gigalis
La confiance augmentée

LIVRE BLANC

2026 : LES 5 MENACES NUMÉRIQUES POUR LES ACTEURS PUBLICS

Février 2026

DGS :

ADOPTER UNE APPROCHE SOUVERAINE POUR ASSURER LA CONTINUITÉ DES SERVICES PUBLICS

Édito

Laurent Dejoie

Président de Gigalis,
Vice-président du Conseil régional des Pays de la Loire
Maire honoraire de Vertou

En 2026, le numérique devient un enjeu politique majeur. Un seuil critique a été franchi en 2025 : l'adoption massive de l'IA générative, l'explosion des cyberattaques visant le service public et enfin le bouleversement de l'ordre géopolitique mondial ont placé le numérique au cœur des priorités de l'État.

Dans ce contexte de menaces croissantes, les collectivités et les établissements publics font face à une double exigence : accélérer leur transformation digitale tout en renforçant leur sécurité.

Le problème n'est pas l'absence de solutions, mais leur inadéquation. Trop souvent, l'offre privée ignore les contraintes du terrain et s'appuie sur des technologies extra-européennes, en décalage avec les principes de souveraineté.

Or, l'enjeu de souveraineté numérique constitue désormais pour les acteurs publics une préoccupation majeure. En première ligne pour répondre à ces enjeux, les DGS sont aujourd'hui à la recherche de partenaires de confiance, ancrés sur le territoire, capables de combiner performance, sécurité et intérêt général.

Prévenir les risques par une approche défensive ne suffit plus ; il nous faut désormais adopter une démarche d'autonomie afin de conquérir notre indépendance numérique. Seule une approche souveraine permettra de garantir la confidentialité de nos données et la robustesse de nos systèmes. L'enjeu est de taille : il s'agit ni plus ni moins d'assurer la continuité de notre service public.

Les défis numériques qui attendent les acteurs publics en 2026 sont nombreux et témoignent d'une vulnérabilité croissante. Nous en détaillons ici cinq : l'envolée du coût des licences propriétaires, l'intensification des cybermenaces ciblant l'action publique, l'ingérence juridique étrangère sur nos données, l'opacité décisionnelle des intelligences artificielles et enfin, le risque de rupture de nos services essentiels face aux tensions géopolitiques mondiales.

Face à ces menaces, il faut à tout prix anticiper. Or, le dernier baromètre Collectivités & Numérique publié par la DINUM montre des structures insuffisamment préparées : 76% des collectivités interrogées ne disposent ni de PCA (Plan de Continuité d'Activité) ni de PRA (Plan de Reprise d'Activité).

Chez Gigalis, nous croyons à la force de la mutualisation ; nous pensons qu'en mettant en commun nos expertises et nos ressources, nous pouvons bâtir des pôles de souveraineté numérique territoriale.

Face à l'hégémonie des acteurs extra-européens, il est temps d'incarner une alternative et de reprendre en main notre destin numérique.

SOMMAIRE

MENACE #1 :

LE PIÈGE BUDGÉTAIRE DES LICENCES NUMÉRIQUES

LE CONSTAT

Une étude récente de l'Open Cloud Coalition estime que dans le secteur public français, pour les outils bureautiques, Microsoft représente 86 à 90% de parts de marché, suivi de près par Google (9 à 13% selon le scénario de calcul retenu)[1]. Alors que l'Union européenne souhaite aller vers davantage de souveraineté numérique, le secteur public européen est largement dépendant des géants américains. Qu'il s'agisse de suites bureautiques (Microsoft Office, Google Workspace…), de logiciels de gestion administrative (ADP, Workday), d'outils de communication (GoogleMeet, Teams, Zoom…) ou encore d'outils créatifs (Adobe Creative Cloud), l'emprise des hyperscalers est bien réelle.

Or, l'illusion de la gratuité ou les tarifs d'appel des premières années laissent place à une réalité plus brutale : pour les acteurs publics, l'augmentation progressive du prix des licences constitue un piège budgétaire. Microsoft a introduit en 2025 des changements significatifs dans sa structure tarifaire, augmentant les dépenses numériques des organisations et des structures publiques.

L'entreprise a d'ores et déjà annoncé une montée en gamme de son offre avec une nouvelle augmentation des prix de Microsoft 365 au 1er juillet 2026. La hausse pourrait atteindre +33% selon la formule choisie, une majoration inédite.

