TENDANCES 2026

DATA, INTELLIGENCE ARTIFICIELLE ET CYBERSÉCURITÉ DANS LES TERRITOIRES

NOTE DE CONJONCTURE

Avec les données de l'Observatoire Data Publica

LA POSTE GROUPE

BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

SOMMAIRE DÉTAILLÉ
P. 3

ÉDITORIAL
P. 4

QUELQUES REPÈRES
P. 5



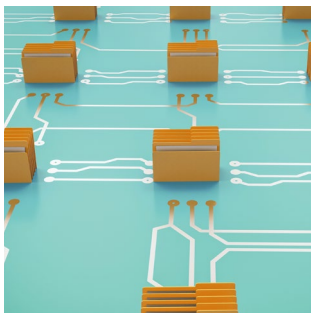
ILS ONT FAIT L'ACTU EN 2026 !
P. 7



LA DATA TERRITORIALE EN 2026
P. 13

2 L'INTELLIGENCE ARTIFICIELLE TERRITORIALE
P. 30





3 LA CYBERSÉCURITÉ DANS LES TERRITOIRES
P. 51

CONCLUSION
P. 74

POUR ALLER PLUS LOIN
P. 75



CARTOGRAPHIE DES TERRITOIRES CITÉS
P. 79

SOMMAIRE

ÉDITORIAL ..... p. 4
QUELQUES REPÈRES ..... p. 5
ILS ONT FAIT L'ACTU EN 2026 ! ..... p. 7

PARTIE 1
LA DATA TERRITORIALE EN 2026 ..... p. 13

Vers un pilotage par la donnée ..... p. 14
Le management de la donnée, stratégie et gouvernance ..... p. 23
La souveraineté numérique : enjeu national, mais pas encore local ? ..... p. 25

PARTIE 2
L'INTELLIGENCE ARTIFICIELLE TERRITORIALE ..... p. 30

Les domaines d'usage de l'IA et les profils des collectivités engagées ..... p. 31
De l'expérimentation au déploiement : l'esquisse d'une méthode ? ..... p. 39
La transformation des organisations et des métiers ..... p. 45

PARTIE 3
LA CYBERSÉCURITÉ DANS LES TERRITOIRES ..... p. 51

Comprendre la menace pour savoir y faire face ..... p. 52
Un chemin pour tous : sensibiliser, anticiper, contractualiser ..... p. 54
Un engagement qui s'accélère pour les grandes collectivités ..... p. 62
Un cadre réglementaire renforcé qui s'impose progressivement aux collectivités ..... p. 68

CONCLUSION ..... p. 74
POUR ALLER PLUS LOIN ..... p. 75
TERRITOIRES CITÉS ..... p. 79

▲ SOMMAIRE

ÉDITORIAL



Stéphanie Fougou,

Directrice générale adjointe
du Groupe La Poste,
Secrétaire générale



Antoine Saintoyant

Directeur de
la Banque des Territoires

Les élections municipales de mars 2026 ont permis l'émergence d'une nouvelle génération d'élus et de décideurs publics, porteuse d'attentes fortes et de défis ambitieux. Dans ce contexte particulier, la Banque des Territoires et le groupe La Poste réaffirment leur engagement à leurs côtés. Ensemble, nous accompagnons les transitions auxquelles ils sont confrontés, avec une conviction : la transition numérique est un levier essentiel pour répondre aux enjeux des territoires, améliorer la qualité du service public et renforcer la relation avec les citoyens.

Cette cinquième édition de la « Note de conjoncture Data, IA & cybersécurité » décrypte les tendances-clés dans un paysage municipal et intercommunal en pleine mutation. Comme chaque année, cette analyse s'appuie sur les données exclusives du baromètre annuel de l'Observatoire Data Publica, notre partenaire.

Cette année, nous vous proposons une plongée inédite dans l'intégration de l'IA, à la fois dans les programmes électoraux et les nominations des nouvelles équipes locales, tandis qu'un sondage Ipsos, mené depuis deux ans auprès des Français, révèle leurs espoirs, leurs attentes et leurs craintes face à cette technologie. Une édition à ne pas manquer pour comprendre les enjeux de demain !

En effet, l'IA s'impose comme un outil incontournable pour permettre une meilleure allocation des moyens, garantir l'efficacité opérationnelle et renforcer la proximité avec les citoyens. Pourtant, son adoption suscite des inquiétudes légitimes, notamment sur sa capacité à transformer les métiers, sa soutenabilité ou encore ses enjeux éthiques. Les territoires pionniers tracent la voie, tandis que d'autres s'interrogent encore sur les cadres de gouvernance à adopter.

Face à ces enjeux, la souveraineté numérique est un pilier essentiel pour bâtir un environnement numérique de confiance. Il est important pour les collectivités de conserver la maîtrise de leurs données, de connaître la localisation de celles-ci et les modèles utilisés.
Face à l'usage massif, parfois détourné, de solutions d'IA extra-européennes, le plan Horizon numérique 2030 place la souveraineté des territoires au cœur de ses priorités. À travers ce plan, le groupe Caisse des dépôts renforce sa volonté, de longue date, d'accompagner les territoires dans leurs transformations, y compris numériques.

Cet engagement s'incarne notamment aujourd'hui dans le programme Territoires d'IA, porté par la Banque des Territoires et destiné à transformer les collectivités avec l'IA souveraine. Dans cette vision, la cybersécurité reste un pilier indissociable. Alors que les collectivités deviennent des cibles privilégiées pour les cyberattaques, il est impératif de sécuriser les données sensibles et de former les agents publics aux bonnes pratiques.

Avec cette édition, la Banque des Territoires et le groupe La Poste, tiers de confiance des territoires, réaffirment leur volonté d'éclairer les acteurs locaux sur les transformations en cours et les défis de demain en matière de transition numérique.

Bonne lecture à toutes et à tous !

▲ SOMMAIRE

QUELQUES REPÈRES

86 % *des collectivités ont déjà mené au moins un projet piloté par la donnée (ou prévoient de le faire dans les prochains mois).*

64 % *des Français font confiance à leur commune ou à leur intercommunalité pour bien utiliser et bien gérer leurs données (contre seulement 44 % à l'Etat).*

Pour que cette confiance reste élevée, **94 %** *des Français considèrent comme prioritaire que les données du service public soient hébergées en France ou en Europe.*

Pour **81 %** *des collectivités, l'utilisation des données sert avant tout à améliorer la qualité du service public .*

44 % *des métropoles font de la souveraineté numérique un enjeu stratégique.*

76 % *des collectivités (hors communes de moins de 3 500 habitants) ont engagé au moins un projet d'IA (ou vont en engager un dans les prochains mois).*

79 % *des Français sont favorables à la construction de systèmes d'IA souverains, qui seraient destinés spécifiquement au service public.*

41 % *des communes (seulement) déclarent s'être dotées d'une stratégie de sécurité informatique.*

▲ SOMMAIRE

L'OBSERVATOIRE DATA PUBLICA

La « Note de conjoncture 2026 » s'appuie sur les résultats des travaux de l'Observatoire Data Publica. **L'Observatoire Data Publica** est une organisation à but non lucratif qui fédère les activités de ses membres en vue de favoriser la réflexion et le débat public sur les usages de la donnée et de l'intelligence artificielle au service de missions d'intérêt général. Chaque année, l'Observatoire produit un baromètre dédié au monde territorial. La réalisation du baromètre bénéficie du soutien de la Banque des Territoires, du groupe La Poste, d'Orange et d'un partenariat avec *La Gazette des communes*.

L'enquête auprès des collectivités a été doublée d'un sondage auprès des Français réalisé pour l'Observatoire Data Publica par **l'Institut Ipsos**.

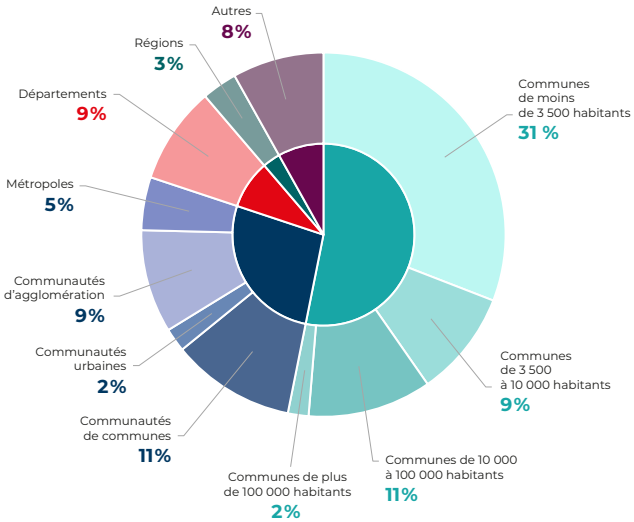
Pour toute information sur les travaux et les publications de l'Observatoire : contact@data-publica.eu

Notices techniques

***L'enquête de l'Observatoire** a été menée durant les mois de juin et juillet 2026 auprès d'un échantillon de **382 collectivités et établissements publics locaux.** L'échantillon rassemble un large panel des collectivités territoriales en France. Certains sujets sont présentés sans les communes de moins de 3500 habitants, la mention en est alors faite.*

***Le sondage du cabinet Ipsos** a été réalisé du 16 au 22 juillet 2026 auprès de 1000 personnes constituant un échantillon national représentatif de la population française âgée de 18 ans et plus, en application de la méthode des quotas : sexe, âge, profession de la personne de référence du foyer, catégorie d'agglomération, département.*

382 collectivités et établissements publics locaux



▲ SOMMAIRE

ILS ONT FAIT L'ACTU EN 2026 !

COMITÉS TERRITO-RIAUX DE LA DONNÉE

Septembre 2025 : installation du premier comité territorial de la donnée en outre-mer

À la Réunion, le conseil régional réunit pour la première fois les acteurs publics du territoire (préfecture, conseil départemental, EPCI, agences de l'État, etc.) et de nombreux producteurs et utilisateurs de données qui présentent un caractère d'intérêt général. Objectif : identifier des thématiques prioritaires pour installer des coopérations autour de la donnée (et de l'intelligence artificielle) et installer une gouvernance adossée à des principes définis en commun. Cette initiative, pionnière en outre-mer, s'inscrit dans la dynamique de création des comités territoriaux de la donnée, inaugurée notamment dans les régions Occitanie, Grand Est, Île-de-France ou encore Pays de la Loire.



SOUVE-RAINETÉ

Février 2026 : la Caisse des dépôts lance le plan Horizon numérique 2030

La Caisse des dépôts annonce la mobilisation de 18 milliards d'euros, d'ici 2030, pour accélérer la transformation numérique et renforcer la souveraineté technologique française et européenne. Le plan Horizon numérique 2030 fixe six priorités parmi lesquelles : faire émerger des champions européens ; développer des solutions souveraines pour les acteurs publics ; accélérer la transition numérique des territoires et des entreprises ; rendre les Français acteurs de leur quotidien numérique.

▲ SOMMAIRE

ÉLECTIONS MUNICIPALES

Mars 2026 : ingérences étrangères, les municipales aussi dans le viseur

Les élections municipales deviennent à leur tour la cible des ingérences numériques étrangères. Viginum, le service de l'État, indique avoir détecté quatre opérations visant spécifiquement le scrutin des 15 et 22 mars 2026, dont deux liées à des modes opératoires prorusses déjà connus.

Faux reportages, comptes inauthentiques, usurpation de médias ou de candidats : les techniques se diversifient avec un recours croissant à l'IA générative. Plus d'une centaine de faux sites en « .fr », imitant notamment des médias locaux, ont été ainsi alimentés par des contenus reformulés par IA. Bonne nouvelle, toutefois : Viginum estime que les opérations détectées ont bénéficié d'une visibilité limitée.



JUMEAUX NUMÉRIQUES

Avril 2026 : lancement de JUNN, le jumeau numérique national au service des territoires



Les jumeaux numériques passent à la vitesse supérieure ! L'État annonce 25 millions d'euros pour développer JUNN, porté par l'IGN, le Cerema et l'Inria. Le projet doit fournir un socle technologique commun et souverain, sur lequel pourront s'appuyer différents jumeaux numériques territoriaux.

Objectif : mutualiser des briques logicielles, des standards d'interopérabilité et des capacités de traitement, de visualisation et de simulation. Les usages envisagés sont nombreux : aménagement urbain, mobilité, gestion de l'eau, prévention des risques naturels ou encore adaptation au changement climatique… Le projet voit grand : autour d'un consortium de 14 partenaires publics et privés avec, pour chef de file, la société VertiGis, une « équipe de France » réunit déjà plus de 200 acteurs.

Après plusieurs années d'expérimentations locales, JUNN vise désormais à donner aux jumeaux numériques un socle commun pour leur permettre de changer d'échelle.

▲ SOMMAIRE

TERRI-TOIRES D'IA

Mai 2026 : la Banque des Territoires veut accélérer le déploiement de l'IA dans les collectivités

La Banque des Territoires lance Territoires d'IA, un programme destiné à accompagner les collectivités dans le déploiement et l'usage de l'intelligence artificielle souveraine. Objectif affiché : accompagner 100 000 agents publics et développer 15 cas d'usage duplicables d'ici 2030.

Le dispositif associe une IA Factory, développée avec Mistral AI, un guichet de cofinancement, de l'appui en ingénierie et des ressources mutualisées. Quatre premiers cas d'usage sont déjà lancés : analyse des pathologies routières en Côte-d'Or, assistance aux secrétaires de mairies rurales dans le Grand Est, traitement des signalements sur la voirie à Bordeaux Métropole et outil d'aide à l'analyse financière des établissements médico-sociaux. Derrière le programme, un même enjeu : faciliter l'adoption de l'IA et favoriser des solutions réutilisables d'un territoire à l'autre.

Territoires d'IA
le programme

EUROPE

Juin 2026 : l'Union européenne veut réduire ses dépendances technologiques



Dans un contexte de dépendance persistante vis-à-vis des technologies américaines et chinoises, la Commission européenne présente une nouvelle série de mesures consacrées à la souveraineté technologique. Semi-conducteurs, IA, cloud et open source sont au cœur du dispositif. Parmi les objectifs affichés : tripler les capacités des centres de données en Europe dans les cinq à sept prochaines années, tout en renforçant les alternatives européennes dans le cloud, l'IA et l'open source.

▲ SOMMAIRE

CYBER-SÉCURITÉ

Juin 2026 : le Cyber Resilience Act commence à s'appliquer

Caméras connectées, compteurs intelligents, logiciels : l'Union européenne (UE) commence à mettre en œuvre son Cyber Resilience Act, qui impose de nouvelles exigences de cybersécurité aux produits comportant des éléments numériques commercialisés en Europe.

Le principe est simple : la sécurité doit être prise en compte dès la conception du produit et tout au long de sa durée de vie. Les fabricants devront notamment corriger les vulnérabilités et assurer les mises à jour de sécurité nécessaires. Pour les collectivités, le texte européen devrait donc se traduire par des produits numériques mieux sécurisés, à l'exclusion des solutions purement cloud.



ÉLECTIONS MUNICIPALES (SUITE)

Juin 2026 : l'IA entre dans les délégations des exécutifs locaux



Après les élections municipales de mars 2026, l'Observatoire Data Publica a analysé les délégations dans les 100 plus grandes villes et les 100 plus grands EPCI. Le numérique reste solidement installé dans ces exécutifs locaux : 87 % d'entre eux ont désigné au moins un élu en charge de ces sujets. La nouveauté vient de l'intelligence artificielle. En 2020, seuls 3 élus municipaux avaient une délégation mentionnant l'IA et aucun dans les EPCI. En 2026, ils sont 14 dans les communes et 14 dans les intercommunalités.

▲ SOMMAIRE

IA : L'AVIS DES INSPECTIONS GÉNÉRALES

Juillet 2026 : l'IA dans l'administration, sujet d'un rapport des inspections générales

Rendu public début juillet, un rapport conjoint de trois inspections générales (celles des finances, de l'administration et des affaires sociales) se penche sur le déploiement de l'IA dans les administrations publiques. Il constate une diffusion rapide mais encore dispersée des usages et souligne que les transformations induites par l'IA sont avant tout organisationnelles et humaines.

Parmi leurs 13 recommandations : associer davantage les agents et les usagers, anticiper l'évolution des emplois et des compétences, renforcer la formation et surtout développer un « dialogue social technologique » autour des stratégies et des projets d'IA. Un message qui fait directement écho aux premières démarches engagées dans les collectivités : le déploiement de l'IA ne peut pas être traité comme un simple projet technique !



DATA ET CANICULE

Juillet 2026 : la data pour identifier les personnes âgées isolées lors d'épisodes de canicule

Depuis 2004, les communes doivent tenir un registre des personnes vulnérables à contacter en cas de fortes chaleurs. Jusqu'ici, l'inscription reposait essentiellement sur le volontariat, avec une couverture très partielle des publics concernés. Un décret publié en juillet 2026 change la donne : désormais, les registres pourront être enrichis automatiquement (sauf opposition des personnes concernées) grâce au croisement de données détenues par les organismes chargés de l'autonomie et de l'action sociale territoriale. Plus de 2 millions de personnes supplémentaires pourraient y être intégrées. Un exemple très concret de ce que le partage de données peut apporter à l'action publique locale.

▲ SOMMAIRE

FUITES À RÉPÉTITION DANS LES SERVICES PUBLICS

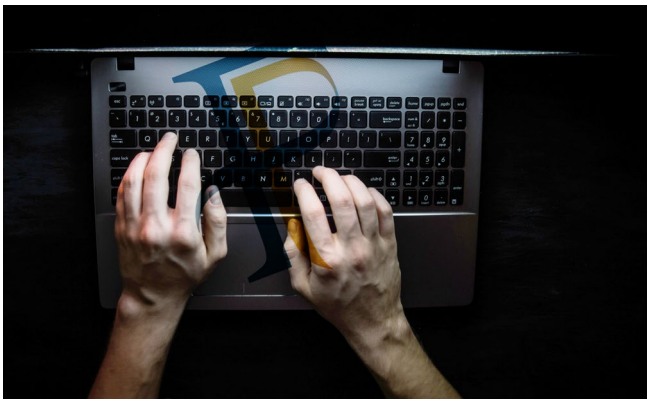
Août 2026 : quand une fuite de données à la DGFiP déclenche une crise politique

Dans le prolongement des fuites de données ayant touché plusieurs services publics depuis le début de l'année, la DGFiP a signalé des intrusions revendiquées par un groupe cybercriminel. Selon le bilan initial communiqué par Bercy, celles-ci auraient permis la consultation ou l'extraction d'informations concernant 678 000 particuliers et professionnels. Les intrusions, qui se seraient déroulées en juin et juillet, reposeraient sur un mode opératoire élémentaire : l'usurpation des identifiants d'un agent et d'un tiers habilité, donnant accès aux systèmes concernés. État civil, coordonnées, situation familiale, revenus, données d'entreprises et informations cadastrales figurent parmi les éléments exfiltrés. La DGFiP a saisi la CNIL, déposé plainte, informé les personnes concernées et engagé des investigations et des mesures complémentaires avec l'Anssi.

Vu les inquiétudes légitimes des citoyens, des instructions ont été données aux ministères et à l'Anssi, qui a mis en place une capacité renforcée de réaction, d'intervention et d'assistance aux services de l'État baptisée Reactiv.

Mais les alertes se succèdent à un rythme de plus en plus élevé, mettant en lumière la vulnérabilité de nos infrastructures face à une menace qui monte inexorablement. Plusieurs administrations et agences de l'État, deux régions, les SDIS de sept départements différents, mais aussi de nombreuses communes et intercommunalités ont ainsi fait l'objet de cyberattaques visant à l'exfiltration de données durant les mois d'août et septembre. Cette situation interroge la robustesse de notre transformation numérique et la continuité du lien de confiance avec les usagers.

Les commissions d'enquête demandées au Sénat et à l'Assemblée nationale devront approfondir, si elles sont créées, les responsabilités politiques et administratives et faire des propositions.



▲ SOMMAIRE

PARTIE 1

LA DATA TERRITORIALE EN 2026

Dans les territoires, l'année 2026 a été marquée par les élections municipales. Les années électorales sont toujours particulières pour le déroulement des projets : certains s'accélèrent en fin de mandat, d'autres sont mis en pause et quelques-uns peuvent être abandonnés. Les projets data n'échappent pas à la règle. En 2026, le nombre de collectivités engagées dans des projets data est relativement stable, même s'il reste élevé (7 collectivités sur 10). C'est une première, car depuis qu'existe le baromètre de l'Observatoire Data Publica (2022), ce nombre n'avait cessé d'augmenter.

Les usages de la donnée demeurent très variés. Strate par strate et compétence par compétence, ils concernent tous les métiers de l'action publique territoriale.

On notera que le sujet a été présent dans les programmes électoraux de façon inédite : data et transparence démocratique, efficience de la gestion publique, inclusion numérique… Logiquement, dans de nombreuses municipalités et intercommunalités, les élus ont hérité d'une délégation qui pourrait rendre visibles les enjeux de la gestion des données. D'autant que l'engouement pour les outils d'intelligence artificielle se heurte souvent à des problèmes de données disponibles. « Pas d'IA sans data ! » nous dit-on… Alors, commençons par la data !

▲ SOMMAIRE

VERS UN PILOTAGE PAR LA DONNÉE

Année après année, une réalité s'impose : tous les métiers de l'action territoriale sont concernés par une progressive « mise en données ». Pour certaines fonctions urbaines, il s'agit dorénavant d'un véritable pilotage par la donnée. On le constate notamment dans les compétences des intercommunalités, avec la gestion de l'eau, des déchets, de l'éclairage public. Le thème de la smart city (« ville intelligente ») est sans doute passé de mode, mais les outils, eux, se généralisent. Cette évolution est parfois liée à des choix technologiques subis. Pensons par exemple à l'arrivée des compteurs Linky dans les bâtiments communaux. La question qui se pose aux collectivités, quelle que soit leur taille, est celle de l'utilisation des données mises à disposition par Enedis : servent-elles uniquement au règlement des factures ou sont-elles analysées pour réduire les consommations électriques ? Dans bien des cas, l'accroissement considérable du volume des données à traiter est aussi le fruit de choix : déploiement d'un éclairage dit « intelligent », utilisation de la lecture automatique des plaques d'immatriculation (LAPI) pour gérer le stationnement, technologies avancées de détection de fuites dans un réseau d'eau, dispositif de vidéoprotection ou parfois même construction d'un jumeau numérique.



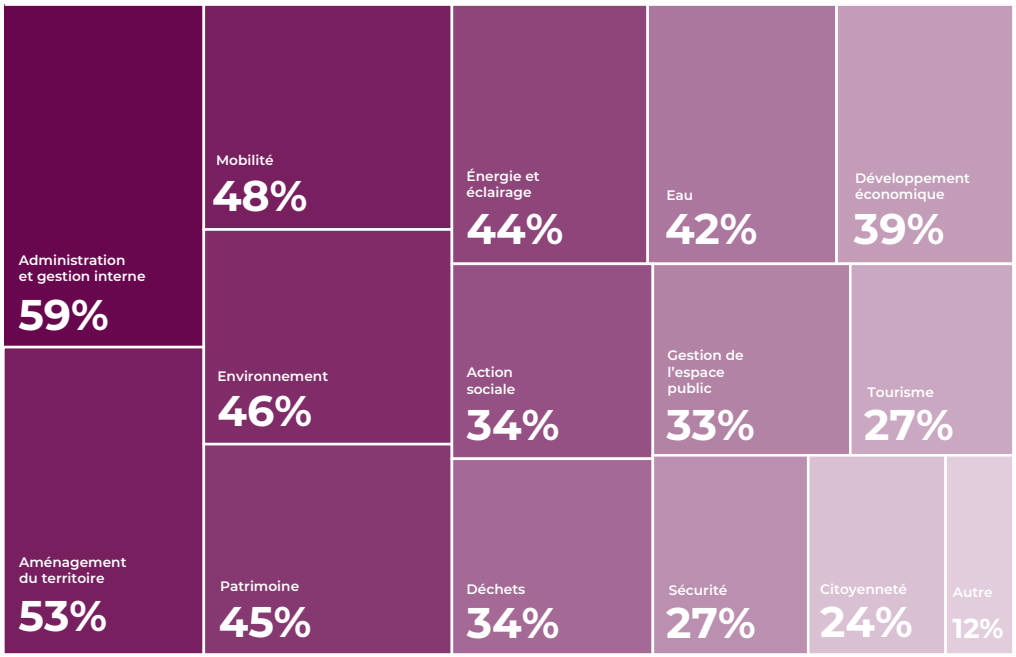
Un point attire l'attention : pour la deuxième année consécutive, le domaine le plus cité par les collectivités dans le baromètre de l'Observatoire Data Publica est celui de l'administration et de la gestion interne. Depuis toujours, la donnée est présente au cœur de la décision publique et de la gestion quotidienne des administrations. Mais, pendant des décennies, les données ont été considérées comme des sous-produits de l'action publique. Elles étaient parfois de piètre qualité, pas toujours bien conservées, peu exploitées. Force est de constater que les choses changent. Les données de gestion sont de plus en plus souvent tenues pour un patrimoine. Leur bonne utilisation devient un enjeu. Cela vaut pour les données des usagers. De plus en plus de territoires veillent à simplifier la relation usager grâce au principe « Dites-le-nous une fois », ce qui suppose de disposer d'un référentiel de données et de contrôler leur qualité. Cela vaut aussi pour les données de gestion. Les tableaux de bord de DG laissent parfois la place à des outils dynamiques qui permettent des mises à jour et des décisions en temps réel. Nous le verrons, cette tendance devrait être largement amplifiée par l'arrivée d'outils de gestion qui intègrent de l'intelligence artificielle.

