ou rejettent les outils numériques en fonction de leur parcours, de leur statut et de leur environnement.
   Certains peuvent s'approprier ces outils parce qu'ils ont déjà été formés ou qu'ils les utilisent directement dans leur activité. D'autres, en revanche, les rejettent car ils les jugent trop complexes ou parce qu'ils n'ont pas ou peu d'accès aux outils et aux réseaux nécessaires à leur utilisation pour des raisons techniques, financières ou géographiques.
   Ce contexte s'est accentué avec l'émergence du Big Data (à partir de 2011) et la numérisation progressive des services publics (depuis les années 2000).
b) **Le Technology Acceptance Model (TAM)** :
   Ce modèle postule que l'intention d'utiliser une technologie dépend de deux variables : la perception de son utilité et la facilité perçue de son utilisation.
   Ce modèle permet d'étudier la manière dont les agents s'intègrent dans un système d'information et de mettre en évidence les écarts entre eux face à l'outil numérique. En effet, tout le monde n'a ni la même perception ni la même utilisation de ces outils. Pour certains, ils représentent un gain de temps ; pour d'autres, une contrainte qui engendre a contrario une perte de temps.
   Des études de besoins sont alors essentielles pour identifier les leviers permettant de mettre en place des formations et des accompagnements ciblés et pertinents, afin de sécuriser au mieux le système d'information (SI) dans une approche humaine et constructive.
c) **Le concept de capabilité :**
   Mis en avant par Amartya Sen et Martha Nussbaum, ce concept montre qu'un agent peut disposer d'un poste informatique (ressource) sans pour autant avoir les compétences nécessaires pour l'utiliser efficacement (capabilité). Il se retrouve alors en situation d'exclusion numérique.
   Ce constat peut également s'appliquer aux usagers des services publics ou privés : ils peuvent posséder un smartphone ou un ordinateur mais ne pas disposer des codes ou des formations nécessaires pour les utiliser. Cette situation peut devenir problématique, voire culpabilisante, lorsque l'on leur assène des phrases comme : « C'est facile, il suffit de passer par Internet ! ».

Dans ce cas, la personne a, en théorie, le choix d'y accéder ou non, car ce n'est pas un problème de ressources matérielles. Elle peut aussi choisir ou non de se former pour acquérir les compétences nécessaires. Ce clivage altère la confiance en soi de l'utilisateur mais aussi celle qu'il place dans l'institution, qui ne lui donne pas toujours les moyens d'être autonome avec les outils qui lui sont proposés, voire imposés.

Fort de ces enseignements théoriques, voyons de plus près quels types de menaces cyber visent les collectivités territoriales et quels moyens celles-ci mettent en place pour y

répondre.

II) Comprendre la cybercriminalité dans le contexte des collectivités territoriales

1) Présentation des différentes menaces impactant les collectivités

Les collectivités territoriales sont confrontées à une variété de menaces cybercriminelles, notamment :

a) Hameçonnage (phishing) :

Elle est l'attaque la plus présente dans les collectivités. Elle consiste dans l'envoi de mails frauduleux visant à récupérer les identifiants et mots de passe d'un utilisateur pour entrer ensuite dans le système d'information en usurpant l'identité de l'agent. Cette technique est également très présente dans notre vie privée avec notamment l'extorsion de données bancaires et a fortiori d'argent. Cette technique représente 46 % des cyberattaques signalées par les collectivités territoriales. Bien que très présente, on constate que si les agents sont suffisamment formés et sensibilisés, celle-ci peut être contournée très facilement et ne pas impacter le système d'information. labo.societenumerique.gouv.fr

b) Rançongiciels (ransomware) :