Ils ont sauté le pas en 2025 : la ville de Lyon et la Métropole du Grand Lyon, les lycées de la Région Île-de-France ou encore l'École Polytechnique ont choisi de renoncer à Microsoft pour basculer vers des solutions alternatives (logiciel libre et/ou français).

Au-delà de ces précurseurs, la tendance s'amplifie considérablement en Europe. En Allemagne, le Land de Schleswig-Holstein a annoncé en 2025 qu'après un investissement initial de 9 millions d'euros pour migrer son administration vers des solutions open source, il économisera désormais 15 millions d'euros par an en frais de licences Microsoft. Cette décision fait jurisprudence outre-Rhin et inspire d'autres Länder.

De plus, selon une enquête de décembre 2025 de l'Open Cloud Coalition, les remises sur volume pour les contrats Enterprise Agreements et MSPA (Microsoft Products and Services Agreement) ont été supprimées progressivement en novembre 2025, accentuant encore la pression budgétaire. Cette stratégie de resserrement tarifaire s'inscrit dans un contexte où Microsoft investit plus de 90 milliards de dollars par an dans ses infrastructures d'IA, et transfère désormais ce coût directement sur ses clients.

Jean-Pierre SABIO, Directeur Général de Gigalis : *« Nous assistons à un transfert massif de richesse publique vers les géants américains. En 2026, la facture Microsoft pour les acteurs publics français dépassera les 800 millions d'euros annuels, une somme qui pourrait financer des milliers de postes dans nos DSI territoriales ou l'essor d'une filière numérique européenne. L'augmentation de 33% annoncée pour juillet 2026 n'est pas une simple indexation inflationniste, c'est un choix stratégique des hyperscalers pour rentabiliser ses investissements colossaux en IA. Les acteurs publics paient aujourd'hui pour des fonctionnalités Copilot dont la valeur ajoutée réelle pour les métiers territoriaux reste encore à démontrer. La question n'est plus seulement budgétaire : c'est une question de souveraineté et de maîtrise de notre destin numérique. »*

POURQUOI C'EST POLITIQUE ?

Car l'argent public s'envole vers les hyperscalers américains au lieu de rester sur le territoire pour bénéficier à l'ensemble de nos infrastructures publiques (écoles, hôpitaux, administrations...).

IMPACTS CONCRETS

- Fragilisation du budget : par l'augmentation continue de la dépense numérique, à chaque renouvellement de licence
- Utilisation limitée des outils : en cas de limite budgétaire atteinte, il faudra par exemple réduire le nombre de licences achetées ou le nombre de services accessibles

SOLUTIONS

- **Analyser et cartographier les usages :** identifier quels services des hyperscalers sont indispensables et lesquels peuvent être remplacés
- **Mettre en place des stratégies hybrides :** migrer vers des outils open source ou souverains pour les applications les plus critiques
- **Mutualiser pour optimiser les coûts :** passer d'une logique de consommation individuelle à une commande publique mutualisée permet de bénéficier de tarifs négociés.

DÉCOUVREZ NOTRE CENTRALE D'ACHATS NUMÉRIQUE

Conçue pour simplifier l'acquisition de solutions technologiques aux entités publiques, elle propose une gamme complète de licences, logiciels et infrastructures. Tous ont été sélectionnés pour leur capacité à s'intégrer durablement au sein de l'écosystème territorial, selon des critères de qualité, de conformité et d'interopérabilité.

MENACE #2 :

DES CYBERATTAQUES DE PLUS EN PLUS NOMBREUSES ET SOPHISTIQUÉES

LE CONSTAT

En 2025, la France a franchi un seuil critique en matière de cybersécurité, avec une multiplication des attaques. Entreprises, organisations publiques, particuliers : personne n'a été épargné. Les nouvelles technologies (IA, cryptomonnaies) mènent à une évolution rapide des modes opératoires, tandis que le secteur de la cybercriminalité s'industrialise, avec des acteurs de plus en plus performants, interconnectés entre eux. La menace n'est désormais plus marginale mais quotidienne.

Une part significative des attaques est liée aux sous-traitants. Les prestataires, éditeurs de logiciels ou partenaires techniques deviennent une porte d'accès privilégiée pour accéder à des organisations aux protocoles de sécurité solides. La généralisation du télétravail et les accès distants mal sécurisés constituent également un facteur aggravant.