Un autre sujet mérite que l'on s'y attarde : l'action sociale. Les données du social sont principalement gérées par les communes et leur CCAS, et les conseils départementaux. Le baromètre 2026 révèle que 64 % des conseils départementaux pilotent certaines politiques sociales par la data et que 15 % prévoient de le faire dans les prochains mois. Un lien peut, sans grand risque, être établi entre ces chiffres, en nette progression, et la nécessité de faire face aux difficultés budgétaires des départements.

▲ SOMMAIRE

Globalement, toutes strates et politiques publiques confondues, 86 % des collectivités ont engagé au moins un projet data dans l'année ou s'apprêtent à le faire. Ce chiffre, bien qu'élevé, est relativement stable. Mais une évolution marquante concerne les petites et même les très petites communes. 47 % des communes de moins de 3 500 habitants ont déjà engagé des projets sur la data et 23 % annoncent vouloir le faire. Elles étaient seulement 6 % dans le premier baromètre en 2022. Il s'agit donc d'un fait notable, qui s'explique de plusieurs manières : mise à disposition de nouveaux outils numériques pour la gestion quotidienne, réduction des coûts – et tout particulièrement des dépenses énergétiques –, apports des délégataires de service public et d'opérateurs mutualisés (des syndicats mixtes, notamment) ou, bien sûr, intérêt des élus. Pour approfondir ce point, nous renvoyons le lecteur à l'entretien mené avec le vice-président de l'Association des petites villes de France (APVF).

Collectivités ayant des projets data en cours pour chacun des domaines* :
**Total hors communes de moins de 3 500 habitants.*



▲ SOMMAIRE

LA DATA AU SERVICE DE LA POLITIQUE DE L'ÉDUCATION

Élancourt

Ville-pilote en matière de modernisation du service public dans de nombreux domaines (scolaire, périscolaire, sécurité…), Élancourt (Yvelines, 26 000 habitants) s'attelle désormais au chantier du pilotage de ses politiques publiques par la donnée, notamment dans les domaines de l'enfance et de l'éducation.

Lancé en septembre 2025, le projet vise à construire des outils d'exploration, de visualisation et d'analyse des données : analyse des taux de fréquentation des structures, évolution de la population scolaire, étude des tarifs, etc.

Le pilotage des politiques publiques par la donnée constitue l'une des priorités du nouveau mandat. Ces outils doivent permettre aux élus comme aux équipes administratives d'éclairer les décisions structurelles en s'appuyant sur des analyses chiffrées, par exemple en anticipant l'évolution des effectifs scolaires pour adapter finement les bâtiments et les services.

La commune ne cache pas son ambition pour ce projet-pilote, sans pour autant vouloir se précipiter. Elle a pleinement conscience que le travail autour de la donnée peut rapidement conduire à multiplier les pistes et les usages. Autre défi majeur : mobiliser les services, qui disposent chacun de leurs propres objectifs, calendriers et vocabulaires métiers.

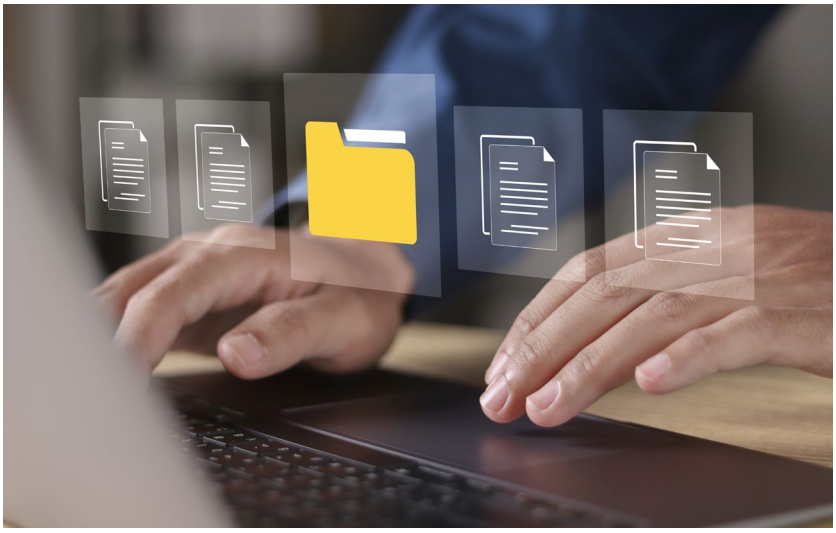
Pour Angélique Ceconi, responsable de la cellule Data et Archives, et Fabien Couturier, directeur des Moyens généraux, qui pilotent conjointement l'initiative avec l'appui de la DSI : *« La réalisation d'un projet data, c'est avant tout dialoguer avec les métiers. »*



▲ SOMMAIRE

DATA ET RELATION À L'USAGER

Grand-Orly Seine Bièvre



Depuis juillet 2025, une solution de suivi est expérimentée pour centraliser les informations issues des différents services et construire à terme un tableau de bord commun à destination de la direction générale et des élus. *« Très récemment, on s'est encore posé la question de l'outil qu'on allait retenir pour conduire une enquête de satisfaction dans le réseau de nos médiathèques. Demain, ce genre de question ne devra plus exister : on utilisera naturellement l'outil unique de la collectivité »*, expliquent Thomas Courtial, directeur du pôle numérique, et Damien Monnerie, chef de projet GRU.

L'objectif est moins de disposer d'un nouvel outil que d'harmoniser progressivement les pratiques, les processus et les bases de connaissances entre les directions. À cette fin, la démarche repose sur un groupe « projet » associant plusieurs métiers – médiathèques, équipements sportifs, accueil des usagers, déchets ou encore communication – afin de construire des règles et des pratiques communes.

Cette harmonisation des processus numériques présente aussi un enjeu de cybersécurité : la multiplication des comptes et des outils de gestion des usagers accroît mécaniquement l'exposition aux risques, ce qui renforce l'intérêt d'une approche commune et maîtrisée.

Pour l'EPT, le principal défi reste cependant organisationnel. Comme le résument les porteurs du projet, *« les agents ont leurs propres métiers à faire, avant d'être des producteurs de données »*. La réussite du projet suppose donc de montrer en quoi la saisie de données fiables, partagées et interopérables contribue à améliorer le service rendu aux habitants.

▲ SOMMAIRE

DATA ET RELATION À L'USAGER

Nanterre

À Nanterre (Hauts-de-Seine, 98 000 habitants), la qualité de la relation à l'usager est un engagement politique fort avec, en 2026, la désignation d'un conseiller municipal aux relations usagers.

Sous l'impulsion de sa direction générale, la Ville met en place, dès janvier 2025, un tableau de bord de suivi et d'analyse des correspondances avec les usagers. Il mesure le nombre de sollicitations et le délai de réponse de chaque direction afin d'identifier les améliorations à apporter à la gestion des échanges. Dans certaines directions, ces enseignements ont permis de clarifier la chaîne de traitement et les acteurs y intervenant, notamment par une meilleure appropriation de l'outil de gestion des correspondances et une homogénéisation des règles de gestion.

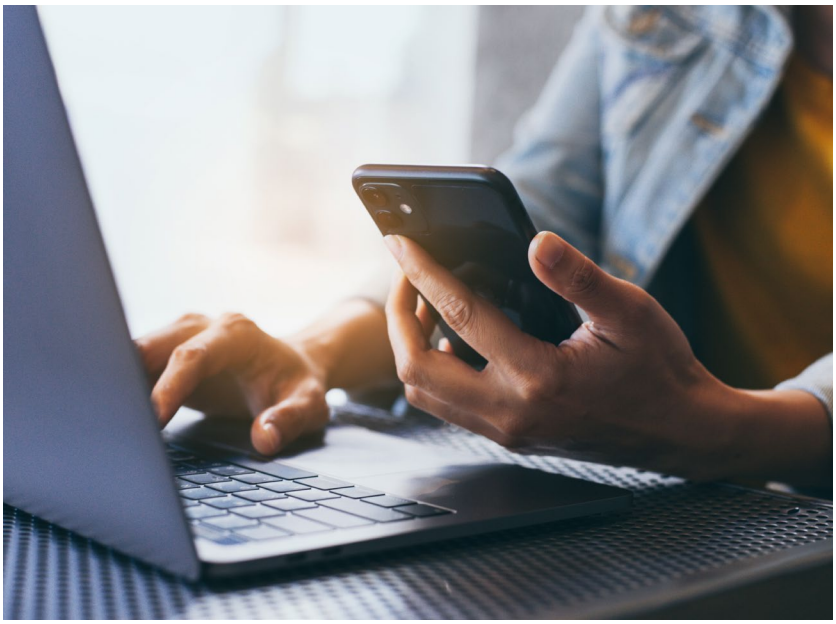
Un an après, cette démarche porte ses fruits : entre janvier 2025 et janvier 2026, le délai moyen de réponse a diminué de 63 %. Mais surtout, ce travail a permis de développer une culture de la relation usager et de mettre en place une gouvernance interne pour la porter afin d'aligner élus, DG et directions sur une même ambition.

Forte de ce premier résultat, Nanterre a déployé le même principe pour la gestion des appels téléphoniques, en mesurant le taux de décroché au sein des différents services. Cette deuxième phase a connu la même réussite : le taux d'injoignabilité téléphonique a diminué de 32 % entre janvier 2025 et janvier 2026.

Selon les directions et services impliqués dans cette démarche (service à la population, secrétariat général, mission « observation et prospective », direction des systèmes d'information et de la transformation numérique), c'est tout le travail de sensibilisation et d'accompagnement des directions métiers qui a ancré cette dynamique de qualité de relation à l'usager dans le quotidien des agents pour le placer au centre, au-delà des logiques métiers.

Pour l'avenir, la collectivité souhaite élargir la méthode aux démarches en ligne et à l'accueil physique des Nanterriens dans l'objectif d'unifier les parcours et de constituer une vision à 360 °.

La gestion de la relation aux usagers constitue ainsi un cas d'usage-pilote d'une démarche plus globale de la stratégie data de la Ville, visant à mieux structurer les données internes et à améliorer le pilotage de l'activité en faisant de l'outillage un levier et non une contrainte.



▲ SOMMAIRE

DATA ET PILOTAGE DES FINANCES DÉPARTEMENTALES

Côte-d'Or



Le projet de prospective financière du département de la Côte-d'Or (540 000 habitants) démarre en 2020, dans le contexte de la crise sanitaire. Alors que de nombreuses analyses anticipent une forte baisse des recettes issues des droits de mutation à titre onéreux et de la cotisation sur la valeur ajoutée des entreprises, le pôle Ressources du département prévoit au contraire une relative stabilité. Pour réduire l'incertitude et objectiver ses hypothèses, la collectivité développe en interne un algorithme de modélisation de l'évolution de ses recettes.

L'enjeu est important pour le territoire : 85 % de ses investissements profitent à des entreprises locales. La qualité du pilotage financier conditionne donc la capacité de la collectivité à préserver son effort d'investissement et à éviter que le soutien au tissu économique ne devienne une variable d'ajustement budgétaire.

Le développement de l'outil a conduit la collectivité à s'interroger sur le choix des indicateurs à mobiliser. *« La France ne manque pas de données disponibles. On était alors tentés d'utiliser tous les indicateurs à notre disposition. Notre enjeu était de ne pas intégrer trop de variables qui ne survivraient pas à l'épreuve du temps »*, confie Stephen Loureiro, directeur de la transformation et adjoint au directeur du pôle Ressources et Accompagnement des transformations.

Certaines variables pouvaient expliquer avec précision des évolutions passées, sans constituer pour autant de bons indicateurs pour l'avenir. Le département a par exemple identifié des corrélations avec le nombre de jeunes adultes présents sur le territoire, mais cette donnée s'est révélée trop difficile à anticiper dans le temps. La Côte-d'Or a donc privilégié la robustesse et l'explicabilité des variables plutôt que la multiplication des indicateurs. Cela n'a pas empêché la collectivité d'aboutir à un algorithme qui, depuis 2021, atteint un niveau d'exactitude de 96 %.

L'année 2025 a permis de confronter le modèle à un contexte financier plus instable. *« Entre 2016 et 2022, modulo la crise sanitaire, on était sur un cycle haussier. Ces deux dernières années, on a cependant connu un crash à la baisse, puis une période de reprise. Cela nous a permis de tester notre outil sur un contexte de variations financières plus importantes »*, confie Stephen Loureiro. Les résultats observés en 2026 restent proches des prévisions produites par le modèle.

Néanmoins, le département conserve une approche prudente : par définition, la prospective financière reste incertaine. L'outil n'a pas vocation à prédire parfaitement l'avenir, mais à mieux éclairer les décisions budgétaires en s'appuyant sur des données robustes, explicables et interopérables.

▲ SOMMAIRE

QU'EN PENSENT LES FRANÇAIS ?

La méfiance des Français à l'égard de l'usage généralisé des données dans la société semble s'installer durablement : en 2026, 64 % considèrent que leur usage croissant est une mauvaise chose, une proportion identique à celle observée en 2025.

Dans ce contexte, la confiance accordée aux acteurs publics locaux résiste. 64 % des Français font confiance aux communes et aux intercommunalités pour la gestion et l'utilisation des données et 60 % aux départements et aux régions. Ces niveaux sont stables par rapport à 2025 et restent nettement supérieurs à ceux accordés à de nombreux acteurs privés, notamment aux réseaux sociaux, auxquels seuls 11 % des Français accordent du crédit.

Mais cette confiance ne signifie pas que l'utilité de la donnée va de soi. 66 % des Français jugent utile son utilisation par les communes et intercommunalités pour améliorer la vie des habitants (contre 70 % en 2024 et 73 % quatre ans plus tôt). Même tendance concernant la data comme outil pour réduire les dépenses publiques, jugée utile par 63 % des Français.

Les bénéfices attendus restent par ailleurs très liés aux usages : améliorer les politiques de santé (pour 48 % des Français), la gestion des déchets (41 %) ou encore les transports et la mobilité (37 %). La confiance reste toute-fois fragile. Si le RGPD est connu de trois Français sur quatre, seuls 37 % déclarent bien voir de quoi il s'agit. Surtout, la confiance dans ce règlement, destiné à protéger les données personnelles, s'érode : elle s'établit à 59 % (contre 66 % en 2022).

LE REGARD DE L'OBSERVATOIRE DATA PUBLICA

La confiance des Français envers les acteurs publics locaux constitue un capital précieux. Mais les résultats de notre enquête montrent surtout que les conditions pour l'entretenir sont désormais clairement posées. Qu'il s'agisse de données, d'intelligence artificielle ou de souveraineté numérique, près de 9 Français sur 10 demandent davantage de maîtrise, de transparence et de garanties : savoir quand une IA est utilisée, conserver un contrôle humain, encadrer les usages ou encore s'assurer que les données du service public sont hébergées en France ou en Europe.

Les collectivités semblent avoir entendu une partie du message. Elles sont nombreuses à se doter de chartes, de cadres internes, de groupes de travail ou de feuilles de route sur l'IA. Certaines commencent également à objectiver leurs dépendances numériques et à interroger plus directement leurs choix technologiques.

Ces démarches peuvent aussi devenir des instruments de confiance vis-à-vis des citoyens et ainsi contribuer à rendre plus concrètes et visibles les garanties apportées. L'enjeu est moins d'ajouter de nouvelles règles que de donner à voir la maîtrise exercée par les acteurs publics sur leurs usages de la donnée et de l'IA.

Les Français indiquent assez clairement la voie. Le capital de confiance existe encore : l'enjeu, désormais, est de l'entretenir par des actes.

▲ SOMMAIRE



JEAN-MICHEL MORER

Vice-président de l'Association des petites villes de France (APVF)

Jean-Michel Morer est vice-président de l'Association des petites villes de France (APVF), chargé du numérique et de l'éducation. Il suit depuis plusieurs années, pour l'APVF, les travaux nationaux sur la cybersécurité, l'inclusion et la souveraineté numérique, en lien avec les services de l'État et les représentants des territoires.

C'est dans les petites collectivités que la progression des usages de la donnée a été la plus forte. Selon le baromètre de l'Observatoire Data Publica, la proportion de communes de moins de 3 500 habitants ayant engagé au moins un projet data est passée de 6 % en 2022 à près de la moitié en 2025. Qu'est-ce qui explique cette évolution ?

Auparavant, les collectivités exploitaient leurs données *via* des solutions hébergées sur leurs propres serveurs, ce qui exigeait une expertise importante. La multiplication des solutions d'éditeurs, le développement du SAAS ont rendu l'exploitation de la donnée plus accessible, non sans soulever une problématique de souveraineté selon le choix de l'hébergeur au niveau du cloud. Un constat : l'engagement dans des projets data dépend moins de la taille d'une collectivité que de son niveau de maturité numérique et des moyens dont elle dispose.

Comment le sujet de la souveraineté numérique est-il appréhendé dans les petites collectivités qui développent des projets d'exploitation de la donnée ?

Les enjeux sont identiques, quelle que soit la strate territoriale. Nous avons collectivement besoin de solutions plus souveraines, ce qui suppose de structurer un écosystème faisant dialoguer éditeurs privés et service public,

> *« La résilience doit toujours être préférée à la performance. »*

au sens large. Cela nécessite impérativement de bâtir une feuille de route interministérielle partagée avec les collectivités, qui soit la plus claire possible. L'État doit organiser ce dialogue afin d'identifier les complémentarités, définir les standards et avancer vers des outils souverains interopérables. Les éditeurs, de leur côté, doivent prendre en compte les besoins des collectivités, notamment la possibilité d'extraire leurs données dans un format adéquat et à moindre effort.

Il faut dès à présent engager un travail de fond afin de construire de véritables alternatives, souveraines et opérationnelles : pour les logiciels métiers, les solutions d'IA, les messageries internes ou collaboratives et les suites bureautiques. Le plus important est de définir une feuille de route cohérente, d'initier une montée en puissance progressive et régulière, en rendant possible ou en encourageant les alliances entre les différents acteurs de l'écosystème numérique européen. C'est la meilleure garantie pour bâtir des alternatives viables face aux Gafam. ●●●

▲ SOMMAIRE

ENTRETIEN

Quelles recommandations donneriez-vous à une petite commune souhaitant se lancer dans un projet data ?

Avant de se lancer dans la valorisation de la donnée, une collectivité doit assurer avant tout ses arrières afin de préserver l'intégrité de cette donnée.

Préalable absolu : construire une politique RGPD et cyber robuste et résiliente à partir de questions simples. Où sont hébergées les données de la collectivité, disposer d'un plan communal d'activité (PCA) lui permettant, en cas de crise majeure liée au numérique, de poursuivre ses missions essentielles. Ce n'est que dans un second temps que l'on peut se pencher sur les usages de la donnée : la résilience doit toujours être préférée à la performance. ■

« Mieux vaut des résultats peu probants au début, mais qui mèneront, dans cinq ans, à des alternatives viables aux Gafam. »



▲ SOMMAIRE

LE MANAGEMENT DE LA DONNÉE, STRATÉGIE ET GOUVERNANCE

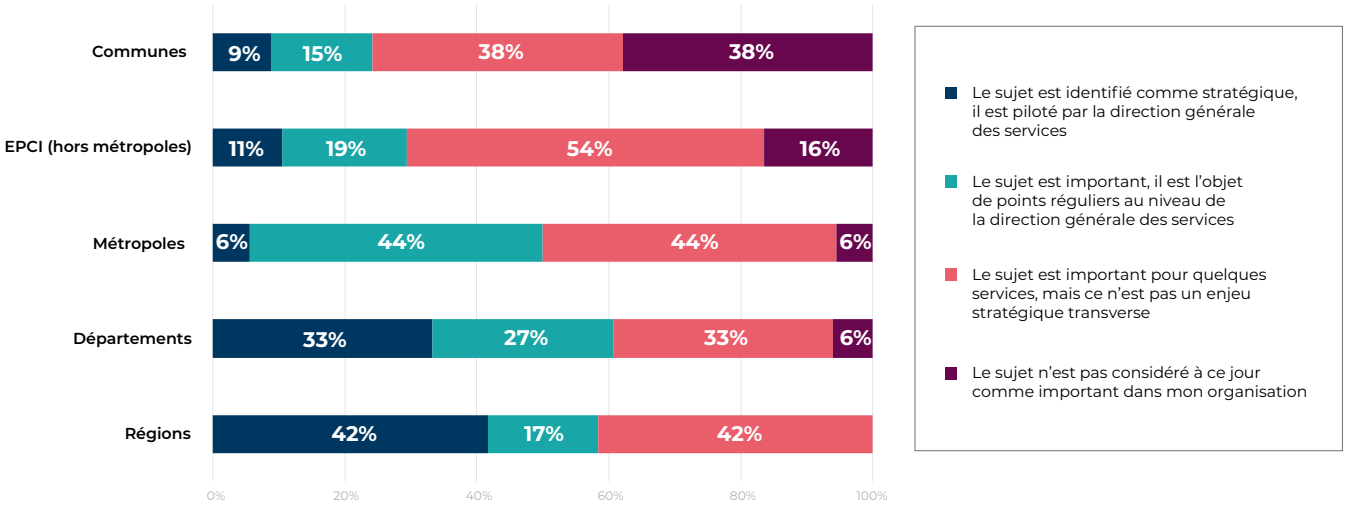
Depuis l'adoption de la loi pour une République numérique en 2016, les observateurs sont nombreux à s'interroger sur le niveau de maturité des administrations publiques locales face aux enjeux de la gestion des données.
Au fil des ans, très logiquement, la multiplication des usages s'accompagne d'une montée en maturité. En 2022, 41 % des collectivités déclaraient un niveau « bon ou correct ». Elles sont 52 % en 2026. On notera avec intérêt la progression encore plus importante dans les communes de petite taille. En quatre ans, nous sommes passés de 23 à 43 % de communes de moins de 3 500 habitants déclarant un niveau de maturité « bon ou correct ».

La maturité progresse aussi de façon significative dans les conseils départementaux (63 % de niveau « bon ou correct »). Elle atteint maintenant un niveau très élevé dans les grandes métropoles (88 %), dont l'Observatoire Data Publica avait pu mesurer l'avance prise dans les usages les plus innovants des données depuis plusieurs années.

Du chemin reste néanmoins à parcourir. L'utilisation, de plus en plus fréquente, des données pour piloter les politiques publiques n'en fait pas pour autant un sujet stratégique. La « Note de conjoncture 2025 » avait mis en exergue l'importance de l'implication des dirigeants territoriaux dans la performance des outils de gestion mis en œuvre. Trop souvent, la data reste un sujet de spécialistes. Cette année, pour la première fois, l'Observatoire Data Publica a souhaité mesurer l'importance stratégique accordée aux données dans les processus de travail internes.

Structurer une stratégie et une gouvernance de la donnée au bénéfice des politiques publiques nécessite des moyens – et l'effet « taille » joue à plein. Dans 50 % des métropoles, 59 % des régions et 60 % des départements, le sujet de la data est piloté ou suivi de façon régulière par la direction générale des services. À ce jour, ce n'est le cas que dans 24 % des communes.

L'importance stratégique des enjeux data :



▲ SOMMAIRE

STRUCTURER LA GOUVERNANCE DE LA DONNÉE

Quimper



La Ville et l'agglomération de Quimper (Finistère, 102 000 habitants) ont engagé une démarche de gouvernance de la donnée à partir d'un constat simple : plusieurs chantiers numériques – évolution du système d'information, développement de l'IA, projets de territoire intelligent, open data ou encore RGPD – se heurtent aux mêmes questions de qualité, de circulation et de maîtrise des données.