C'est l'attaque la plus répertoriée dans les collectivités territoriales avec, en 2020, un taux de 30% des institutions touchées, soit une augmentation de 50% par rapport aux années précédentes. Contrairement à l'hameçonnage, celle-ci cause directement des dégâts. Le mode opératoire consiste dans l'envoi d'un mail contenant un lien ou une pièce jointe qui va infiltrer le système d'information en cryptant les données, les rendant inaccessibles. Cette attaque est très préjudiciable car, en plus de paralyser les systèmes, elle peut engendrer une fuite d'informations confidentielles et mettre en péril plus largement les sociétés et les associations qui travaillent avec les collectivités par un effet rebond. Elle a également des conséquences négatives sur la réputation de la collectivité et est responsable d'une forme de défiance de la part des usagers. Il peut y avoir également des retombées juridiques si des informations personnelles sont exfiltrées, rompant ainsi avec les devoirs de la collectivité vis-à-vis de la RGPD. La mise en place d'une infrastructure adéquate permettra de réduire la cyberattaque et à priori de ne pas avoir à verser une rançon pour récupérer les données.

c) Arnaques au président :

Cette technique permet aux cybercriminels de se faire passer pour un supérieur hiérarchique ou un responsable afin d'obtenir des données sensibles voir confidentielles. Cela reste peu courant au sein des collectivités bien qu'il existe un risque réel que cette technique puisse un jour être utilisée pour nuire à une personnalité ou à une collectivité dans le cadre d'ingérence étrangère par exemple.

d) Ingénierie sociale :

Elle consiste en un appel avec prise en main sur le poste de la personne qui aurait reçu un mail frauduleux. La victime est alors manipulée pour obtenir des informations confidentielles ou compromettre le système en envoyant un ransomware.
Un agent peut alors être manipulé par un cyberattaquant lui demandant de payer une rançon ou de transmettre des documents spécifiques, sous couvert de la menace de chantage d'amplifier l'attaque si ce qu'il exige n'est pas fait par l'agent rapidement.
Dans la précipitation, l'agent va payer personnellement la rançon sans savoir si des données ont été corrompues ou subtilisées.
Ministère de l'intérieur. État de la menace liée au numérique en 2019 (2019)

On voit donc que ces menaces exploitent souvent des vulnérabilités humaines et techniques, rendant les collectivités territoriales particulièrement vulnérables.

2) Une problématique encore peu étudiée

Bien que la fracture numérique soit largement documentée dans les sphères éducatives ou citoyennes, les études spécifiques sur les agents des collectivités territoriales restent rares. Plusieurs lacunes sont identifiables :

a) Manque de données empiriques sur le sujet :
Les bases de données ne sont pas exhaustives et manque d'interconnexion pour permettre d'avoir une vision d'ensemble des incidents cyber dans les collectivités territoriales en croisant les données. À cet état de fait s'ajoutent la peur ou la honte d'en parler publiquement, ce qui contribue également à biaiser les résultats.

b) Défaut d'indicateurs :
Il n'existe que peu d'indicateurs pour évaluer le niveau de résilience et/ou la maturité des collectivités en termes de cybersécurité. Les outils d'auto-diagnostique ne sont parfois pas adaptés ou peu abordables pour des petites structures.

c) Absence d'études et d'analyse :
L'absence d'études et d'analyses sur plusieurs années ne permet pas de mesurer l'impact de ces cybers attaques sur la perception interne et externe de la collectivité attaquée. De plus, très peu d'études existent sur les coûts engendrés par ces attaques et leurs répercussions en interne (stress des agents, honte ou mal-être de celui ou celle qui en est la cause).

d) Sous-exploration du facteur humain :
Le facteur humain qui comporte les erreurs, les comportements, ou encore le manque de formation est cité comme central mais reste peu exploré en profondeur dans les recherches appliquées au secteur public.

On déplore enfin un manque d'études et d'analyses sur la culture numérique des élus et des agents, ainsi que sur les freins à l'implémentation des bonnes pratiques.

L'analyse de cette problématique nécessite une approche pluridisciplinaire. C'est pourquoi je propose la mise en place d'un questionnaire visant à mieux saisir la complexité des trajectoires d'appropriation ou de rejet du numérique. Les résultats de cette enquête feront l'objet d'un prochain article. En l'absence de la systématisation d'un feed-back des agents vers la collectivité voyons comment le travail et le bien-être de ces derniers sont impactés par la fracture numérique.