Au niveau des modes opératoires, le phishing et les logiciels malveillants (malwares) restent des outils privilégiés. Les rançongiciels (ransomwares) sont en léger recul : les organisations ont pris l'habitude de sauvegarder régulièrement leurs données, rendant l'attaque moins critique. Enfin, l'IA générative permet de mettre en place des attaques de plus en plus sophistiquées : deepfakes vocaux ou vidéo, arnaques personnalisées, messages ultra-ciblés.

Les collectivités territoriales, les organismes publics et les administrations sont de plus en plus visés. France Travail, La Poste, le ministère de l'Intérieur, le département des Hauts-de-Seine...tous ont subi des cyberattaques massives en 2025. Une vague coordonnée d'attaques DDoS a également paralysé les sites de plus de 20 grandes mairies parmi lesquelles Lyon et Marseille. L'Anssi et le ministère de l'Intérieur estiment que l'administration publique est désormais le secteur le plus ciblé en Europe. Les établissements hospitaliers, détenteurs de données de santé, constituent également des cibles de choix. Les petites et moyennes communes, quant à elles, sont particulièrement vulnérables : leur maturité en matière de cybersécurité reste très variable. Dommage lorsque l'on sait que les coûts de sécurisation du système informatique sont inférieurs au coût moyen d'une cyberattaque, ainsi que le rappelle la Cour dans un rapport de juin 2025[1].

Le rapport de la Cour révèle des chiffres alarmants. Le coût direct moyen d'une cyberattaque pour une collectivité territoriale s'élève à 960 000 euros (Aix-Marseille-Provence, mars 2020) pouvant atteindre 1,5 million d'euros (ville de Bondy, novembre 2020). À l'échelle nationale, le coût des cyberattaques réussies pour les organisations privées et publiques françaises est estimé à 2 milliards d'euros en 2022, un chiffre qui ne cesse de croître. En 2023, selon la plateforme Cybermalveillance.gouv.fr, les collectivités et administrations ont vu les attaques par hameçonnage augmenter de 26%, le piratage de comptes de 22% et les fraudes de 36%. L'ANSSI a traité 4 386 événements de sécurité en 2024, soit une hausse de 15% par rapport à 2023. La multiplication des attaques s'accompagne d'une industrialisation du secteur cybercriminel : des plateformes de Ransomware-as-a-Service permettent désormais à des acteurs peu qualifiés de lancer des attaques sophistiquées pour quelques centaines d'euros. En parallèle, l'IA générative démocratise la création de deepfakes vocaux et vidéo, rendant les arnaques au faux président ou faux technicien informatique quasi indétectables.

Dans ce contexte de menace croissante, la fin de la période de tolérance et d'apprentissage pour la directive européenne NIS 2 doit être perçue comme une opportunité de résilience davantage que comme une contrainte. Les administrations centrales et locales, les établissements de santé publics et les collectivités territoriales concernées devront démontrer des exigences de cybersécurité renforcées, notifier tout incident à l'Anssi et effectuer des audits réguliers.

Filipe Bica, Directeur cybersécurité, cloud et IA chez Gigalis : *"En 2026, la menace change de nature : l'objectif n'est plus seulement le vol de données, mais la paralysie de l'action publique. Nous sommes passés du piratage opportuniste au sabotage ciblé d'infrastructures critiques. Dans ce contexte sensible, la directive NIS 2 acte un changement de paradigme : la sécurité numérique sort du bureau du DSI pour entrer dans celui de l'élu. Il engage sa responsabilité pénale sur le sujet et devient personnellement garant de la défense numérique de son territoire."*

Cette analyse trouve un écho direct dans la Stratégie nationale de cybersécurité 2026-2030 dévoilée le 29 janvier 2026 par Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique. La stratégie acte un changement de doctrine : fini l'illusion du « zéro incident », place à la préparation systématique aux crises. La ministre a d'ailleurs lancé une alerte spécifique lors de la présentation à Bordeaux : « Les collectivités sont une cible claire pour les municipales 2026 ». Cette déclaration n'est pas anodine : elle confirme que les acteurs malveillants cibleront les infrastructures locales dans un objectif de déstabilisation politique. Face à cette menace, le gouvernement prévoit le lancement d'une marque nationale de prévention, sur le modèle des campagnes de sécurité routière, ainsi qu'un label de confiance cybersécurité destiné aux PME. Surtout, la stratégie positionne la résilience comme second pilier structurant : préparer la Nation aux crises dues aux cyberattaques, rehausser le niveau global de cyber-protection et faciliter les parcours vers une meilleure cybersécurité. Les exercices de crise, inspirés de Rempar 2025, sont érigés en levier central. Mais une interrogation demeure : comment accompagner les petites communes, les PME et les associations sans transformer ces exigences de préparation en charge inabsorbable ? La stratégie affirme l'inclusion de tous, mais laisse ouverte la question du niveau d'exigence différencié et de l'accompagnement financier pour les acteurs les moins outillés.