Soutenue par le programme Action cœur de ville, la démarche vise à mieux organiser la gestion du patrimoine informationnel des deux collectivités. L'objectif est d'éviter que chaque projet ne traite séparément ses besoins en données, ses droits d'accès ou ses règles de qualité.

« Dans le cadre d'un projet de territoire intelligent sur la gestion des bâtiments, nous nous sommes rendu compte que nous avions besoin d'un économe de flux pour récupérer les données de nos capteurs », témoigne Stéphane Lenoel, DGA Ressources de la Ville et de l'agglomération. Ce type de situation a conduit Quimper à considérer que la gestion de la donnée devait être anticipée dès la conception des projets, plutôt que traitée au cas par cas, une fois les outils déployés.

La gouvernance de la donnée devient ainsi un levier pour structurer des processus communs et durables, garantir la qualité et la circulation des informations, et mieux maîtriser les droits associés tout au long du cycle de vie de la donnée. Pour la Ville et l'agglomération, l'enjeu est de sortir d'une logique de projets numériques en silo pour installer progressivement une gestion transversale du patrimoine informationnel.

Des obstacles encore très présents

S'engager dans une démarche de gestion stratégique des données prend du temps. Et les équipes territoriales n'en ont pas ! 62 % des collectivités indiquent que le manque de temps est le principal obstacle à une meilleure utilisation des données par leurs services. Pour les plus grandes, viennent ensuite le manque de compétences et les difficultés de recrutement. La question n'est pas nouvelle : il est difficile, depuis plusieurs années, d'attirer vers le service public local des experts de la donnée et l'on peut supposer qu'il en sera de même demain avec les experts de l'IA.

Un autre sujet interroge les territoires : les investissements nécessaires pour sécuriser et protéger les données issues des nombreux logiciels de gestion. Avec une priorité : garantir la protection des données des usagers et être en stricte conformité avec le RGPD. D'ailleurs, cette conformité est omniprésente dans les critères mis en place lors de l'acquisition de solutions numériques (pour 90 % des collectivités). De façon corollaire, le choix d'un hébergement français ou européen est très majoritairement prioritaire (77 % des collectivités).

▲ SOMMAIRE

LA SOUVERAINETÉ NUMÉRIQUE : ENJEU NATIONAL, MAIS PAS ENCORE LOCAL ?

Souveraineté politique, souveraineté économique, souveraineté stratégique et géopolitique… Jamais la question n'a été aussi présente dans les débats nationaux et dans l'actualité médiatique. Sans oublier les questions de cybersécurité, traitées dans la partie 3 de cette « Note de conjoncture ».

En 2026, plusieurs initiatives notables ont été engagées ou accélérées pour renforcer la souveraineté numérique des services publics locaux. Mais le sujet est complexe. À l'échelle d'une seule collectivité, il est difficile – et parfois coûteux – d'opter pour des solutions informatiques d'origine française ou européenne, avec un code connu et un hébergement des données maîtrisé, gages d'une certaine souveraineté.

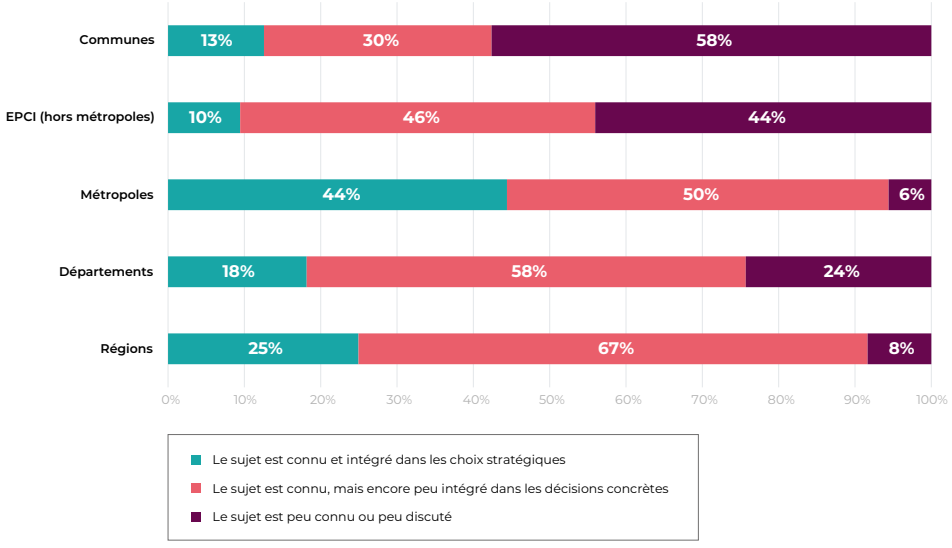
Globalement, 15 % des collectivités estiment que la question de la souveraineté est bien identifiée et intégrée dans leurs choix stratégiques. Beaucoup diront : « Seulement 15 % ! » Les collectivités ont en effet du mal à identifier les enjeux, qui ne sont pas les mêmes pour tous les métiers. Certains systèmes sont plus sensibles, voire critiques, que d'autres. Le baromètre de l'Observatoire Data Publica montre que les régions et les métropoles se sont rapidement engagées sur le sujet. C'est par exemple le cas de la région Occitanie, qui abandonne progressivement les logiciels Microsoft pour ses services mais aussi pour les lycées. D'autres régions s'engagent dans un cadre collectif à travers l'initiative TIE Break, rejointe par Montpellier Méditerranée Métropole.

ANSSI

Définition de la souveraineté :

Système dont la conception, le déploiement et l'exploitation garantissent à l'entité publique bénéficiaire une maîtrise effective sur ses données, ses algorithmes et ses infrastructures, sans exposition à un risque de dépendance critique vis-à-vis d'acteurs soumis à des législations extra-européennes.

La prise en compte des enjeux de souveraineté par type de collectivité :



▲ SOMMAIRE

CONSTRUIRE SA SOUVERAINETÉ NUMÉRIQUE DANS UN CADRE COLLECTIF

Montpellier



Collectivité engagée de longue date sur les sujets numériques (avec l'adoption, en 2024, d'une « Stratégie de la donnée et de l'IA »), Montpellier Méditerranée Métropole (Hérault, 522 000 habitants) a mis en œuvre une démarche forte autour de la souveraineté numérique. Sur ce sujet, la collectivité occitane a fait le choix d'avancer en collectif, en rejoignant la démarche TIE Break, coordonnée par les Interconnectés.

La métropole s'est rapidement impliquée dans les travaux du collectif en concevant un outil d'évaluation des dépendances aux logiciels et aux périphériques non européens, partagé avec les collectivités membres de l'initiative en 2025. Montpellier, ayant fait son autodiagnostic au moyen de cet outil, a mesuré un taux de dépendance à des produits non européens de 52 %, ce qui représente un total de 6 millions d'euros.

Montpellier Méditerranée Métropole a poursuivi ses travaux en construisant un outil de diagnostic sur une maille plus fine, intégrant chacun des composants du SI et des briques logicielles. Et ce afin d'objectiver les dépendances et de répondre aux questions-clés de la souveraineté numérique territoriale : qui est fournisseur de l'outil ? Où vont mes données ? Et dans quelle mesure la collectivité reste propriétaire des données qui sont traitées ?

En complément, un groupe de travail pilote la démarche au sein de la DSI et une délibération sera présentée au prochain conseil municipal pour que soit adoptée officiellement une trajectoire de souveraineté numérique.

Pour Frédéric Nicolas, chargé de mission « souveraineté numérique » à la métropole, ce travail est de longue haleine. Notamment, parce que les collectivités doivent toujours honorer leurs contrats en cours. Il nécessite de s'organiser sur le temps long, pour prévoir des actions échelonnées qui mèneront *in fine* à une plus grande maîtrise du numérique pour les services de la collectivité.

Au niveau national, les travaux pilotés par les Interconnectés se poursuivent avec la publication du manifeste « Pour une trajectoire d'indépendance numérique responsable », présenté à la ministre déléguée à l'IA et au numérique et qui prévoit un plan d'action pour sortir des dépendances numériques extra-européennes ainsi que des critères d'achat public indépendants. L'association a également produit une « Charte d'engagement pour l'indépendance numérique responsable » qui incite les acteurs publics et privés à œuvrer, chacun dans son domaine, à un plus grand niveau d'indépendance numérique.

Fin 2026, les 40 collectivités engagées dans TIE Break continuent leurs travaux *via* une Fabrique de l'indépendance numérique responsable, qui met en œuvre le plan d'action défini dans leur manifeste au moyen d'une organisation coopérative.

▲ SOMMAIRE



ARNO PONS

Directeur général du think tank Digital New Deal

Arno Pons est délégué général du think tank Digital New Deal, qui travaille depuis dix ans sur les enjeux de la souveraineté numérique. Il est notamment l'auteur d'une série de rapports sur le numérique de confiance. Il a également créé une activité de do tank qui vise à accompagner la création de consortiums européens de coopération sur la donnée et l'intelligence artificielle.

Au nom de Digital New Deal, Arno Pons préside l'aDRI, association à but non lucratif qui a créé l'indice de résilience numérique (IRN), un référentiel gratuit et en accès libre qui vise à mesurer les dépendances et vulnérabilités numériques des organisations. Un outil concret au service d'une souveraineté numérique européenne renforcée.

Qu'est-ce que l'IRN et quels sont ses objectifs ?

L'IRN est un outil de pilotage stratégique qui mesure le niveau de dépendance des chaînes de valeur technologique des organisations. Il offre aux décideurs une vision complète de la résilience sur l'ensemble des enjeux technologiques : stockage des données, chaîne d'approvisionnement, cybersécurité, appropriation managériale des risques, soutenabilité environnementale, etc.

Nous avons lancé l'outil en janvier 2026, en partant du constat qu'il existe bien des outils de mesure de la résilience numérique, mais que ceux-ci restent systématiquement cantonnés à des domaines spécifiques (cybersécurité ou numérique responsable, par exemple). Avec l'aDRI, nous avons créé une méthode couvrant les différents enjeux du numérique au sein d'un même standard pour offrir aux entreprises et aux administrations un référentiel unique et cohérent. Cette approche souligne aussi que les décisions numériques constituent un continuum.

L'IRN mesure le niveau de risque dans les différents processus métiers, en commençant par les plus critiques, avant de descendre en granularité sur l'ensemble des actifs numériques. Nous travaillons actuellement à une labellisation IRN des processus métiers des organisations.

L'IRN doit contribuer à augmenter le niveau d'autonomie numérique des organisations : aujourd'hui, nous restons dépendants des États-Unis dans les domaines du logiciel et du cloud. À l'échelle européenne, cela représente un coût annuel de 264 milliards d'euros, versés aux entreprises du numérique états-uniennes, finançant environ 2 millions d'emplois, selon les chiffres du Cigref. Ce sont autant de moyens offerts aux entreprises américaines pour développer leurs offres, au détriment de notre écosystème.
Le retour de Donald Trump à la Maison Blanche met en exergue le danger que représente cette situation pour notre société et notre économie : du jour au lendemain, le prix des prestataires peut augmenter de 300 %… Cela devient un véritable enjeu de vie ou de mort. Si l'on nous rabâchait il y a quelques décennies que « personne ●●●

> *« La souveraineté pleine et entière n'existe pas : nous avons tous des dépendances. »*

▲ SOMMAIRE

n'a jamais été licencié pour avoir acheté IBM », il vaut mieux aujourd'hui privilégier des produits européens, fussent-ils moins matures, plutôt que des offres américaines, porteuses d'un vrai risque d'instabilité contractuelle. Il devient vital de construire des solutions alternatives.
Pour autant, la souveraineté pleine et entière n'existe pas : nous avons tous des dépendances, en défense comme en énergie. Le numérique ne fait pas exception. Nous préférons viser l'autonomie stratégique : être maître de ses décisions et choisir ses interdépendances. Il faut les mesurer pour continuer de s'appuyer sur les meilleures technologies disponibles, tout en s'assurant qu'aucun processus ne dépend d'un seul fournisseur ou d'un seul État. Il faut pouvoir arbitrer en connaissance de cause sur l'existence de dépendances, les assumer et les diversifier.

En quoi l'outil incarne une approche européenne de la souveraineté numérique ?

Penser la souveraineté numérique à l'échelle nationale n'aurait pas de sens. Notre écosystème numérique, c'est l'Europe et la régulation harmonisée est le socle de la confiance dans nos technologies. Ce n'est que sur cette base que l'on peut construire des alternatives viables et faire dialoguer des écosystèmes qui nous permettront de construire des alternatives sérieuses aux outils américains.

L'IRN prend alors le périmètre européen comme base des évaluations et, avec l'aDRI, nous accompagnons son déploiement à l'échelle de l'UE.
La souveraineté numérique ne peut être qu'une souveraineté européenne.

Quels conseils donneriez-vous à une collectivité qui souhaite développer son autonomie numérique ?

Le premier conseil serait de réaliser un audit complet de ses dépendances numériques pour identifier les besoins de montée en maîtrise. Pour ce faire, l'IRN est à disposition des collectivités.

Le second conseil serait de travailler en collectif. Beaucoup de territoires, en France comme en Europe, ont déjà réalisé des travaux en la matière. Il faut profiter de cette dynamique pour développer une approche coordonnée, qui profitera à l'interopérabilité des standards et des solutions.

Cette dynamique émerge aujourd'hui, particulièrement en matière d'IA, avec des programmes comme Territoires d'IA, porté par la Banque des Territoires. Cependant, il ne faut pas oublier que le socle du numérique, c'est avant tout la donnée. Les collectivités doivent renforcer leur coopération sur la data : comment la partager, la croiser entre territoires, mais aussi avec l'écosystème privé. Nous sommes convaincus que le chantier des « data spaces » est prometteur pour avancer vers des données et une IA européenne de confiance, avec une gouvernance claire au service d'une bonne orchestration de nos data. ■

> *« La souveraineté numérique ne peut être qu'une souveraineté européenne. »*

▲ SOMMAIRE

QU'EN PENSENT LES FRANÇAIS ?



La souveraineté numérique fait désormais partie du débat public, sans être encore une notion familière pour tous. 61 % des Français en ont entendu parler, mais seulement 29 % déclarent bien voir de quoi il s'agit.

Pourtant, lorsqu'on leur soumet des mesures concrètes, les attentes sont très nettes. 91 % jugent « prioritaire ou important » de choisir des logiciels français ou européens pour la gestion quotidienne du service public et 89 % expriment la même attente pour les systèmes d'intelligence artificielle. 87 % soutiennent également l'investissement dans des infrastructures numériques (comme les data centers) nationales afin d'héberger davantage de données en France.

Cette préoccupation ne concerne d'ailleurs pas seulement l'IA : 94 % des Français considèrent comme « prioritaire ou important » que les données utilisées par le service public soient hébergées en France ou en Europe. C'est même, parmi les mesures proposées, celle qui recueille la plus forte proportion de réponses « prioritaires » (67 %).

Un paradoxe apparent : les Français connaissent encore mal la notion de souveraineté numérique, mais ils en plébiscitent largement les principales traductions concrètes.

▲ SOMMAIRE

PARTIE 2

L'INTELLIGENCE ARTIFICIELLE TERRITORIALE

Après trois années de très forte progression du nombre de collectivités engagées dans des projets d'IA, 2026 semble être une année de transition et de consolidation. En 2025, la note de conjoncture évoquait un réel engouement, notamment du fait de l'adoption massive d'outils d'IA générative et de leur intégration dans le fonctionnement quotidien des services. Mais tout semble indiquer que les collectivités ont besoin de recul pour tirer les enseignements de leurs premiers pas.

De nouvelles préoccupations se font jour. Elles concernent la méthode, l'encadrement des usages, la mesure des impacts de l'IA et la stabilisation du choix des outils (après les étapes de test). Un enjeu central apparaît : celui de la transformation des métiers et son corollaire, parfois oublié, le dialogue social. Des préoccupations financières émergent. Le marché de l'IA est dominé par des offres freemium, la gratuité ou des rabais considérables servant de prix d'appel. Mais les décideurs publics (comme ceux du privé, d'ailleurs) sont rattrapés par la réalité des coûts, au risque de remettre parfois en cause des choix initiaux pour privilégier des outils plus pérennes, moins spectaculaires mais durablement intégrés dans la gestion publique et l'activité quotidienne des services.

S'il est trop tôt pour parler de « maturité » – les besoins de formation restent énormes –, 2026 est sans conteste une année de stabilisation, mais aussi d'observation. Dernière étape avant la généralisation ?

▲ SOMMAIRE

LES DOMAINES D'USAGE DE L'IA ET LES PROFILS DES COLLECTIVITÉS ENGAGÉES

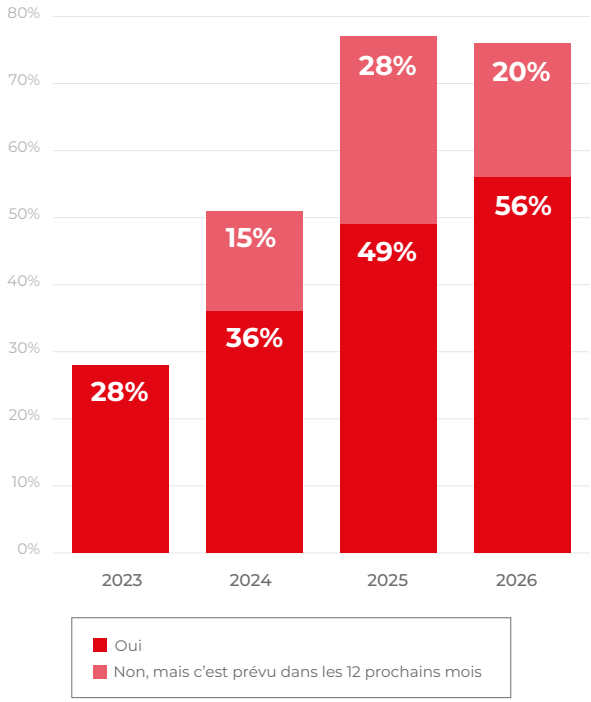


Les chiffres sont spectaculaires. Ils confirment, après l'explosion des usages mesurée par l'Observatoire Data Publica en 2025, que les collectivités territoriales se sont massivement engagées dans des projets de déploiement de l'IA. Plus d'une sur deux (56 % hors communes de moins de 3 500 habitants) a engagé au moins un projet d'IA. Contrairement aux idées reçues, le service public (local) est en avance par rapport à des filières économiques importantes, y compris en comparaison de PME et d'ETI de taille significative (seulement 18 % des entreprises françaises utilisaient l'intelligence artificielle en 2025, selon l'Insee).

Bien sûr, l'effet « taille » joue à plein. En 2026, 100 % des régions et 94 % des métropoles ont engagé une démarche autour de l'IA, ce qui confirme une tendance forte observée en 2025 et même en 2024, pour quelques pionniers. Fait marquant en 2026 : avec une année de décalage, les conseils départementaux s'engagent de façon résolue dans la démarche (70 % des conseils départementaux ont lancé au moins un projet contre 40 % en 2025). Il faut peut-être y voir un lien avec une impulsion nationale donnée par départements de France, mais aussi avec la progression des travaux départementaux sur la data commentés dans la partie 1 de cette note.

Un autre chiffre mérite l'attention : 20 % des collectivités qui n'ont pas encore franchi le pas déclarent vouloir le faire dans les douze prochains mois. La somme des intentions affichées et des projets déjà engagés se stabilise autour d'une proportion de trois collectivités sur quatre.

Pourcentage de collectivités ayant engagé des expérimentations IA.
(Total hors communes de moins de 3 500 habitants.)



▲ SOMMAIRE

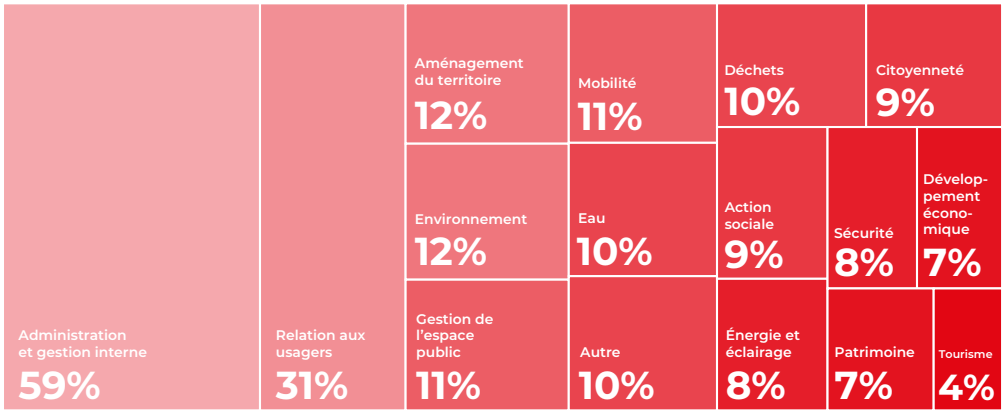
IA du quotidien et IA métiers

Tous les métiers sont concernés ! Il s'agit d'une confirmation qui mérite que l'on entre dans le détail. 54 % des collectivités menant des projets d'utilisation de l'IA déclarent le faire pour la gestion interne (45 % en 2024) et 31 % pour la relation aux usagers (20 % en 2024). La progression est très nette et se traduit par une « IA du quotidien » mise à la disposition des agents publics qui sont à la recherche de gains de temps et d'efficacité pour gérer leur activité. Bien sûr, il s'agit d'une traduction concrète du déploiement – plus ou moins encadré – d'outils d'IA générative. Comme Vibe (Mistral AI), ChatGPT (OpenAI), Claude (Anthropic) ou Copilot (Microsoft), que les collectivités mettent à disposition ou dont elles autorisent l'usage.

Ces outils sont très différents de ceux utilisés dans les filières techniques au service des fonctions urbaines. On y retrouve des outils de modélisation prédictive ou des outils d'IA intégrés à des automatismes pour la gestion des déchets (10 %), de l'eau (9 %), de l'éclairage ou de l'énergie des bâtiments publics (8 %). On y retrouve aussi les outils qui permettent le fonctionnement de carrefours dits « intelligents » (11 % des projets concernent la mobilité), la gestion d'incidents dans l'espace public (11 %) ou, directement, la sécurité et la vidéoprotection (8 %).

En complément, une autre étude retient l'attention, menée de façon spécifique sur les métiers de la communication territoriale par la coopérative Cap'Com. Dans 96 % des collectivités interrogées, on constate que les collaborateurs ont recours à de l'IA générative pour produire du contenu (textes et illustrations pour le site Internet ou le magazine de la commune, billets pour les réseaux sociaux, etc.). De là à penser que les métiers de la communication publique pourraient être remplacés demain par des IA, il n'y a qu'un pas. C'est l'une des questions qui a été posée au délégué général de Cap'Com.

Domaines dans lesquels des projets ayant recours à de l'IA sont en cours en 2026 :



▲ SOMMAIRE



Crédit photo : Cap'Com

YVES CHARMONT

Expert en communication publique, ancien délégué général de Cap'Com

Cap'Com représente et anime une communauté de 25 000 communicants du service public local. L'organisation a récemment publié une enquête sur l'IA dans les métiers de la communication territoriale, mesurant l'impact de ces outils pour les directions de la communication. Retour sur les résultats de cette étude, réalisée en partenariat avec l'Observatoire Data Publica.

Comment est née l'idée de réaliser une enquête sur l'IA pour les communicants du service public local ?

Cap'Com s'est rapidement saisi du sujet de l'IA. Au début, personne ne savait ce que ça pouvait amener pour nos métiers. Nous avons alors lancé des travaux pour appréhender ce nouvel objet. En 2023, nous avons réalisé une première exploration des usages pour la communication. En 2025, nous avons publié « La Boussole de l'IA », identifiant les points de vigilance dans l'usage d'IA génératives. Avec cette nouvelle enquête, nous voulons compléter ces travaux en mesurant, avec des chiffres concrets, l'impact de l'IA sur les directions de la communication.

Quels sont les enseignements majeurs de cette enquête ?

L'enseignement le plus important est aussi le plus contre-intuitif : les postes des agents de la communication ne sont pas majoritairement menacés par l'IA. En effet, leurs tâches ne se résument plus à créer des plaquettes ou des posts pour les réseaux : en examinant les fiches métiers du CNFPT, on observe que l'IA n'est pertinente que pour environ 30 % des missions des agents de la communication publique. Elle ne peut pas mener un débat avec les habitants sur l'aménagement d'un quartier, interpréter une réaction dubitative au sein d'une assemblée de citoyens… En somme, elle ne va pas chercher l'âme d'un territoire. En revanche, l'IA constitue une menace sérieuse pour les agences de communication, qui sont de plus en plus délaissées par les collectivités.