III) Manifestations de la fracture numérique chez les agents

La fracture numérique se manifeste de manière concrète dans les collectivités territoriales à travers plusieurs dimensions, observées à la fois dans la littérature académique et dans les rapports institutionnels récents.

1) Inégalités d'équipement et d'accès aux outils numériques

a) Disparités d'accès aux outils :

Des rapports émanant de la Cour des comptes ainsi que du CNFPT (Centre national de la fonction publique territoriale), notamment celui intitulé "Transition numérique et agents publics : quels enjeux ?" (2021), soulignent les importantes disparités d'accès aux équipements informatiques et numériques au sein des petites collectivités territoriales. Ces disparités concernent en particulier les services techniques et de proximité qui restent souvent à la marge des investissements numériques. Dans ces services dits "déconnectés", les agents disposent rarement d'un poste informatique individuel ou d'un accès stable à une connexion internet.

b) Inégalités d'accès structurelles aux ressources :

Lorsque ces agents souhaitent utiliser des outils numériques, ils sont contraints de partager le matériel disponible ou de se déplacer dans un autre bâtiment, généralement situé au siège de la collectivité, pour accéder à un ordinateur ou à un logiciel métier. Dans certains cas, ils doivent utiliser leurs équipements personnels (téléphones portables, ordinateurs) pour remplir des missions professionnelles, comme indiquer leur position, comptabiliser leurs heures ou consulter leur messagerie. C'est notamment le cas des aides à domicile ou des agents intervenant dans les services à la personne, pour qui le recours à des dispositifs numériques personnels devient une solution palliative mais non encadrée, révélant ainsi une forme d'inégalité structurelle d'accès aux ressources numériques au sein des collectivités.

2) Compétences numériques inégales selon les profils

Selon l'INSEE en 2021, 38 % des agents publics estiment ne pas être à l'aise avec les outils numériques.
Ce chiffre monte à plus de 50 % pour les agents de catégorie C.

Le CNFPT relève également en 2020 un manque d'équipement et de formation, notamment dans les petites collectivités. Mais il ne faut pas négliger les collectivités de taille plus importantes dans lesquelles un brassage important d'agents techniques issus de nombreux services déconnectés sont oubliés. Ils ne sont pris que très peu en compte du fait qu'ils travaillent sur des établissements déportés, hors siège, celui-ci se situant généralement dans de grandes villes où l'accès aux réseaux est bien meilleur que dans les communes éloignées de ce point central, avec des réseaux plus dégradés.
Dans l'étude menée par Aillerie & Schafer (2013) dans **"**Les agents publics face à la transition numérique" (Revue française d'administration publique), des agents administratifs de petites collectivités expriment leur malaise et leur stress face à la généralisation des logiciels métiers sans accompagnements et formations adaptés. Cela bouleverse leur façon de travailler. Bien qu'ils puissent être à l'aise avec l'outil numérique, ils se retrouvent souvent avec des connaissances obsolètes qui ne répondent plus au standard des applications métiers et des services web. Et cela à la suite d'une évolution technique proposée par la collectivité (parapheur électronique, nouveau logiciel de paye, nouveau système d'impression…) précisément sans accompagnements et/ou formations préalables.

3) Résistance au changement et sentiment de déclassement

Tout ceci accentue un sentiment de mise à l'écart chez les plus âgés et les moins qualifiés. Ce sentiment naît clairement d'un manque de formation à l'outil pour mieux appréhender les changements. Cet accompagnement passe par de la remise à niveau régulière et des formations prenant en compte l'humain face à ses nouveaux défis. Cela peut mener à une rupture voire à une défiance vis-à-vis de la collectivité, l'agent ne se sentant plus considéré. Plusieurs travaux montrent que cette résistance n'est pas uniquement liée à une peur du progrès mais à une perte de repères professionnels.