POURQUOI C'EST POLITIQUE ?

Car dans un contexte géopolitique de plus en plus préoccupant, l'objectif n'est plus le vol de données à des fins commerciales, mais la paralysie de l'action publique et la déstabilisation de l'État français. La cybersécurité s'affirme de plus en plus comme socle essentiel de la continuité républicaine.

IMPACTS CONCRETS

- **Fuite des données sensibles et/ou menaces de divulgation**
- **Dégradation du service public :** messagerie ou logiciel RH inaccessibles
- **Interruption du service public :** prestations sociales suspendues, état civil inaccessible, écoles fermées, chaîne de secours entravée…

SOLUTIONS

- **Sensibiliser et former en continu :** la plupart des attaques commencent par une vulnérabilité humaine. Phishing, ransomware… il suffit que quelqu'un saisisse ses identifiants sur une page de connexion usurpée pour que tout le système soit mis en danger. L'usage individuel d'une IA générative non encadrée par la DSI (shadow AI) constitue également un facteur de risque majeur.
- **Sauvegarder régulièrement les données :** en cas de ransomware, la restauration de données à partir d'une sauvegarde fiable permet de reprendre l'activité rapidement. La demande de rançon devient inefficace.
- **Adopter une stratégie de cybersécurité proactive plutôt que réactive :** filtrage des emails et de la navigation, mise à jour automatisée des systèmes… Face à la multiplication des attaques, le modèle Zero Trust gagne du terrain. Le principe ? Ne jamais accorder de confiance implicite à une machine ou à un utilisateur. Dans les faits, l'approche se traduit par une vérification permanente, une segmentation des systèmes d'information, un contrôle affiné des privilèges selon les profils.
- **Élaborer un plan de continuité d'activité (PCA) ou plan de reprise d'activité (PRA) :** ce document, qui permet à une organisation de maintenir ses activités essentielles pendant une interruption de service, est hautement stratégique. Il constitue une brique essentielle de la résilience numérique du service public.
- **Développer des logiques de communauté pour unir nos forces :** dans un contexte de menace systémique, aucun acteur public ne peut faire face seul. L'heure est à la mutualisation et à la coopération. Des logiques de communauté émergent pour partager l'information, mutualiser les capacités de défense et de prévention contre les incidents. C'est le principe des CSIRT territoriaux (Computer Security Incident Response Team), qui offrent aux entreprises et acteurs publics de leur région une assistance en cas de cyberattaque.

REJOIGNEZ NOTRE PROGRAMME DE CYBER RÉSILIENCE TERRITORIALE

L'isolement des acteurs publics accroît leur vulnérabilité. Pour y remédier, ce programme fédère les acteurs autour d'un bouclier commun. Il offre l'accès à un écosystème de défense complet, structuré pour assurer une protection robuste et pérenne des systèmes et infrastructures et permettre ainsi la continuité des services essentiels.

MENACE #3 :

RISQUES D'INGÉRENCE EXTRA-EUROPÉENNE

LE CONSTAT

Plusieurs lois extra-européennes rendent nos données vulnérables et exploitables. Le principe de l'extraterritorialité s'applique ainsi à travers le Cloud Act, qui permet aux autorités américaines d'exiger des données détenues par toute entreprise américaine, même si ses serveurs sont situés hors des États-Unis. Les principaux fournisseurs cloud (Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud) sont ainsi soumis à ce régime. Le géant chinois Alibaba a par ailleurs annoncé l'ouverture de son premier data center en France en 2026. D'autres lois de localisation en Chine, en Russie et bientôt en Inde exposent également les acteurs européens dès lors que leurs partenaires ou fournisseurs utilisent des infrastructures hébergées dans ces pays. Le risque d'ingérence est réel.