À l'inverse, notre étude confirme certaines dynamiques pressenties : 92 % des directions de la communication déclarent avoir déjà utilisé de l'IA, avec un recours significativement plus élevé dans les grandes collectivités et les petites communes. Tout le monde utilise l'IA donc, mais 58 % des directions se limitent à des solutions gratuites : dans les collectivités, on utilise l'IA, mais on ne la paie pas. ●●●

> *« Dans les collectivités, on utilise l'IA, mais on ne la paie pas. »*

▲ SOMMAIRE

ENTRETIEN

> « *L'IA, ça reste aujourd'hui une part d'impensé et une part d'inavoué.* »

Par quel angle les directions de la communication abordent-elles le sujet de l'IA aujourd'hui ?

Elles se positionnent plutôt comme des vigies, en accompagnant la transformation numérique. Ce rôle de garde-fou reste cependant peu formalisé : seules 2 % des collectivités interrogées ont mis en place une charte spécifique à l'IA dans la communication. La part de *« shadow AI*[1] *»* est également importante : l'IA, ça reste aujourd'hui une part d'impensé… et une part d'inavoué. ■

L'utilisation de l'IA générative par les communicants du service public local

https://www.cap-com.org/lutilisation-de-lia-generative-par-les-communicants-du-service-public-local



1. *Le shadow AI désigne l'utilisation d'outils ou de services d'intelligence artificielle au travail, sans l'approbation, la connaissance ni la supervision de la direction de l'entreprise ou de la collectivité.*

▲ SOMMAIRE

Tout le monde teste et expérimente

Des ressources humaines à la gestion de la voirie, les expérimentations de l'IA se multiplient.

L'IA POUR LE SERVICE PUBLIC COMMUNAL

Saint-Cloud



Commune de 30 000 habitants bordant la Seine, Saint-Cloud (Hauts-de-Seine) s'est engagée en 2025 dans une démarche globale autour de l'intelligence artificielle, avec un objectif : mieux comprendre cette technologie, en maîtriser les risques et identifier les usages réellement utiles au service public.

Portée par le maire et la DGS, la démarche commence par un travail d'acculturation des élus, directeurs et encadrants. *« L'IA : tout le monde en parle. Ça suscite des peurs comme de l'engouement »*, résume Nathalie Bernard, DGS de la commune. Ces temps mêlent sensibilisation aux risques, exploration des cas d'usage et prise en main des outils. Ils ont notamment conduit à l'adoption d'une charte interne de l'IA, déclinée dans un guide de bonnes pratiques destiné aux agents. Après avoir posé ce cadre, la collectivité a engagé plusieurs expérimentations avec une ligne de conduite assumée : ne pas essuyer les plâtres et ne tester des solutions que si leur utilité paraît suffisamment vraisemblable. Cette prudence n'empêche pas l'expérimentation, mais elle conduit Saint-Cloud à interroger systématiquement la valeur ajoutée réelle de l'IA. *« Quand il y a une canicule, ce n'est pas l'IA qui va porter de l'eau aux gens »*, rappelle Nathalie Bernard.

La collectivité souligne aussi que certains besoins, présentés comme des cas d'usage de l'IA, peuvent parfois être mieux traités par une bonne organisation de l'information et une gestion efficace des données.

Deux expérimentations ont été menées dans le domaine des ressources humaines : l'assistance à la rédaction d'offres de recrutement et le rapprochement entre les CV des candidats et les fiches de poste. La première a permis de mesurer des gains de temps significatifs. La seconde a donné des résultats plus mitigés, insuffisants à ce stade pour démontrer un avantage décisif par rapport au travail des agents.

Aujourd'hui, Saint-Cloud poursuit cette démarche progressive avec de nouveaux cas d'usage, parmi lesquels la génération de comptes rendus de conseils municipaux. Pour la collectivité, l'enjeu n'est donc pas de multiplier les expérimentations mais d'identifier celles qui améliorent réellement le fonctionnement du service public.

▲ SOMMAIRE

L'IA POUR LE SERVICE PUBLIC COMMUNAL

Cannes

La Ville de Cannes (Alpes-Maritimes, 74 300 habitants) a fait le choix d'une approche résolument volontariste de l'intelligence artificielle, car elle est convaincue que son appropriation peut constituer un levier de performance pour le service public local. Elle expérimente plusieurs usages de l'IA dans des domaines variés de l'action municipale.

Portée par la DGS et le maire, la démarche a démarré début 2025 par un sondage révélant qu'une partie des agents municipaux utilisaient déjà l'IA dans leurs fonctions. Face à ce besoin d'outils, la Ville décide de déployer l'IA dans l'ensemble de ses champs d'action.

Une première expérimentation concluante a porté sur les diagnostics de voirie, pour détecter les dégradations et programmer les travaux. Les gains de temps sont substantiels : *« Ce que l'intelligence artificielle a produit en quelques heures, des équipes de terrain auraient mis des mois pour le réaliser »*, confie Karin Topin-Condomitti, DGS de la commune.

D'autres expérimentations concernent les usages administratifs : rédaction de courriers, comptes rendus, analyse juridique, traduction, aide à la production des rapports des délégataires et des marchés, analyse des offres… Plus de mille agents ont été déjà formés à ces usages, qui suscitent un engouement important dans les services. Pour l'avenir, Cannes prévoit d'équiper, dès janvier 2027, ses véhicules de propreté urbaine de caméras embarquées afin de cartographier l'état de la ville. Elle souhaite aussi étendre l'IA au suivi de son patrimoine arboré *via* un jumeau numérique couvrant à terme 15 000 arbres (contre 4 000 suivis aujourd'hui par les agents de la commune).



▲ SOMMAIRE

Municipales 2026 : l'IA fait son entrée dans les programmes

À l'occasion des élections municipales de mars 2026, l'Observatoire Data Publica a analysé les programmes des listes candidates dans les 42 villes de France de plus de 100 000 habitants. Au total, près de 270 propositions en lien avec la donnée, l'intelligence artificielle et le numérique ont été recensées et étudiées.

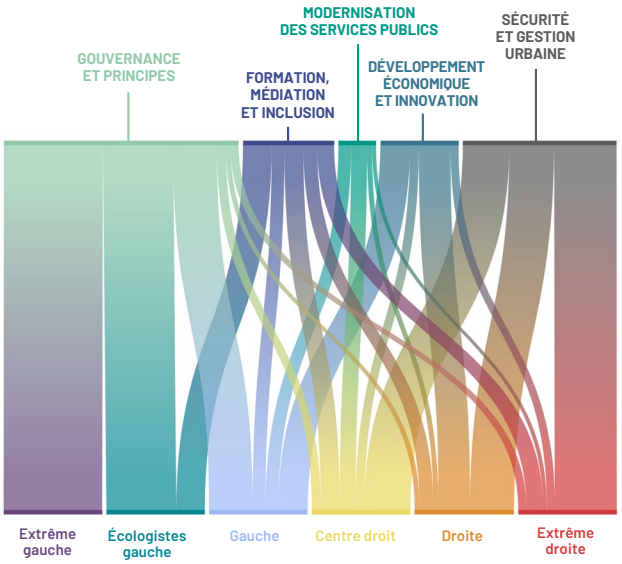
Premier enseignement : les sujets numériques figurent bien dans les priorités politiques. Deux programmes sur trois intègrent des propositions en lien avec cette thématique. Quasi absente lors des élections municipales de 2020, l'IA fait son entrée en force dans les programmes : près d'une proposition sur deux (48 %) concerne ainsi l'intelligence artificielle, son usage ou son encadrement avec, toutefois, des priorités qui varient selon l'orientation politique des candidats.

Les propositions traduisent des visions politiques de l'IA parfois opposées

Dans les propositions, l'Observatoire Data Publica a identifié cinq registres distincts. Les deux principaux sont l'IA au service de la sécurité et de la gestion urbaine (détection comportementale, éclairage, déchets, mobilité) et l'IA comme sujet de gouvernance et de principes (encadrement, chartes, opposition à certains usages, etc.). Ils concentrent près de deux propositions sur trois. Les autres registres positionnent l'IA comme levier de développement économique (15 % des propositions), enjeu de formation et d'inclusion (14 %) et, enfin, outil de modernisation des services publics (9 %).

Plus remarquable est le fait que les blocs politiques ne mobilisent pas tous les mêmes registres en lien avec l'intelligence artificielle. À droite et à l'extrême droite de l'échiquier, l'IA est principalement envisagée comme un outil opérationnel au service de la sécurité et de la gestion urbaine (détection comportementale, circulation, éclairage intelligent). Par exemple, 63 % des propositions issues de l'extrême droite concernent ce registre. À gauche, les propositions se concentrent davantage sur les enjeux de gouvernance, de transparence et de principes (éthique, souveraineté, frugalité). Par exemple, 71 % des propositions issues des écologistes relèvent de ce registre. Entre ces deux pôles, les autres blocs politiques combinent plusieurs registres en articulant modernisation des services publics, développement économique et inclusion.

Analyse par bloc politique des registres IA :



datapublica
L'OBSERVATOIRE

▲ SOMMAIRE

Le portage politique à la traîne ?

Après les élections vient le temps de la mise en œuvre des programmes. Seules 35 % des collectivités du baromètre 2026 déclarent que l'IA fait l'objet d'un portage politique dans leur organisation. Sans surprise, c'est dans les régions (67 %) et les métropoles (44 %) que le portage politique est le plus fort (priorités affichées, arbitrages, impulsion donnée). À l'inverse, il n'existe aucun portage politique du sujet IA dans la très grande majorité (88 %) des communes de moins de 3 500 habitants.

QU'EN PENSENT LES FRANÇAIS ?



Les Français sont de plus en plus méfiants vis-à-vis de l'IA, sans nier son utilité potentielle pour le service public.

Ils restent très partagés face à l'intelligence artificielle, avec une tendance qui se dégrade encore en 2026. 55 % expriment désormais un sentiment négatif à l'évocation de l'IA (contre 51 % en 2025). L'inquiétude reste un sentiment dominant pour 45 % et le nombre de Français rejetant l'IA progresse nettement : de 5 % à 10 % en un an. Cette défiance s'appuie sur des craintes désormais bien installées : dépendance excessive à l'IA, perte de contrôle humain, menace sur l'emploi.

Pour autant, les Français ne rejettent pas les usages de l'IA en bloc. Ils continuent de lui reconnaître un potentiel important dans plusieurs domaines : en particulier, la santé, mais aussi la gestion de l'énergie, de l'eau, de la sécurité, de l'urbanisme ou des transports.

Les Français exigent du service public qu'il maîtrise son usage de l'IA. 87 % préfèrent que le service public garde le contrôle le plus strict possible sur les outils d'IA, quitte à perdre en efficacité. Et 81 % préfèrent avoir affaire à un humain plutôt qu'à une messagerie instantanée pilotée par une IA. Les garde-fous attendus sont eux aussi très clairs : 93 % jugent « prioritaire ou important » d'être informés chaque fois qu'une IA est utilisée ; 92 % souhaitent une charte encadrant les usages autorisés ou interdits. Enfin, la question environnementale progresse : 79 % estiment que le service public doit limiter le recours massif aux données et à l'IA en raison de leur impact environnemental, même si cela réduit son efficacité.

En 2026, les Français ne rejettent donc pas l'IA dans le service public. Ils l'acceptent à condition qu'elle reste utile, maîtrisée et surtout placée sous contrôle humain.

À la lecture des programmes électoraux comme des attentes exprimées par les Français, un constat s'impose : la diffusion de l'IA dans le service public local ne peut se faire à l'emporte-pièce et sans méthode. Comment les collectivités – notamment celles qui expérimentent ces outils depuis plusieurs mois, voire plusieurs années – envisagent-elles aujourd'hui leur passage à l'échelle ?

▲ SOMMAIRE

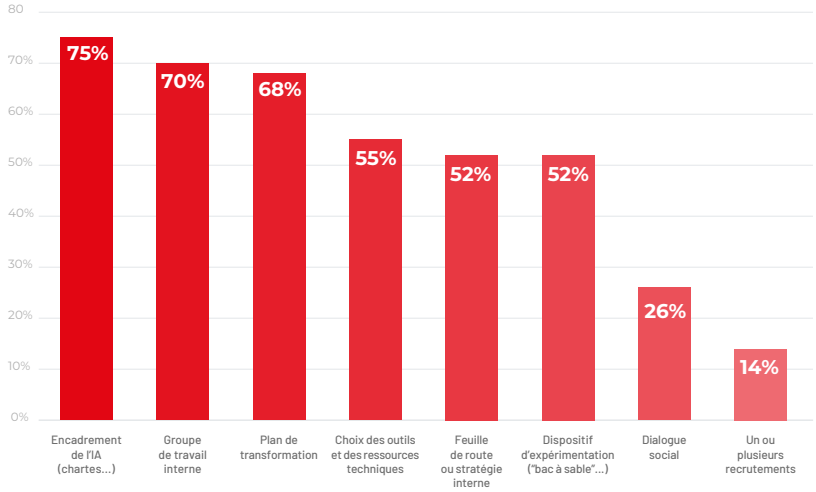
DE L'EXPÉRIMENTATION AU DÉPLOIEMENT : L'ESQUISSE D'UNE MÉTHODE ?

En 2025, la principale préoccupation des territoires engagés dans un projet d'IA était d'en garder la maîtrise et d'encadrer les usages. C'est la raison pour laquelle 57 % des collectivités concernées déclaraient vouloir se doter d'un document de référence : dans la majorité des cas, d'une charte interne. Ces chartes sont de plus en plus nombreuses. Nous les retrouvons aujourd'hui dans des collectivités de toutes tailles. Les modalités d'élaboration varient d'un territoire à l'autre : écriture interne, utilisation d'un modèle « clés en main », association des agents, mobilisation et, parfois, vote des élus, et même mobilisation citoyenne… Dans tous les cas, la démarche apparaît utile. Elle permet de comprendre des enjeux complexes et de s'en saisir : contrôle des biais et des erreurs, impact environnemental, protection de la vie privée, coût réel, formation des agents, etc. En 2026, 75 % des collectivités engagées dans un projet d'IA se sont attelées à la production d'une charte ou d'un document de référence interne pour encadrer les usages de l'IA !

Mais elles ne s'arrêtent pas là. Les résultats du baromètre 2026 permettent d'esquisser une véritable méthode pour une introduction utile et maîtrisée de l'IA dans le service public local. Une grande majorité de collectivités met en place des groupes de travail internes (70 %). Elles anticipent et prennent en compte les besoins de formation des agents qui utiliseront l'IA (68 %). On rappellera utilement que la formation des utilisateurs de l'IA est une obligation prévue par le règlement européen sur l'IA depuis 2025, pour tous les employeurs.
Les collectivités engagées dans une démarche IA sont aussi nombreuses à essayer d'en planifier le déploiement, avec des étapes et des priorités, parfois pour l'accélérer, parfois pour réguler des « coups partis » ou l'IA clandestine que l'on appelle le « *shadow AI* ». Plus de la moitié d'entre elles (55 %) se dotent d'une feuille de route interne. On notera que les collectivités les plus grandes créent des postes de chef de projet IA pour piloter ces démarches (c'est le cas pour 39 % des métropoles et 42 % des régions).

Attention : seules 26 % des collectivités concernées ont inscrit le sujet de l'IA à l'ordre du jour du dialogue social. Il est pourtant communément admis que ces outils ont un véritable impact sur l'organisation et les conditions de travail des agents concernés (c'est même souvent l'objectif recherché !). De nombreuses jurisprudences sont intervenues en 2026 – dans le privé, pour l'instant –, conduisant à l'arrêt du déploiement de projets d'IA, faute d'avoir informé et consulté les instances paritaires. Précision importante : plusieurs concernent des phases de test et non des déploiements pérennes.

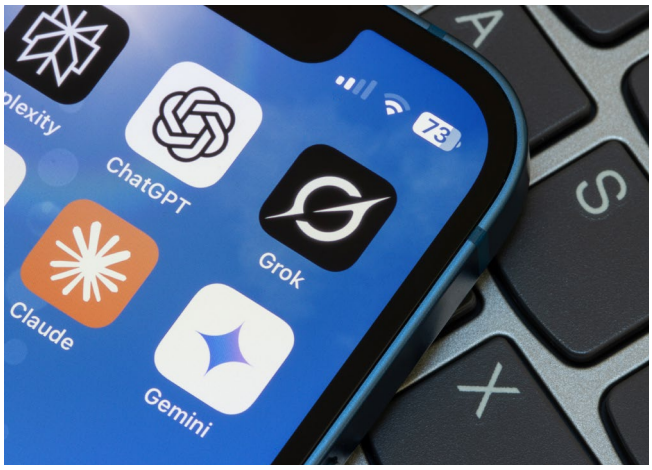
Les démarches IA engagées par les collectivités.



SOMMAIRE

Si ces démarches d'accompagnement de l'IA s'organisent, c'est que le sujet n'est pas simple. La recherche des impacts positifs de l'IA – notamment, en termes de rapidité ou de qualité d'exécution – s'accompagne du nécessaire contrôle des risques et doit être contrebalancée par ses impacts négatifs, notamment environnementaux. Les collectivités engagées soulignent la présence de nombreux obstacles. Le manque de compétences internes est un frein pour 54 % d'entre elles. 47 % redoutent des difficultés financières pour faire face aux coûts réels des projets. Ceux-ci, parfois importants, se mesurent en termes de ressources humaines à mobiliser, de formation, d'organisation, sans parler du prix des licences, qui ne fera qu'augmenter dans les prochaines années. Pour 36 % d'entre elles, l'impact environnemental (et sa difficile mesure) est aussi un frein. 43 % soulignent des problématiques juridiques qui interviennent très vite dans la commande publique pour garantir la maîtrise des données de la collectivité et la souveraineté des systèmes d'IA utilisés.

Année après année, un autre indicateur retient notre attention : l'obstacle majeur que constitue la qualité des données pour faire fonctionner de façon performante des systèmes d'IA. Le baromètre 2026 de l'Observatoire Data Publica montre que 28 % des collectivités qui n'ont pas débuté dans l'IA anticipent que la disponibilité et la qualité de leurs propres données pourraient être un problème. 44 % de celles qui ont commencé un projet d'IA font le constat que cet obstacle est majeur et que, bien souvent, il a été sous-estimé auparavant. *« On a été rattrapés par la data ! »* témoignait la DGS d'une grande collectivité lors d'un colloque professionnel en début d'année.



Trois ans après l'arrivée de ChatGPT, le choix des outils d'IA générative dans les collectivités est aussi une difficulté (pour 41 %, il est difficile de trancher face à la profusion des offres). Mais après les premiers tâtonnements, quelques tendances semblent se dessiner. Les collectivités (une sur trois) qui ont fait le choix d'autoriser et parfois de mettre à disposition un ou plusieurs outils sont nombreuses à privilégier Copilot (55 %), mais aussi Mistral Vibe (52 %). Ces chiffres sont intéressants, Microsoft intégrant systématiquement son IA dans les suites bureautiques, là où le recours à Mistral Vibe relève plus certainement d'un choix de souveraineté numérique. Suivent Claude (23 %), ChatGPT (21 %) et Gemini (16 %). On notera aussi la percée de l'entreprise française DelibIA, citée par 18 % des collectivités, qui intègre Mistral Vibe dans ses briques de service IA.

▲ SOMMAIRE

La souveraineté en pratique

Observatoire interne de l'IA, création d'une plateforme servicielle : les collectivités veulent utiliser l'IA dans un cadre maîtrisé.

LE DÉPLOIEMENT D'UN OUTIL SOUVERAIN

Rennes



Depuis novembre 2025, Rennes Métropole (Ille-et-Vilaine, 480 200 habitants) expérimente RAGaRenn, un système d'IA conçu par l'université de Rennes. Cette expérimentation s'inscrit dans une démarche plus large, engagée par la collectivité autour de l'intelligence artificielle, avec notamment la création d'un observatoire de l'IA générative et la publication d'un rapport consacré au sujet.

Pour Johan Theuret, directeur général adjoint chargé du pôle Ressources portant les sujets d'intelligence artificielle au sein de la collectivité, l'objectif est de mettre à la disposition des agents un environnement d'usage sécurisé, conçu pour limiter les risques de fuite de données et fonctionnant à partir des data centers locaux. Cela permet d'utiliser en toute confiance le patrimoine documentaire de Rennes Métropole pour mieux répondre aux questions des agents.

Aujourd'hui, les principales fonctionnalités expérimentées sont la rédaction, la génération de comptes rendus, la synthèse et l'analyse de documents, l'aide à la réflexion ainsi que l'assistance à la génération de formules de tableurs. Emmie Niard, responsable de mission IA au sein de la collectivité, identifie de premiers résultats encourageants : les agents font état, pour certains de ces usages, d'un niveau de performance équivalent à celui des grands modèles d'IA américains, avec un outil souverain et significativement moins énergivore. Toutefois, certaines fonctionnalités – telles que la génération de présentations – ne se sont pas encore montrées concluantes.

Des temps réguliers de formation à l'outil sont proposés aux agents. L'objectif à terme est la conception d'une plateforme servicielle qui regroupera au même endroit l'ensemble des outils et des fonctionnalités IA de Rennes Métropole et de la Ville de Rennes.

▲ SOMMAIRE



FRANÇOIS SAUVADET

Ancien ministre, président de Départements de France, président du département de la Côte-d'Or

> *« Notre ambition est claire : faire de la donnée et de l'IA des outils au service de décisions publiques plus efficaces, plus anticipatrices et toujours plus humaines. »*

Où en sont aujourd'hui les départements dans leur appropriation de la data et de l'IA ?

L'intelligence artificielle est désormais une réalité dans les départements : plus de la moitié d'entre eux sont engagés dans des projets concrets. Mais la réussite de cette transformation repose moins sur la technologie que sur l'appropriation par les agents. L'objectif est simple : utiliser l'IA pour alléger les tâches les plus chronophages et permettre aux professionnels de se recentrer sur leur cœur de métier. Cette dynamique se construit progressivement à partir d'usages concrets et d'une culture de la donnée partagée. Notre ambition, c'est de mettre l'innovation au service de politiques publiques plus efficaces, plus réactives et mieux adaptées aux réalités des départements.

L'action sociale est au cœur des compétences des départements. Comment la donnée et l'IA peuvent-elles contribuer à améliorer ce service public ?

Dans ce domaine qui représente jusqu'à 70 % des budgets des départements, la donnée et l'intelligence artificielle peuvent nous aider à mieux anticiper les besoins, à renforcer l'accompagnement des publics les plus fragiles et à lutter contre le non-recours aux droits. Elles offrent également de nouvelles capacités d'analyse pour adapter nos politiques aux grands défis démographiques, sociaux et économiques de notre pays. Pour autant, et c'est là une ligne claire que nous défendons, dans les politiques de solidarité, l'algorithme ne pourra jamais remplacer le discernement humain. L'IA doit assister la décision publique, sans jamais s'y substituer.

Comment les départements peuvent-ils développer l'usage des données et de l'IA, tout en maîtrisant les risques ?

L'innovation ne peut se développer durablement que dans un cadre de confiance. Pour les départements, cela repose sur trois priorités. La souveraineté d'abord, parce que les données de nos concitoyens doivent être hébergées et traitées dans des environnements sécurisés respectant les normes européennes. L'éthique ensuite, avec des règles claires garantissant la protection des données personnelles, la transparence des usages et la maîtrise humaine des décisions. Enfin, la responsabilité, qui passe par la formation des agents et l'accompagnement des élus. Nous défendons une IA de confiance, au service des citoyens, et non une technologie subie ou imposée.

Quel rôle joue l'association Départements de France pour accompagner les élus et les administrations dans ces transformations ?

Départements de France agit comme un accélérateur collectif de la transformation numérique. Nous rassemblons les élus départementaux au sein de la commission « Innovation, numérique et IA » afin de réfléchir sur les orientations stratégiques et les innovations les plus pertinentes pour l'action publique. Nous animons également le Club Data-IA, qui permet aux départements de partager leurs retours d'expérience, leurs méthodes et leurs cas d'usage afin de mutualiser les réussites et d'éviter les démarches isolées. Enfin, avec le programme « Départements Data », nous accompagnons les collectivités dans la valorisation de leurs données pour améliorer le pilotage des politiques publiques et renforcer leur souveraineté numérique.

Notre ambition est claire : faire de la donnée et de l'IA des outils au service de décisions publiques plus efficaces, plus anticipatrices et toujours plus humaines. ■

▲ SOMMAIRE

ENTRETIEN



SCHÉHÉRAZADE ABBOUB

Avocate associée chez Alerion Avocats
et cofondatrice de l'Observatoire Data Publica,
coautrice du clausier Data & IA

Comment est née l'idée de ce clausier Data & IA ?