Dans ma collectivité, la mise en place d'un nouveau système de rationalisation des impressions a précisément soulevé des questionnements, voire de la défiance. La nouveauté consistait à s'authentifier pour permettre l'impression de ses travaux. Il a fallu rassurer les agents en leur démontrant que ni leur nom, ni ce qu'ils prévoyaient d'imprimer n'étaient répertoriés. Que cela n'avait pour seul but que de nous (DSI) permettre de gérer et de quantifier les impressions afin d'améliorer le service.

4) Isolement et stress numérique

Certains agents, peu technophiles à l'origine, se trouvent en grande difficulté lorsque leurs habitudes de travail sont modifiées sans accompagnement adapté. Confrontés à des outils numériques nouveaux ou à des procédures dématérialisées, l'adaptation est plus ou moins possible et facile. Certains cherchent à se former par eux-mêmes ou sollicitent des formations spécifiques, tandis que d'autres, découragés, préfèrent déléguer ces tâches à un collègue ou à un membre de leur entourage familial.

Un exemple illustratif est celui d'un agent des espaces verts dont le seul moyen de communication professionnel était un téléphone mobile "à touches". Cet agent m'a confié

ne pas être à l'aise avec la lecture et m'a expliqué que c'était son épouse qui l'aidait à remplir son entretien professionnel annuel et à consulter sa messagerie électronique professionnelle, estimant ne pas être en mesure de le faire seul.

La généralisation rapide de la dématérialisation, en particulier sans formation ni accompagnement adéquat, est génératrice de stress et d'un profond sentiment de mise à l'écart. Cette situation est d'autant plus marquée chez les agents en situation de travail déporté (hors siège de la collectivité) ou peu formés. Le rapport de l'ANACT (agence Nationale pour l'Amélioration des conditions de travail) (2021) met en évidence les risques psychosociaux liés à l'usage du numérique dans le cadre professionnel : surcharge cognitive, isolement, sentiment de perte de sens ou d'inutilité. Ces effets délétères, souvent invisibles, méritent une attention particulière dans la conduite du changement numérique au sein des collectivités.

ANACT, Transformation numérique et qualité de vie au travail dans les collectivités locales, 2021.

5) Freins à l'évolution professionnelle

Le numérique constitue aujourd'hui un critère central dans les métiers administratifs des collectivités territoriales. L'ensemble des fonctions impliquant la gestion ou le traitement de données requiert désormais un accès aux outils numériques et à une connexion réseau stable. Par conséquent, les agents exerçant ces fonctions doivent justifier d'un niveau minimal de compétences numériques pour pouvoir y postuler, ce qui induit une forme de sélection implicite à l'entrée dans ces postes.

Dans une logique d'inclusion, certains postes sont heureusement aménagés afin d'être accessibles aux personnes en situation de handicap, notamment visuel, grâce à des dispositifs d'assistance numérique spécifiques (logiciels de synthèse vocale, claviers adaptés, etc.), permettant leur maintien dans l'emploi. Toutefois, ces initiatives restent limitées.

De manière plus générale, les obstacles d'ordre physique ou les lacunes en matière de formation freinent l'évolution professionnelle d'un certain nombre d'agents. Le CNFPT (2021) souligne à cet égard que de nombreux agents en difficulté avec les outils numériques se sentent enfermés dans leur poste, n'accédant ni aux concours internes ni aux opportunités de mobilité, faute de formations adaptées ou de reconnaissance de leurs compétences acquises en dehors du cadre numérique.

CNFPT, LES IMPACTS DE LA TRANSITION NUMERIQUE SUR LES METIERS DE LA FONCTION PUBLIQUE TERRITORIAL, 2021. Consulté sur : www.cnfpt.fr

L'absence de politiques de réduction de la fracture numérique des agents entraine la mise en place d'un cercle vicieux dans lequel les collectivités territoriales sont toujours plus fragilisé face à la menace cyber grandissante.