En juin 2025, lors d'une audition historique devant la commission d'enquête du Sénat, Microsoft France a explicitement reconnu que, face à une injonction de la justice américaine, l'entreprise serait contrainte de transmettre les données de ses clients français, même lorsque celles-ci sont hébergées en Europe. « Si nous y sommes contraints, nous remettons les données », a admis Anton Carniaux, directeur juridique de Microsoft France. Ce constat cristallise une réalité inquiétante : la souveraineté numérique française reste largement théorique dès lors que nos infrastructures reposent sur des acteurs extra-européens. Or, selon l'Open Cloud Coalition, le marché public français des outils bureautiques est aujourd'hui très largement dominé par Microsoft, plaçant les administrations dans une situation de dépendance structurelle.Or, selon une étude de l'Open Cloud Coalition, Microsoft détient 86 à 90% du marché public français en matière d'outils bureautiques. En clair : l'essentiel de nos données publiques se trouve potentiellement accessible aux autorités américaines, et ce malgré le RGPD.

Filipe Bica, Directeur cybersécurité, cloud et IA chez Gigalis : *« Le Cloud Act et les lois chinoises de cybersécurité exposent les données publiques à une ingérence juridique directe. L'audition de Microsoft devant le Sénat en juin 2025 a définitivement levé le voile : confier nos données à des acteurs soumis à des législations extraterritoriales, c'est renoncer au contrôle sur nos informations les plus sensibles. Les collectivités ne peuvent plus ignorer cette réalité. Dans un contexte géopolitique instable, seule une relocalisation des données sur des infrastructures souveraines garantit une immunité juridique totale. »*

POURQUOI C'EST POLITIQUE ?

Car ce risque touche à la souveraineté économique, à la sécurité nationale et à la compétitivité économique. Les données de l'État (état civil, urbanisme, santé) constituent une denrée particulièrement sensible.

IMPACTS CONCRETS

- **Fuite des données sensibles :** les données des administrations pourraient alors être exploitées à des fins politiques, économiques ou malveillantes.
- **Insécurité juridique :** le Cloud Act entre en conflit direct avec le RGPD, créant un dilemme juridique qui place la collectivité dans une situation d'insécurité permanente

SOLUTION

- **Évaluer systématiquement les fournisseurs :** en vérifiant la nationalité juridique de l'entreprise et les clauses de protection des données présentes dans le contrat.
- **Relocaliser les données :** en choisissant des services cloud utilisant un data center situé dans l'UE. Le plus haut standard en matière de sécurité reste la certification SecNumCloud, le label de qualification de l'Anssi.
- **Opter pour un chiffrement de bout en bout :** crypter les données avant de les envoyer à un tiers permet de les rendre illisibles et dès lors inutilisables.

DÉCOUVREZ LE DATACENTER DE PROXIMITÉ OPÉRÉ PAR GIGALIS

Situé en Vendée, ce datacenter garantit aux acteurs publics une sanctuarisation totale de leurs données. Il offre également un hébergement cloud souverain : distribué et opéré par un opérateur public, sous juridiction exclusive française, il assure une immunité juridique totale face aux menaces d'ingérence extra-européennes.

MENACE #4 :

DES MODÈLES D'IA OPAQUES

LE CONSTAT

2025 a été l'année de l'adoption massive des IA génératives. 45% des Français seraient désormais des utilisateurs actifs[1]. Plébiscité par 72% des utilisateurs, ChatGPT (OpenAI) arrive largement en tête des outils, devant Gemini (Google) puis Copilot (Microsoft).

Or, ces IA reposent sur des modèles complexes et opaques. Sans même parler des IA génératives qui affirment parfois avec aplomb des éléments factuellement faux, le manque de transparence quant aux modalités d'entraînement pose la question des biais dans les données, et donc dans les réponses proposées. Impossible de garantir que l'algorithme qui assiste une décision d'urbanisme ou une politique locale connaisse les spécificités de notre territoire.

De plus, l'incertitude demeure quant à la collecte, au stockage et à l'utilisation des données par ces modèles. La CNIL souligne ainsi la grande complexité des projets IA utilisant des données personnelles (par exemple, comparer les consommations en eau des foyers d'une agglomération afin de produire des recommandations personnalisées). De tels projets touchent à plusieurs réglementations : Code des relations entre le public et l'administration (CRPA), RGPD, IA Act...

Enfin, l'adoption a été si rapide qu'elle a bien souvent pris de court les directions. Le shadow IA, qui désigne l'utilisation d'outils d'IA sans l'approbation ou la supervision du système d'information, représente ainsi un risque significatif pour les entités publiques.

Une étude Cyberhaven de juin 2023 révèle que 11% des employés ont utilisé ChatGPT sur leur lieu de travail, et 9% d'entre eux y ont copié des données de l'entreprise. Le cas emblématique de Samsung illustre parfaitement ce risque : des employés ont utilisé la fonctionnalité de correction de code directement sur la plateforme web de ChatGPT, exposant ainsi des informations confidentielles. Dans le secteur public, les risques sont décuplés. Un agent territorial qui soumet à ChatGPT un extrait de délibération contenant des données personnelles de citoyens viole potentiellement le RGPD, sans même en avoir conscience. En mai 2025, un prestigieux cabinet d'avocats américain, Butler Snow, a fait face à des sanctions judiciaires après avoir soumis des documents contenant des citations juridiques entièrement fabriquées par un chatbot IA. Le juge a dénoncé un « manque de diligence et de jugement » dans cette affaire très médiatisée. Les hallucinations des IA ne sont pas anecdotiques : elles peuvent produire des faux précédents juridiques, des statistiques inventées ou des recommandations basées sur des corrélations fictives, avec des conséquences potentiellement graves pour la prise de décision publique.

Les assureurs ont pris la mesure du risque. En 2025, AXA a créé SecureGPT, son propre outil d'IA générative interne, et intégré une extension dédiée à l'IA générative dans son produit CyberRiskConnect. Le risque d'hallucination est désormais considéré comme un risque systémique par les acteurs de l'assurance : lorsqu'un fournisseur d'IA déploie une mise à jour défectueuse ou commet une erreur dans les poids d'un modèle, ce ne sont pas des utilisateurs isolés qui sont affectés mais des milliers simultanément.

Un agent juridique autonome produisant des hallucinations systématiques et déployé dans plusieurs centaines d'organisations pourrait générer des fausses citations juridiques à grande échelle, créant un effet de contagion immédiat. Face à ce constat, l'IA Act européen, entré partiellement en vigueur en février 2025 et pleinement applicable en août 2026, impose désormais des mesures strictes en matière de transparence et de gouvernance des systèmes d'IA.

Jean-Pierre Sabio, Directeur Général de Gigalis: *"Avec l'arrivée massive des IA génératives, les décideurs ont pris conscience de l'impératif de se doter d'un outil souverain. Certaines données confiées à l'IA peuvent sembler anecdotiques, mais une fois agrégées et analysées, elles peuvent poser de sérieux risques de confidentialité et de sécurité. D'où la nécessité de recourir à des outils souverains".*

POURQUOI C'EST POLITIQUE ?

Car confier les données personnelles de concitoyens ou prendre des décisions publiques à l'aide d'un outil étranger au fonctionnement opaque équivaut à renoncer à notre souveraineté numérique.

IMPACTS CONCRETS

- **Prise de décision erronée :** en raison des biais ou de possibles hallucinations, des analyses prédictives peuvent conduire à des politiques mal ciblées ou à une mauvaise allocation des ressources publiques
- **Collecte et utilisation des données publiques :** les requêtes, métadonnées ou même des extraits de documents internes peuvent être stockés et exploités à des fins d'entraînement des modèles d'IA
- **Vulnérabilité accrue de l'organisation :** les outils d'IA générative accumulent de nombreuses données personnelles sur les utilisateurs réguliers, qui deviennent dès lors des cibles privilégiées (publicités ultra-personnalisées, risques de cyberattaques).

SOLUTION

- **Mettre en place une charte d'utilisation claire de l'IA générative :** afin de sécuriser les usages internes. Les bonnes pratiques incluent :
  - la notion de data minimalism : ne transmettre que les données strictement nécessaires
  - l'anonymisation et la pseudonymisation des données
  - l'harmonisation et la standardisation des prompts dès lors qu'ils concernent les usagers
  - la mise en place d'alertes ou de filtres de protection (mots interdits) pour éviter l'usage de données sensibles

- **Opter pour des modèles souverains ou open-source :** afin de respecter le RGPD et de garantir sécurité et confidentialité.

BESOIN D'AIDE POUR CONSTRUIRE UN PROJET IA EFFICACE ET SÉCURISÉ ? DÉCOUVREZ LA FABRIQUE IA TERRITORIALE.

À travers notre centrale d'achat publique, accessible à tout moment pour tous les acteurs publics, vous avez accès à 12 entreprises françaises sélectionnées dans le cadre du marché "IA et Open Source". Cette task force territoriale vous accompagne pas à pas dans vos projets et usages concrets de l'IA.

MENACE #5 :

PERTE DE L'ACCÈS AUX SERVICES ESSENTIELS

LE CONSTAT

L'hyperdépendance aux infrastructures et outils américains crée une vulnérabilité systémique. En 2026, l'accès à nos outils essentiels (messagerie, fichiers partagés, outils de communication) est désormais tributaire de la stabilité géopolitique. En cas de conflit commercial, de tensions diplomatiques ou même en raison d'une décision arbitraire, les fournisseurs américains peuvent restreindre l'accès, modifier les conditions ou imposer des exigences de localisation des données. Dans le pire des scénarios, un territoire pourrait même se retrouver "déconnecté" en quelques minutes.

Les tensions géopolitiques croissantes de 2025 ont placé cette menace au premier plan. En janvier 2026, dans un contexte de sanctions douanières imposées par les États-Unis à plusieurs pays européens dont la France, des experts ont évoqué publiquement la possibilité d'un blocage numérique ciblé visant les entreprises et administrations européennes. Si un tel scénario se matérialisait, des millions d'utilisateurs pourraient perdre l'accès à leurs messageries, fichiers partagés et outils de travail collaboratif en quelques heures.

L'histoire récente offre plusieurs précédents inquiétants : en 2025, suite à des sanctions américaines, Microsoft a suspendu temporairement certains services à la Cour pénale internationale. Plus largement, entre 2020 et 2025, plusieurs pannes majeures ont affecté Gmail, Google Drive et Microsoft 365, paralysant pendant plusieurs heures l'activité de millions d'organisations à travers le monde. Si ces interruptions étaient jusqu'à présent d'origine technique, le risque politique s'ajoute désormais à l'équation. La relocalisation progressive des services numériques sur des infrastructures souveraines n'est plus une option stratégique, mais une nécessité opérationnelle pour garantir la continuité du service public.

Filipe Bica, Directeur cybersécurité, cloud et IA chez Gigalis : *« En 2026, la souveraineté numérique cesse d'être un débat idéologique pour devenir une question de résilience opérationnelle. Les tensions diplomatiques entre les États-Unis et l'Europe illustrent la fragilité d'un modèle où nos services essentiels dépendent d'acteurs soumis à des législations étrangères. Une collectivité qui confie ses outils critiques à un fournisseur américain s'expose à un risque de rupture brutale en cas de crise diplomatique ou commerciale. Ce n'est plus de la théorie : nous avons observé en 2025 des suspensions de services pour motifs politiques. La question n'est plus de savoir si un tel événement peut survenir, mais quand il surviendra. »*

POURQUOI C'EST POLITIQUE ?

Car la continuité de notre service public passe par l'autonomie de nos flux de données. Dans un monde soumis à des tensions géopolitiques croissantes, la souveraineté numérique devient un enjeu crucial.

IMPACTS CONCRETS

- **Rupture partielle ou totale du service public :** état civil, portails administratifs, plateforme de santé… en cas de restriction ou d'interdiction d'accès, les services essentiels connaîtraient une interruption brutale, dommageable à l'ensemble des concitoyens.

SOLUTION

- **Opter pour des outils souverains :** pour cela, il faut commencer par identifier les applications critiques (messagerie, visioconférence, stockage, Gestion Electronique des Documents) puis migrer progressivement vers des outils souverains, français ou européens.
- **Élaborer un plan de continuité d'activité (PCA) spécifique aux ruptures géopolitiques :** ce document stratégique est indispensable pour éviter la panique et assurer la continuité de service. Il pourra envisager divers scénarios (perte d'accès brutale ou dégradation progressive) et comporter une solution de bascule automatisée.

QUI SOMMES-NOUS ?

Acteur territorial du numérique, et désormais Groupement d'Intérêt Public (GIP), Gigalis opère depuis vingt ans les infrastructures et services numériques des Pays de la Loire.

Véritable tiers de confiance, nous accompagnons les acteurs publics dans leur transformation numérique avec des services souverains, performants et sécurisés (réseau public, cloud local, solutions de cybersécurité adaptées).

Ensemble, bâtissons un numérique d'intérêt général !

Pour en savoir plus : *Gigalis, opérateur public de services numériques*