Cette publication, fruit d'une collaboration entre les Interconnectés et Data Publica, s'inscrit dans la continuité d'un travail engagé depuis de nombreuses années pour mettre à disposition des collectivités territoriales des ressources juridiques concrètes sur la donnée et, désormais, sur l'intelligence artificielle. Après plusieurs guides et clausiers élaborés avec la Banque des Territoires et des fédérations d'élus, il nous a semblé indispensable d'actualiser ces outils à l'heure où l'usage de l'IA connaît une accélération sans précédent.

Que trouveront les collectivités dans ce document ?

Un outil pratique. Le clausier rassemble des clauses directement mobilisables dans les contrats publics afin de garantir la maîtrise des données, la réversibilité des solutions, la transparence, la cybersécurité et l'encadrement des usages de l'IA. Mon conseil est simple : mieux vaut intégrer des clauses Data et IA, même perfectibles, que ne rien prévoir. Elles constituent le premier levier de souveraineté numérique des collectivités.

Des collectivités ont-elles déjà ouvert la voie ?

Certains territoires se sont saisis, depuis plusieurs années, du sujet de la donnée dans leurs contrats. Dijon Métropole a été pionnière lors de son projet de smart city. Puis de nombreuses collectivités se sont emparées du sujet : Orléans, Paris-Saclay, Grand Paris Sud, Clermont-Ferrand, Saint-Nazaire, Caux Seine agglo et bien d'autres… Aujourd'hui, les régions Grand Est, Pays de la Loire ou Hauts-de-France participent également à cette dynamique en proposant des ressources et des clausiers à destination de leurs territoires.

Quels obstacles avez-vous rencontrés ?

Le principal défi n'est pas juridique. Les clauses n'ont d'intérêt que si les collectivités, leurs agents et leurs partenaires comprennent les enjeux liés à la donnée et à l'IA. Il faut donc accompagner, former et sensibiliser. La contractualisation est une condition nécessaire, mais elle ne remplace pas l'acculturation. ●●●

▲ SOMMAIRE

Certaines entreprises considèrent-elles ces exigences comme excessives ?

Notre expérience montre le contraire. Nous observons davantage des échanges et des demandes d'explication que de véritables blocages. Les entreprises sont elles aussi confrontées aux enjeux de gouvernance des données et de l'IA. Lorsqu'elles comprennent les objectifs poursuivis – protection des données continuité du service public, transparence et souveraineté –, le dialogue s'installe naturellement.

Quels seront les prochains enjeux ?

Deux priorités s'imposent. D'abord, continuer à rendre le droit de la donnée et de l'IA accessible à toutes les collectivités, quels que soient leur taille et leurs moyens. Ensuite, accompagner l'appropriation des nouveaux textes européens (AI Act, Data Act, Data Governance Act) afin qu'ils deviennent des outils opérationnels au service de l'action publique et non de simples réglementations supplémentaires. ■



Téléchargez le clausier Data & IA :

SOMMAIRE

LA TRANSFORMATION DES ORGANISATIONS ET DES MÉTIERS

Passé les premiers choix et les premiers tests, les collectivités installent officiellement des outils. Pour l'IA du quotidien, dédiée à la gestion administrative et parfois à la relation aux usagers, la mesure du déploiement n'est pas toujours simple. Les usages varient d'un utilisateur à l'autre. Certains, les plus jeunes notamment, sont enthousiastes et très consommateurs de prompts. D'autres sont prudents, réticents, voire réfractaires.

Pourtant, la mesure des usages est essentielle, car elle permettra de vérifier la pertinence des choix effectués et même, dans certains cas, l'utilité réelle des systèmes d'IA, parfois vendus accompagnés de promesses excessives.

Interrogées par l'Observatoire Data Publica, les collectivités dressent un premier tableau contrasté, qui mêle quelques déceptions mais aussi des attentes fortes pour l'avenir. 28 % considèrent les impacts comme très limités, mais 39 % mettent en avant des gains de temps significatifs et 24 % une accélération dans le traitement des procédures. Reste à décider de l'affectation du gain de temps, souvent consacré à des tâches jusqu'ici délaissées. 10 % des collectivités estiment d'ores et déjà avoir des retombées positives sur la qualité du service et 5 % sur les économies budgétaires.

À noter : 40 % des collectivités qui ont engagé des projets reconnaissent ne pas avoir, pour le moment, mis en place d'outil de suivi ni de mesure des impacts. Un chiffre élevé au regard des enjeux stratégiques et des transformations induites sur le service public.



▲ SOMMAIRE



Crédit photo : Anne-Charlotte Compan

HÉLÈNE GUILLET

Présidente nationale du Syndicat national des directions générales des collectivités territoriales (SNDGCT)

Le SNDGCT regroupe près de 4 000 adhérents. Il se donne pour mission de promouvoir et de valoriser les métiers de direction générale, d'apporter une contribution issue du terrain sur des enjeux pour le monde territorial et de capitaliser sur les bonnes pratiques. Il organise des groupes de travail de professionnels et sollicite le concours de partenaires publics et privés concernés par l'intérêt général. En novembre 2025, le SNDGCT a publié les résultats d'une enquête sur le déploiement de l'IA. L'occasion de faire le point avec Hélène Guillet, sa présidente.

Comment les sujets de la donnée et de l'intelligence artificielle affectent-ils le travail des directions générales des collectivités ? Comment s'approprient-elles ces enjeux ?

Dans notre enquête, il y a un an, l'IA apparaissait déjà comme une préoccupation majeure des directions générales. La donnée, en revanche, était beaucoup moins citée. Depuis, les choses ont certainement évolué. Pour toutes les directions générales qui débutent dans l'IA, il apparaît comme une évidence que les sujets sont liés. Je plaide pour une approche stratégique globale, car la gestion des données et le recours à l'IA sont indissociables lorsque l'on s'inscrit dans une logique de performance publique. Et cette approche globale doit mobiliser toutes les strates, y compris les DG.

Comment le rôle des directions générales évolue-t-il avec l'arrivée de l'IA dans une collectivité ?

Les DG sont progressivement passées d'une supervision, parfois lointaine, des systèmes d'information à un pilotage beaucoup plus resserré. Elles ont intégré la triple dimension de l'IA : politique, stratégique et opérationnelle.
Le sujet de l'IA est nouveau, mais les questions qui se posent aux directions générales sont bien connues : capacité à saisir des opportunités de gain de performance ; prise de recul pour ne pas se laisser attirer par des effets de mode ou des discours commerciaux ; attention portée à la montée en compétence de son organisation ; travail de coopération avec l'ensemble des protagonistes ; capacité à rendre compte aux élus comme aux parties prenantes des territoires…
L'IA est un sujet stratégique, donc un sujet pour les directions générales.

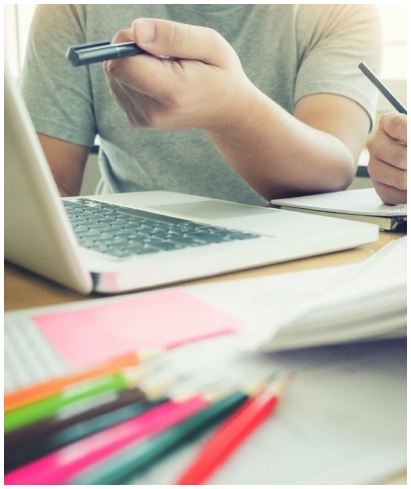
Comment et sous quel angle le syndicat professionnel que vous présidez s'est-il saisi du sujet ?

Le SNDGCT aide ses adhérents à comprendre les tendances émergentes et à se saisir de celles-ci. S'engager sur ce sujet relevait donc d'une évidence et c'est Marie-Claude Sivagnanam, vice-présidente du SNDGCT, qui a piloté cet engagement avec une approche à la fois stratégique et pragmatique. Nous avons commencé par une large enquête auprès de nos adhérents. Celle-ci a fait ressortir cinq priorités qui structurent les démarches et précisent les enjeux de développement de l'IA dans les collectivités : efficience et modernisation, acculturation et transformation humaine, sécurité et conformité, éthique et souveraineté, sobriété et impact environnemental. Cette enquête et les nombreuses expériences partagées ont été le point de départ du développement de notre présence sur tous ces thèmes. Nous produisons des analyses issues de groupes de travail et nous prenons la parole sans jamais perdre de vue un objectif opérationnel : proposer aux membres des directions générales des outils pragmatiques et faciles à mettre en œuvre. Nos synthèses des enjeux sont destinées en priorité aux équipes dirigeantes pour leur faire gagner un temps précieux d'information et de formation. Notre panorama, très documenté, permet ainsi à chacun de se situer et d'évaluer le degré de maturité de sa collectivité sur le sujet. Bref, notre but est et reste, y compris sur des sujets complexes comme l'IA, de répondre aux besoins des DG. ■

▲ SOMMAIRE

LE DIALOGUE SOCIAL SUR L'IA DANS LE LOIRET

Loiret



Tout au long de l'année 2025, le département du Loiret (691 300 habitants) a mené une démarche structurée autour de l'IA générative : celle-ci a combiné recueil des besoins métiers, expérimentation de cas d'usage, formation des agents et mise en place d'une gouvernance spécifique avec, notamment, un réseau de référents dans les directions. Dès le départ, la collectivité a fait le choix d'y associer les organisations syndicales très en amont, avant même le lancement des expérimentations

Lancée sous l'impulsion de la direction générale en 2024, la démarche a conduit à formaliser le rôle de Sandrine Gérard, directrice du service aux territoires et cheffe de projet IA générative.

Un premier passage en comité social territorial (CST), en décembre 2024, a permis de présenter l'ensemble de la démarche : objectifs, composition du groupe de projet, durée des expérimentations, mais aussi principes appelés à encadrer les usages de l'IA générative autour de la transparence, de la coopération, de la responsabilité et du respect des agents.

Ensuite, le dialogue s'est poursuivi de façon régulière et même en dehors des instances formelles. Les organisations représentatives ont été pleinement associées à la rédaction de la charte encadrant l'usage de l'IA générative. Leurs contributions ont porté sur des sujets très concrets : obligation de mentionner le recours à une IA, lorsqu'elle sert substantiellement à une production ; clarification de la responsabilité des agents ou encore articulation entre l'usage de ces outils et leurs obligations déontologiques.

En mars 2026, la collectivité est revenue devant le CST avec le bilan des expérimentations, le plan de déploiement des outils et les licences retenues, la gouvernance IA de la collectivité ainsi qu'une charte d'utilisation spécifique pour un outil d'enregistrement audio et de synthèse des réunions. L'ensemble de la démarche a reçu un avis favorable, voté à l'unanimité.

Désormais, le dialogue social se poursuit au fil du déploiement des outils. Selon Sandrine Gérard, l'acceptation du dispositif est notamment due au fait d'y avoir associé les organisations représentatives de manière très précoce et régulière. Ainsi, l'expérience du Loiret montre combien la qualité du dialogue social peut faciliter l'appropriation et l'acceptation des projets d'IA.

SOMMAIRE



Crédit photo : © Inria Photo B.Fourrier

YANN FERGUSON

Docteur en sociologie à l'Inria, chercheur associé au Certop et directeur scientifique du LaborIA

Un mot sur le LaborIA et ses travaux concernant les agents publics ?

Historiquement, le LaborIA a pour vocation de créer des connaissances sur l'IA au travail pour éclairer les politiques publiques. Mais, assez rapidement, les ministères économiques et financiers nous ont demandé une étude sur leurs cas d'usage internes afin de mieux appréhender comment ceux-ci sont appropriés par leurs agents. Et récemment, nous avons été mobilisés pour analyser l'expérimentation du déploiement d'un modèle d'IA générative auprès de 10 000 agents volontaires issus de différents ministères. Il est évidemment trop tôt pour en tirer des enseignements, mais voici quelques constats : tous les ministères ont une feuille de route et une équipe pour la piloter, à l'instar de la plupart des départements, régions ou métropoles ; le *« shadow AI »* est un phénomène identifié et majeur ; les démarches sont assez proches de celles engagées dans le monde économique, mais le principe d'une IA de service public et d'intérêt général comme ceux de souveraineté, d'organisation du travail, de statut des agents ou de dialogue social posent des problématiques différentes.

Quels sont les effets de l'IA sur l'emploi, le travail et les métiers dans les collectivités territoriales ?

Concernant l'emploi, il y a corrélation mais pas causalité. Pendant que les projets d'IA se multiplient, les collectivités sont toutes sous tension financière, ce qui impacte les possibilités et le type de recrutement, sans qu'on puisse l'imputer à l'IA. Globalement, pour le moment, l'intégration de l'IA est trop récente et expérimentale pour parler d'effets sur le travail. Comme dans la plupart des organisations, il s'agit surtout d'IA générative et celle-ci est pensée comme un assistant individuel qui accélère, pour chacun, l'exécution des tâches. Cela peut apporter des gains, mais il ne faut pas confondre accélération individuelle et gains de productivité, qui sont le résultat d'une transformation plus globale..

On dit que le déploiement de l'IA permettra des gains de productivité en réorientant les agents vers des tâches à forte valeur ajoutée. Quel regard portez-vous sur cette idée ?

Cette promesse ne passe pas l'examen. Au contraire, toutes les études montrent que les usages s'orientent majoritairement vers des tâches complexes de créativité, de résolution de problèmes techniques, voire humains, ou de traitement de l'information. Les tâches réputées les plus simples ou les plus répétitives, notamment administratives, sont plus adaptées à des algorithmes classiques, déterministes, moins performants mais plus mécaniques. L'IA générative est plus performante mais moins prévisible, ce qui la rend plus adaptée à des activités peu structurées, aux résultats moins exacts. ●●●

> *« Il ne faut pas confondre accélération individuelle et gains de productivité, qui sont le résultat d'une transformation plus globale. »*

SOMMAIRE

AVIS D'EXPERT

Quels impacts sur les relations sociales au travail anticipez-vous ?

La forme de l'assistant personnel n'est pas sans incidence sur les collectifs. Progressivement, le réflexe « demander à l'IA » se substitue au réflexe « demander aux collègues ». Les responsables de la transformation multiplient le lexique anthropomorphisant : un « collègue », un « stagiaire », un « expert », un « assistant », un « alternant » qu'il faudrait « manager ». Cela facilite l'adoption, mais au prix d'une confusion. On ne peut pas qualifier l'IA à la fois d'« outil » et de « collègue », ce sont des registres totalement différents. On observe également un phénomène d'élargissement volontaire des tâches : avec son assistant, chacun s'improvise un peu juriste, codeur ou communicant. Une paresse relationnelle se développe, nouvelle étape après la messagerie mail et le télétravail. Le numérique permet d'éviter l'autre, qui nous paraît d'autant moins supportable que le travail est un des derniers espaces de sociabilité non choisie. Il est, à ce titre, un lieu d'apprentissage de la différence essentiel à la démocratie. L'assistant IA pourrait fragiliser cette richesse…

Quels conseils donneriez-vous à une collectivité souhaitant engager une démarche IA en ayant un impact positif sur sa QVCT* ?

Une limite récurrente (que j'observe dans toutes les organisations) est de réduire l'évaluation de la réussite de leur projet IA à l'adoption de la solution et au temps individuel gagné. Le premier indicateur est tautologique : un projet IA serait réussi quand la solution est utilisée. Or, on oublie que l'IA est un outil, un moyen, au service d'une finalité : améliorer le travail, sa qualité, le service rendu, son efficience. C'est l'incidence de l'IA sur cette finalité qui devrait être mesurée. Quant au gain de temps, il est généralement individuel, local et immédiat. À ce titre, on observe des déplacements de charge. Individuel : présenter à l'oral un rapport rédigé par l'IA demande un surcroît d'effort cognitif, car la trace de production est moins profonde. Collectif : les agents reçoivent des dossiers de la part d'usagers, de prestataires, de demandeurs de subvention, de collègues, qui sont de plus en plus nombreux et longs et, parfois, un peu vides. C'est pourquoi j'invite les collectivités à adopter des mesures beaucoup plus larges de l'efficacité de l'IA autour de cinq dimensions : le travail réel, le travail bien fait, les compétences, la gouvernance, les types de technologies mobilisées. Tous ces critères convergent vers la même idée : ne pas céder à la tentation des choix à court terme pour intégrer l'IA de façon économiquement, socialement et écologiquement soutenable. ■

> *« Progressivement, le réflexe "demander à l'IA" se substitue au réflexe "demander aux collègues". »*

** Qualité de vie et conditions de travail.*

▲ SOMMAIRE

LE REGARD DE L'OBSERVATOIRE DATA PUBLICA

L'IA générative s'est installée dans le quotidien de nombreux agents publics. Mais cette « IA du quotidien » reste encore largement une IA individuelle : chacun apprend à l'utiliser pour rédiger, résumer, rechercher ou préparer son travail. Dans notre dernier cahier, *IA et territoires : après la découverte, le temps des premiers choix*, nous avions déjà choisi de déplacer la question de « quels métiers seront remplacés ? » vers celle de la transformation du travail et des métiers. Les résultats de cette année invitent à pousser le raisonnement un cran plus loin : comment passer de l'appropriation individuelle à une appropriation collective de l'IA ?

La question est d'abord celle des apprentissages : comment éviter que chacun construise seul ses usages, ses méthodes et ses bonnes pratiques ? Mais elle touche plus largement à l'organisation du travail. Comme le souligne Yann Ferguson, l'IA peut aussi nous exposer à une forme de « paresse relationnelle » : pourquoi solliciter un collègue, confronter un point de vue à un autre ou construire une réponse à plusieurs lorsque l'IA peut nous répondre immédiatement ?

La transformation des métiers ne se jouera donc pas seulement dans le face-à-face entre un agent et son assistant IA. Elle dépendra aussi de notre capacité à partager les apprentissages, à repenser collectivement le travail et à préserver les interactions qui font vivre les organisations.

Si la « paresse relationnelle » nous guette, il est temps de remettre du collectif dans nos usages de l'IA !



▲ SOMMAIRE

PARTIE 3

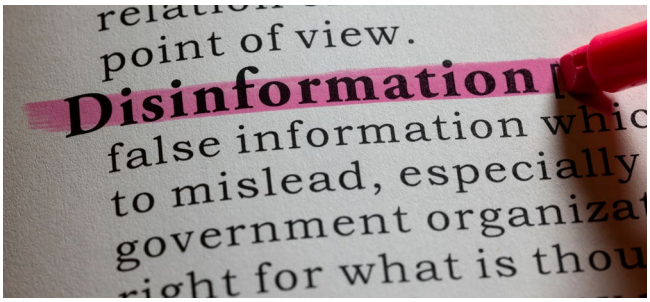
LA CYBERSÉCURITÉ DANS LES TERRITOIRES

En 2025, les ministères et les collectivités territoriales ont représenté 24 % des incidents traités par l'Anssi, soit le deuxième ensemble sectoriel le plus touché après l'éducation et la recherche. Les collectivités gèrent des données sensibles, assurent des services essentiels et s'appuient sur des prestataires dont la défaillance peut affecter les citoyens.

La cybersécurité n'est plus un sujet technique secondaire : elle garantit la protection des données personnelles et la confiance des citoyens ; elle engage la continuité du service public et la résilience des territoires.

▲ SOMMAIRE

COMPRENDRE LA MENACE POUR SAVOIR Y FAIRE FACE



À mesure que la transformation numérique irrigue l'ensemble de la société, la cybermenace s'intensifie et s'installe durablement.

Les tendances observées ces dernières années le confirment[2].

La menace est désormais structurelle. Elle n'épargne aucune organisation et émane d'acteurs organisés, dont les modes d'action deviennent plus difficiles à appréhender, dans un environnement technologique et opérationnel complexe. Les frontières entre cybercriminalité, hacktivisme et opérations conduites ou soutenues par des États apparaissent de plus en plus poreuses.

Les attaques par rançongiciel demeurent une menace majeure. Les cybercriminels recourent à la double, voire à la triple, extorsion[3] en combinant chiffrement des systèmes, vol des données et pression exercée sur les organisations ciblées, leurs partenaires, leurs clients ou usagers.
Les collectivités figurent parmi les organisations les plus exposées.

Les attaques motivées par des revendications idéologiques ou géopolitiques progressent également. Dans un contexte international tendu, les collectivités territoriales sont régulièrement visées par des campagnes de déni de service distribué (DDoS), qui cherchent principalement à produire un retentissement médiatique[4].

La chaîne de sous-traitance confirme parallèlement sa place de cible privilégiée. Plusieurs intrusions signalées en 2025 ont mis en évidence les risques portant sur les plateformes numériques mutualisées ou sur les prestataires assurant des services essentiels pour plusieurs collectivités. Une compromission unique peut ainsi se propager à un grand nombre d'organisations[5].

Enfin, les vulnérabilités humaines demeurent l'un des principaux points d'entrée des attaquants, avec une hausse de l'ingénierie sociale[6].

Deux évolutions viennent encore accentuer la menace. La première est la déstabilisation informationnelle, qui s'est notamment manifestée lors des élections municipales de mars 2026[7].
La seconde tient à l'intelligence artificielle, devenue un levier d'efficacité, d'apprentissage et de passage à l'échelle pour les attaquants.

Vincent Strubel, directeur général de l'Anssi, lors de son audition devant la commission des affaires économiques du Sénat, le 28 juillet 2026 :

« Nous sommes sur une marée haute de menaces, qui continue à monter et dont nous ne connaissons pas le sommet. »

2. Sources : rapports de l'Anssi, Cybermalveillance.gouv.fr, ComCyber-MI, ministère de l'Intérieur, CNIL.

3. La double extorsion consiste à faire pression sur les victimes en exfiltrant et en chiffrant les données de son système d'information, d'une part, et en menaçant de les divulguer, d'autre part. Cette double approche peut être complétée par d'autres moyens de pression, comme des attaques en déni de service distribué (DDoS) ou des tentatives d'extorsion auprès de partenaires ou de clients de l'entité victime dans des attaques dites « par triple extorsion » (source : Anssi).

4. ComCyber-MI, « Rapport annuel sur la cybercriminalité 2026 », avril 2026.

5. Ibid.

6. Ensemble de méthodes permettant de connaître précisément le profil et l'environnement d'une cible pour rendre plus efficace sa manipulation. Les données utilisées sont à la fois celles disponibles sur les réseaux et celles exfiltrées à l'occasion d'une cyberattaque.

7. Viginum, « Rapport sur la protection du débat public contre les ingérences numériques étrangères durant les élections municipales des 15 et 22 mars 2026 », juin 2026, accessible en ligne : www.sgdsn.gouv.fr/viginum/publications/protection-du-debat-public-contre-les-ingerences-numeriques-etrangeres-durant

SOMMAIRE

UNE CYBERATTAQUE D'OPPORTUNITÉ RAPIDEMENT CONTENUE

Haut-de-Seine



Le département des Hauts-de-Seine a été victime d'une cyberattaque d'opportunité en mai 2025. Emmanuel Bonnet, CIO/CISO du département, revient sur la gestion de cette crise, les enseignements qui en ont été tirés et les procédures mises en place depuis lors.

Le 12 mai 2025, lors d'une maintenance applicative planifiée, un technicien télécharge un outil *via* une recherche Google, victime d'un lien piégé (technique de *SEO poisoning*). Ce logiciel contenait un code malveillant qui, bien qu'ayant déclenché de très légères alertes, n'a pas été immédiatement identifié comme critique.

Comment avez-vous géré la crise, lorsque vous avez pris conscience du problème ?

Comme il s'agissait d'une intervention de routine, il n'y a pas eu d'« alerte rouge » déclenchée. Après quelques jours, face à d'autres alertes signalant que l'Active Directory pouvait être compromis, nous avons coupé le courant électrique de nos salles machines le lundi 19 mai. Ce fut assez violent mais efficace. Les pôles Solidarités, Finances et RH, dépendants d'applications *on premise*, ont subi un arrêt complet. L'infrastructure des collèges du département a été temporairement perturbée. Mais l'analyse d'experts extérieurs a démontré qu'aucune donnée n'avait été exfiltrée ni chiffrée grâce à une réaction très rapide : l'attaque a été stoppée à l'étape 4 sur 10.

Y a-t-il eu d'autres conséquences ?