IV) Impact de la fracture numérique des agents sur la gestion du risque cyber dans leur collectivité

1) Motivations et modes opératoires des cybercriminels ciblant le secteur public

a) Raisons pour lesquelles les cybercriminels ciblent les collectivités territoriales :

- **Motivations financières** : Le vol de données personnelles et bancaires dans le but de les revendre sur le marché noir ou d'exiger des rançons.
  Docaposte. Cybersécurité des collectivités territoriales : les enjeux (2025)
- **Espionnage et sabotage** : des acteurs étatiques ou soutenus par des États peuvent viser les infrastructures locales pour des raisons géopolitiques et d'ingérences.
- **Activisme (hacktivisme)** : des groupes peuvent attaquer des collectivités pour promouvoir des causes politiques ou sociales.

b) Répercussions de ces attaques :

Tous les modes opératoires décrits ci-dessus entraînent des répercussions qui peuvent être désastreuses :

- **Financières** : coûts liés à la restauration des systèmes et à l'emploi des agents malgré un système d'information hors service le temps de la mise en place d'un plan de continuité d'activité et d'un retour à la normale ou en mode dégradé des services.
- **Juridiques** : responsabilité en cas de non-conformité aux réglementations sur la protection des données (RGPD), pouvant entraîner des sanctions et des procédures judiciaires lourdes.
- **Opérationnelles** : perturbation des services publics essentiels, affectant directement les citoyens. Cela s'est déjà produit dans de nombreux hôpitaux. Blocs opératoires inutilisables, imageries et dossiers patients non accessibles…
  Moins grave mais tout aussi préjudiciable, on pensera aussi à des attaques ayant eu lieu lors de la clôture des demandes de subventions ou de mises en paiement importants, mettant ainsi en difficulté les organismes et entreprises en lien avec l'administration.
- **Réputationnelles** : perte de confiance des administrés et dégradation de l'image de la collectivité et des services publics et plus généralement du numérique.

Il est donc crucial pour les collectivités territoriales de renforcer leur cybersécurité, de former leur personnel et de mettre en place des plans de réponse aux incidents pour atténuer ces risques.

2) Une faible culture numérique des agents territoriaux, facteur de vulnérabilité accrue

La fracture numérique chez les agents des collectivités territoriales se traduit souvent par une faible maîtrise des outils numériques de base, y compris ceux liés à la sécurité informatique. Une enquête menée par Les Interconnectés, en partenariat avec Pix et Syntec Numérique, révèle qu'environ 27 % des agents territoriaux sont classés comme "débutants", tandis que 28 % ne possèdent que des compétences numériques élémentaires. Moins d'un tiers d'entre eux se considèrent réellement autonomes dans leurs usages numériques, ce qui inclut la gestion des mots de passe, la navigation sécurisée et la reconnaissance des menaces en ligne (Les Interconnectés, 2023).

Ce déficit de culture numérique rend les agents plus susceptibles de commettre des erreurs humaines, principal vecteur d'intrusion dans les systèmes d'information selon l'ANSSI, notamment en cliquant sur des liens frauduleux, en réutilisant des mots de passe à sécurité faible ou en négligeant les protocoles internes de sécurité.

Baromètre de la maturité numérique des territoires 2023
Consulté sur : www.interconnectes.com

3) Une exposition accrue aux attaques de type ingénierie sociale et hameçonnage

Les collectivités dont les agents sont peu formés au numérique sont particulièrement vulnérables aux attaques d'ingénierie sociale, qui exploitent l'ignorance ou la naïveté des utilisateurs pour pénétrer les systèmes. Selon Cybermalveillance.gouv.fr en 2022, les techniques d'hameçonnage (phishing) constituent la première méthode d'attaque contre les collectivités, représentant environ 46 % des incidents recensés. Cette part est nettement plus élevée dans les petites communes, souvent éloignées des dispositifs de formation et d'accompagnement.

L'absence de réflexes en matière de vérification des sources, l'ouverture imprudente de pièces jointes, ou encore la diffusion non sécurisée d'informations sensibles facilitent ces attaques, qui peuvent mener à des vols de données ou à l'installation de rançongiciels.

Cybermalveillance.gouv.fr. (2022). Enquête sur l'état de la menace cyber dans les collectivités locales. Consulté sur : cybermalveillance.gouv.fr

4) Des capacités de prévention et de réaction limitées

La fracture numérique ne se limite pas aux usages individuels, elle affecte également la capacité institutionnelle à structurer une réponse efficace face aux cybermenaces. Dans les collectivités à faibles ressources humaines et techniques, souvent rurales ou de petite taille, le manque de personnel compétent empêche la mise en œuvre de mesures proactives telles que les audits de sécurité, la segmentation des réseaux ou la sauvegarde régulière des données.

Docaposte, en 2023, rapporte que 17 % des collectivités territoriales interrogées ont été victimes d'au moins une cyberattaque, avec pour conséquences l'interruption des services

publics essentiels, la compromission de données sensibles et une perte de confiance des usagers. Ces incidents sont aggravés par un manque de préparation organisationnelle, en lien direct avec une sous-qualification des équipes.

Docaposte. (2023). Cybersécurité des collectivités territoriales : les enjeux. Consulté sur : docaposte.com

5) Impact psychologique et organisationnel des cyberattaques

Au-delà des conséquences techniques et financières, les cyberattaques ont également un impact psychologique significatif sur les agents peu familiarisés avec les outils numériques. L'incertitude liée à la gestion de crise, la peur de la faute, ou encore la perte de contrôle sur leur environnement de travail peuvent engendrer du stress, de l'anxiété ou un désengagement numérique, freinant encore davantage leurs capacités d'adaptation.

Ce phénomène engendre un cercle vicieux : plus la fracture numérique est importante, plus la cybersécurité est fragile ; plus la cybersécurité est fragile, plus les agents sont exposés à des tensions organisationnelles et personnelles.

Hornetsecurity (2024) La cybersécurité, point névralgique des mairies et collectivités

La fracture numérique constitue ainsi un facteur aggravant du risque cyber dans les collectivités territoriales, en fragilisant à la fois la composante humaine, organisationnelle et technologique de la sécurité numérique. L'urgence d'un plan de formation ciblé, couplé à une politique d'accompagnement des agents les moins aguerris, apparaît comme un levier stratégique de résilience territoriale.

V) Réponses institutionnelles et leviers d'action

1) Initiatives de formation et d'accompagnement

Le Centre National de la Fonction Publique Territoriale (CNFPT) joue un rôle central dans le développement des compétences numériques des agents territoriaux. Il propose des plans de formation adaptés aux besoins des collectivités, incluant des modules sur la transition numérique, la cybersécurité et l'utilisation des outils numériques.

En 2024, le CNFPT a renforcé son engagement en signant une convention avec le Groupement d'Intérêt Public Pix, visant à évaluer et améliorer les compétences numériques des agents via une plateforme en ligne.

Par ailleurs, des dispositifs tels que le tutorat, le coaching numérique et la mise en place de référents internes sont encouragés pour accompagner les agents dans l'appropriation des outils numériques.
D'autres partenaires permettent d'accompagner les collectivités pour apporter une véritable

expertise comme l'ANSSI, le Campus Cyber, des structures privées également comme Orange Cyberdéfense, Atos.
Tout cela permet aux structures d'apporter aux collectivités les compétences qu'elles n'ont pas pour développer au mieux la "cyber-bienveillance", concept en pleine émergence dans la sphère associative et privée.

2) Adaptation des outils numériques

L'accessibilité numérique est une priorité pour garantir l'inclusion de tous les agents, notamment ceux en situation de handicap. Le CNFPT propose des formations spécifiques pour sensibiliser les collectivités à l'importance de l'accessibilité dans la conception des outils numériques.

De plus, l'ergonomie et la simplicité d'usage des logiciels métiers sont essentiels pour favoriser leur adoption. Des études soulignent l'importance de concevoir des interfaces intuitives et adaptées aux besoins des utilisateurs pour améliorer l'efficacité et réduire les risques liés à une mauvaise utilisation.
La encore, la formation aux outils du numérique en général doit devenir un droit des agents pour ne pas se retrouver en échec et promouvoir l'égalité des chances et ce, qu'importe le métier et le lieu.