Hormis le premier jour, nos quelque 4 000 agents ont rapidement pu utiliser leurs outils de travail de bureau : ils avaient été migrés sur le cloud, ainsi qu'une partie des applications métiers, comme la gestion des marchés publics. Le plus ennuyeux, une fois la crise connue, a été notre bannissement immédiat par la plupart de nos fournisseurs et de nos partenaires. Une fois le risque écarté, nous avons dû les appeler un à un pour rétablir les liaisons. Le rapport d'enquête a été rendu fin juin 2025. Il a fallu ensuite plus de six mois pour redémarrer l'ensemble des applications, en veillant minutieusement à ce qu'aucun code malveillant ne subsiste sur les serveurs. Enfin, un long travail a été nécessaire pour réintégrer informatiquement toutes les données collectées à la main ou en mode dégradé durant l'arrêt des systèmes.

Quel retour d'expérience en tirez-vous ?

Nous avons revu et renforcé nos process de sécurité : la mise en place de la double authentification pour tous les agents a été accélérée ; la sécurité de l'Active Directory, renforcée selon les règles de l'art ; un contrôle très strict, un véritable « sas de quarantaine », a été instauré pour toute nouvelle installation de logiciel. En complément des actions de sensibilisation existantes, notamment des tests de phishing, une nouvelle plateforme ludique de sensibilisation va être déployée, permettant une formation continue à travers des sessions courtes. Et nous venons d'envoyer un questionnaire à tous les agents pour collecter leurs réactions et ressentis face à cette crise, nous donnant ainsi des indicateurs sur les prochaines actions à mener.

▲ SOMMAIRE

LE REGARD DU CYBERCERCLE

Face à ce constat, une conviction s'impose : mieux comprendre l'espace numérique et les menaces qui s'y développent est aujourd'hui une nécessité pour les collectivités pour leur permettre de mieux anticiper, de mieux se préparer et d'agir. Cette connaissance et la veille qui doit l'accompagner sont d'autant plus fondamentales que le contexte ne cesse d'évoluer, l'intelligence artificielle accélérant encore les processus de transformation, sans parler à plus long terme des bouleversements induits par le quantique. Le défi pour les collectivités réside ainsi aujourd'hui dans leur capacité à anticiper pour assurer la continuité de leurs missions de service public, la protection des citoyens, et pour piloter une transformation numérique fondée sur la confiance. Dans cet objectif, partager les retours d'expérience est précieux pour comprendre et anticiper au mieux.

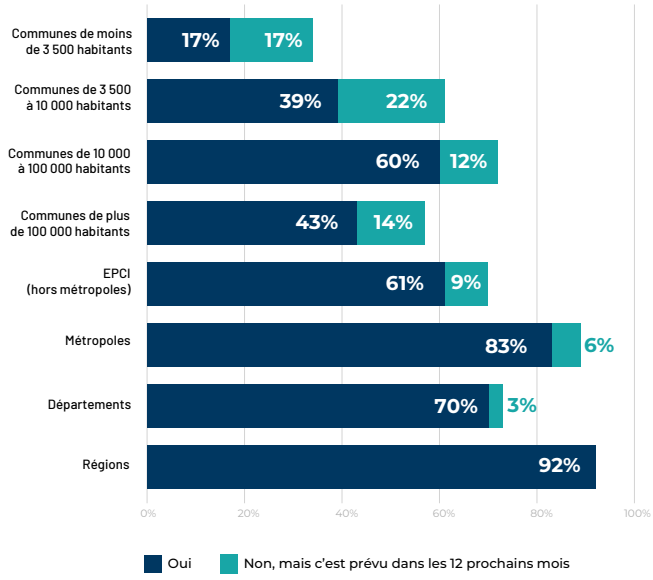
UN CHEMIN POUR TOUS : SENSIBILISER, ANTICIPER, CONTRACTUALISER

Dans un contexte de menace durable, toutes les collectivités, quelle que soit leur taille, peuvent engager des actions pour renforcer leur protection, limiter l'impact d'une cyberattaque et préserver la continuité de leurs missions. Deux conditions sont essentielles : avoir conscience du risque et engager l'ensemble de la collectivité en matière de risque cyber. Trois leviers d'action sont particulièrement structurants :

Sensibiliser les agents et les élus

Les agents territoriaux manipulent quotidiennement de nombreuses données personnelles, des outils métiers et des accès parfois critiques, engageant des enjeux majeurs pour la vie des citoyens : leur vigilance individuelle devient une composante essentielle de la résilience collective. Conscientes de cet enjeu, de nombreuses collectivités (et pas uniquement les plus grandes) engagent des actions de sensibilisation internes, auprès des agents mais aussi des élus. Identifier un courriel frauduleux, utiliser des mots de passe robustes, verrouiller son poste, signaler rapidement un incident, protéger les informations sensibles ou adopter les bons comportements en mobilité… sont autant de réflexes simples mais décisifs, de bonnes pratiques qui structurent les politiques de sensibilisation mises en œuvre.

La réalisation de formations pour les agents et les élus :



▲ SOMMAIRE

LA SENSIBILISATION DES AGENTS COMME PREMIER REMPART CYBER

Hettange-Grande

La commune d'Hettange-Grande (Moselle, en région Grand Est) a mis en place, en novembre 2025, une action de sensibilisation interne en s'appuyant sur les formations en cybersécurité du CNFPT. Destinée aux agents municipaux, cette démarche vise à réduire les risques liés aux usages numériques quotidiens – mots de passe, mobilité, RGPD – et à installer des réflexes de sécurité simples dans les pratiques administratives.

Après un diagnostic des risques les plus fréquents, les agents ont été répartis en fonction de leurs profils (accueil, encadrants, direction, technique) et ont suivi une formation complète : théorique (e-learning, classe virtuelle) puis pratique grâce à des ateliers les mettant dans différentes situations (e-mails factices, QR codes suspects, *phishing* interne, etc.).

Un débriefing sur les bons et les mauvais usages numériques a été réalisé, puis des fiches « mémo » distribuées et affichées (règles de mots de passe, signalement d'incidents, verrouillage de session, filtres de confidentialité à l'écran). Un parcours d'accueil numérique a été mis en place pour chaque nouveau collaborateur.

Un suivi sous forme de tableau de bord (taux de participation, scores obtenus aux quiz et nombre d'incidents déclarés) est partagé régulièrement en comité interne.

Résultats : les agents identifient mieux les tentatives d'hameçonnage, les erreurs de manipulation diminuent sensiblement et les délais de réaction en cas d'alerte se raccourcissent.

La posture de sécurité de la collectivité s'améliore sans alourdir le quotidien des équipes, illustrant une approche pragmatique de montée en compétence interne avec le concours d'un acteur de formation de la fonction publique territoriale.



En corollaire, des collectivités se saisissent de l'enjeu sociétal de la sensibilisation de leurs administrés. Partant du constat que la résilience globale du territoire s'appuie aussi sur une culture de la cybersécurité partagée par l'ensemble de la population, elles mènent des actions auprès des citoyens autour des usages sécurisés du numérique : elles ciblent par exemple des élèves ou organisent des ateliers numériques ouverts à tous.

▲ SOMMAIRE

LA CYBERSÉCURITÉ DÈS L'ÉCOLE : UNE DÉMARCHE ENGAGÉE

Roumois Seine



En 2025, la communauté de communes Roumois Seine (Eure et Seine-Maritime, en région Normandie) a lancé une campagne de sensibilisation à la cybersécurité à destination des élèves du territoire, du CM1 à la quatrième. Au total, 41 classes ont bénéficié d'une session d'une heure et demie : 800 élèves ont été sensibilisés en 2025, 971 en 2026.

Partant d'une feuille blanche, les directions des établissements scolaires et les services intercommunaux ont coconstruit ce programme sous la houlette de Yannick Boudet, vice-président chargé du sport et du territoire intelligent, à l'initiative de la démarche. Animées par deux agents de médiation de la communauté de communes, les interventions en classe abordent les bonnes pratiques pour sécuriser les usages numériques du quotidien. Les agents alternent vidéos, échanges collectifs et ateliers pratiques en prenant appui sur des ressources provenant de Cybermalveillance.gouv.fr, de l'Anssi et d'Internet Sans Crainte, ainsi que sur des outils pédagogiques éprouvés, tels que les jeux sérieux *Gafa tes données, Le Chronocrypteur* et *Cyber-Enquête*. Ces interventions sont ponctuées par un temps d'échange sur la cybersécurité avec les enseignants.

Le déploiement du dispositif a été prioritairement orienté vers les secteurs les moins couverts par les actions de médiation numérique préexistantes afin de réduire les disparités d'accès à la sensibilisation au niveau du territoire.

Cette dynamique s'inscrit dans une stratégie globale de cybersécurité portée au sein de la collectivité. Elle se renforcera encore à la rentrée prochaine, favorisant la construction, dès le plus jeune âge, d'une culture de cybersécurité partagée sur le territoire.

Et Yannick Boudet de conclure : *« C'est un investissement pour la collectivité, mais l'enjeu est majeur, tant les jeunes sont confrontés de plus en plus tôt au numérique. Notre démarche a reçu un très bon accueil aussi bien auprès des élèves que des professeurs. Mon vœu serait que ce type d'action soit intégré systématiquement dans les programmes. »*

Anticiper le risque avec les PCA-PRA

La cyberrésilience des collectivités suppose d'anticiper la continuité des services essentiels, la coordination des métiers, la communication de crise et la reprise progressive de l'activité en mode dégradé.

Les collectivités intègrent de plus en plus le risque cyber dans la mise en œuvre du plan de continuité d'activité (PCA) et du plan de reprise d'activité (PRA).

Cette démarche oblige chaque service à identifier ses missions essentielles – état civil, action sociale, paie, écoles, collecte des déchets, relation aux usagers – et à analyser ses dépendances aux applications, aux données, aux prestataires et aux infrastructures numériques. Elle permet de définir des priorités de reprise, des modes dégradés, des chaînes d'alerte et des responsabilités claires entre élus, direction générale, DSI, métiers, communication et partenaires externes.

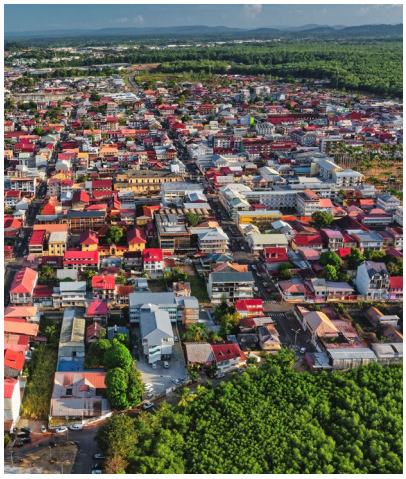
L'intérêt est également très opérationnel : documents accessibles hors ligne, annuaires de crise, procédures d'escalade, sauvegardes vérifiées, scénarios de bascule et tests réguliers réduisent les délais de réaction et limitent les interruptions de service.

Le PCA-PRA devient un outil de coordination autant qu'un outil de sécurité.

▲ SOMMAIRE

RENFORCER LA RÉSILIENCE DES SERVICES PUBLICS LOCAUX

Centre littoral de Guyane



La communauté d'agglomération du Centre littoral (CACL) rassemble plus de 153 000 Guyanais. Elle a engagé, dès 2025, une démarche structurante pour assurer la continuité de ses services essentiels en cas de crise majeure.

Cyberattaque, incendie, panne informatique, coupure réseau ou défaillance matérielle : le projet vise à préparer la collectivité à différents scénarios susceptibles d'interrompre son fonctionnement. Il prévoit d'abord une cartographie complète des processus métiers critiques, l'identification de leurs dépendances aux systèmes d'information et une analyse des risques associés.

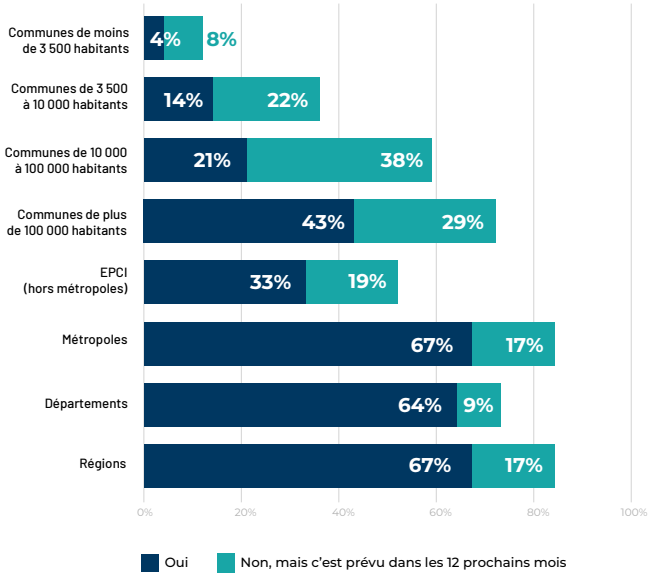
Cette démarche s'est traduite par la mise en place du PCA, intégrant l'organisation des ressources humaines, la hiérarchisation des priorités et les modes dégradés de fonctionnement. Elle s'accompagne du PRA, fondé sur des sauvegardes, des dispositifs de redondance et des scénarios de bascule.

Une gouvernance dédiée (associant SSI, DSI et métiers) a été installée avec des procédures d'escalade, des outils de communication de crise, un journal de bord et des tests réguliers. La documentation a été également transférée vers un espace de stockage sécurisé.

Cette structuration permet de réduire les délais de réaction, d'améliorer la coordination entre services et de limiter les interruptions, tout en maintenant les agents en capacité d'agir en situation dégradée.

Par ailleurs, les élus plébiscitent de plus en plus les exercices de gestion de crise cyber, surtout au sein des grandes collectivités. Cette année, 36 % des collectivités de plus de 3 500 habitants en ont organisé et 22 % ont prévu de le faire dans les prochains mois, une progression de 22 points en deux ans.

La mise en place d'exercices de gestion de crise cyber par les collectivités :



▲ SOMMAIRE

MANCHE NUMÉRIQUE : UN EXERCICE DE CRISE CYBER POUR PROVOQUER UN ÉLECTROCHOC

Manche



Le 4 décembre 2025, le syndicat Manche numérique a organisé un exercice de gestion de crise cyber réunissant une centaine d'élus et d'agents territoriaux du département.

Objectif : provoquer une prise de conscience. *« L'idée était de créer un électrochoc… et nous y sommes arrivés ! »* résume Rachid Mammeri, DGS du syndicat mixte.

Pendant une heure et demie, les participants ont été plongés dans un scénario réaliste. Dès 13 h 30, des écoles et des mairies signalent des pannes : documents inaccessibles, plateforme de gestion des dossiers « élèves » indisponible, services numériques bloqués. Très vite, la question du déclenchement d'une cellule de crise se pose. Qui mobiliser ? Quels contacts activer ? Comment communiquer ?

L'exercice révèle plusieurs fragilités : absence de service informatique dans certaines collectivités, dépendance à des prestataires externes, défaut de cartographie des systèmes d'information, méconnaissance du CSIRT normand ou de la plateforme 17Cyber. La communication se tend, alors que les outils numériques habituels deviennent inutilisables.

L'effet a été immédiat : dès le lendemain, une vingtaine de ses 400 adhérents demandaient un accompagnement. Depuis, Manche numérique a mis en place des fiches « réflexes », des contacts de crise hors ligne et une « mallette cyber » comprenant un ordinateur et un téléphone opérationnels. Le syndicat envisage désormais une offre de DSI mutualisée afin d'élever collectivement le niveau de cyberrésilience du territoire.

manche numer:que
TERRITOIRES • RÉSEAUX • SERVICES

▲ SOMMAIRE



LIONEL PÉRÈS

Lionel Pérès, ancien DGS de Vaison-la-Romaine (Vaucluse, en région Provence-Alpes-Côte d'Azur), auteur de « Cyberattaque : assurer la continuité des services publics locaux » (éditions Territorial, 2025)

ANTICIPER LA CRISE POUR ASSURER LA CONTINUITÉ DU SERVICE PUBLIC

Vous insistez sur le fait que la sécurité numérique est d'abord un sujet de gouvernance. Pourquoi ?

Parce que le dirigeant ne peut pas déléguer entièrement le sujet à la direction des systèmes d'information. La DSI maîtrise les moyens techniques. La direction générale connaît les missions de la collectivité, ses priorités et ses données les plus sensibles. C'est à elle d'identifier ce que j'appelle les « joyaux de la couronne » et de décider ce qui doit être protégé en premier.

Sans ce dialogue, chacun se retrouve en difficulté. La bonne démarche consiste à articuler deux responsabilités : le dirigeant indique ce qui est critique ; le DSI propose les moyens adaptés pour le sécuriser.

La notion de souveraineté numérique, qui est aujourd'hui un enjeu dont les dirigeants se sont saisis, peut aussi contribuer à replacer ces arbitrages au bon niveau.

Pourquoi la cybersécurité reste-t-elle encore difficile à porter auprès des dirigeants territoriaux ?

Le terme lui-même crée une distance. Lorsqu'on parle de « cybersécurité », de nombreux dirigeants pensent immédiatement qu'il s'agit d'un sujet technique et renvoient vers leur DSI.

Il est souvent plus efficace de parler de « sécurité numérique », de « transformation numérique de confiance » ou de « continuité d'activité ».

Introduire la dimension de la sécurité au sein de sujets déjà identifiés par les décideurs, par exemple celui de l'intelligence artificielle, permet parfois de franchir cette première barrière.

Malgré tout, la prise de conscience reste insuffisante. Les dirigeants déjà convaincus continuent d'avancer, ceux qui ne se sentent pas concernés s'engagent encore difficilement. Le dialogue entre pairs est alors essentiel : un DGS qui témoigne de sa propre démarche peut rendre le sujet plus concret et accessible.

Votre livre est justement né de ce besoin de rendre la démarche accessible…

Après une séance de sensibilisation menée par un « gendarme référent cyber », je me suis demandé : par où commencer pour assurer la continuité de ma collectivité ? J'ai trouvé de nombreuses ressources sur la continuité de l'activité industrielle, mais presque rien sur la continuité des services publics locaux.

Avec mon équipe, nous avons donc construit une méthode. Le livre est issu de ce retour d'expérience. J'ai voulu écrire l'ouvrage que j'aurais aimé trouver au moment de me lancer : un guide concret, sans jargon, destiné aux secrétaires généraux de mairie, aux DGS, aux élus et, plus largement, aux non-spécialistes. Un kit de survie pour débuter, une boussole pour s'orienter.

Le très bon accueil reçu par le livre montre que cette entrée par la continuité d'activité répond à un besoin. ●●●

▲ SOMMAIRE

AVIS D'EXPERT

Comment une collectivité peut-elle construire un PCA efficace en matière cyber ?

Il faut partir des missions et non des outils. Chaque service commence par lister ce qu'il doit accomplir. Il identifie ensuite les missions qui dépendent du système d'information, les logiciels ou les prestataires mobilisés, puis il recherche le mode dégradé permettant d'assurer la continuité de l'activité en cas d'indisponibilité des ressources numériques.

Les agents connaissent leur métier et trouvent souvent par eux-mêmes la solution la plus robuste.

Cette cartographie permet également d'anticiper l'impact de certains incidents partiels : si un éditeur devient indisponible, la collectivité sait quels métiers sont concernés et quels modes dégradés déclencher.

Le PCA de la collectivité résulte de l'agrégation des plans de continuité de chaque service. Il doit se construire dans un dialogue entre métiers, informatique et gouvernance et s'inscrire dans une démarche d'amélioration continue. ■

Insérer la cybersécurité dans les contrats

La cybersécurité devient un sujet de commande publique, de contractualisation et de pilotage des prestataires. À mesure que les services numériques locaux sont externalisés – hébergement, cloud, infogérance, logiciels métiers, archivage –, la résilience des collectivités dépend aussi de leur capacité à intégrer des exigences cyber opposables dans leurs marchés et leurs contrats.

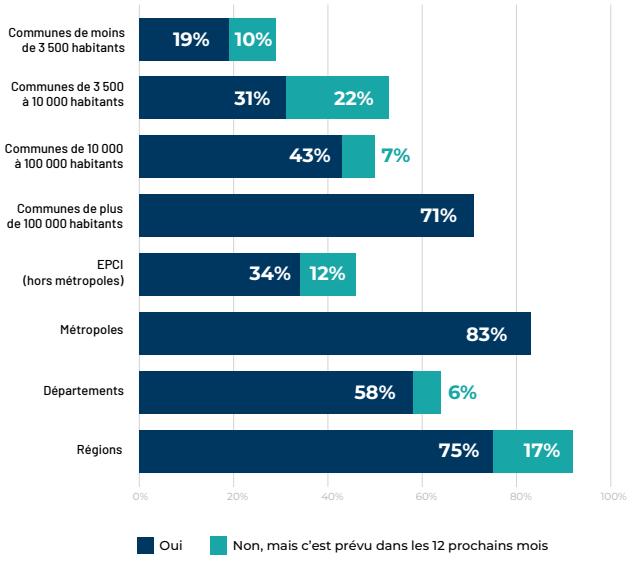
Les évolutions législatives autour de la sécurisation des marchés publics numériques traduisent cette montée en puissance. Clauses d'hébergement, exigences de sécurité, réversibilité, récupération des données en fin de contrat, conditions d'archivage, localisation des données, recours à des solutions qualifiées ou certifiées : ces éléments deviennent des outils concrets de maîtrise des risques.

Un volet qui entre dans le champ de responsabilité sociétale des collectivités : le développement d'une culture de cybersécurité partagée par les citoyens renforce la résilience globale du territoire.

Ainsi, les collectivités ont renforcé leur capacité à prévenir les incidents, à réagir plus vite en cas d'attaque et à maintenir la continuité des services publics.

Mais un obstacle demeure : la nécessité de disposer de ressources internes pour porter ces leviers juridiques et contractuels. Renforcer les compétences des collectivités en matière de commande publique sur le numérique et la cybersécurité devient une condition de souveraineté, de maîtrise des coûts, de protection des données et de continuité des services publics.

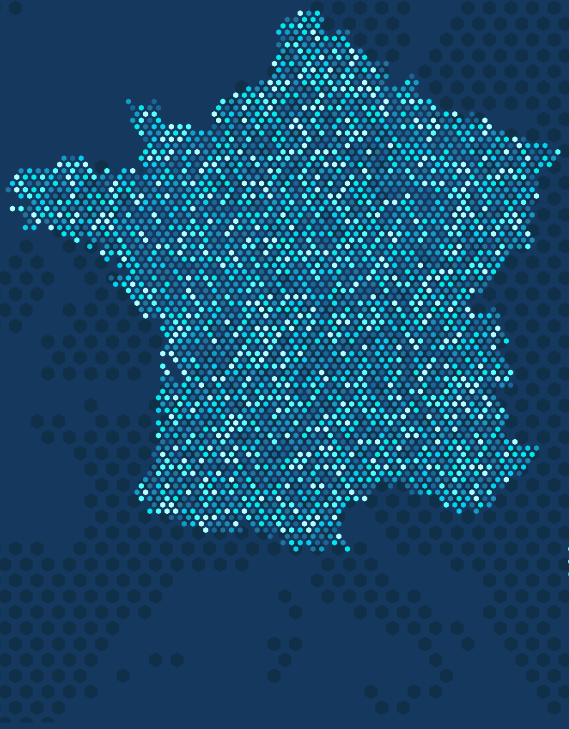
L'intégration de clauses de sécurité dans les contrats informatiques :



▲ SOMMAIRE

LES CSIRT TERRITORIAUX : UN DISPOSITIF ÉTAT-RÉGION SUR LES TERRITOIRES

Dans leur rapport d'activité 2025[8], les CSIRT territoriaux se présentent comme des maillons de proximité dans l'organisation de la réponse cyber au service des acteurs locaux. Issus d'une dynamique portée par l'Anssi et les régions depuis 2021, ils visent à proposer une réponse de premier niveau aux incidents, mais aussi des actions de prévention, de sensibilisation, de diagnostic et de mise en relation avec des prestataires adaptés aux réalités de chaque territoire. Ils présentent une offre mutualisée et accessible pour des bénéficiaires qui peuvent être dépourvus de ressources cyber internes. La montée en puissance, soulignée dans le rapport, d'une communauté inter-CSIRT fondée sur le partage d'outils, de pratiques, d'incidentologies territoriales et de retours d'expérience favorise l'harmonisation et l'optimisation entre les différents territoires.



LE REGARD DU CYBERCERCLE

Les collectivités inscrivent de plus en plus la cybersécurité dans une démarche de résilience et de continuité de leurs missions : elle ne se limite plus à la protection technique du système d'information. En sortant du champ *stricto sensu* de la DSI à travers les PCA-PRA et les exercices de gestion de crise, elle devient un facteur d'action transverse, pris en compte par les différents services et favorisant la création d'une culture commune. Au-delà, les collectivités intègrent de plus en plus dans leur champ de responsabilité sociétale et politique l'acculturation à la cybersécurité de leurs administrés. Ce double mouvement montre combien la vision de la cybersécurité par les collectivités amorce un changement de perception pour devenir un axe de politique publique fédérateur, tant en interne qu'en externe.