3) Gouvernance numérique inclusive

Une gouvernance numérique inclusive implique la participation active des agents dans la définition et la mise en œuvre des projets numériques.
Le CNFPT encourage les collectivités à adopter des approches collaboratives, intégrant les retours d'expérience des agents pour adapter les outils et les processus aux réalités du terrain.

Des initiatives telles que les boîtes à idées numériques ou les plateformes participatives permettent de recueillir les suggestions des agents, favorisant ainsi une meilleure appropriation des outils numériques et une réduction de la fracture numérique au sein des collectivités. La mise en place de questionnaires pertinents permettant de mettre en lumière les habitudes de consommation du numérique des agents ouvrirait également la voie à la conception d'outils de formations indispensables. Ce point nous semble constituer un prérequis indispensable aux opérations de sensibilisation et de prévention des risques actuellement menées.

Conclusion

Cet article a mis en évidence que la fracture numérique constitue un enjeu majeur pour la sécurité des systèmes d'information au sein des collectivités territoriales. Même avec une infrastructure performante (accessibilité aux outils numériques, sécurisation des réseaux informatiques), l'humain reste la principale porte d'entrée des menaces. Sans une bonne compréhension du numérique parmi les agents administratifs qui passe nécessairement par un accompagnement aux évolutions technologiques, la mise en place d'un feed-back via des enquêtes réalisées en interne ainsi que des

formations de mise à niveau et de sensibilisation, il est difficile d'imaginer la mise en place de politiques efficaces et adaptées.

Il est donc essentiel que les collectivités se fassent accompagner par des structures dédiées afin de lutter efficacement contre la cyber-malveillance, nouvelle donnée qu'elles doivent de toute urgence considérer comme une priorité afin de relever les défis des décennies à venir, protéger leurs données, leur budget ainsi que la santé mentale de leurs agents qu'elles se doivent de faire monter en compétences et en capabilité.

S'il est illusoire de penser complétement éliminer ces menaces, cet article démontre qu'il est possible pour les collectivités publiques de mieux les anticiper et s'y préparer en impulsant des changements coordonnés sur les plans politiques et budgétaires, tant au niveau national que local.

Nous appelons de nos vœux les collectivités à placer l'humain au cœur de ces changements à travers la prise en compte et la généralisation d'un concept en pleine émergence : la cyber-bienveillance.

Bibliographie

Docaposte. (2023). Cybersécurité des collectivités territoriales : les enjeux. Consulté sur : docaposte.com

Aillerie & Schafer, Les agents publics face à la transition numérique, Revue française d'administration publique, 2013

Sillicon.fr, 2025, Collectivités la CNIL prépare NIS 2 , Consulté sur : silicon.fr

Senat, 2025, CS Cybersécurité : compte rendu de la semaine du 3 février 2025, https://www.senat.fr/compte-rendu-commissions/20250203/cs_cybersecurite.html#toc2,

Senat, 2023, Les collectivités territoriales face au défi de la cybersécurité, Consulté sur : https://www.senat.fr/rap/r21-283/r21-283.html

Olivier Kempf,2020, Cybersécurité et résilience : les grandes oubliées des territoires, Consulté sur : https://frstrategie.org/publications/notes/cybersecurite-resilience-grandes-oubliees-territoires-2020

Numérique : quelles conséquences sur les agents publics ?, [Dossier] Numérique : quelles conséquences sur les agents publics ? - INTERCOMMUNALITES DE FRANCE, 2024

Attour Amel, Longhi Christian, « Fracture numérique, le chaînon manquant. Les services d'e-administration locale dans les communes françaises », *Les Cahiers du numérique*, 2009/1 (Vol. 5), p. 119-146.La cybersécurité, point névralgique des mairies et collectivités,

Hornetsecurity (2024) La cybersécurité, point névralgique des mairies et collectivités

LOI n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique

Cybermalveillance, Programme de sensibilisation aux risques numériques dans les collectivités territoriales, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales, 2021, 2025.

Léna Jabre , Services publics numériques : quelles mesures pour réduire la fracture numérique?, Gazette des communes, 2021