8. *Anssi, « Rapport d'activité des CSIRT territoriaux 2025 », accessible en ligne : https://cyberocc.com/wp-content/uploads/2026/04/Rapport-dactivite-des-csirts-territoriaux-2025.pdf*

▲ SOMMAIRE

UN ENGAGEMENT QUI S'ACCÉLÈRE POUR LES GRANDES COLLECTIVITÉS

La prise de conscience des grandes collectivités face aux enjeux de cybersécurité continue de se renforcer en s'inscrivant dans des stratégies numériques plus globales.

Dans leur démarche, ces collectivités affichent une volonté de renforcer leur autonomie stratégique, intègrent les enjeux liés à l'intelligence artificielle et étendent leur champ d'action jusqu'à la sécurité informationnelle.

L'autonomie stratégique : une dimension de la cybersécurité au service de la résilience des collectivités

Les grandes collectivités ne se contentent plus d'acheter des solutions : elles s'organisent pour peser sur le marché et reprendre la main sur leurs dépendances technologiques dans un objectif de maîtrise de leur trajectoire numérique.

La question ne porte pas seulement sur la nationalité des solutions retenues, même si l'exposition à des droits extraterritoriaux ou à des risques de rupture de service (*« kill switch »*) reste un critère de plus en plus affirmé. Elle relève aussi de la capacité des acteurs publics locaux à éviter des rapports trop déséquilibrés avec certains fournisseurs dominants : hausse progressive des coûts, évolution unilatérale des conditions contractuelles, difficulté à changer de solution, perte de maîtrise technique ou fonctionnelle.

La relation client-fournisseur devient un enjeu central. Les collectivités recherchent des partenaires capables d'échanger sur leurs besoins, d'adapter les solutions aux contraintes du service public local et d'inscrire la relation dans la durée par un dialogue constructif entre experts. Certaines vont encore plus loin, en se tournant vers des solutions open source qu'elles peuvent contribuer à faire évoluer à des fins de mutualisation et de maintien en condition opérationnelle.

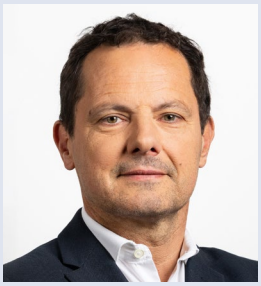
Cette bascule stratégique se manifeste notamment par des groupements de commandes ou des centrales d'achat qui réorientent leurs cahiers des charges pour y inclure des critères d'autonomie ; par des communautés d'usages de solutions open source ; par des coopérations entre régions, métropoles et syndicats mixtes pour offrir des services numériques aux petites communes.

Un enjeu global qui a été au cœur des travaux de la commission d'enquête de l'Assemblée nationale sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique. Dans son rapport publié le 8 juillet 2026[9], la commission affiche son soutien aux communs numériques, à l'open source, à l'interopérabilité et aux achats groupés, présentés comme des leviers de maîtrise technologique et de résilience.

Cette dimension d'autonomie devient ainsi un critère opérationnel de cybersécurité : elle participe pleinement à la maîtrise des données, des coûts et des infrastructures dans une stratégie affirmée, tout en optimisant la résilience des services publics.

9. *Rapport de la commission d'enquête de l'Assemblée nationale, juillet 2026, accessible en ligne : www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete*

▲ SOMMAIRE



JÉRÔME DURAIN

Président de la région Bourgogne-Franche-Comté

Vous avez affirmé que « la cybersécurité n'est plus une option mais une condition essentielle de la continuité du service public ». Pourriez-vous développer votre position ?

Ma conviction est que les risques numériques concernent tout le monde : nos familles, nos hôpitaux, nos mairies, nos services publics et notre système de défense. Lorsqu'une attaque met un hôpital en difficulté, comme cela s'est produit en octobre 2025 au CHIHC de Pontarlier, dont le retour à la normale n'est pas attendu avant 2027, elle peut mettre des vies en danger. Elle fragilise aussi la confiance des citoyens. La menace est globale, qu'elle émane d'escrocs motivés par l'argent ou de puissances étrangères cherchant à nuire.

Nous restons très attachés à la solidité des bâtiments ou à la robustesse des réseaux de transport, mais nos infrastructures numériques sont aujourd'hui tout aussi essentielles. Leur sécurisation conditionne le versement des aides, la délivrance des actes administratifs, le fonctionnement des transports ou des lycées.

Il est évident que les collectivités territoriales sont devenues des cibles, parce qu'elles assurent des services publics essentiels, parce qu'elles ont des données sensibles et parce qu'elles sont aussi très nombreuses, assez atomisées et parfois mal préparées.

La Bourgogne-Franche-Comté s'est dotée d'une stratégie régionale de cybersécurité. Quels en étaient les objectifs majeurs ? Comment l'avez-vous élaborée ? Et quels moyens sont aujourd'hui mis en place ?

Notre premier objectif est d'élever le niveau de protection de la région elle-même : sécuriser nos systèmes d'information et nos procédures, former nos agents et réduire les incidents. Mais un écosystème n'est protégé que si chacun de ses maillons est sécurisé : notre action concerne donc aussi l'ensemble du territoire régional. Nous avons travaillé cette stratégie avec les services de la région, l'Anssi, la préfecture de région et l'ARNia (Agence régionale du numérique et de l'intelligence artificielle), qui porte notre politique en faveur de la cybersécurité. Celle-ci s'appuie sur l'ARNia et le CSIRT Bourgogne-Franche-Comté.

La cybersécurité est clairement fléchée comme une priorité politique de notre action numérique.

Vous avez justement confié à l'ARNIa une mission de diagnostic, de sensibilisation et d'accompagnement auprès des principaux opérateurs de la région. Quel en est le but ?

Ce travail est en cours, les conclusions sont attendues en fin d'année. Nous voulons développer une véritable culture de la confiance et de la vigilance sur notre territoire. Un mot de passe trop faible, un courriel frauduleux ou une mauvaise pratique sont autant de portes ouvertes aux attaquants. La formation est donc première.

Au-delà du diagnostic, j'attends de l'ARNIa qu'elle aide nos opérateurs à corriger leurs vulnérabilités, à mieux prévenir les incidents et, plus largement, qu'elle fasse progresser le niveau de maturité cyber du territoire. La région a financé l'ARNia à hauteur de 730 000 euros en 2026. Cette dernière recense 1 800 communes adhérentes sur les 3 600 que compte la région.

●●●

▲ SOMMAIRE

La région soutient également le CSIRT Bourgogne-Franche-Comté. Quel modèle de service public territorial de la cybersécurité souhaitez-vous construire, notamment pour les petites collectivités et les structures aux moyens limités ?

Ce modèle doit reposer sur la proximité, la mutualisation et la solidarité. La région peut recruter des experts et investir dans des outils avancés. Pour une commune de 1 500 habitants ou un petit établissement public, c'est souvent inaccessible. Sur un territoire qui compte 3 600 communes et 114 intercommunalités, il faut donc aider les structures plus petites, qui n'ont pas les mêmes moyens, pour éviter une fracture numérique de sécurité. Et leur offrir l'accès à un certain niveau d'expertise et d'accompagnement. Dans la jungle des offres privées, pour lesquelles il n'y a pas d'expertise publique ni d'aide à la décision, il faut assurer une forme d'égalité d'accès à la sécurité numérique dans une philosophie de solidarité territoriale.

Le CSIRT apporte ce premier niveau de service : alerter, qualifier l'incident, donner les premiers conseils, orienter la collectivité vers les acteurs compétents et l'aider à revenir à la normale. Une structure publique doit aussi jouer le rôle de tiers de confiance et d'aide à la décision face à l'abondance d'offres privées.

Quel message adresseriez-vous aux élus qui considèrent encore que la cybersécurité relève principalement des informaticiens ?

Les incidents n'arrivent pas qu'aux autres. Il faut comprendre que personne n'est à l'abri, qu'une petite taille ne protège pas des cyberattaques et que l'intelligence artificielle démultiplie en outre les risques. Chaque élu doit se saisir du sujet avec volontarisme. Cela fait partie de la responsabilité des maires et des exécutifs : la cybersécurité relève de la gouvernance et de la continuité du service public. Je pense que beaucoup baissent les bras. Ils ne voient rien sur étagère, rien n'est accessible, rien n'est naturel. En donnant accès à un service de proximité et à des compétences mutualisées, la région offre une réponse aux élus pour devenir acteurs de ce sujet au lieu de s'en remettre à la bonne fortune. ■

> *« Les risques numériques concernent tout le monde : nos familles, nos hôpitaux, nos mairies, nos services publics et notre système de défense. »*

L'intelligence artificielle et la cybersécurité au service de la transformation numérique des collectivités

De grandes collectivités développent désormais des stratégies globales de transformation numérique associant intelligence artificielle et cybersécurité.

L'enjeu est double : il s'agit, d'une part, de développer l'IA, tout en sécurisant son utilisation et, d'autre part, de renforcer la cybersécurité avec l'appui de l'IA, en l'intégrant dans un cadre de confiance, de supervision humaine et de gouvernance claire.

▲ SOMMAIRE

MUTUALISER POUR RENFORCER L'AUTONOMIE STRATÉGIQUE DES TERRITOIRES

Face à la complexité croissante de la cybersécurité, la mutualisation constitue un levier structurant pour les collectivités. Elle permet de dépasser les limites liées à la taille des organisations, à la disponibilité des compétences ou aux contraintes budgétaires et de donner accès à des solutions qui, autrement, seraient difficiles à mobiliser.

Une démarche vertueuse de mutualisation repose, d'abord, sur sa gouvernance. Lorsque les acteurs territoriaux chargés de la cybersécurité participent directement à la définition des besoins et à la rédaction des marchés, les solutions proposées sont davantage en prise avec les réalités opérationnelles.
La logique n'est plus seulement celle d'un achat standardisé, mais elle repose sur l'expérience concrète des utilisateurs.

Ainsi, les marchés conçus en co-construction avec des DSI ou des RSSI facilitent l'usage d'outils adaptés, financièrement soutenables et techniquement accessibles. Ils contribuent également à mieux intégrer des exigences de protection des données, de transparence, d'éthique et d'autonomie, des critères fondamentaux dans les choix de sécurité numérique.

La mutualisation permet de partager l'expertise, d'optimiser les processus et de réduire les coûts, sans renoncer aux exigences de qualité ou de sécurité. Les petites collectivités peuvent ainsi accéder à des ressources comparables à celles des structures les mieux dotées grâce au rééquilibrage du rapport client-fournisseur.

Au-delà de l'achat, cette dynamique, lorsqu'elle est portée par les experts cyber des collectivités, peut également soutenir le développement de solutions open source adaptées aux besoins des territoires. C'est tout le sens de la Canut (Centrale d'achat du numérique et des télécoms), fondée en 2023 et qui étudie actuellement la création d'une fabrique de logiciels open source.

Pour Christophe Lombard,
président de la Canut :

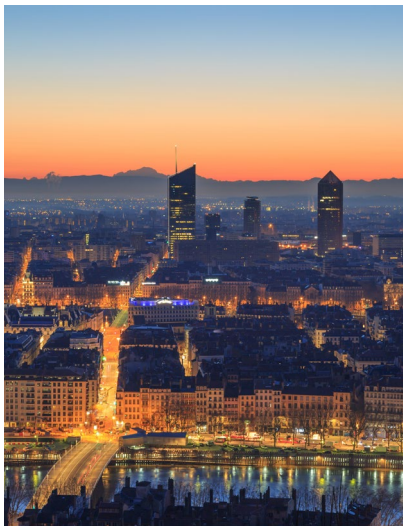
« Cette initiative vise à développer des outils souverains, transparents et adaptés aux spécificités des collectivités locales, tout en évitant la dépendance aux solutions propriétaires. Une démarche qui s'inscrit pleinement dans l'enjeu de la souveraineté numérique en offrant aux communes, quelle que soit leur taille, les moyens de maîtriser leurs infrastructures et leurs données. »



▲ SOMMAIRE

UNE STRATÉGIE NUMÉRIQUE OÙ L'IA ET LA CYBERSÉCURITÉ AVANCENT DE CONCERT

Rhône



Face à l'accélération des usages numériques et à la multiplication des cybermenaces, le département du Rhône a fait le choix d'une approche originale : développer l'intelligence artificielle, tout en renforçant simultanément la cybersécurité.

Depuis plusieurs années, le département conduit une transformation numérique ambitieuse. Cette trajectoire repose sur trois piliers : la modernisation des processus, la valorisation de la donnée et l'intégration progressive de l'intelligence artificielle dans les métiers. L'IA est envisagée comme un outil d'assistance aux agents, leur permettant de gagner du temps, d'améliorer l'analyse de l'information, de faciliter la rédaction de documents ou de soutenir la prise de décision.

Cette ouverture à l'IA s'accompagne d'un cadre de gouvernance exigeant. Le département a défini une charte d'usage reposant sur des principes de responsabilité, de transparence et de sécurité. Les agents et les managers bénéficient également d'actions de formation et d'acculturation afin de favoriser des usages maîtrisés et conformes aux valeurs du service public. L'objectif est clair : l'intelligence artificielle doit rester un outil au service de l'humain, sans jamais se substituer au discernement ni à la responsabilité des agents.

Parallèlement, la cybersécurité constitue une priorité stratégique. Anticipant les exigences de la directive européenne NIS 2, le département renforce sa cybergouvernance, ses dispositifs de surveillance, ses mécanismes de sauvegarde et ses procédures de gestion de crise. Une démarche structurée est engagée pour faire de la cybersécurité un sujet de gouvernance porté au plus haut niveau de la collectivité. La sensibilisation des agents, la gestion des risques et la résilience des infrastructures sont au cœur de cette politique.

Le département est également conscient que l'IA crée de nouveaux risques : fuites de données, manipulation des modèles, biais décisionnels ou encore dépendance technologique. C'est pourquoi sa stratégie associe systématiquement innovation, souveraineté numérique et cybersécurité en se rapprochant de Mistral AI et en intégrant désormais la résilience numérique dans ses actions. L'usage privilégié de solutions sécurisées, la protection des données publiques et la réflexion sur les infrastructures numériques souveraines témoignent de cette volonté de maîtriser l'ensemble de la chaîne de confiance numérique.

En conjuguant IA, cybersécurité, gouvernance de la donnée et montée en compétence des agents, le département du Rhône construit un modèle de transformation numérique responsable. Une ambition au service d'une administration plus efficace, plus résiliente et toujours plus attentive à la protection des citoyens comme de leurs données.

Daniel Coissard, directeur de l'innovation numérique et des systèmes d'information du département du Rhône, déclare :

« Loin d'opposer innovation et protection, ces deux dimensions sont indissociables pour garantir un service public moderne, performant et digne de confiance. »

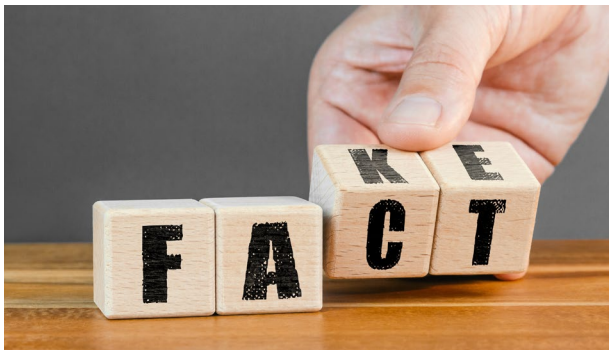
▲ SOMMAIRE

La sécurité informationnelle : un nouveau champ d'action pour les collectivités

Alors que les ingérences numériques étrangères ont été particulièrement fortes lors des élections communales de mars 2026, comme le montre le rapport de Viginum publié en juin 2026, de grandes collectivités se saisissent de cet enjeu en l'inscrivant dans une démarche élargie de confiance numérique sur leurs territoires.
La sécurité informationnelle devient ainsi progressivement une nouvelle dimension de la sécurité du numérique portée dans les territoires, en s'intégrant dans des stratégies d'éducation et de protection du citoyen. Deux axes structurent cette démarche : l'éducation à la lutte contre la désinformation et le développement de l'esprit critique.

DES INITIATIVES MULTIPLES POUR FAIRE FACE À LA DÉSINFORMATION

Des collectivités portent des actions pour renforcer la sécurité et la résilience informationnelle de leur population. Le département de la Gironde s'appuie sur son réseau de bibliothèques pour organiser, en 2026, la 6e Quinzaine du numérique sur le thème « Info ou intox : musclez votre regard sur les médias ». Les départements de Haute-Garonne et des Bouches-du-Rhône intègrent ces enjeux dans leurs politiques éducatives *via* des ateliers pour les jeunes, des actions dans les collèges et des événements autour de l'esprit critique. Autre acteur territorial qui s'intéresse désormais à cet enjeu : l'Université, comme celle de Caen, qui s'est engagée dans un programme de recherche sur la désinformation qui devrait à terme irriguer le territoire : Lucide (Lutte contre l'infodémie et développement de l'esprit critique).



LE REGARD DU CYBERCERCLE

Le champ de la sécurité du numérique ne cesse de s'enrichir, que ce soit par des critères nouveaux d'appréciation, comme l'autonomie stratégique, par des innovations structurantes, comme l'intelligence artificielle et demain le quantique, ou par des concepts concomitants, comme la sécurité informationnelle. Cette évolution enrichie nécessite des compétences de plus en plus nombreuses et larges, associant techniques et sciences humaines et sociales. L'un des enjeux pour les collectivités va être à la fois d'identifier et de qualifier ces besoins en ressources humaines, de développer l'attractivité pour attirer les profils nécessaires et d'engager des plans de formation interne adaptés, avec un défi : faire travailler ces différentes composantes ensemble et autour d'objectifs communs.

▲ SOMMAIRE

UN CADRE RÉGLEMENTAIRE RENFORCÉ QUI S'IMPOSE PROGRESSIVEMENT AUX COLLECTIVITÉS

Depuis 2010, quatre textes sont venus structurer les obligations qui s'imposent aux collectivités en matière de sécurité numérique : le RGS, l'eIDAS, le RGPD et le HDS.

Avec le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité[10], ce cadre réglementaire se renforce. En transposant les trois textes européens – REC, NIS 2 et DORA –, il élargit le champ des obligations applicables aux acteurs publics et privés, avec des exigences renforcées en matière de gestion des risques, de notification des incidents, de supervision et de sanctions.

La France a fait le choix d'intégrer certaines collectivités dans le périmètre de la transposition de NIS 2[11] : régions, départements, communes de plus de 30 000 habitants et certains groupements. Les plus petites communes ne sont pas concernées de la même manière, mais elles pourront être indirectement impactées *via* leur intercommunalité, leurs opérateurs, leurs prestataires ou les services mutualisés dont elles dépendent. Autre point à souligner, pour les collectivités, dans ce projet de loi : l'article 5 bis A, qui impose de prendre en compte, dans le plan communal de sauvegarde (PCS), « les risques informatiques ayant un impact important sur la fourniture des services dus à la population » en modifiant l'article L. 731-3 du Code de la sécurité intérieure[12].

Le RGPD demeure un socle structurant pour la confiance numérique des collectivités. Mais alors que cette réglementation fête ses dix ans, le dernier rapport annuel de la CNIL[13] marque une évolution majeure : la conformité au RGPD ne peut plus être pensée indépendamment de la cybersécurité. En inscrivant la cybersécurité des collectivités territoriales parmi ses priorités de contrôle pour 2026, la CNIL rappelle que la protection des données constitue une condition de confiance dans le service public local.

Enfin, le cadre européen pèse davantage sur les fournisseurs des collectivités. Avec le Cyber Resilience Act, qui s'impose en partie dès septembre 2026, la cybersécurité des produits comportant des éléments numériques (hors certaines solutions cloud) devient une obligation[14] pour les fabricants, importateurs et distributeurs, dès la conception et tout au long du cycle de vie. Pour les collectivités, cela nécessite de renforcer le service des achats et le service juridique par des compétences spécifiques.



10. Voir le projet de loi : www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731

11. D'après le texte du 10 septembre 2025, voté par la commission spéciale, en attente de vote en séance à l'Assemblée nationale.

12. Cet article s'inscrit dans la dynamique de la proposition de loi déposée le 16 septembre 2025 au Sénat par le sénateur Mickaël Vallet et plusieurs de ses collègues.

13. CNIL, « Protéger les données de chacun pour sécuriser l'avenir numérique de tous », rapport annuel 2025, mars 2026, accessible en ligne : www.cnil.fr/fr/rapport-annuel-2025

14. Règlement du Parlement européen concernant les exigences de cybersécurité pour les produits comportant des éléments numériques : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R2847

▲ SOMMAIRE



PHILIPPE LATOMBE

Député de la Vendée

LA RÉGLEMENTATION ET LES POLITIQUES PUBLIQUES EN SOUTIEN AUX COLLECTIVITÉS

Philippe Latombe est député de la Vendée, président de la commission spéciale de l'Assemblée nationale pour le projet de loi résilience, président de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique.

Quel constat dressez-vous de l'avancée de la cybersécurité dans les collectivités ?

Certaines collectivités ont fait de gros efforts, mais je constate aussi un manque de priorisation de la cybersécurité par un grand nombre d'entre elles malgré les menaces croissantes et des attaques marquantes. J'ai rencontré des collectivités, et non des moindres, qui n'ont jamais cartographié leur système d'information et qui ignorent le nombre exact de leurs postes de travail, tout en externalisant de plus en plus. Cette complexité non maîtrisée les rend vulnérables.

La cybermenace a beaucoup évolué ces derniers mois. On l'a vu lors des dernières élections municipales, avec des campagnes de déstabilisation qui ont ciblé les collectivités. Le contexte géopolitique actuel se traduit au niveau cyber et la période d'élections à venir va constituer un cadre amplificateur pour des cyberattaques. Par ailleurs, l'intelligence artificielle offre désormais aux attaquants des moyens plus sophistiqués, capables d'identifier seuls et d'exploiter des vulnérabilités de manière autonome, facilement accessibles. Les collectivités ne sont pas prêtes à ce changement d'échelle.

L'intégration des collectivités dans le cadre de la directive NIS 2 peut-elle être un levier suffisant ?

Le choix de la France d'intégrer les collectivités pose immédiatement une question : comment les aider à monter en compétence ? Celles qui ont déjà subi une attaque ont généralement engagé des efforts. Pour les autres, il faut faire de la pédagogie, mais une pédagogie positive : leur expliquer l'intérêt de se protéger avant de subir une cyberattaque. Pour une PME, par exemple, cela peut éviter de perdre un client, une semaine de production, voire des stocks.

La réglementation produira probablement un premier effet : des agents s'en saisiront, construiront des indicateurs et feront remonter le sujet au niveau de la gouvernance. L'inscription dans le budget sera aussi une nécessité, en réorientant les investissements en matière numérique. Mais on ne peut pas demander le même niveau d'exigence à une très petite collectivité et à une grande collectivité : la proportionnalité est indispensable.

En ce qui concerne le volet « sanctions » prévu pour les collectivités, conformément à la décision du Conseil d'État, je défends une logique liée à la remédiation. Lorsqu'une collectivité est victime d'une attaque, l'Anssi peut établir un plan pour remettre son système d'information à niveau. Si la collectivité ne respecte pas ce plan, alors une sanction devient légitime. L'objectif est de s'assurer qu'elle a tiré les enseignements de l'incident et qu'elle ne laisse pas perdurer les mêmes vulnérabilités. ●●●

▲ SOMMAIRE

Quelles sont les solutions que l'État pourrait apporter pour accompagner les collectivités ?

Je vois, tout d'abord, un levier budgétaire très concret : considérer qu'une partie des dépenses nécessaires à la montée en maturité cyber, notamment l'acquisition de licences, relève de l'investissement plutôt que du seul fonctionnement. Cela permettrait notamment de rendre ces dépenses éligibles à des mécanismes d'aide à l'investissement. Et ce changement de nature passe par la loi.

Autre levier : favoriser la mutualisation en faisant évoluer le cadre législatif ou réglementaire. Aujourd'hui, des collectivités appartenant à une même communauté de communes ou d'agglomération peuvent passer ensemble un marché pour construire un système d'information mutualisé. En revanche, il est beaucoup plus difficile, pour des collectivités éloignées géographiquement, de se répartir le développement de plusieurs modules et de lancer un appel d'offres commun et suffisamment large. Il faut trouver un cadre comme celui du secteur hospitalier : une centrale d'achat peut organiser un projet auquel plusieurs établissements contribuent, avec un orchestrateur chargé de faire fonctionner ensemble les différents modules afin que tous bénéficient de la solution. Nous devons rendre possible ce type d'organisation pour les collectivités.

Soyons conscients que le contexte budgétaire contraint de l'État ne permet plus de financer de grandes politiques d'accompagnement, comme ce fut le cas en 2021 avec « Cybersécuriser les territoires », volet inauguré dans le cadre de France Relance.

L'État propose déjà un certain nombre de dispositifs dans les territoires : représentants régionaux de l'Anssi, structures territoriales comme les campus cyber ou les CSIRT, 17Cyber… Les gendarmes ont réalisé des pré-audits, mais je ne les vois pas aller plus loin, vu les sujets qu'ils doivent aussi gérer. L'Anssi a un représentant, parfois deux, en région et n'a plus, selon moi, les moyens de développer les représentants territoriaux en volume.

L'enjeu, aujourd'hui, pour tous ces dispositifs, est donc leur coordination. Dans certains territoires, l'intelligence collective et des habitudes anciennes de coopération permettent aux acteurs de travailler ensemble dans une démarche public-privé. Dans d'autres, alors qu'elles relèvent du même représentant régional de l'Anssi, les structures dialoguent peu. L'enjeu n'est donc pas d'ajouter de nouveaux intervenants mais de rendre l'écosystème lisible et cohérent.

Comment doivent être réparties les responsabilités ?

Les collectivités attendent beaucoup de l'État, tandis que l'État attend beaucoup des collectivités. À un moment, chacun doit prendre ses responsabilités. Les élus doivent l'assumer dans leurs choix budgétaires et organisationnels. Cette responsabilité passe aussi par une analyse de risques plus large. Il ne suffit plus aujourd'hui d'identifier les failles techniques : il faut évaluer la dépendance à un seul logiciel ou à un seul fournisseur au-delà de l'approche géopolitique qui pouvait être menée. C'est ce que nous avons souligné dans le rapport de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique. En Allemagne, certains Länder ont ainsi cartographié leurs environnements, investi dans des compétences internes et engagé des bascules vers l'open source. Toutefois, la comparaison doit rester prudente, car la France se caractérise par des collectivités très nombreuses et de tailles extrêmement différentes. Enfin, la cybersécurité devrait constituer la base de la coopération numérique européenne. Allemands, Polonais, Estoniens et Français sont confrontés aux mêmes menaces. Nous devons partager nos approches et nos réponses en matière de cybersécurité, qui représente un socle commun pour le numérique. ■

▲ SOMMAIRE



GASTON GAUTRENEAU

Référent cybersécurité, ingénieur au service de l'expertise technologique de la CNIL

LA CYBERSÉCURITÉ, CONDITION DE LA CONFIANCE DANS LES TERRITOIRES

Dix ans après l'adoption du règlement général sur la protection des données (RGPD), qui s'applique dans l'UE depuis le 25 mai 2018, la sécurité des données demeure un défi permanent. Pour les collectivités territoriales, qui traitent au quotidien l'état civil, le versement de prestations sociales ou des données financières, elle constitue un facteur important de la confiance des citoyens.

Aujourd'hui, vu de la CNIL, comment se présente la cybermenace ?

En 2025, la CNIL a reçu 6 167 notifications de violations de données personnelles. Après un record atteint en 2024, ce nombre a encore augmenté de 9,5 %. Deux constats s'imposent : ces violations sont de plus en plus massives (une quarantaine de celles-ci ont concerné plus d'un million de personnes en 2025) et elles impliquent fréquemment un prestataire, un même incident chez un éditeur de solutions pouvant se répercuter chez des centaines de responsables de traitement. Ces incidents alimentent directement les plaintes reçues par la CNIL, elles aussi à un niveau record, avec 20 150 plaintes, soit une hausse de plus de 10 %.

Quels sont les principaux types d'attaques que vous constatez ?

Le principal vecteur d'attaque demeure l'hameçonnage *(phishing)* : un courriel piégé suffit souvent à ouvrir la porte du système d'information. Les attaques les plus répandues visent les messageries en ligne et reposent sur les rançongiciels. Ces derniers connaissent une évolution préoccupante : au-delà des phases de chiffrement, qui rendent les données indisponibles et font peser un risque sur leur disponibilité, on constate une tendance des attaquants à privilégier désormais l'exfiltration des données. Le risque principal porte donc désormais sur la confidentialité : les données des personnes concernées sont dérobées puis potentiellement divulguées ou revendues.

Les chiffres de la CNIL confirment la prééminence de la cybermenace : en 2025, le piratage représente la moitié des notifications de violations et la très grande majorité d'entre elles (94 %) se traduit par une perte de confidentialité, c'est-à-dire un accès ou une copie de données par un tiers. La majorité des violations a pour origine un acte externe malveillant et les rançongiciels, à eux seuls, sont à l'origine de 539 notifications.

Que révèlent les contrôles de la CNIL dans les collectivités ?

La cybersécurité constitue un axe majeur du plan stratégique 2025-2028 de la CNIL. Celui-ci se décline dans tous ses champs d'action, y compris dans son rôle de « gendarme du numérique » : la sécurité est un angle majeur dans environ un tiers de ses contrôles, près d'un quart des mesures correctrices qu'elle prononce et près d'un tiers de ses sanctions. En 2025, la CNIL a fait de la cybersécurité des collectivités une thématique de contrôle prioritaire, avec 17 missions menées auprès de 15 organismes : communes, départements, régions et sous-traitants. Parmi les manquements les plus récurrents constatés figurent des serveurs reposant sur des systèmes d'exploitation obsolètes, l'absence d'homologation au référentiel général de sécurité (RGS), le recours à des certificats non qualifiés par l'Anssi ou une multiplication de logiciels et de téléservices compliquant la gestion des habilitations et des mots de passe. ●●●

▲ SOMMAIRE

Fait notable : ces manquements ne sont pas corrélés à la taille de la collectivité. La sécurité est donc d'abord une affaire d'organisation et de méthode, avant d'être une question de moyens.

Quelles mesures prioritaires recommanderiez-vous aux collectivités ?

Les attaquants privilégient les intrusions les plus faciles à mener. Quelques mesures, ni coûteuses ni techniquement complexes, réduisent fortement le risque. À lui seul, le déploiement de l'authentification multifacteur est décisif : près de 80 % des violations de grande ampleur constatées par la CNIL en 2024 ont été permises par l'usurpation d'un compte protégé par un simple mot de passe. Face aux attaques par la messagerie, la CNIL recommande de sensibiliser régulièrement le personnel, de sécuriser les postes de travail (antivirus, EDR, etc.), de sécuriser les serveurs de messagerie (mises à jour), d'instaurer une procédure permettant à chaque agent de signaler un courriel identifié comme malveillant et, enfin, de déployer une authentification multifacteur pour l'accès à la messagerie et les accès à distance aux systèmes d'information.

Pour limiter l'impact d'une perte ou d'un vol de supports, la CNIL préconise également de tenir à jour la gestion et la cartographie du parc informatique, d'imposer une authentification robuste, de chiffrer les données stockées sur les supports (disques durs, clés USB, etc.) et, là encore, de sensibiliser régulièrement les équipes.

Ces bonnes pratiques doivent s'inscrire dans un socle de sécurité plus large : politique de mots de passe robustes, authentification multifacteur sur les comptes à privilèges et les messageries, mises à jour automatiques, sauvegardes selon la règle du « 3-2-1 » (trois copies, deux supports, une hors ligne), installation d'applications depuis les seuls magasins officiels et séparation des usages personnels et professionnels.

En cas d'attaque, la conduite à tenir est claire : ne pas payer de rançon, isoler la machine, préserver les preuves et déclarer l'attaque aux autorités compétentes, dont la CNIL.

En quoi les recommandations du RGPD constituent-elles un socle de confiance numérique pour les collectivités ?

L'une des meilleures protections reste de ne pas détenir des données inutiles ou obsolètes : par la minimisation et la limitation des durées de conservation, le RGPD réduit mécaniquement la surface d'exposition – les données que l'on ne possède pas ou plus ne peuvent être volées.

Lorsque survient une violation susceptible d'engendrer un risque pour les droits et libertés, elle doit être notifiée à la CNIL dans les soixante-douze heures. L'enjeu, pour les habitants, est concret : derrière chaque notification, ce sont des usagers dont l'état civil, la situation sociale ou financière, peuvent être divulgués, ce qui les expose à des messages frauduleux, des usurpations d'identité, voire des vols, du harcèlement, etc. Le RGPD impose, en complément de la notification à la CNIL, d'informer directement les personnes concernées, lorsque le risque est élevé, afin qu'elles puissent prendre des mesures pour se protéger.

La CNIL poursuit son engagement aux côtés des collectivités : accompagnement, outils pratiques et contrôles. Après avoir fortement incité, au printemps 2025, les organismes gérant de grandes bases de données à généraliser l'authentification multifacteur pour les accès à distance, elle a mené une campagne de contrôles tout au long de 2026. Dix ans après l'adoption du RGPD, la sécurité des données n'est pas une contrainte supplémentaire : elle est le socle d'un numérique de confiance, éthique et souverain. ■

▲ SOMMAIRE

CHIFFRES-CLÉS : LES VIOLATIONS DE DONNÉES EN 2025 (SOURCE : CNIL)

6 167

notifications de violations de données reçues par la CNIL, soit près de 16 par jour

19 %

des notifications concernent l'administration publique, ce qui en fait le secteur le plus touché

50 %

du total des notifications relève du piratage informatique

94 %

des notifications portent sur une perte de confidentialité

539

violations résultent d'une attaque par rançongiciel (9 % du total)

23

sanctions prononcées par la CNIL comportaient au moins un manquement à la sécurité des données

LE REGARD DU CYBERCERCLE

Au-delà des obligations juridiques qui s'accentuent, c'est la philosophie même de la cybersécurité publique locale qui évolue progressivement vers une logique de résilience : continuité d'activité, reprise des services, gestion de crise, maîtrise des dépendances et capacité à maintenir les missions prioritaires. Pour les collectivités, cela implique de relier plus étroitement cybersécurité, PCA-PRA, cartographie des services essentiels, pilotage des prestataires et gouvernance de crise. Autre constat : la protection des données personnelles n'est plus seulement un sujet de conformité juridique, de transparence ou de droits des personnes ; elle repose désormais directement sur la capacité des organisations à sécuriser leurs systèmes d'information.

Cette double évolution permet de changer le regard que les collectivités peuvent avoir sur la cybersécurité en l'inscrivant dans des concepts et des plans d'action qui leur sont plus familiers. Elle les encourage à structurer leur gouvernance, à objectiver les risques, à sécuriser leurs achats numériques et à inscrire la cybersécurité dans une trajectoire durable de confiance, de souveraineté et de résilience territoriale.

Demeure néanmoins posé l'enjeu de leur accompagnement dans cette dynamique de changement.

CYBER CERCLE

▲ SOMMAIRE

CONCLUSION

Cette cinquième « Note de conjoncture » montre combien la situation a changé en quelques années.

La donnée est désormais présente dans toutes les catégories de collectivités et dans un nombre croissant de politiques publiques. Sa progression dans les petites communes est l'un des enseignements marquants de cette édition. Les usages de la donnée ne sont plus réservés aux territoires les mieux dotés – et c'est une bonne nouvelle !

L'intelligence artificielle continue, elle aussi, de progresser en 2026, à un rythme toutefois moins rapide que lors des deux années précédentes. Les expérimentations se poursuivent et les questions du déploiement se posent désormais plus directement. Choix des outils, qualité des données, compétences, cadre juridique, moyens financiers : les préoccupations deviennent très concrètes.

Une méthode semble progressivement s'esquisser, avec la mise en place de chartes, de formations, de groupes de travail ou encore de feuilles de route.

La mesure et la maîtrise des dépendances technologiques deviennent plus présentes pour les collectivités. Il en va de même pour la cybersécurité, alors qu'elles restent fortement exposées aux cyberattaques. Maîtrise, dépendances et, plus généralement, souveraineté numérique : ces sujets prennent désormais une place croissante dans les choix numériques des acteurs publics locaux.

2027 sera à son tour une année particulière. Les scrutins nationaux se dérouleront dans un contexte géopolitique incertain, où les questions de souveraineté et de sécurité numériques resteront sans doute centrales.

Dans les territoires, nous continuerons à observer les choix des nouvelles équipes municipales et intercommunales, la diffusion des usages et les effets des projets en cours de déploiement.

Rendez-vous dans un an pour la prochaine « Note de conjoncture » !



▲ SOMMAIRE

POUR ALLER PLUS LOIN

DATA ET INTELLIGENCE ARTIFICIELLE

Les publications de l'Observatoire Data Publica et de ses partenaires

L'ensemble des travaux de l'Observatoire Data Publica : cahiers de recherche, études et sondages
https://observatoire.data-publica.eu/les-publications/

Municipales 2026 : les propositions en lien avec la data et l'IA
https://observatoire.data-publica.eu/wp-content/uploads/2026/04/ObservatoireDataPublica_EtudeMunicipales2026.pdf

---

Municipales 2026 : les élus en charge du numérique
https://observatoire.data-publica.eu/wp-content/uploads/2026/06/Etudes_municipales_2026_elus_Vdef.pdf

---

Le poster des chartes IA des territoires (2026)
https://api.groupe-keran.com/api/upload/2ba168b348bc051fb02c39e3aa84171d.pdf

---

« Anticiper l'impact de l'IA sur les métiers et outiller le dialogue social » (2026)
https://numerique360.banquedesterritoires.fr/gouvernance-socles-technologiques/connaissances/anticiper-limpact-de-lia-sur-les-metiers-et-outiller-le-dialogue-social/

Le clausier Data & IA (2026)
https://www.interconnectes.com/documents/b1d20d8b-ea3e-f111-8ef3-000d3a4af15b/clausier-data-et-ia-2026

▲ SOMMAIRE

Des publications et des rapports officiels sur la gestion des données et l'IA

Le programme Territoires d'IA de la Banque des Territoires

www.banquedesterritoires.fr/territoires-ia

IGF, « Le déploiement de l'IA dans les administrations publiques » (juillet 2026)

https://www.igf.finances.gouv.fr/files/live/sites/igf/files/contributed/Rapports%20de%20mission/2025/2025-E-081%20D%c3%a9ploiement%20IA.pdf

---

Politique nationale pour les services publics « Notre IA » (2026)

https://www.numerique.gouv.fr/sinformer/espace-presse/intelligence-artificielle-ia-utile-humaine-souveraine-services-publics/

SNDGCT, « Note de réflexion sur l'IA » (2026)

https://www.sndgct.fr/articles/195207-resultats-de-l-etude-sur-le-deploiement-de-lia-dans-les-collectivites

---

Observatoire de la MNT, « Les managers territoriaux et l'IA » (2026)

https://www.mnt.fr/articles/observatoire-mnt-les-managers-territoriaux-et-ia

---

LaborIA, « Étude des impacts de l'IA sur le travail » (2024)

https://www.laboria.ai/wp-content/uploads/2024/05/Synthese_generale_LaborIA_Explorer.pdf

Des projets conduits par les territoires

« L'IA au service de l'analyse des rapports de délégataires : l'expérience de la ville de Cannes »

https://numerique360.banquedesterritoires.fr/gouvernance-socles-technologiques/retours-experiences/lia-au-service-de-lanalyse-des-rapports-de-delegataires-lexperience-de-la-ville-de-cannes-06/

« Lyon adopte une charte d'usage de l'IA issue d'un travail de concertation avec les agents »

https://numerique360.banquedesterritoires.fr/gouvernance-socles-technologiques/retours-experiences/lyon-69-adopte-une-charte-dusage-de-lia-issue-dun-travail-de-concertation-avec-les-agents/

« IA au département du Loiret : 5 leçons d'une expérimentation qui change la donne »

https://www.ia4business.info/ia-au-departement-du-loiret-5-lecons-dune-experimentation-qui-change-la-donne-2025-2026

▲ SOMMAIRE

CYBERSÉCURITÉ

Comprendre la cybermenace et ses évolutions



Anssi, « Panorama de la cybermenace 2025 » (mars 2026)
https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2025/



ComCyber-MI, « Rapport annuel sur la cybercriminalité 2026 » (avril 2026)
https://www.interieur.gouv.fr/documentation/rapports/rapport-annuel-sur-cybercriminalite-2026.html

---



Cybermalveillance.gouv.fr, « Rapport d'activité 2025 » (mars 2026)
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025



CNIL, « Protéger les données de chacun pour sécuriser l'avenir numérique de tous », rapport annuel 2025 (mai 2026)
https://www.cnil.fr/fr/rapport-annuel-2025



Viginum, SGDSN
« Rapport sur la protection du débat public contre les ingérences numériques étrangères durant les élections municipales des 15 et 22 mars 2026 » (juin 2026)
https://www.sgdsn.gouv.fr/viginum/publications/protection-du-debat-public-contre-les-ingerences-numeriques-etrangeres-durant

Renforcer la cyberrésilience des territoires



Lionel Pérès, *Cyberattaque : assurer la continuité des services publics locaux. Méthodologie, modèles de documents et retours d'expérience,* Territorial, 2025
https://www.lgdj.fr/cyberattaque-assurer-la-continuite-des-services-publics-locaux-9782818623633.html

---



Anssi, « Kit d'exercice de gestion de crise d'origine cyber pour les collectivités territoriales »
https://cyber.gouv.fr/securisation/gestion-de-crise/entrainement-crise/kit-exercice-collectivites-territoriales/



ComCyber-MI, AMF, « CapCyber : crises & collectivités », formation en ligne inédite pour préparer les élus et leurs agents aux crises cyber
https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2026/cybersecurite-une-formation-en-ligne-inedite-pour-preparer-les-elus-et-leurs-agents-aux-crises-cyber

---



Anssi, MesServicesCyber
https://messervices.cyber.gouv.fr/

▲ SOMMAIRE

Cybermalveillance, AMF
« Méthode clé en main pour sensibiliser les agents des collectivités » (2025)
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-methode-cle-sensibiliser-agents-collectivites

---

Anssi, « CyberEnjeux. Former à la cybersécurité par le jeu »
https://messervices.cyber.gouv.fr/ressources/cyber-enjeux.html

---

Cybermalveillance, « Le numérique, pas de panique ! » un livret pour les 9-12 ans
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/livret-numerique-pas-de-panique

Renforcer la sécurité informationnelle

Guillaume Chillet, « Souveraineté cognitive : le maillon humain de la confiance numérique », parole d'expert du CyberCercle (2026)
https://cybercercle.com/paroledexpert-guillaume-chillet_13022026/

Guillaume Chillet, *Petit Traité de souveraineté cognitive*, autoédition, 2026
https://www.amazon.fr/trait%C3%A9-souverainet%C3%A9-cognitive-Guillaume-Chillet/dp/B0GKY4W6MK

Viginum, SGDSN, « Protéger le débat public numérique en contexte électoral » (2025)
https://www.sgdsn.gouv.fr/files/files/Publications/Guide_sensibilisation_elections_municipales_vdef.pdf

---

Viginum, SGDSN
« Kits de sensibilisation sur les ingérences numériques étrangères »
pour jeunes publics et adultes
https://www.sgdsn.gouv.fr/viginum/publications/kits-de-sensibilisation-sur-les-ingerences-numeriques-etrangeres

Éclairer la commande publique sur le numérique

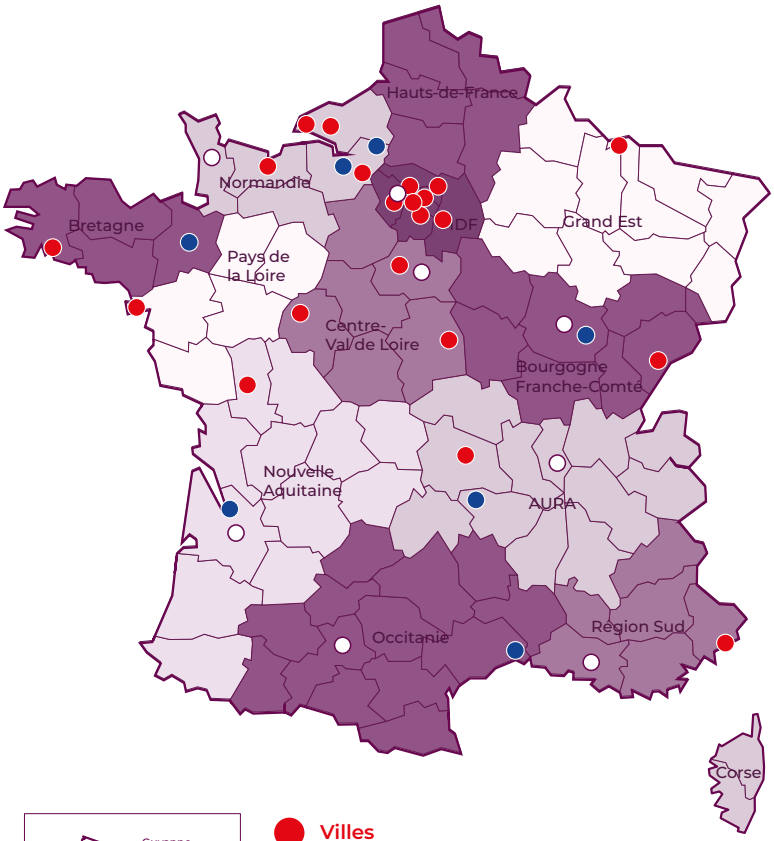
Assemblée nationale, « Rapport sur la proposition de loi relative à la sécurisation des marchés publics numériques » (février 2026)
https://www.assemblee-nationale.fr/dyn/17/rapports/cion_lois/l17b2522_rapport-fond

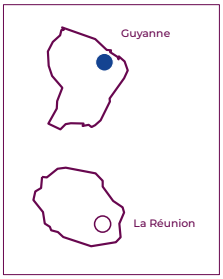
---

Assemblée nationale, « Les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France », rapport de la commission d'enquête (juillet 2026)
https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete

▲ SOMMAIRE

LES TERRITOIRES CITÉS





- Villes
- Intercommunalités
- Départements
- Régions

- BORDEAUX MÉTROPOLE : P. 9
- BOURGOGNE-FRANCHE-COMTÉ : P. 63
- BOUCHES-DU-RHÔNE : P. 67
- CAEN : P. 67
- CANNES : P. 36
- CAUX SEINE AGGLO : P. 43
- CLERMONT-FERRAND : P. 43
- CÔTE-D'OR : P. 19
- DIJON MÉTROPOLE : P. 43
- ÉLANCOURT : P. 16
- GIRONDE : P. 67
- GRAND EST : P. 7, 9, 43
- GRAND PARIS SUD : P. 43
- GRAND-ORLY SEINE BIÈVRE : P. 17
- GUYANE : P. 57
- HAUTS-DE-FRANCE : P. 43
- HAUTS-DE-SEINE : P. 53
- HAUTE-GARONNE : P. 67
- HETTANGE-GRANDE : P. 55
- ÎLE-DE-FRANCE : P. 7
- LA RÉUNION : P. 7
- LOIRET : P. 47
- MANCHE : P. 58
- MONTPELLIER MÉDITERRANÉE MÉTROPOLE : P. 25, 26
- NANTERRE : P. 18
- OCCITANIE : P. 7, 25
- ORLÉANS : P. 43
- PARIS-SACLAY : P. 43
- PAYS DE LA LOIRE : P. 7, 43
- PONTARLIER : P. 63
- QUIMPER : P. 24
- RENNES MÉTROPOLE : P. 41
- RHÔNE : P. 66
- ROUMOIS SEINE : P. 56
- SAINT-CLOUD : P. 35
- SAINT-NAZAIRE : P. 43
- VAISON-LA-ROMAINE : P. 59

▲ SOMMAIRE

Retrouvez vos contacts des relations institutionnelles de La Poste en région

www.lapostegroupe.com/fr/contacts-presse-et-institutionnels-du-groupe-en-region

Retrouvez vos contacts de la Banque des Territoires en région

www.banquedesterritoires.fr/directions-regionales

La Poste - SA au capital de 6 447 643 996 euros - 356 000 000 RCS PARIS - Siège social : 9 RUE DU COLONEL PIERRE AVIA - 75015 PARIS.
Production Direction de la communication Caisse des Dépôts - Réalisation : PRC NA-AURA - Crédits photo : © stock.adobe.com. Ce document est imprimé sur du papier issu de sources responsables (FSC). Octobre 2026.

LA POSTE GROUPE

BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE