FNCCR
SERVICES PUBLICS LOCAUX DE L'ÉNERGIE, DE L'EAU, DE L'ENVIRONNEMENT ET DES E-COMMUNICATIONS

CLUBNUMÉRIQUE & TERRITOIRES
POUR UN NUMÉRIQUE ÉTHIQUE. SOUVERAIN ET SÛR

GUIDE POUR UN NUMERIQUE ETHIQUE, SOUVERAIN ET SÛR

ÉDITOS

Patrick CHAIZE,
Vice-président «Numérique» de la FNCCR et Sénateur de l'Ain

UN GUIDE POUR FAIRE DE LA SOUVERAINETÉ, DE LA CYBERSÉCURITÉ ET DE LA PROTECTION DE NOS VALEURS FONDAMENTALES DES PRIORITÉS SOUTENUES PAR L'ENSEMBLE DES ACTEURS TERRITORIAUX

Depuis toujours, la FNCCR s'engage aux côtés des collectivités locales pour garantir la souveraineté et la sécurité des infrastructures essentielles. Aujourd'hui, cette mission s'étend naturellement aux enjeux numériques, un domaine désormais incontournable pour la gestion de l'énergie, de l'environnement et bien sûr, des télécommunications. Dans un contexte où la transposition de la directive NIS 2 va significativement renforcer les obligations de cybersécurité, notre priorité est d'accompagner nos adhérents vers des pratiques numériques plus résilientes, sûres et imperméables aux législations extraterritoriales telles que le Cloud Act qui permet à des juges américains de réquisitionner les données stockées par les acteurs américains, quel que soit l'emplacement de leurs infrastructures dans le monde.
Ce guide, préparé en collaboration avec le Club Numérique & Territoires de Com'Publics, s'inscrit dans cette dynamique. Son objectif principal est d'offrir aux collectivités les outils nécessaires pour naviguer dans l'écosystème complexe du numérique éthique, souverain et sûr. Conçu pour sensibiliser les élus et les décideurs territoriaux, ce guide fournit des recommandations pratiques et des critères clairs pour choisir des solutions technologiques en adéquation avec ces valeurs.
Ce défi s'inscrit dans un choix sociétal : accepter la dépendance aux grandes puissances étrangères ou investir dans notre autonomie stratégique. Pour que la confiance des citoyens et des entreprises perdure, il est crucial que les collectivités flèchent leurs investissements vers des infrastructures robustes et partagent leur expertise. Sans cela, nous risquons non seulement l'intégrité de nos services publics numériques, mais aussi la stabilité et la pérennité des territoires intelligents.
Pour la FNCCR, il est temps de faire de la souveraineté, de la cybersécurité et de la protection de nos valeurs fondamentales des priorités nationales partagées et soutenues par l'ensemble des acteurs territoriaux.

Marc TEYSSIER D'ORFEUIL,
Délégué général du Club Numérique & Territoires

UN CLUB ET UN GUIDE AU SERVICE D'UN NUMÉRIQUE PROPRE À NOS VALEURS EUROPÉENNES

Depuis 2016, le Club Numérique & Territoires de Com'Publics rassemble les acteurs du numérique et les décideurs publics autour d'un objectif commun : promouvoir un numérique à la fois éthique, souverain et sûr.
Alors que la transposition de la directive NIS 2 s'apprête à renforcer significativement la protection et les obligations des acteurs publics, des collectivités et des entreprises en matière de sécurité et de souveraineté des infrastructures, il est essentiel que ces derniers soient armés pour répondre aux menaces toujours plus sophistiquées (ransomware par états tiers, hameçonnage, fuite de données, etc.).
S'ajoute à ces enjeux un contexte où l'effritement de la confiance envers les institutions politiques se fait de plus en plus sentir. C'est pourquoi les enjeux de numérique éthique nous tiennent aussi à cœur. La transparence et la traçabilité des solutions numériques mises au service des politiques publiques deviennent des leviers stratégiques indispensables pour restaurer et renforcer la confiance des administrés, mais aussi nous différencier des grandes nations du numérique que sont les USA et la Chine sur le marché mondial.
C'est pourquoi le Club et la FNCCR ont co-construit un guide pratique. Pensé à travers une série de trois ateliers de travail et de nombreux entretiens, ce guide se veut une référence pour sensibiliser et orienter les collectivités et autres décideurs publics et leur offrir les outils nécessaires pour faire des choix éclairés en matière de solutions technologiques, loin du « Confiance Washing » mis en avant par certaines grandes entreprises nationales ou extraterritoriales.
Il valorise notamment les initiatives des TPE/PME et les exemples concrets de collectivités ayant pris le virage de la confiance numérique. Mais surtout, il propose des recommandations claires et concrètes en matière de commande publique. Car notre ambition ultime est bien de défendre un cadre propice à l'émergence d'un écosystème numérique européen compétitif et respectueux de nos libertés individuelles et de notre souveraineté numérique.
Ensemble, faisons d'un numérique propre à nos valeurs non seulement une priorité, mais une réalité tangible au service de nos territoires, des citoyens et de nos entreprises !

SOMMAIRE

UN GUIDE POUR SENSIBILISER LES COLLECTIVITÉS AU NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR : UN ENJEU ÉMINEMMENT (GÉO)POLITIQUE ET DE CONFIANCE

Jean-Luc SALLABERRY,
Responsable du pôle Numérique de la FNCR

Pourquoi ce guide ? Pourquoi la FNCCR a-t-elle choisi de s'emparer de ce sujet ?

La souveraineté numérique et la cybersécurité sont intimement liées. Elles sont devenues un enjeu crucial pour les collectivités territoriales en raison de la multiplication des attaques informatiques, qui sont parfois motivées par des demandes de rançons, mais aussi par des considérations géopolitiques. Par exemple, des communes ayant affiché leur soutien à l'Ukraine en arborant son drapeau en ligne se sont retrouvées sous le feu de cyberattaques étrangères.
Cela révèle une vulnérabilité inédite des collectivités locales, qui montre qu'en matière de cybersécurité, les menaces ne se concentrent plus seulement sur l'État ou les grandes institutions, mais peuvent atteindre des entités publiques de moindre envergure.
Notre guide vise à sensibiliser ces collectivités aux risques encourus et à les accompagner dans une démarche de sécurisation. À la FNCCR, nous travaillons principalement sur des services essentiels comme l'énergie, l'eau, les transports et la fibre optique, indépendamment des maîtres d'ouvrage. Il est donc logique de donner la priorité à la sécurisation des systèmes d'information (SI) de nos membres.

Comment définissez-vous un numérique éthique, souverain et sûr ?

Pour nous, un numérique éthique, souverain et sûr implique une identification et une protection des données essentielles. Avec l'explosion des données, il est évident que nous ne pourrons pas tout sécuriser, il faut donc cibler. Cette approche est celle de la directive européenne NIS2, qui vise à définir les systèmes d'informations essentiels.
À la FNCCR, nous avons identifié plusieurs types de données essentielles : les données personnelles et les archives, qui ont un caractère de conservation incontournable, ainsi que les données « temps réel » qui servent au bon fonctionnement de nos services publics pour l'énergie, l'eau, les transports ou encore le numérique.
S'agissant des archives par exemple, les Archives nationales jouent un rôle central dans la conservation des données critiques de l'État, notamment en les stockant dans les data centres publics de l'Etat. Elles sont considérées comme sensibles et donc mieux protégées. Il nous semble évident de prévoir le même niveau de garantie pour les archives territoriales.
Il est ainsi crucial que chaque collectivité sache déterminer quelles données sont à sécuriser en priorité. Pour répondre à cet enjeu, la FNCCR pourrait lancer une étude pour identifier les données essentielles propres à chaque collectivité, hiérarchiser leur protection et renforcer ainsi leur résilience face aux cybermenaces.
J'insiste sur le fait que la directive NIS2 représente une avancée importante, mais elle reste insuffisante, d'où la nécessité de débattre de sa surtransposition. Certains souhaitent aller plus loin dans la définition des données essentielles, car la directive reste relativement vague en la matière, se contentant de définir des domaines prioritaires. Or, des données telles que les données personnelles et les archives, qui sont pourtant essentielles, ne sont pas explicitement incluses dans ces domaines.

Qu'implique un numérique souverain ?

La souveraineté numérique implique des infrastructures sécurisées, notamment s'agissant du cloud. Nous insistons sur la distinction entre un cloud souverain, qui repose sur des infrastructures contrôlées directement par la puissance publique, et des solutions privées plus vulnérables à des lois extraterritoriales, qui permettent à des États étrangers d'accéder à nos données. Nous sommes conscients des handicaps financiers qui peuvent peser sur les collectivités, nous préconisons de mutualiser des offres de cloud de très haut niveau, comme l'ont fait par exemple le département du Val-d'Oise et la ville de Paris.
En outre, nous estimons qu'un numérique souverain repose sur la possibilité d'un accès direct des autorités publiques aux data centres. Pour la FNCCR, il est d'intérêt de restreindre cet accès aux seules personnes habilitées et dédiées aux services publics. La question d'une habilitation spécifique pour ces intervenants se pose, à l'image de celle accordée aux conservateurs d'archives, qui gèrent des données sensibles, comme les dossiers de naissance sous X.

Quels leviers identifiez-vous pour renforcer le développement de solutions cloud souveraines face aux géants internationaux ?

Soutenir les acteurs numériques européens est essentiel pour assurer notre souveraineté numérique, en particulier dans le domaine du cloud, où les couches de développement locales sont encore inexistantes. Il est crucial de construire ces infrastructures en Europe pour limiter la dépendance aux acteurs non-européens. C'est un objectif que portait Thierry Breton, mais le jeu des alliances en Europe complexifie la coopération à l'échelle européenne. C'est regrettable car aux États-Unis, le financement par la DARPA a permis le développement de start-ups et des grands groupes numériques actuels aux visées géopolitiques, ce qui montre l'importance d'un soutien similaire en Europe pour défendre nos intérêts numériques et géostratégiques.

Que répondez-vous aux collectivités qui souhaitent franchir le cap de la souveraineté et de la sécurité, mais qui sont liées par des contrats à long terme avec des prestataires externes ?

Ne pas attendre la fin des contrats mais les renégocier pour adapter les clauses aux exigences actuelles. Si cela s'avère impossible, une modification législative pourrait être nécessaire, comme cela a été fait avec la loi pour une République numérique, qui impose aux opérateurs de fournir les données collectées, même a posteriori, aux services publics concernés dès la promulgation.

Comment appréhendez-vous l'investissement nécessaire pour se conformer à NIS2 ?

L'adoption de la directive NIS2 entraînera des coûts pour toutes les parties impliquées, mais cela constitue avant tout un choix politique majeur. C'est un véritable choix de société et de gouvernance publique : soit nous acceptons de rester dépendants d'autres pays, soit nous décidons de préserver et de renforcer notre autonomie stratégique.

Notre principale préconisation est évidemment encore une fois la mutualisation pour réduire les coûts. A cet effet, nous réfléchissons d'ailleurs à l'intérêt d'un texte législatif sur la création d'une compétence de gestion souveraine des données au sein de toutes les collectivités territoriales et de leurs groupements. Cette compétence concernerait l'ensemble des données, qu'elles soient publiques ou privées, ayant un rôle dans les politiques publiques, telles que celles relatives aux délégations de services publics (DSP). L'objectif est notamment de créer le cadre juridique adéquat permettant aux collectivités de mutualiser ressources et solutions.

Selon vous, quelle devrait être la priorité des collectivités pour garantir une politique de territoires intelligents souveraine ?

Ma préconisation prioritaire pour les collectivités est de flécher prioritairement leur budget vers la cybersécurité, même dans un contexte de réduction budgétaire, car elle garantit la confiance dans nos services publics numériques. Pour que les citoyens et les entreprises puissent se reposer sur un réseau sécurisé, il est indispensable de mettre en œuvre la directive NIS2.
Nous avons estimé qu'il faudrait à terme au moins 500 RSSI (responsables de la sécurité des systèmes d'information) dédiés à la sécurisation des territoires. C'est beaucoup et nous sommes très loin du compte !
Il est essentiel de faire comprendre à tous que la cybersécurité n'est pas un besoin temporaire mais une priorité durable et cruciale. Sans cette vigilance, l'intégrité de nos réseaux est en jeu – et avec elle, notre accès aux données, au pilotage, et même à Internet. La qualité et la sécurité des réseaux sont le socle de cette confiance ; sans elles, le réseau s'effondre, et la confiance s'évapore.

NOTRE AMBITION

SENSIBILISER LES ÉLUS TERRITORIAUX ET NATIONAUX AUX ENJEUX DE NUMÉRIQUE DE CONFIANCE (DANGERS / OPPORTUNITÉS)

PROPOSER UN CAHIER DES CHARGES CLAIR POUR MIEUX IDENTIFIER LES SOLUTIONS DE CONFIANCE

VALORISER LES COLLECTIVITÉS ET ACTEURS ÉCONOMIQUES AYANT FAIT LE CHOIX DE SOLUTIONS DE CONFIANCE

QUI SOMMES-NOUS ?

FNCCR

SERVICES PUBLICS LOCAUX DE L'ÉNERGIE, DE L'EAU, DE L'ENVIRONNEMENT ET DES E-COMMUNICATIONS

La FNCCR (Fédération nationale des collectivités concédantes et régies) est une association regroupant depuis 1934 des collectivités locales et leurs groupements.
Depuis quinze ans elle accompagne et accélère le déploiement de réseaux d'initiative publique pour garantir l'accès au très haut débit et promeut le développement des usages et services numériques aux citoyens.
À ce titre la FNCCR milite pour une gestion territoriale et souveraine des données publiques et privées utiles aux services publics au bénéfice des collectivités et des citoyens.

L'ORGANISATION DES ACTIVITÉS

La commission numérique

Présidée par Patrick CHAIZE, Vice-président délégué au numérique, une commission ad hoc réunit les élus représentant les collectivités adhérentes.
Espace de dialogue et de concertation, cette commission permet d'arrêter des positions communes et de fixer les priorités de la feuille de route fédérale en matière de numérique.

Les activités du département numérique sont structurées autour de 5 principaux domaines :

- Infrastructures de communications électroniques
- Données territoriales et information géographique
- Services et usages numériques
- Territoires connectés et durables
- Cybersécurité

FÉDÉRER POUR ACCOMPAGNER, PESER ET AGIR ENSEMBLE

Par la mise en réseau et le recueil des expériences de terrain, l'accompagnement proposé aux adhérents couvre et s'adapte en continu aux besoins opérationnels de leurs agents et aux orientations stratégiques de leurs élus. S'il peut évoluer, cet accompagnement repose néanmoins et promeut en permanence une vision mutualisée et péréquée du développement numérique dans les territoires.
Pour mener ses activités en matière de numérique, la FNCCR s'appuie sur un large écosystème d'associations de collectivités, généralistes ou spécialisées, de fédérations professionnelles, de partenaires institutionnels et médias. Forte de sa représentativité et de ses expertises, elle est reconnue comme un interlocuteur incontournable par les pouvoirs publics et les autorités de régulation. Elle est régulièrement consultée, auditionnée ou directement associée aux travaux d'instances nationales, de chantiers temporaires ou de programmes (inter)ministériels installés dans la durée.

LES SERVICES RÉSERVÉS AUX ADHÉRENTS

En fonction de leurs centres d'intérêt et de leurs missions, les adhérents au numérique peuvent accéder et participer « à la carte » à tout ou partie des activités proposées au sein des 5 volets thématiques :

- Groupes de travail et animation de communautés de pratiques
- SVP Numérique : guichet de questions/réponses personnalisées
- Modules de formation à tarifs préférentiels, certifiés Qualiopi
- Etudes de connaissance et de prospective menées en propre ou en Partenariat
- Documents de référence *(techniques, juridiques, économiques)*
- Congrès, colloques et manifestations
- Projets collectifs et partenariaux *(observatoire, centre de ressources, etc)*
- Conseils et notes d'analyse en affaires publiques et juridiques
- Bouquet de services d'information, de communication et de collaboration en ligne *(site web, lettre d'information, espaces collaboratifs, visioconférence)*
- Plateforme de partage et de valorisation de données : France Data Réseau

QUI SOMMES-NOUS?

CLUB NUMÉRIQUE & TERRITOIRES

POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR

Lancé en 2016, le Club fédère ses partenaires économiques et un écosystème institutionnel engagé autour d'un objectif : faire avancer les solutions en faveur du numérique de confiance (éthique, souverain et sûr) en sensibilisant les pouvoirs publics aux risques pesant sur nos valeurs avec les modèles extra-européens mais aussi les opportunités qu'il offre pour nos entreprises

POURQUOI UN CLUB ?

Le Club Numérique & Territoires de Com'Publics lance en 2024, avec la FNCCR, une initiative structurante dédiée à la défense d'un numérique porteur de valeurs européennes et d'autonomie stratégique.

Il est conçu comme un espace de dialogue pour :

- **Porter collectivement des messages clés** auprès de la puissance publique : actions de sensibilisation
- **Créer un climat positif** pour permettre la diffusion des messages de ses partenaires
- **Favoriser l'identification des leviers et des verrous** à débloquer pour permettre la défense d'intérêt de ses partenaires.
- **Nouer des liens solides et pertinents entre les acteurs européens de l'écosystème privé et la puissance publique**
- **Faire connaître l'existence et la qualité des solutions françaises**

LES ACTIVITÉS DU CLUB

- **4 – 5 rencontres-débats annuelles** dans un format convivial et décomplexé autour d'acteurs publics et privés (parlementaires, administrations, etc.)
- **Une veille institutionnelle** envoyée quotidiennement
- **Lobbying mutualisé : en fonction de l'actualité, note(s) de position du Club** portant les messages fédérateurs de ses partenaires
- **Des livrables stratégiques : guide/livre blanc à destination des décideurs publics**

1 - PROTECTION DE LA VIE PRIVÉE & DES LIBERTÉS INDIVIDUELLES

RETOUR SUR L'ATELIER DE TRAVAIL du lundi 30 septembre 2024

Organisé par la FNCCR et le Club Numérique & Territoires sur le thème :

COMMENT GARANTIR LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES DONNÉES PERSONNELLES TOUT EN TIRANT PARTI DES INNOVATIONS NUMÉRIQUES DANS DES TERRITOIRES DE PLUS EN PLUS CONNECTÉS ?

INTRODUCTION DE LINDA SISSI

« Ce troisième atelier a permis d'examiner les enjeux de protection des libertés individuelles liés à l'utilisation d'outils numériques, notamment pour la captation de flux et d'images dans le contexte des territoires intelligents.

Il en ressort qu'une solution vraiment protectrice repose sur deux principes : empêcher les usages abusifs des données en interne et prévenir les risques de fuites externes.

Le cadre juridique qui encadre la protection des libertés individuelles dans le domaine des technologies repose sur des textes clés, comme la Charte des Droits Fondamentaux de l'Union Européenne et le Règlement Général sur la Protection des Données (RGPD), qui impose un principe de proportionnalité. Cela signifie que l'usage des données personnelles doit être strictement nécessaire au service rendu.

Ce principe est fondamental, car il établit une ligne claire : d'un côté, il y a le respect des obligations du RGPD, qui encadre rigoureusement le traitement des données personnelles ; de l'autre, il y a un choix éthique d'éviter l'utilisation de ces données personnelles quand elles ne sont pas indispensables, par exemple, dans des contextes comme le comptage de piétons ou la gestion des parkings.

Lors de nos échanges, nous avons d'ailleurs constaté que le «traitement de la vidéo algorithmique» est une notion parfois floue. Il est essentiel de bien distinguer les utilisations de la Safe City, afin de garantir la sécurité des personnes et des biens, qui sont légitimes et encadrées, des applications Smart City, c'est à dire des territoires intelligents, comme l'analyse des flux touristiques ou de mobilité, qui demandent une vigilance particulière pour éviter tout usage abusif des données.

Cet atelier a été l'occasion de clarifier ces questions et de développer ensemble des solutions qui assurent à la fois la sécurité et le respect des libertés individuelles.

LISTE DES PARTICIPANTS

ACTEURS PUBLICS

Herinirina FANEVAMAMPIANDRA, *Chargée de mission innovation Énergie et Réseaux, S.I.E.L (Territoire d'énergie Loire)*
Fabrice LÉRIQUE, *Chargé de mission Transition numérique, Région Hauts-de-France*
Audrey LINKENHELD, *Sénatrice du Nord*
Sophie METTE, *Députée de Gironde*
Gilles PIRMAN, *Chargé de mission Stratégie des territoires, ANSSI*
Magali ROGER, *Chargée de mission Innovation sociale et Médiation numérique, MEL (Métropole Européenne de Lille)*

ACTEURS ECONOMIQUES

Fabrice COUPRIE, *Président, Mediomatrix*
Laurent DAUDE, *Président, Groupe B.Conseil*
Jean-Baptiste POLJAK, *Président, UPCITI*
Nicolas SAINTHERANT, *Directeur innovation, Qarnot Computing*

L'EQUIPE ORGANISATRICE

Jean-Luc SALLABERY, *Chef du Département Numérique, FNCCR*
Linda SISSI, Déléguée, *Club Numérique & Territoires, Com'Publics*
Guillaume METIVIER, *Délégué collectivités Mobilités – énergies, Com'Publics*
Claire GUIBAUD, *Assistante, département numérique, FNCCR*

QUELS ENJEUX ET QUELS RISQUES POUR NOS DONNÉES PERSONNELLES ?

Smart City contre Safe City ou l'importance de distinguer les outils selon les usages

Avant tout débat, il a été précisé l'intérêt de distinguer clairement les usages liés au développement des villes surveillées (Safe City) de ceux liés au développement des Territoires intelligents (Smart Cities). Tous les participants se sont accordés pour dire que la vidéosurveillance, lorsqu'elle est encadrée, est extrêmement importante du point de vue de la sécurité. Il n'est pas question de revenir sur le sujet. Toutefois, celle-ci est bien à distinguer du captage d'images réalisé dans le cadre des Territoires intelligents : comptage piétons, flux de circulation, éclairage public, etc.

Monétisation des données, fuite d'images… Les risques liés à l'utilisation de solutions peu protectrice des libertés individuelles

Les intervenants ont identifié deux risques principaux. D'abord, celui de la confiance du public : chaque utilisation détournée ou

mal sécurisée de données nuit aux perceptions des citoyens vis-à-vis des futures initiatives numériques. Un exemple marquant est l'information récente selon laquelle un fournisseur de caméras de surveillance publiques aurait vendu les données des vitesses de circulation des véhicules à des assureurs. Ce genre de pratique explique pourquoi certaines villes hésitent à installer des dispositifs de captation d'image.

Le second risque est la fuite de données. Par exemple, dans certains départements, des entreprises en charge des mises à jour des modèles visuels ont récupéré des téraoctets de données sans floutage, entraînant des fuites d'images sensibles.

UN POSITIONNEMENT A TROUVER A L'INTERNATIONAL : FAIRE DE NOS VALEURS UN AVANTAGE COMPETITIF

Protection des données personnelles : un retard en France ?

Certains intervenants ont pointé le fait qu'en France, la vie privée n'est pas aussi prioritaire qu'elle peut l'être dans d'autres pays européens, comme en Norvège. En France, les peurs alimentées par les théories du complot sécuritaires tendent à favoriser l'installation de dispositifs de captation d'images, qui sont aujourd'hui perçus comme des technologies incontournables en milieu urbain. Mais cela soulève une question : avons-nous vraiment besoin, dans un cadre non sécuritaire, de stocker des visages ou des plaques d'immatriculation pour gérer le stationnement ou compter les touristes ? Sans réflexion approfondie, ces pratiques pourraient aboutir à des scandales et à l'arrêt de projets numériques dans les collectivités.

En France, la CNIL intensifie ses actions pour garantir la conformité aux normes de protection des données et sensibiliser les entreprises et collectivités au principe de proportionnalité. Celui-ci implique celui de la minimisation de la captation de données au strict minimum.

À Amsterdam, les collectivités anonymisent les captations d'images en interne avant toute utilisation par leurs prestataires privés, ce qui permet la désignation d'un tiers de confiance public et limite les risques de fuite d'images en haute résolution.

L'enjeu économique de l'expansion internationale des questions de vie privée

Nos valeurs européennes constituent en réalité une véritable opportunité pour que les solutions françaises et européennes, adoptant dès leur conception des standards élevés en matière de protection des données personnelles, deviennent des références dans un monde de plus en plus connecté et marqué par des dispositifs intrusifs, comme les réseaux sociaux. En effet, le développement international du respect de la vie privée représente un atout économique non négligeable, avec des pays comme Monaco et ou même les Etats-Unis, qui s'engagent sérieusement à proportionner la production de données à leur utilisation réelle. Cela pourrait conférer à nos entreprises un avantage concurrentiel significatif.

Et cela commence par distinguer clairement les usages et les solutions technologiques associés : Des dispositifs dédiés aux usages sécuritaires, indispensables et légitimes, accessibles par des garants de l'autorité et des solutions conçues pour les territoires intelligents.

QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

D'après la Cnil[1], c'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Peu importe que ces informations soient confidentielles ou publiques.

A NOTER : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

ATTENTION : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

1 https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi

TRANSPARENCE ET TRAÇABILITÉ POUR GAGNER LA CONFIANCE DES CITOYENS

Une méfiance redoublée pour les solutions publiques : adopter plus de traçabilité et de transparence

Les intervenants publics ont constaté que lorsqu'une solution numérique provient des pouvoirs publics, il faut systématiquement redoubler de vigilance, car la méfiance des citoyens devient plus marquée. Pour tous, la transparence et la traçabilité des données est la clé vers la confiance des administrés. Ainsi, certains recommandent, pour chaque nouvelle installation, de prévoir une présentation détaillée, précisant le cheminement exact des données, au moyen d'un QR code apposé à proximité des capteurs par exemple. Car lorsque des soupçons de mauvais usage émergent, il est souvent trop tard. Certains citoyens interviennent alors directement auprès des Mairies, mettant fin aux initiatives dès leur lancement.
Ces phénomènes rappellent également les réticences exprimées durant la crise sanitaire avec le déploiement de l'application TousAntiCovid : de nombreux citoyens craignaient que le Gouvernement ne collecte leurs données personnelles à des fins différentes que celles initialement prévues par l'application. Et pourtant, le paradoxe veut que ces mêmes citoyens utilisent pour beaucoup en parallèle des applications privées peu sécurisées.

Quel cahier des charges pour des capteurs par exemple ?

Le premier principe sur lequel les équipes souhaitent particulièrement se concentrer est celui de la proportionnalité. Dans ce contexte, la proportionnalité est définie comme l'adéquation des données aux usages précisément définis au début du projet, sans aller au-delà.

Dans le cadre des territoires intelligents, l'une des premières recommandations a donc été de privilégier des méthodes de captation non intrusives, visant à empêcher la collecte de données personnelles, notamment en réduisant la qualité des images captées by design et non pas à posteriori. En effet, un simple floutage après coup est réversible et ne peut ne pas suffire à éviter certains usages non prévus initialement (suivi du parcours d'une personnes en raison de son origine ethnique ou religieuse, mise à l'écart de SDF, etc.). Encore une fois, des solutions à visée sécuritaire existent pour les cas problématiques. Inutile d'y adjoindre des outils visant à gagner la confiance de tous.

Un autre principe clé est la minimisation des données, c'est-à-dire la collecte stricte des informations nécessaires au projet et rien de plus. À cela s'ajoute un troisième élément : la limitation de la conservation des données dans le temps, de sorte qu'elles soient supprimées dès qu'elles ont été exploitées.

Enfin, le traitement local des données est également un point d'attention important pour éviter leur diffusion inutile. Il arrive qu'une simple connexion à Internet fasse perdre la main sur des données.

UN RÔLE PLUS CONSEQUENT POUR LA CNIL

Sensibilisation, accompagnement, sanction…Pour un guichet unique de la CNIL ?

La sensibilisation, l'accompagnement et la sanction sont trois axes essentiels pour un cadre de protection des données qui soit à la fois efficace et accessible. Le cadre réglementaire actuel prévoit bien la sanction de certains comportements abusifs en matière de données personnelles. Cependant, dans les faits, ceux qui font un usage inapproprié ne sont pas toujours rappelés à l'ordre automatiquement. C'est pour cette raison que de nombreux élus appellent à concevoir des solutions numériques intégrant dès le départ des couches de protection et d'assurabilité.
Un point crucial pour renforcer ce cadre est le rôle de la CNIL. En France, nous avons la chance d'avoir cet organisme de régulation, mais son accès pour les citoyens, les acteurs publics et les professionnels reste complexe. Actuellement, trouver le bon interlocuteur pour des questions spécifiques est difficile, ce qui pousse certains à poser leurs questions de manière dispersée, parfois sans obtenir de réponses claires. L'idéal serait que la CNIL devienne un véritable guichet unique : un lieu où chacun pourrait obtenir des réponses concrètes et un accompagnement sur le respect des bonnes pratiques, mais aussi où des sanctions pourraient être envisagées pour les manquements avérés.
Pour réaliser cet objectif, il serait nécessaire d'accroître les moyens de la CNIL et de développer son périmètre de pouvoir.

LE PRINCIPE DE PROPORTIONNALITÉ DANS LE DROIT EUROPÉEN [2]

Il s'agit d'un principe fondamental qui vise à garantir que les mesures prises par les autorités publiques ou les acteurs privés dans le cadre de l'application de la loi soient adaptées, nécessaires et proportionnées par rapport aux objectifs visés. Il concerne directement la captation et le traitement de données à caractère personnel.
Le principe de proportionnalité est implicitement abordé dans plusieurs articles du RGPD (art 5,6,9). Il implique trois critères principaux :

1. **Nécessité :** La collecte et le traitement des données doivent être nécessaires pour atteindre un objectif légitime. Si d'autres méthodes moins intrusives existent, elles doivent être privilégiées.
2. **Adaptation :** La mesure doit être adaptée à l'objectif recherché. Elle doit être en lien direct avec la finalité et ne pas aller au-delà de ce qui est nécessaire.
3. **Proportionnalité stricte :** L'impact de la mesure sur les droits et libertés des individus ne doit pas être disproportionné par rapport aux bénéfices ou objectifs poursuivis.

2 https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd

LES RECOMMANDATIONS DES INTERVENANTS

1. **Respect du principe de proportionnalité :** S'assurer que la collecte de données soit strictement nécessaire aux objectifs définis au début du projet, sans excès.
2. **Distinguer les usages et développer des infrastructures dédiées :** Clarifier la différence entre les outils de la Safe City (sécuritaires et encadrés) et ceux des Smart Cities (territoires intelligents) qui ne nécessitent pas toujours de captation de données personnelles, et développer des infrastructures différentes
3. **Captation non intrusive :** Privilégier des méthodes de captation qui ne collectent pas de données personnelles, comme la réduction de la qualité des images dès la conception.
4. **Minimisation des données :** Collecter uniquement les informations nécessaires au projet et rien de plus.
5. **Limitation de la conservation des données :** Supprimer les données dès qu'elles ont été utilisées pour éviter toute conservation excessive.
6. **Traitement local des données :** Veiller à ce que les données soient traitées localement pour prévenir leur fuite, idéalement sans connexion Internet.
7. **Transparence et traçabilité :** Proposer une présentation détaillée et ouverte des données collectées, par exemple via des QR codes, pour rassurer les citoyens sur le cheminement des données des solutions choisies.
8. **Renforcement de la CNIL :** Faire de la CNIL un guichet unique accessible pour obtenir des conseils et des sanctions, avec un élargissement de ses moyens et de son périmètre d'action.

LA POSITION DE LA CNIL SUR LE NUMÉRIQUE ÉTHIQUE

Le cas de la vidéosurveillance algorithmique dans le cadre de la loi JO 2024 notamment

La Commission nationale de l'informatique et des libertés (Cnil) a, à l'issue d'une consultation publique, publié en 2022 une position[1] structurante sur l'utilisation de la vidéosurveillance algorithmique dans les lieux publics. Le déploiement de ces technologies, bien que potentiellement utile pour optimiser la sécurité pose des questions cruciales sur la protection des droits et libertés individuelles lorsqu'il s'agit de piloter des territoires intelligents. Depuis 2017, la Cnil souligne la nécessité d'un cadre juridique adapté pour encadrer ces innovations, face à l'inadéquation de la législation actuelle.

L'essor des caméras dotées de logiciels d'intelligence artificielle permet aujourd'hui une analyse automatisée des comportements et une catégorisation en temps réel des personnes. Par exemple, ces dispositifs peuvent compter les piétons, les véhicules ou analyser la fréquentation de centres commerciaux selon des critères tels que l'âge ou le genre, influençant ainsi la stratégie publicitaire ou l'aménagement des espaces. Toutefois, la Cnil alerte sur le caractère potentiellement intrusif de ces technologies, qui pourraient accentuer la surveillance généralisée.

Dans sa publication, l'organisme propose au législateur d'établir un cadre réglementaire plus précis pour ces dispositifs en les soumettant à une base légale adaptée en fonction des circonstances. L'argument de « l'intérêt légitime », par exemple, ne saurait justifier une atteinte disproportionnée aux attentes des personnes, telles que l'analyse de l'humeur des clients pour adapter les publicités en magasin. De plus, elle insiste sur le principe de proportionnalité, à savoir que lien entre le dispositif et ses objectifs doit être démontré avant toute mise en œuvre.

Dans le cadre spécifique des Jeux Olympiques 2024 de Paris, la Cnil a exprimé des préoccupations particulières. Elle reconnaît la nécessité de renforcer la sécurité lors de cet événement mondial, mais insiste sur l'importance de ne pas sacrifier les droits fondamentaux à la vie privée. Les dispositifs de vidéosurveillance augmentée, utilisant l'intelligence artificielle pour repérer des comportements anormaux, doivent rester exceptionnels et être strictement encadrés.

La Cnil a notamment préconisé que ces déploiements soient limités dans le temps et entourés de mesures de protection telles que le « privacy by design ». De plus, elle a mis en garde contre une généralisation de l'usage de telles technologies après les JO sans cadre réglementaire renforcé. La Cnil a enfin souligné l'importance de distinguer ce qui est « éthiquement et socialement souhaitable » pour préserver les valeurs démocratiques.

Loi JO 2024 :
Quelle suite pour l'expérimentation de la vidéo-algorithmique dans l'espace public ?

L'article 7 de la loi relative aux Jeux Olympiques et Paralympiques de 2024[2] autorise jusqu'au 31 mars 2025 l'expérimentation de « caméras augmentées » afin de de tester des solutions algorithmiques couplées en temps réel aux caméras de vidéo-protection, tout en interdisant la reconnaissance faciale.
Un rapport d'évaluation indépendant, mené par Christian Vigouroux[3], Président de section honoraire au Conseil d'État sera présenté au Parlement en décembre 2024. Cette évaluation inclura un collège de personnalités qualifiées ainsi qu'un collège d'utilisateurs.

1 https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position
2 https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000036742954
3 https://www.interieur.gouv.fr/actualites/grands-dossiers/a-linterieur-des-jeux-olympiques-et-paralympiques-de-paris-2024/securite

> *« L'ÉTHIQUE ET LA SOUVERAINETÉ NUMÉRIQUE NE S'ARRÊTENT PAS AUX NORMES LÉGALES, ELLES EXIGENT IMPULSION POLITIQUE ET CONFIANCE*

Philippe LATOMBE,
Député de Vendée

Une définition du numérique éthique à clarifier : le cas de la vidéosurveillance algorithmique

L'éthique dans le domaine numérique va bien au-delà de la simple conformité aux règlements, tels que le RGPD ou l'IA Act ; elle englobe aussi la manière dont les outils de surveillance sont utilisés, leurs finalités réelles, et surtout la transparence de leur mise en œuvre. Par exemple, si l'anonymisation « by design » est une obligation légale pour protéger la vie privée des individus, l'éthique exige d'aller plus loin, de s'interroger sur le fait que chaque action entreprise soit justifiée par des raisons légitimes et non par des intentions cachées. Ce questionnement va au-delà de la biométrie ou de la simple conformité légale ; il s'agit d'interroger les intentions sous-jacentes.
Par exemple, une collectivité souhaitant utiliser un logiciel de vidéoprotection pour détecter les individus victimes de malaise notamment cardiaque (passage en position couchée) peut se voir reprocher des intentions cachées si elle s'en sert pour identifier les sans-abris dormant dans la rue. Dans ce cas, l'éthique impose à l'entreprise de vidéoprotection de refuser cette demande, non conforme aux bonnes pratiques.
Ainsi, l'éthique se construit progressivement, cas après cas, et se base sur des règles générales nées de l'expérience. Pour éviter les dérives, la mise en place d'un comité d'éthique, à l'image de celui d'évaluation de l'expérimentation de la vidéosurveillance intelligente présidé par Christian Vigouroux, serait une bonne idée. Ce comité, composé de techniciens, d'experts en sciences humaines et de fonctionnaires, permettrait d'équilibrer les préoccupations techniques avec les considérations humaines, garantissant ainsi que les décisions prises soient informées, justes, et respectueuses de la dignité humaine.

Bien comprendre les risques des solutions peu protectrices des libertés individuelles : un enjeu stratégique

Le premier risque lié à l'usage des logiciels de surveillance ne réside pas tant dans la fuite de données vers l'extérieur, mais dans leur mauvaise utilisation à des fins personnelles, malveillantes ou abusives. Par exemple, un officier de police municipale pourrait détourner un logiciel de vidéoprotection algorithmique déployé par sa collectivité – comme cela a déjà été observé avec un logiciel d'origine israélienne – pour surveiller des activités personnelles, telles que des suspicions de comportement au sein de son entourage, ce qui constitue un usage à des fins privées non prévues par la législation. À plus grande échelle, des technologies comme la reconnaissance faciale pourraient également être détournées, par exemple à des fins électorales, sans que les citoyens en soient informés. Il est à noter également que l'accès privilégié à certaines informations peut également constituer pour les agents publics un levier dans le cadre de leur progression de carrière, ce qui accroit la menace de dérive.
Ce type de dérive souligne l'importance de mettre en place une traçabilité rigoureuse de chaque utilisation, afin de permettre le suivi et le contrôle de toute exploitation des systèmes.

Transfert de données : des menaces sous-estimées pour notre souveraineté

Concernant le risque stratégique de transfert de données vers un État tiers, celui-ci représente une menace significative en raison de l'accès privilégié qu'il pourrait offrir à des informations hautement sensibles, telles que les déplacements individuels, les flux de trafic, voire des données biométriques, révélant notamment le nombre de véhicules présents dans un lieu spécifique. À titre d'illustration, la majorité des machines agricoles utilisées en France sont fabriquées aux États-Unis et intègrent des GPS ainsi que des capteurs capables d'analyser le volume et la qualité des céréales récoltées. Les données collectées sont transférées outre-Atlantique, permettant ainsi d'évaluer avec précision la production agricole française, tant en volume qu'en qualité, et de prévoir les cours du marché des céréales. L'agrégation de données, même sectorielles, s'avère précieuse pour dresser un tableau général, qu'il s'agisse de l'état de santé d'une population ou de tendances de consommation énergétique. Ces informations peuvent se transformer en levier de négociation économique internationale et impacter les marchés mondiaux. Celui qui détient une quantité supérieure d'informations sur un produit ou un service en tire un avantage stratégique non négligeable.

Protection et promotion de solutions technologiques souveraines : mode d'emploi

L'utilisation de matériel non européen, tel que les caméras ou

les passerelles 5G de certains fournisseurs, pose des questions cruciales en matière de sécurité, notamment en raison des risques potentiels de « backdoors » (« porte dérobée » inconnue de l'utilisateur d'un logiciel, qui permet un accès illégitime) et autres vulnérabilités dans les infrastructures. Afin de garantir une sécurité optimale, l'une des solutions, selon l'usage souhaité, serait d'opter pour du matériel fabriqué en France ou en Europe, associé à un réseau filaire directement relié aux autorités, comme les préfectures. Par ailleurs, l'utilisation de solutions on premise (sur un serveur propre) pour les logiciels, ainsi que de balises et capteurs permettant de contrôler les flux sortants, est pertinente pour garantir la sécurité des systèmes. La traçabilité des accès, assurée par des logs et des registres, est également indispensable pour une gestion transparente et responsable des infrastructures. Il est en outre crucial de définir si les accès aux systèmes s'effectuent via des comptes génériques ou des comptes individuels personnalisés, ce choix ayant un impact significatif sur la robustesse de la sécurité des infrastructures.

Si l'utilisation du cloud offre une simplicité d'accès et une plus grande flexibilité, il est impératif de privilégier des solutions européennes, idéalement contrôlables par la CNIL, avec des infrastructures situées en Europe.

En cas de fuite de données, la localisation des infrastructures en Europe permettrait de désigner un responsable légal susceptible de faire l'objet de sanctions pénales. Ces sanctions, reconnues pour leur effet dissuasif, restent cependant appliquées de manière insuffisante en France et en Europe, en comparaison avec les pratiques en vigueur aux États-Unis.

L'expérimentation encadrée par la Loi relative aux Jeux Olympiques et Paralympiques de 2024, traduit cette orientation. L'objectif était de recourir à des logiciels européens, certifiés par la CNIL, déployés en *on premise* et dotés de mécanismes de blocage pour interdire l'usage de la biométrie. L'évaluation en cours de cette expérimentation permettra d'en tirer des enseignements pour les initiatives futures.

Je souhaiterais également mettre en lumière une actualité parlante : Google a récemment engagé une action contre Microsoft pour des pratiques présumées anticoncurrentielles, une affaire susceptible d'influencer la réglementation et l'accès aux marchés. Cet épisode illustre les tensions croissantes autour de l'influence des GAFAM et renforce la nécessité de protéger les acteurs européens contre les pratiques anticoncurrentielles et les législations extraterritoriales.

Pour une commande publique dynamique soutenue par des incitations au niveau national

Historiquement, les collectivités utilisent la commande publique pour dynamiser l'économie locale et soutenir l'activité sur les territoires. Ainsi, il serait pertinent d'inclure dans les appels d'offres une exigence stipulant que les opérateurs doivent être exemptés des règles extraterritoriales non européennes. Toutefois, tant qu'une masse critique d'acteurs européens ne soutient pas cette démarche, la mise en place effective de telles initiatives restera limitée. Ce principe est pourtant essentiel pour les territoires : les grands groupes internationaux comme Microsoft et Google, qui ne paient pas d'impôts sur les sociétés en France, n'apportent aucun retour direct aux territoires lorsqu'ils sont sollicités.

Pour autant, les collectivités territoriales ont besoin d'incitations et de soutiens réglementaires et législatifs au niveau national pour favoriser le développement de solutions alternatives. La question du financement est centrale, impliquant une réévaluation de la répartition des budgets (Capex/Opex) et des dotations de fonctionnement afin d'encourager l'innovation tout en respectant l'éthique et la réglementation en vigueur. Ainsi, il est impératif de définir une clé de répartition partagée entre la dotation globale de fonctionnement (DGF) destinée aux licences logicielles et l'investissement requis pour la transformation du système d'information.

LES RECOMMANDATIONS DE PHILIPPE LATOMBE :

1. Encourager les collectivités à **inclure des critères éthiques dès la phase de conception de leurs cahiers des charges**, afin de s'assurer que les technologies respectent les droits et libertés individuelles.

2. **Fixer des standards stricts pour les fournisseurs**, incluant la conformité aux principes éthiques relatifs à la protection de la vie privée.

3. **Instaurer systématiquement des mesures de traçabilité des accès aux systèmes**, via des logs et des registres, pour assurer une gestion transparente et responsable.
   - Possiblement, connecter directement les équipements de surveillance à un réseau filaire reliant les infrastructures locales aux autorités, comme les préfectures, afin d'assurer un contrôle optimal.

4. **A l'image du comité Vigouroux, mettre en place dans la mesure du possible un comité éthique** pour encadrer l'utilisation des technologies de surveillance, incluant des techniciens, des experts en sciences humaines et des fonctionnaires.

5. **Assurer que les données et les outils de surveillance restent sous un contrôle juridique strict** pour faciliter la responsabilité en cas de mauvaise utilisation :
   - **Privilégier l'utilisation de matériel fabriqué et localisé en France ou en Europe**, en évitant les équipements non européens susceptibles de présenter des vulnérabilités (solutions non soumises aux règles extraterritoriales) ;
   - **Favoriser le stockage de données en *on-premise*** pour garantir un contrôle accru
   - **Labelliser les solutions cloud européennes pour assurer sécurité et souveraineté**, en complément du SecNumCloud.

6. Sur le modèle des Etats-Unis, **renforcer la mise en œuvre de sanctions aux acteurs en cas de non-conformité** avec les réglementations en vigueur.

7. Mettre en place des incitations au niveau national pour aider les acteurs souverains à se protéger contre les règles extraterritoriales européennes :
   - **Réévaluer la répartition des budgets (Capex/Opex)**
   - **Revoir le partage des clés de dotation.**

> *« A L'INSTAR DES ETATS-UNIS, IL EST URGENT QUE LA FRANCE SE DOTE D'UNE VÉRITABLE POLITIQUE D'INCENTIVE FINANCIÈRE POUR SOUTENIR SES ACTEURS ÉCONOMIQUES*

Miroslav SVIEZENY,
Qarnot Computing

Allier calcul intensif et récupération de chaleur pour un cloud computing durable

Qarnot se distingue dans le cloud computing par une approche unique qui associe calcul intensif (HPC), efficacité énergétique et récupération de chaleur. Nous avons développé une plateforme cloud spécialement conçue pour les besoins de calcul intensif, comme ceux des entreprises d'ingénierie et d'aérospatial, qui réalisent des simulations de tests de conception de fusées ou d'avions. Désormais réalisées "in silico" (sur ordinateur), ces simulations gagnent en rapidité et en efficacité tout en requérant d'importantes ressources informatiques.
Notre autre spécificité repose sur un réseau de serveurs préconfigurés pour des logiciels de simulation, installés dans des lieux où leur chaleur est récupérée pour chauffer, par exemple, de grandes piscines,centres aquatiques. Ce modèle, qui récupère jusqu'à 95 % de l'énergie produite par les serveurs, permet un chauffage durable et économique, au bénéfice des collectivités.
Pour les grandes collectivités, notre solution offre un double avantage énergétique. D'abord, Qarnot prend en charge le déploiement des équipements, demandant seulement un engagement à long terme des collectivités pour acheter la chaleur récupérée, avec des prix fixes sur 20 ans, offrant une stabilité rare dans le secteur énergétique. Ensuite, ce partenariat fournit une alternative locale et économique pour les besoins en HPC des entreprises locales.

« Il y a encore beaucoup de déclaratif dans les engagements énergétiques des grandes entreprises technologiques »

Les grandes entreprises extra-territoriales annoncent souvent des bilans carbones neutres, mais la réalité inclut une grande part de compensation. Par exemple, certains géants se sont fait reprocher d'omettre, dans leurs calculs de PUE (Power Usage Effectiveness), l'impact environnemental lié à la consommation d'eau nécessaire au refroidissement des serveurs. Chez Qarnot, nous avons inversé cette logique en concevant l'équivalent d'une baie informatique qui non seulement refroidit, mais récupère la chaleur pour des besoins de chauffage local.
En Europe, il y a encore beaucoup de déclaratif dans les engagements énergétiques des grandes entreprises technologiques. Qarnot souhaite offrir une alternative qui limite réellement l'empreinte carbone et contribue à une consommation énergétique circulaire. Cela passe par un engagement fort pour la revalorisation des ressources énergétiques, car dans le secteur du calcul, le coût énergétique est un sujet prioritaire que l'on ne peut plus ignorer.

« Les opportunités offertes par des solutions alignées avec nos valeurs européennes sont considérables »

La souveraineté numérique est essentielle et repose sur deux éléments fondamentaux : les plateformes logicielles et les infrastructures matérielles. En matière de cloud computing souverain, Qarnot offre des serveurs et infrastructures hébergés sur le territoire français, loin des data centers des GAFAM. Nos installations permettent de garantir une indépendance vis-à-vis des acteurs américains, et d'éviter que nos infrastructures de calcul ne tombent sous juridiction étrangère, ce qui est crucial pour la confidentialité des données sensibles.
En effet, aux États-Unis, des lois permettent de récupérer toutes les données traitées dans des infrastructures américaines, même si elles sont situées hors de leur territoire. À court terme, ce risque n'est pas forcément visible, mais sur le long terme, il pourrait y

avoir des conséquences sérieuses. En France, on réfléchit souvent à court terme, ce qui nuit à une vision plus stratégique de la souveraineté numérique.
Les opportunités offertes par des solutions alignées avec nos valeurs européennes sont considérables. Non seulement elles renforcent notre indépendance en matière de données, mais elles créent aussi un écosystème de calcul haute performance local qui peut être mis à disposition des entreprises, universités et instituts de recherche.

« Il est urgent que la France se dote d'une agence type DARPA pour soutenir des acteurs économique locaux »

Le financement de l'innovation en Europe, surtout pour les infrastructures physiques, reste un vrai défi. En France, les investissements ont souvent privilégié le développement de logiciels, laissant un déficit en matière d'infrastructure. Par conséquent, des entreprises comme OVH ont dû se tourner vers des fonds américains pour lever le capital nécessaire à leur expansion. Ce manque de soutien empêche beaucoup de nos startups de se développer chez nous, alors même que le secteur éducatif et la recherche française sont parmi les meilleurs au monde pour l'émergence de nouvelles technologies.
Par ailleurs, aux États-Unis, les entreprises technologiques bénéficient souvent de commandes publiques qui leur permettent de croître plus rapidement et de se renforcer sur le marché. À l'inverse, chez Qarnot, notre part de commandes publiques reste proche de zéro, bien que nous soyons parfaitement certifiés et compétents pour les servir. Nous aurions pu travailler avec les centres de recherche, les universités, voire des institutions sanitaires pour fournir des solutions cloud certifiées HDS. Nos sites ont déjà des certifications HDS et nous avons entrepris le processus pour obtenir la certification SecNumCloud. Cependant, il faudrait une impulsion politique forte, avec des financements adaptés, pour donner aux acteurs locaux les moyens de répondre aux besoins de calcul intensif des secteurs publics et stratégiques français.
À cet égard, il est urgent que la France se dote d'une agence type DARPA pour soutenir des acteurs locaux comme Qarnot qui participent à l'innovation et à la sécurité numérique européenne.

LA DARPA, UN MODÈLE AMÉRICAIN DE SOUTIEN AUX ENTREPRISES À SUIVRE POUR L'EUROPE

La Defense Advanced Research Projects Agency (DARPA) est une agence américaine de recherche en défense, créée en 1958, qui finance et développe des technologies de pointe, à l'origine d'innovations majeures comme Internet et le GPS, les vaccins utilisant l'ARN messager, les drones ou encore des entreprises comme Space X.
Dotée d'un budget annuel de 3 milliards de dollars, elle fait figure de modèle pour l'écosystème européen par sa capacité à impulser des objectifs, financer des technologies de pointe et à transformer des projets de rupture en succès industriels structurants.
Malheureusement, l'Europe peine à suivre le rythme de l'innovation face aux États-Unis, avec des investissements privés dans l'innovation deux fois inférieurs et un budget de R&D ne dépassant pas 2 % de son PIB, bien en dessous des 3,5 % américains et de l'objectif européen de 3 %.
Pour autant, l'idée de créer une «DARPA européenne»* a été défendue à plusieurs reprises** par Emmanuel Macron et figure également parmi les 170 propositions remises à la Présidente de la Commission européenne par de Mario Draghi.

LES RECOMMANDATIONS DE MIROSLAV QARNOT :

1. **Sensibiliser les plus hauts niveaux de l'État à l'importance stratégique de développer des infrastructures françaises** afin de susciter un engagement fort.
2. **Stimuler l'investissement public et privé dans les technologies et les acteurs nationaux pour prévenir leur départ** à l'étranger, où ils trouvent un écosystème d'investissement plus favorable.
   - Offrir **des incitations fiscales attractives** pour les investisseurs privés qui soutiennent les entreprises locales dans le cloud computing.
   - **Créer une agence nationale inspirée de la DARPA américaine** qui a vu naître les grands acteurs technologiques actuels : Mettre en place une structure dédiée pour soutenir les acteurs locaux, offrant des financements adaptés via un guichet unique pour les infrastructures physiques notamment.
3. **Soutenir davantage les entreprises développant des solutions de calcul intensif.**
4. **Renforcer les aides aux entreprises qui adoptent des modèles énergétiques circulaires** et qui mettent en œuvre des solutions de récupération de chaleur.

*https://www.vie-publique.fr/files/rapport/pdf/280510.pdf
**https://www.elysee.fr/emmanuel-macron/2024/04/24/discours-sur-leurope

> ***GÉNÉRER DE LA DATA UTILE AU SERVICE DE BESOINS CONCRETS : C'EST AINSI QUE NOUS GAGNERONS LES COLLECTIVITÉS À LA CAUSE ÉTHIQUE ET SOUVERAINE***

Didier ARZ,
Directeur général des services, Morbihan Énergies

Anne EUSÈBE,
Cheffe de projet Territoire d'innovation

Notre rôle : faire en sorte que les collectivités se réapproprient leurs données

Notre projet territoires intelligents est construit autour du pilotage de la donnée pour renforcer la sobriété et l'efficacité énergétique des territoires. La démarche est complexe, car notre objectif n'est pas de servir Morbihan Énergies, mais bien les territoires eux-mêmes. Cela nécessite un discours clair et accessible car, au-delà des solutions techniques, il est essentiel que les équipes se comprennent pour assurer la transversalité de nos métiers.
Notre ambition est de faire en sorte que les élus territoriaux (re) prennent la main sur le pilotage de la donnée, en l'adaptant aux besoins de leur territoire.

Gagner l'adhésion des collectivités par une véritable plus-value en matière de service

Notre feuille de route a été élaborée en intégrant les services associés à nos métiers, tels que l'éclairage public, la production d'énergies renouvelables, la maîtrise de l'énergie et la gestion de réseaux. Pour enrichir notre approche, nous avons installé des capteurs permettant de récolter des données précieuses.
Nous avons pris le parti de partir des besoins concrets de chaque territoire, en commençant par définir précisément leurs attentes et cas d'usage. Notre mission n'est pas de créer de la donnée pour elle-même, mais de générer de la data utile et valorisable qui réponde à des besoins réels avec un niveau de service attractif et engageant pour les usagers. Par exemple, un village de 200 habitants n'aura pas nécessairement besoin d'une surveillance détaillée de la pollution émise par une route traversante, mais pourra en revanche s'intéresser à des données utiles pour la sécurité de ses résidents. Faire preuve d'éthique, c'est avant tout se mettre à la portée du client final, en privilégiant la transparence et l'agrégation d'outils tout en garantissant la sécurité de la chaîne de données, de sa collecte à sa valorisation.
Cette approche permet aux collectivités d'envisager notre démarche comme une vraie plus-value en termes de service. Notre succès repose sans doute sur cette vision, et nous sommes fiers d'incarner ce rôle de tiers de confiance.

Territoires d'innovation et capteurs de flux touristiques : des solutions à la fois éthiques et performantes

L'initiative Territoires d'Innovation illustre bien notre engagement en faveur de solutions à la fois éthiques et performantes. Sur l'Ile-aux-Moines, ainsi que dans d'autres secteurs voisins, nous avons mis en place un dispositif de capteurs permettant de recueillir des données anonymisées sur la fréquentation touristique. Ces informations, accessibles via une plateforme numérique, encouragent les visiteurs à privilégier les périodes de moindre affluence, profitant ainsi aux commerçants et aux acteurs locaux du tourisme. Cette approche de la gestion de données démontre notre attention à la protection de la vie privée, un enjeu de plus en plus sensible pour les usagers. Depuis le lancement du programme, initialement réticents, ceux-ci sont rassurés quant à la sécurité et la pertinence de la collecte de leurs données.
Cette évolution a été cruciale pour accompagner certaines collectivités qui, auparavant, utilisaient des systèmes de vidéosurveillance peu sécurisés, accessibles sur les téléphones portables des équipes.
Aujourd'hui, notre démarche proactive en matière de transparence et de protection permet aux collectivités d'aborder la transition numérique de manière sereine et conforme aux attentes actuelles.

Morbihan Teradata : Pour une maîtrise de toute la chaîne de traitement des données

Avec une plateforme IoT et des services d'Hypervision, il est essentiel pour nous de maîtriser toute la chaîne de traitement des données. Actuellement, nous explorons une stratégie d'externalisation du stockage des données. C'est dans cette optique que le projet Morbihan Teradata a été conçu : cet équipement vise à alléger la charge cognitive des maires tout en leur offrant une solution locale et souveraine. En intégrant l'externalisation du stockage dans une démarche durable, nous avançons en partenariat avec les communes pour envisager la création d'un data center dédié. Cette approche progressive nous permet de poser des fondations solides pour le futur du stockage souverain au service des territoires.

Interopérabilité, réversibilité et proximité : trois critères essentiels de notre commande publique

Dans le cadre de la rédaction de nos cahiers des charges pour le choix de nos prestataires, nous intégrons des clauses spécifiques, en particulier en matière environnementale et éthique. Nous exigeons, par exemple, une production locale des matériaux, des pratiques de recyclage, ainsi qu'une traçabilité des lieux de fabrication et des composants utilisés. Par ailleurs, la sécurité et la protection des données sont primordiales : nous demandons ainsi aux entreprises de nous fournir leur Politique de Sécurité des Systèmes d'Information (PSSI).
Nous insistons également sur l'importance de l'interopérabilité, et à ce titre, chaque prestataire doit se conformer à notre charte d'interopérabilité qui se traduit par des engagements de transparence, de réversibilité et de traçabilité des données.

Réinventer le financement des équipements pour un pilotage des données efficace et économique

Il est indispensable de repenser les modèles de financement au sein des collectivités. Aujourd'hui, certains marchés restent encore à développer, comme celui de la flexibilité, alors même que le pilotage, notamment des bâtiments, devient essentiel. Le problème, c'est que les offres des fournisseurs sont souvent construites avec un Capex faible et un Opex élevé, alors que les collectivités ont besoin exactement du contraire pour pouvoir maîtriser leurs budgets de fonctionnement.
L'objectif serait donc de trouver de nouveaux modèles de financement et de subvention qui permettraient de couvrir ces coûts. On le sait bien, les collectivités sont en pleine adaptation budgétaire et vont probablement devoir faire des coupes ici et là. Il est donc essentiel de proposer des solutions qui permettent de rendre ce pilotage viable sur le long terme.

LES RECOMMANDATIONS DE DIDIER ARZ :

1. **Encourager la réappropriation des données par les collectivités** : Permettre aux élus de piloter et d'adapter les données aux besoins spécifiques de leurs territoires en développant un langage commun pour faciliter la compréhension et la prise de décision.
2. Au-delà de l'approche par la donnée, **assurer une valeur ajoutée tangible pour les collectivités** : Construire des services intuitifs et utiles, générant des donnés facilement exploitables et valorisables pour renforcer la perception positive des territoires sur les nouvelles technologies.
3. **Privilégier des capteurs protecteurs de la vie privée pour une collecte de données éthique** : Installer des capteurs de comptage (piétons, parking) garants du privacy by design.
4. **Proposer une charte d'interopérabilité** : Construire une charte pour garantir la protection, le stockage, et la gestion sécurisée des données, permettant la transparence, la réversibilité, et la traçabilité.
5. **Repenser les modèles de financement en faveur du CAPEX** afin de répondre aux contraintes budgétaires des collectivités et soutenir le pilotage économique des équipements.
6. **Intégrer des critères éthiques et environnementaux dans la commande publique** : Insister sur la production locale, la recyclabilité des matériaux, et la sécurité des données dans le choix des prestataires.
7. **Explorer des solutions comme le stockage local des données**, via des partenariats avec les communes pour une infrastructure souveraine et durable, **telle que le projet Morbihan Teradata.**

PAS BESOIN DE NOUS FAIRE CONFIANCE : VERS PLUS DE DE TRAÇABILITÉ POUR EMBARQUER LES CITOYENS

Jean-Baptiste POLJAK,
UPCITI

Souveraineté numérique : concilier autonomie stratégique et ouverture technologique

La souveraineté numérique ne doit pas être confondue avec un protectionnisme strict ni une limitation aux seules solutions nationales. Elle consiste avant tout à garantir la capacité de contrôle sur les données, c'est-à-dire la possibilité de définir les modalités de stockage des données (emplacement, durée de conservation, etc.) et d'interrompre un service si nécessaire. Bien entendu, une attention particulière doit être portée aux lois extraterritoriales qui pourraient limiter cette indépendance. A mon sens, pour garantir une véritable autonomie, les infrastructures doivent être principalement à capital public ou français/ européen. Cependant, il est nécessaire de s'interroger sur la pertinence de ces critères en ce qui concerne les solutions qui permettent des couches logicielles indépendantes des infrastructures qui les hébergent.
Le défi est donc de construire un environnement numérique garantissant aux autorités un contrôle solide et pérenne, tout en évitant un protectionnisme excessif qui pourrait freiner par ailleurs la concurrence de nos entreprises à l'étranger, par réciprocité.

Éthique : La transparence comme clé du succès des projets numériques

L'éthique est fondamentale pour garantir la vie privée et la liberté des individus. Sans éthique, il n'y a pas de confiance, et sans confiance, la numérisation, essentielle pour simplifier les démarches administratives, sera ralentie. C'est donc selon moi au secteur public de la promouvoir. Pour se faire, la transparence est cruciale : il est de plus en plus important pour les citoyens de comprendre clairement quelles données sont utilisées, à quelles fins, et pendant combien de temps, afin qu'ils puissent participer sereinement. Par exemple, pour certains équipements IoT, nous avons installé des QR codes qui permettent aux citoyens de s'informer sur le fonctionnement et la gestion des données du dispositif. Cela a transformé la perception initiale négative du public envers ces installations, car les gens ont pu comprendre leur fonction réelle. L'exemple de l'application gouvernementale Stop Covid montre comment un manque de clarté a engendré une méfiance parmi les utilisateurs. Certains géants du numérique, comme Apple, informe, pour chaque application de l'App Store, quelles données sont collectées, témoignant d'une prise de conscience des enjeux commerciaux liés à la confiance des utilisateurs. Or, il est essentiel que le rôle de tiers de confiance ne soit pas dévolu à des entreprises privées, mais qu'il soit assumé par des entités publiques.

Plus de traçabilité pour embarquer les citoyens

De plus, la traçabilité des données est importante pour garantir la responsabilité dans leur gestion. Il est crucial de savoir qui a sollicité, consulté, modifié ou récupéré les données, tout comme il était impensable il y a quelques années de laisser un commerce photocopier une carte d'identité sans garanties appropriées.
Par exemple, j'aimerais beaucoup que le site Ameli permette de vérifier si mon dernier rapport médical a été consulté par des entités telles que les mutuelles ou les médecins, comment mes données sont utilisées ou si elles ont servi dans l'entraînement d'algorithmes, etc. Un autre exemple est celui de France Identité, où, malgré la véritable praticité de l'application, il y a un manque de transparence sur les types de données traitées et leur traitement. Le choix de définir par décret les modalités de certaines dispositions du projet de loi sur les Jeux Olympiques 2024, notamment en ce qui concerne l'utilisation de la vidéo algorithmique, ne contribue également pas à la confiance des citoyens.

Notre principe : « pas besoin de nous faire confiance » : des solutions protectrices « by design »

Upciti propose des capteurs d'analyse d'images, installés principalement sur les mâts d'éclairage public, qui fournissent aux services et applications de la ville intelligente des données sur le stationnement, le trafic, la fréquentation piétonne, la gestion des déchets et le bruit. Conçues selon le principe «privacy by design», nos solutions reposent sur une technologie volontairement limitée, qui empêche la collecte de données personnelles telles que le genre ou la couleur de peau, des informations dont nous n'avons pas besoin pour les services visés (par exemple, le comptage des places de parking). Ainsi, nous appliquons notre principe : « Pas besoin de nous faire confiance », puisque nos technologies sont techniquement conçues pour éviter toute dérive.
Par ailleurs, nous estimons que l'anonymisation à posteriori n'est réellement fiable que si elle est assurée en amont par un

organisme public garant des droits fondamentaux, comme le fait la ville d'Amsterdam avec ses algorithmes de floutage. Cette anonymisation doit intervenir avant toute transmission des données aux entreprises privées, car le risque d'abus reste trop grand pour ces acteurs.

Être conscient que nos données sont stratégiques pour les entreprises privées

Il faut bien être conscient que les données personnelles sont devenues si stratégiques que certaines entreprises finiront inévitablement par en abuser. Le fameux «je n'ai rien à cacher» ne justifie pas que nos vies deviennent transparentes pour autant. Par exemple, certaines sociétés de vidéosurveillance vendent déjà les plaques d'immatriculation aux compagnies d'assurance, ce qui pourrait permettre à celles-ci d'ajuster les primes en fonction des déplacements de chacun. Cette perte de contrôle sur ses propres données est bien réelle.
Les collectivités, quant à elles, ne vendraient jamais les données de leurs citoyens, mais elles risquent d'être perçues comme complices de ces dérives en raison de leurs partenariats avec certains prestataires peu scrupuleux.

Respecter le principe de proportionnalité selon les usages : distinguer RGPD et minimisation des données

Les collectivités sont de plus en plus sensibles aux enjeux de confidentialité, et en Europe, certaines villes imposent des audits stricts avant d'adopter de nouvelles technologies. C'est le cas de Stavanger en Finlande, qui a notamment exigé que nous détaillions strictement l'origine des données : proviennent-elles de sources internes ou de fournisseurs ? Sont-elles anonymisées ? Je précise qu'il ne s'agit pas d'un audit RGPD, qui se concentre sur le traitement des données personnelles. Ici, l'objectif est justement de prouver que nous minimisons le risque de traitement de ces données en appliquant le principe de proportionnalité de la CNIL et de la Charte de l'UE. Ces audits garantissent que les données personnelles ne sont ni inutilement collectées ni traitées.

L'importance d'une vision stratégique au niveau politique

Je pense qu'il n'est jamais trop tard pour bien faire et surtout ce type de changement de politique sur le numérique ne se fait pas en une semaine. Heureusement, il est possible (et préférable) d'y aller par étape, mais il faut avoir une idée très claire de l'objectif final. Tous les choix de solutions numériques, de développement, de choix d'infrastructure doivent être guidé par un fil directeur clair qui permettra de garantir la bonne articulation entre toutes les initiatives, passées et futures.
Il ne s'agit pas d'un sujet technique, il s'agit d'un sujet politique et il ne faut pas se laisser impressionner par l'apparente complexité, il faut faire des choix et s'assurer que ces choix guident chaque décision par la suite.
Se lancer dans ces sujets est une réponse concrète au manque de confiance des résidents sur les services numériques et les bénéfices liés à la transparence sur ces sujets dépassent très largement les efforts à y consacrer.

LES RECOMMANDATIONS DE JEAN-BAPTISTE POLJAK

1. **Vision politique : guider chaque choix technique et infrastructurel par une stratégie de souveraineté et de transparence claire.**

2. **Distinguer souveraineté et protectionnisme** en acceptant des technologies étrangères (ex : couches logicielles) dans le cadre d'infrastructures locales contrôlées, garantissant ainsi la sécurité sans isolation technologique.

3. **Garantir,** en revanche, **que les infrastructures numériques (serveurs, data centers, etc.) soient sous le contrôle de capitaux publics ou européens** pour éviter toute soumission aux lois extraterritoriales étrangères.

4. **Promouvoir l'éthique par la transparence et la traçabilité :**
   - **Informer clairement les citoyens sur les types de données collectées**, leur finalité, leur durée de conservation et leur localisation, afin d'encourager la confiance dans les services publics numériques.
   - **Déployer des outils d'information des citoyens** à travers des outils simples et visibles, comme des QR codes sur les équipements, pour expliquer l'utilisation des données et renforcer la perception de transparence.
   - **Mettre systématiquement en place des systèmes de traçabilité des données personnelles** permettant de suivre l'accès, les modifications, et les utilisations pour plus de transparence et de sécurité.

5. **Appliquer le principe de proportionnalité** (Charte de l'UE, RGDP) :
   - **Minimiser la collecte de données personnelles par défaut :** Développer des technologies «privacy by design» qui limitent automatiquement l'accès aux informations personnelles, afin d'éviter tout besoin de «confiance aveugle».
   - Dans le cadre des territoires intelligents : Adopter des capteurs et des algorithmes sans possibilité de reconnaissance des individus.

6. Lorsque nécessaire, **confier le processus d'anonymisation à des acteurs publics avant toute transmission à des entreprises privées**, comme le fait la ville d'Amsterdam.

7. **Établir des audits stricts de protection des données** pour évaluer les risques avant de travailler avec des technologies impliquant des données sensibles.

> *« IL FAUT UNE APPROCHE RESPONSABLE DE LA COLLECTE DES DONNÉES POUR UN NUMÉRIQUE AU SERVICE DE L'ENVIRONNEMENT ET DE LA SÉCURITÉ COLLECTIVE*

Jean-Christophe MIFSUD,
Président & CEO

Pierre QUINTARD,
Directeur du Développement Commercial ELLONA

L'intelligence situationnelle au service de la prévention et de la gestion des risques dans les territoires

Ellona est une entreprise spécialisée dans l'intelligence situationnelle qui développe des boîtiers innovants capables de s'adapter à divers environnements, qu'ils soient intérieurs ou extérieurs. Ces dispositifs sophistiqués permettent de capter un large éventail de variables, notamment les vibrations, les altercations, les sons, la lumière, les odeurs, les particules, ainsi que la qualité de l'air. L'objectif principal de ces capteurs est de fournir une compréhension approfondie de l'environnement, des situations délicates et des comportements humains afin de prévenir les risques potentiels.
Grâce à l'intégration de l'intelligence artificielle, les solutions d'Ellona offrent la possibilité de paramétrer des alertes en temps réel et de déclencher des actions de remédiation adaptées. Cette capacité à capter et analyser en temps réel les variables de notre écosystème (sons, odeurs, qualité de l'air, fumée, etc.) permet de fluidifier la prise de décision en apportant immédiatement les mesures adaptées à chaque situation.
Implantée originellement dans des zones stratégiques telles que les ports et les aéroports internationaux pour anticiper et prévenir divers risques, Ellona diversifie aujourd'hui l'utilisation de ses technologies en les déployant peu à peu dans l'espace public et en s'adaptant aux besoins des territoires.

Des solutions éthiques et respectueuses de la vie privée grâce à des capteurs sensoriels anonymisés « by design »

Par ses solutions, l'entreprise a à cœur de répondre aux enjeux d'un numérique éthique en développant des technologies au service de l'environnement et de la sécurité collective. De plus, grâce à l'intelligence situationnelle qu'elle propose, Ellona protège la vie privée, car elle ne procède pas à la captation d'images, mais utilise la détection des autres sens, garantissant ainsi une approche respectueuse et responsable de la collecte et de l'utilisation des données. Il est important de souligner qu'Ellona représente une solution franco-française dont les technologies fonctionnent au sein d'un data center souverain, assurant ainsi la sécurité et la maîtrise des données collectées tout en préservant la souveraineté numérique.

Des collaborations avec les territoires pour un environnement urbain plus sain : l'exemple de Toulouse Métropole

Ellona a récemment joué un rôle clé dans le succès du projet préliminaire de digitalisation de la ville de Toulouse, en contribuant à poser les bases d'un déploiement à plus grande échelle sur l'ensemble de l'agglomération, prévu pour les années 2025-2026. Le projet consiste notamment en un suivi rigoureux des émissions environnementales, avec pour objectif de réduire l'empreinte carbone. Les capteurs d'Ellona, enrichis par l'IA et des bases de données complètes (sons, odeurs, allergènes), permettent de détecter les événements susceptibles d'affecter la santé et la sécurité des citoyens. Ellona s'engage ainsi à accompagner les métropoles et municipalités dans la mise en place de politiques RSE efficaces.

Une entreprise face aux défis de l'accompagnement des scale-up technologiques

Aujourd'hui, un des principaux freins à l'essor des entreprises technologiques en France réside dans l'absence de fonds de scale-up véritablement adaptés aux besoins spécifiques des startups à fort potentiel. Si le pays est capable de soutenir l'amorçage de projets, il peine à accompagner leur montée en puissance, notamment dans les domaines de pointe qui requièrent des efforts R&D importants dans des délais courts afin de maintenir leur avance technologique. Cette lacune conduit de nombreuses entreprises à se tourner vers des marchés étrangers, comme les États-Unis ou

les Émirats, où des capacités financières plus importantes sont disponibles pour les entreprises à forts potentiels. Ce manque de soutien constitue un véritable défi pour la souveraineté numérique. Ellona, pionnière sur les données sensorielles, se confronte directement à ce défi. En effet, ces nouvelles données reposent sur des infrastructures technologiques encore perfectibles et des efforts continus doivent être menés pour maintenir son avance et s'affirmer comme l'acteur majeur d'un domaine en plein expansion, et ceci à l'échelle planétaire. Il faudrait revoir la philosophie derrière les investissements en France et davantage miser sur la confiance en nos entreprises ! D'ailleurs Ellona est implantée donc plus de 10 pays, dont à Singapour et au Japon où les exigences technologiques sont extrêmement pointues.

LES RECOMMANDATIONS DE JEAN-CHRISTOPHE MIFSUD ET PIERRE QUINTARD

1. **A l'image de l'intelligence situationnelle, développer des technologies respectueuses de la vie privée**, en particulier en utilisant quand cela est possible **des capteurs sensoriels anonymisés « by design »** (son, odeur, bruit), afin d'assurer la collecte de données sans recourir à la captation d'images parfois intrusive et peu utile.
2. **Revoir les mécanismes de soutien aux scale-up en France**, en particulier dans le secteur technologique, en créant des fonds et des structures adaptées pour accompagner la croissance des startups à fort potentiel, favoriser leur développement à l'échelle internationale et éviter la fuite à l'étranger de nos pépites.
3. **Accélérer la promotion de l'internationalisation des entreprises innovantes françaises.**

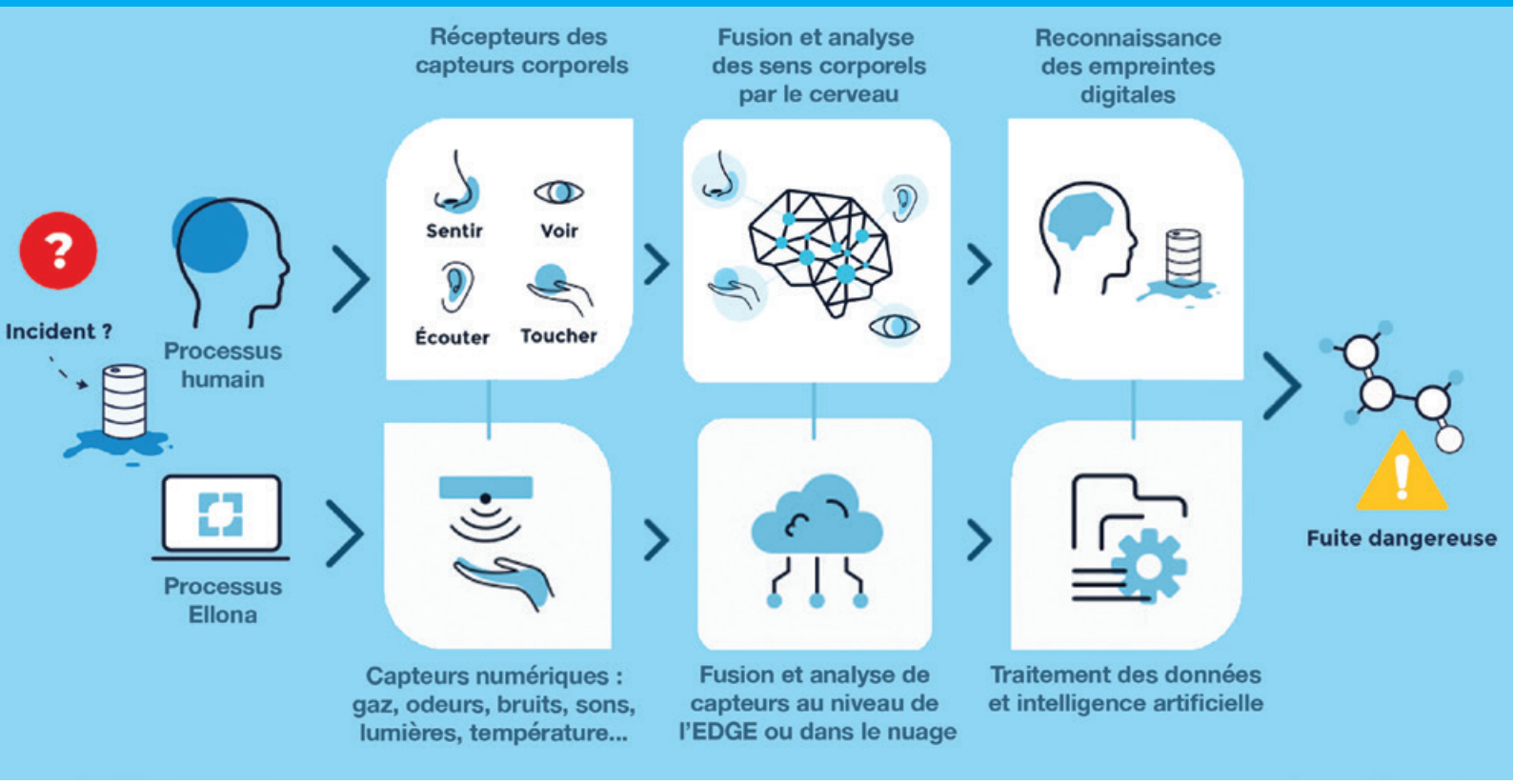
Quelles applications ?

Les secteurs dans lesquels la technologie d'Ellona peut s'implanter sont multiples :

- **Sites industriels**
- **Ports et aéroports**
- **Armement et sécurité**
- **Recyclage des déchets**
- **Traitement des eaux usées**
- **Construction**
- **Propreté**
- **Bureaux** (entreprises, écoles)

Ellona propose également de la fabrication sur mesure pour intégration dans vos solutions déjà existantes !

La numérisation des sens humains et de l'expertise professionnelle en faveur d'une intelligence environnementale avancée



2 - SOUVERAINETÉ NUMÉRIQUE

RETOUR SUR L'ATELIER DE TRAVAIL DU lundi 9 septembre 2024

Organisé par la FNCCR et le Club Numérique & Territoires sur le thème :

NUMÉRIQUE & TERRITOIRES : QUELLES STRATÉGIES ET LEVIERS POUR RENFORCER L'ADOPTION DE SOLUTIONS GARANTISSANT LA SOUVERAINETÉ DES DONNÉES ?

INTRODUCTION DE JEAN-LUC SALLABERRY

« Notre démarche se concentre avant tout sur la souveraineté des données, qu'elles soient territoriales ou sectorielles. Dès qu'elles sont géolocalisables, ces données entrent dans une dimension nationale, soulevant des défis politiques et techniques cruciaux, particulièrement dans le cadre de la directive européenne NIS 2 et des initiatives en cybersécurité. Pour garantir un environnement numérique sécurisé et souverain, il est impératif de construire des systèmes robustes qui protègent les informations sensibles des territoires, de l'État, des hôpitaux et des entreprises. Cette souveraineté est primordiale pour les TPE et PME, acteurs clés de l'économie locale, qui, en pleine croissance, nécessitent des protections spécifiques adaptées aux risques cyber. Les grandes entreprises, bien que mieux armées, ne sont pas exemptes de risques, ce qui souligne l'importance d'un écosystème national solide. Pour la FNCCR, cet enjeu est devenu prioritaire, car si les services publics ont longtemps été la première préoccupation, le développement économique relève également de la responsabilité des collectivités. L'objectif est donc double : assurer une protection optimale des données et développer un écosystème national fiable. En ce sens, notre atelier vise à identifier ensemble les besoins spécifiques des collectivités, valoriser les initiatives existantes et aider les élus dans leurs choix de partenaires.

POURQUOI SE TOURNER VERS UN NUMÉRIQUE GARANT DE NOTRE SOUVERAINETÉ NUMÉRIQUE ?

La souveraineté numérique est un objectif ambitieux et crucial, reposant sur deux piliers : l'autonomie stratégique et le développement d'un écosystème économique national et européen capable de rivaliser avec les grandes entreprises extraterritoriales, tant en Europe qu'à l'international. L'autonomie stratégique implique avant tout le contrôle des données, garantissant la maîtrise et la protection de nos informations sensibles ou non. Pour y parvenir, il est essentiel de disposer d'infrastructures assurant l'indépendance et la sécurité des réseaux et systèmes. L'utilisation de logiciels doit également être pensée pour favoriser l'autonomie technologique et la résilience face aux menaces extérieures.

Maîtrise des données face aux menaces de réquisition extraterritoriales

Ainsi, la souveraineté numérique implique que les collectivités conservent un contrôle total sur leurs données, à l'abri de toute législation extraterritoriale, notamment le Cloud Act américain, qui permet aujourd'hui à des autorités étrangères d'accéder à des informations stratégiques. Ce point est essentiel pour

LISTE DES PARTICIPANTS

ACTEURS PUBLICS

Cécile CHABRELE, *Cheffe de projet Développement numérique territorial, Mairie du Lamentin*
Pascal CHEVALLOT, *Ingénieur développement de services mutualisés pour la transition numérique, SYANE (Syndicat des Énergies et de l'Aménagement numérique de la Haute-Savoie)*
Helena LAOUISSET-ROYER, *collaboratrice de* **Pascal SAVOLDELLI**, *Sénateur du Val-de-Marne*
Fabrice LÉRIQUE, *Chargé de mission Transition numérique, Régions Hauts-de-France*
Marc LOUIS-MARIE, *Référent RGPD, Mairie du Lamentin*
Gabriela MARTIN, *Directrice, Open Data France*
Arnaud MERCIER, *Conseiller Numérique, Politique publique de la donnée, Innovation, et Parcours usager, Métropole Aix-Marseille-Provence*
Philippe PORTAL, *Administrateur général chargé de mission auprès de la Directrice, Direction des entreprises et partenariats de sécurité et des armes - Ministère de l'Intérieur*
Magali ROGER, *Chargée de mission Innovation sociale et Médiation numérique, MEL (Métropole Européenne de Lille)*
Bertrand SERP, *Vice-président transition digitale, Toulouse Métropole*
Jonathan SIDGWICK, *Directeur SIG, Communauté d'agglomération du Grand Montauban*
Louis TONDEUR, *Chargé de mission aménagement numérique, MEL (Métropole Européenne de Lille)*

ACTEURS ECONOMIQUES

Fabrice COUPRIE, *Président, Mediomatrix*
Laurent DAUDE, *Président, Groupe B.Conseil*
Jean-Baptiste POLJAK, *Président, UPCITI*
Pierre QUINTARD, *Ellona*
Nicolas SAINTHERANT, *Directeur innovation, Qarnot Computing*

L'EQUIPE ORGANISATRICE

Jean-Luc SALLABERY, *Chef du Département Numérique, FNCCR*
Linda SISSI, Déléguée, *Club Numérique & Territoires, Com'Publics*
Guillaume METIVIER, *Délégué collectivités Mobilités – énergies, Com'Publics*
Claire GUIBAUD, *Assistante, département numérique, FNCCR*

garantir que les données sensibles restent sous la juridiction nationale, renforçant ainsi la protection de la confidentialité et l'autonomie des collectivités. Les participants s'accordent sur l'importance du choix d'un data center souverain, public ou privé, dont la définition va bien au-delà de la localisation en territoire national ou européen (voir plus bas).

Le cloud et la couche logicielle : des vulnérabilités peu prises en compte

Certains intervenants ont souligné que la gestion de l'infrastructure seule ne suffit pas à garantir la souveraineté des données. La couche logicielle joue un rôle tout aussi crucial. De nombreuses collectivités utilisent encore des solutions comme Office 365, ce qui les prive du contrôle total sur leurs données. De plus, des changements récents dans les conditions d'utilisation de plateformes comme Adobe soulignent cette vulnérabilité. En effet, Adobe a modifié ses conditions pour permettre l'exploitation commerciale ou de renseignement de tout contenu crée sur ses plateformes cloud, sans offrir d'autres options aux utilisateurs, ce qui renforce la nécessité d'une maîtrise totale des outils et des données.

FISA, PATRIOT ACT, PRIVACY SHIELD, DATA PRIVACY FRAMEWORK… OÙ EN EST-ON DU CADRE LÉGAL DE TRANSFERT DE DONNÉES ENTRE L'UE ET LES ETATS-UNIS ?

Les relations entre les États-Unis et l'Union européenne concernant la protection des données ont été marquées par des tensions autour des lois américaines telles que le **FISA** (1978) et le **Patriot Act** (2001), qui permettent une surveillance accrue, y compris de citoyens étrangers, au nom de la sécurité nationale. Pour encadrer les transferts de données, les accords **Safe Harbor** (2000-2015) et **Privacy Shield** (2016-2020) ont été successivement mis en place, mais tous deux ont été invalidés par la Cour de justice de l'Union européenne* notamment à travers l'arrêt dit Schrems II (2020) en raison de préoccupations sur les pratiques de surveillance américaines, jugées intrusive et incompatibles avec le RGPD. En 2023, l'**EU-U.S. Data Privacy Framework** a été négocié pour garantir un niveau de protection plus élevé et inclure des mécanismes de recours, bien que des questions de conformité subsistent.

LES FREINS A LEVER POUR UNE TRANSITION ACCELERÉE VERS UN NUMERIQUE SOUVERAIN AU SEIN DES COLLECTIVITÉS

Disparités dans la gestion des enjeux de données et de cybersécurité selon les collectivités : un constat partagé

Les niveaux de compréhension et de sensibilisation à la souveraineté numérique varient grandement, même parmi les villes et syndicats qui collaborent régulièrement avec des experts. Cette diversité de maturité face aux enjeux numériques ne dépend pas nécessairement de la taille des collectivités : ainsi, certaines grandes collectivités montrent peu d'intérêt pour ces questions, tandis que certaines plus petites s'impliquent activement.
Pour autant, les collectivités, quelle que soit leur taille, sont parfois amenées à sous-estimer ces enjeux, même pour des données considérées comme étant de moindre envergure comme celles liées au trafic, qui, pourtant, si elles sont exposées, peuvent révéler des informations sensibles.

La sensibilisation de toute la chaîne humaine : la clé de la souveraineté numérique

Le facteur humain se révèle ici crucial : si la technologie apporte des solutions, elle nécessite d'être accompagnée par une sensibilisation appropriée. Toute la chaîne humaine en lien avec ces données doit être concernée : collectivités et pouvoirs publics, administrés et entreprises.
La prise de conscience des risques est essentielle pour accompagner toute stratégie de cybersécurité et pallier le décalage générationnel, parfois marqué, dans la compréhension des enjeux numériques. Les simulations de cybersécurité montrent également que l'utilisateur final demeure souvent le maillon faible, par exemple lorsqu'il clique sur des liens ou pièces jointes piégés. Si l'infaillibilité est impossible, renforcer les protections à ce niveau peut limiter les risques d'exposition. Des formations continues semblent à propos. Il faut changer de paradigme, la sécurité de nos données est un enjeu durable et en constante mutation de la vie des collectivités au 21ème siècle !

Interopérabilité, réversibilité et proximité : trois critères essentiels de notre commande NIS 2 : Une opportunité de repenser le dialogue entre l'État et les collectivités

Si la défense et la sécurité intérieure bénéficient d'une vigilance accrue de la part de l'État, d'autres secteurs restent en retrait. En effet, aujourd'hui, l'État ne considère pas toujours cette priorité dans les secteurs de l'éducation, de l'environnement et de la santé, où les marchés publics peuvent surprendre les observateurs sensibilisés aux enjeux de souveraineté (l'exemple de l'attribution de l'hébergement des données du Health Data Hub à un acteur extraterritorial est parlant).
Il est regrettable qu'un cloisonnement existe entre l'État et les collectivités, moins sensibilisées à cette urgence. La directive NIS 2, en élargissant le périmètre de sécurité à de nouveaux services publics essentiels, offre une opportunité de repenser cette souveraineté de manière globale et d'harmoniser les cadres de protection.

La difficiles résistance à l'influence des grands acteurs

La résistance face à l'influence des grands acteurs technologiques constitue un défi important pour certaines collectivités, soucieuses de préserver leur autonomie numérique. Pour autant, certaines administrations choisissent, par exemple, de ne pas adopter les

* https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue

dernières solutions de grandes entreprises comme Office 365, préférant rester sur des versions antérieures malgré les défis que cela implique.
Dans le secteur privé, la situation est similaire, en particulier pour les startups, souvent attirées par des crédits cloud offerts par des acteurs majeurs, ce qui les rend progressivement dépendantes des infrastructures et services de ces fournisseurs, principalement américains. Bien que des lois comme la SREN[1] tentent de limiter ces dépendances pour renforcer la souveraineté numérique, les enjeux restent présents. Pour surmonter cette pression, il est essentiel de tracer des lignes claires sur les limites de la souveraineté numérique et d'identifier les opportunités qui permettraient aux collectivités et entreprises de renforcer leur indépendance technologique.

Une ambition de souveraineté freinée par un manque de repères

Les collectivités manifestent une volonté croissante de renforcer leur souveraineté numérique, mais elles manquent souvent d'informations claires sur les actions à entreprendre pour y parvenir. L'enjeu principal pour elles reste de trouver des prestataires en adéquation avec leurs exigences de souveraineté, un défi majeur dans un contexte de dépendance aux solutions externalisées. Certains intervenants ont pu constater un manque de contrôle sur certaines acquisitions logicielles, qui échappent même parfois à leur Direction des Systèmes d'Information (DSI) lors de décisions décentralisées.

Décalage temporel entre les besoins et le rythme administratif

Les collectivités, confrontées à un manque d'alignement entre leur rythme administratif et celui des prestataires, peinent à suivre le rythme d'évolution des solutions technologiques, notamment pour des mairies qui, dans un contexte insulaire, sont confrontées à des contraintes supplémentaires. Cette discordance temporelle limite ainsi la capacité à progresser efficacement vers une transformation numérique cohérente et adaptée aux réalités locales.

Pour une approche progressive afin d'embarquer les collectivités de toutes tailles

Une approche progressive est essentielle pour accompagner les collectivités de toutes tailles vers une souveraineté numérique accrue. Souvent contraintes par des obligations de mise aux normes et des ressources limitées, notamment les plus petites, elles ont déjà consenti de nombreux efforts d'adaptation. Une démarche par étapes leur permettrait ainsi d'avancer concrètement sans s'enfermer dans des choix qui pourraient limiter leurs évolutions futures.
Dans ce contexte, il est également recommandé de ne pas rejeter systématiquement les solutions étrangères, comme celles de Microsoft, qui restent profondément intégrées dans les systèmes bureautiques des collectivités. De nombreux agents ont été formés sur ces outils, rendant un changement de système complexe et parfois source de résistance. L'adoption de nouvelles solutions doit donc se faire progressivement, en tenant compte de ces réalités, pour garantir une transition harmonieuse et faciliter l'appropriation des nouvelles pratiques.

RELEVER LE DÉFI DU FINANCEMENT

Relever le défi de la transition numérique souveraine sans dépendre des subventions de l'État

Face aux contraintes budgétaires actuelles, l'État est confronté à des coupes budgétaires complexes. Dans ce contexte, il devient essentiel que les collectivités apprennent à fonctionner sans dépendre des financements étatiques. Cette situation exige une évolution culturelle : il est temps de privilégier une organisation autonome et de renforcer les collaborations locales. La mutualisation peut également apporter une solution, notamment au niveau territorial, comme les départements et les intercommunalités, qui peuvent ainsi partager infrastructures, ressources humaines et techniques. Cette démarche collaborative permettrait aux collectivités de bénéficier d'un accompagnement efficace et adapté aux nouvelles exigences réglementaires, tout en optimisant les coûts et les ressources disponibles.
Bien que difficile à instaurer, cette approche d'autosuffisance pourrait permettre aux collectivités de surpasser les normes et pratiques de l'État en matière d'efficacité.

CE QUE L'ÉLECTION DE DONALD TRUMP POURRAIT CHANGER POUR NOS ENTREPRISES

L'élection de Donald Trump pourrait avoir plusieurs répercussions sur l'industrie technologique européenne. Son approche protectionniste, visant à augmenter les droits de douane et à réduire les relations commerciales internationales, pourrait perturber les chaînes d'approvisionnement mondiales, en particulier celles liées aux semi-conducteurs, et nuire à l'accès de nos technologies sur le sol américain. Le ministre délégué chargé de l'Europe, Benjamin Haddad*, a d'ailleurs souligné la nécessité pour l'Europe de se préparer à des échanges potentiellement tendus avec les États-Unis et à défendre ses intérêts avec détermination.
Dans ce contexte, la pression croissante pour une autonomie stratégique européenne pourrait inciter les pays de l'UE à accélérer leurs efforts d'indépendance notamment en accroissant les investissements dans l'IA et dans des secteurs stratégiques comme le quantique (où les États-Unis dominent).
Benjamin Haddad a ainsi plaidé en faveur de la mise en œuvre du rapport Draghi**, qui recommande d'investir dans la réindustrialisation, une DARPA européenne et d'unifier les marchés de capitaux pour achever le marché unique. Cette approche renforcerait selon lui la compétitivité européenne et donnerait aux entreprises du continent les moyens de rivaliser avec leurs homologues américains, tout en préservant un cadre régulatoire robuste face à des figures comme Elon Musk, récemment nommé Ministre de l'efficacité gouvernementale dans la prochaine administration Trump.

1 https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/

* https://www.radiofrance.fr/franceinter/podcasts/l-invite-de-7h50/l-invite-de-7h50-du-mercredi-06-novembre-2024-2994423
**https://sgae.gouv.fr/sites/SGAE/accueil/a-propos-du-sgae/actualites/mario-draghi-remet-son-rapport-s.html

LE LEVIER ESSENTIEL DE LA COMMANDE PUBLIQUE : QUEL CLAUSIER POUR GARANTIR UN NUMERIQUE SOUVERAIN ? PARTAGE D'EXPERIENCE ET BRAINSTORMING

LE CLOUD ACT (2018) : UN POINT DE TENSION ENTRE L'UE ET LES ETATS-UNIS

Le Cloud Act (Clarifying Lawful Overseas Use of Data Act)*, en vigueur depuis mars 2018, autorise les autorités américaines à exiger des entreprises basées aux États-Unis qu'elles fournissent des données qu'elles stockent, y compris sur des serveurs à l'étranger, dans le cadre d'enquêtes criminelles. Cette législation crée des tensions en Europe, car elle contraint les entreprises américaines à transmettre des données même lorsqu'elles sont protégées par des normes européennes**.

La création d'un clausier intégrant des critères de souveraineté dans les marchés publics structurerait les appels d'offres autour de critères clairs, renforçant ainsi l'indépendance technologique des collectivités.

Hébergement des données : datacenters souverains / cloud, réversibilité et nature des capitaux

L'hébergement souverain des données sur des datacenters nationaux ou européens constitue un pilier essentiel de la souveraineté numérique. Mais comment s'assurer de leur « souveraineté », à savoir la maîtrise totale des données, la réduction de la dépendance à des solutions étrangères et l'imperméabilité aux lois extraterritoriales ?
Il faut d'abord avoir à l'esprit que selon les besoins et les ressources, les collectivités peuvent faire le choix d'un data centre public internalisé qui permet de garantir cette souveraineté, ou d'un data centre privé. Dans ce cas, les critères de sélection sont plus complexes.
La question de la localisation en territoires européens est évidement un préalable, mais elle ne suffit pas. Au-delà du SecNumCloud, qui est déjà un très bon indicateur, il faudrait idéalement se tourner vers une infrastructure dont on a la garantie qu'elle a été financée par des fonds nationaux ou européens.
Autres critères importants : ceux de la réversibilité et de l'interopérabilité dès le sourcing. Cela permet de choisir des solutions transitoires, conformes partiellement au départ mais évolutives, afin d'éviter des impasses technologiques et de garantir une flexibilité maximale tout en permettant une concurrence saine dans les achats publics.

Données essentielles et directive NIS 2

La transposition de la directive NIS 2 marque une avancée cruciale dans le renforcement de la cybersécurité et de la souveraineté des collectivités, en élargissant la qualification de «données essentielles» à un périmètre plus vaste de données traitées localement comme celles relatives à la santé, aux PMI, ou encore aux archives départementales. La directive impacte également des secteurs stratégiques tels que l'eau, l'énergie, les réseaux de chaleur, et les télécommunications. Elle va également obliger de nouveaux acteurs, y compris certains opérateurs de télécommunications et délégataires de la fibre optique, à se soumettre à des obligations de cybersécurité accrues.
Cette approche soulève une question centrale de souveraineté critique : il est indispensable de s'assurer que ces données essentielles restent sous un contrôle européen, voire français, pour protéger les infrastructures stratégiques. La tendance à externaliser les systèmes d'information, avec certaines données hébergées par des prestataires de services publics (DSP) dans des datacenters à l'étranger, amplifie ces enjeux. Des clauses de souveraineté visant à maintenir le contrôle de ces données critiques deviennent donc nécessaires dans les appels d'offres pour protéger les intérêts nationaux.

Le diable se cache dans les détails : vigilance sur l'accès à internet

Pour tous, la souveraineté numérique se joue souvent dans les détails. Même si une solution couvre 90 % des besoins, les 10 % restants peuvent représenter des vulnérabilités significatives. Par exemple, certaines couches de logiciels même installés localement, nécessitent un accès à Internet, ce qui limite l'indépendance totale. C'est pourquoi certains participants préconisent des solutions logicielles développées par des acteurs locaux. Pour autant, d'autres estiment que l'enjeu principal réside dans les infrastructures, le traitement des données via logiciel étant considéré comme peu stratégique. Ils s'accordent tous sur le fait que ce à quoi il faut être principalement attentif est le cloud : un prestataire SecNumCloud à minima (bien qu'il autorise 39% de capitaux extra-européens[5]). Mais là encore, si la solution est locale et détenue par des fonds français ou européens, le risque est encore réduit.

SYNTHÈSE : CRITÈRES CLÉS POUR UN NUMÉRIQUE SOUVERAIN

1. **Infrastructure :** Hébergement en Europe, indépendance vis-à-vis des lois extraterritoriales, capitaux européens, et maintien d'un écosystème concurrentiel, interopérabilité, réversibilité.
2. **Logiciels / Cloud : Certification SecNumCloud à minima,** entreprise et capitaux européens, interopérabilité, réversibilité.
3. **En cas de prestataires extra-européens :** Garantir la maîtrise du stockage et l'accès aux données, imposer des critères de réversibilité

3 https://www.senat.fr/rap/r19-007-1/r19-007-11.pdf
4 https://www.bercynumerique.finances.gouv.fr/cloud-act-le-royaume-uni-et-les-etats-unis-vont-partager-les-donnees-de-leurs-citoyens
5 https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf
*https://www.senat.fr/rap/r19-007-1/r19-007-11.pdf
** https://www.bercynumerique.finances.gouv.fr/cloud-act-le-royaume-uni-et-les-etats-unis-vont-partager-les-donnees-de-leurs-citoyens

SOUTENIR NOS ACTEURS ÉCONOMIQUES

Protectionnisme versus souveraineté : ne pas porter préjudice à nos champions du numérique à l'international

Pour autant, certains intervenants estiment qu'il est important de ne pas restreindre la souveraineté numérique à des solutions strictement européennes, car la capacité d'une technologie à satisfaire des critères de sécurité et de souveraineté ne dépend pas uniquement de son origine géographique. L'important est de maîtriser le stockage et l'accès aux données tout en garantissant une infrastructure souveraine et flexible, permettant de répondre aux exigences locales.
En effet, il s'agirait de ne pas partir en guerre contre des marchés qui tendent parfois les bras aux acteurs européens du numérique. La recherche de la réciprocité en matière de concurrence saine constitue le fil conducteur de la vision de certains intervenants.

Un modèle stratégique et exportable pour l'international

La souveraineté numérique est également perçue comme un levier stratégique pour les entreprises françaises par les intervenants. En adoptant un modèle distinct des États-Unis ou de la Chine, qui privilégie la sécurisation et la durabilité plutôt que la simple rentabilité, les entreprises françaises peuvent s'implanter durablement à l'international. Par exemple, l'adaptation de solutions souveraines aux exigences locales d'autres pays (comme en Arabie Saoudite) montre le potentiel de ce modèle français dans les marchés émergents.

Pérennité des PME et mutualisation

Pour garantir l'inclusion des TPE-PME dans les marchés publics, les intervenants encouragent la mutualisation de petites entreprises, favorisant ainsi leur compétitivité face aux grands groupes. Pour assurer la fiabilité de ces regroupements, une structure de coordination – comme une « tête de pont » – pourrait jouer un rôle clé, en renforçant l'efficacité des solutions proposées tout en inspirant confiance aux collectivités.

LES RECOMMANDATIONS DES INTERVENANTS :

1 Faire le choix d'infrastructures souveraines
- Localisés en Europe, pour garantir une maîtrise des données et réduire les dépendances aux lois extraterritoriales.
- Exiger des garanties pour assurer la sécurité et l'interopérabilité des solutions de stockage de données.
  A noter : La certification SecNumCloud est un premier gage de sécurité mais, selon certains intervenants, ne constitue pas pour autant l'Alfa et l'Omega car elle permet une part minimale de capitaux extra-européens.
- Privilégier l'utilisation d'infrastructures supportées par des capitaux exclusivement européens.
- S'assurer de la réversibilité des solutions pour permettre des transitions sans blocage.

2 Encourager l'utilisation de logiciels souverains :
- Éviter les solutions qui limitent le contrôle des données, comme certaines plateformes cloud qui réservent des droits d'utilisation des contenus (e.g., Adobe).
- Favoriser des logiciels développés par des acteurs locaux pour une maîtrise complète de la couche logicielle, réduisant les vulnérabilités liées à l'accès à Internet.

3 Harmoniser la cybersécurité à travers la directive NIS 2 :
- Anticiper les nouvelles exigences de cybersécurité et de souveraineté liées à l'élargissement de la qualification de «données essentielles» à certaines données traitées quotidiennement au sein des collectivités de toutes nature : archives, eau, énergie, transports…
- S'assurer qu'elles restent sous hébergement national ou européen.

4 Améliorer la sensibilisation à tous les niveaux :
- Mettre en place des formations continues et des simulations pour renforcer la prise de conscience des risques parmi tous les acteurs (collectivités, entreprises, citoyens).
- Engager une communication efficace pour surmonter le manque d'intérêt de certaines collectivités envers les enjeux numériques critiques.

5 Faciliter la transition numérique avec une approche progressive :
- Adopter une stratégie par étapes pour soutenir les collectivités de toutes tailles, en particulier les plus petites, afin d'éviter les choix bloquants et de garantir une adaptation en douceur aux nouvelles exigences.
- Ne pas exclure systématiquement les solutions non-européennes, mais garantir leur conformité avec des critères de souveraineté et de flexibilité / réversibilité.

6 Créer un modèle exportable et compétitif :
- Encourager les entreprises françaises à se démarquer sur le marché international en valorisant la sécurité et la durabilité de leurs solutions souveraines, adaptées aux exigences locales d'autres pays.
- Favoriser la mutualisation des PME pour qu'elles puissent rivaliser avec les grands groupes sur les marchés publics et renforcer leur pérennité par des collaborations territoriales.

7 Indépendance financière des collectivités :
- Promouvoir des initiatives d'autofinancement et de mutualisation au sein des collectivités pour réduire la dépendance aux subventions de l'État, notamment en mutualisant infrastructures et ressources entre départements et intercommunalités.

LE CONTEXTE

La FNCCR et le Club Numérique & Territoires de Com'Publics ont entrepris la rédaction d'un guide destiné aux collectivités territoriales afin de les accompagner dans le choix de leurs solutions technologiques.
Notre démarche repose sur **trois piliers principaux : la souveraineté numérique** (autonomie stratégique, développement d'un véritable écosystème compétitif pour les acteurs français et européens, etc.), **la protection des libertés individuelles** (solutions garantes « by design » de la vie privée et des données personnelles), et **la cybersécurité**, avec une attention complémentaire aux enjeux de **numérique responsable**.

Ainsi, notre guide poursuit trois ambitions principales :

- **Sensibiliser les élus territoriaux et nationaux** aux enjeux d'un numérique éthique, souverain, sûr et responsable (dangers et opportunités).
- **Proposer des critères clairs pour mieux identifier les solutions éthiques, souveraines et sures**, portées notamment par les TPE/PME, incluant des recommandations concrètes et des cas pratiques.
- **Valoriser les collectivités et acteurs économiques** ayant fait le choix de solutions de confiance à travers des témoignages.

Les travaux de ce guide s'articulent autour de **trois à quatre ateliers de travail coanimés avec la FNCCR**, ainsi que d'une **série d'entretiens semi-directifs mettant en valeur la vision et les solutions portées par ses contributeurs.**

Patrick CHAIZE,
Sénateur de l'Ain,
Président de l'AVICCA,
Vice-président
de la FNCCR

Garantir la souveraineté numérique à tous les échelons : un véritable choix politique

La souveraineté numérique est une notion complexe s'articulant autour de plusieurs axes : les infrastructures, les usages et la sécurité des données. Il convient en particulier de considérer les matériels actifs installés sur les réseaux qui constituent un point de fragilité car ils ne sont actuellement plus construits par des fabricants européens. Donc nous dépendons de la Chine ou des États-Unis. En termes d'usage, nous réutilisons un certain nombre de processus sur lesquels nous n'avons pas la main. Nous devrions pouvoir garantir la souveraineté de nos infrastructures et des processus, notamment par un label.
Il est ainsi nécessaire de faire des choix volontaires en matière de sécurité. Or, les utilisateurs, y compris des collectivités territoriales, peuvent être confrontés à un dilemme politique : privilégier la sécurité et la souveraineté, ce qui, en l'état actuel des choses, peut engendrer des contraintes financières et de disponibilité, ou accepter le risque d'une perte de souveraineté. Cette éventuelle perte pourrait être durable, car un engrenage se créerait. Si nous ne nous posons pas la question aujourd'hui, le développement de systèmes souverains n'aura pas lieu, faute de demande, et nous serons débordés.

Les limites de la sécurisation de nos infrastructures : un enjeu d'impulsion au plus haut niveau

L'État a démontré sa capacité à sécuriser ses propres data centers pour des sujets critiques, comme la Défense, mais elle n'est pas systématiquement étendue à l'ensemble des données stratégiques, comme celles de la santé. Ainsi, le ministère de la Santé s'appuie sur une solution extraterritoriale pour l'hébergement de la plateforme des données de santé Health Data Hub. Selon ses responsables, le basculement vers un autre produit nécessiterait un coût de transition trop élevé. Pourtant, plus le temps passe, et moins il est simple de procéder à une modification en faveur de solutions plus souveraines. Ce constat met en lumière l'urgence d'une action proactive avant qu'il ne soit trop tard.

Embarquer toutes les parties prenantes dans une vision partagée

Les débats autour de la loi visant à sécuriser et réguler l'espace numérique (SREN) ont permis de mener des travaux concrets. Le Sénat s'attache à porter la souveraineté numérique à son plus haut niveau, mais se heurte à certaines limites, notamment politiques. Le véritable enjeu réside dans le fait que ces discussions demeurent confinées au cercle des experts, ce qui freine la prise de conscience collective. Trop souvent, les préoccupations liées

à la sécurité ou souveraineté numériques sont perçues comme exagérées par les collègues, alors qu'une fois le problème apparu, il est souvent trop tard. Telegram, à travers son manque de coopération affirmée sur des enquêtes policières et judiciaires liées à l'exploitation d'enfants en ligne, illustre bien cette situation. Une vulgarisation accrue est donc nécessaire pour rendre ces enjeux accessibles à tous.
Un exemple frappant est celui des collectivités locales : il y a un an, environ la moitié des communes françaises utilisaient encore des adresses Wanadoo sans protection. Des efforts ont été initiés pour leur fournir des solutions de cybersécurité, mais sans suivi suffisant en raison d'un manque de sensibilisation. Les collectivités locales, également engagées dans des activités économiques, devraient s'approprier cette approche. Par ailleurs, il existe une véritable demande de la part des TPE et des PME pour un lien plus étroit avec l'État et les collectivités, beaucoup étant demandeuses d'un accompagnement plus actif de la part de Bercy ou de l'ANSSI.

Collectivités territoriales : Quels leviers pour une commande publique éthique, souveraine et sûre ?

La commande publique constitue un levier essentiel pour renforcer la compétitivité des acteurs européens et nationaux, notamment les TPE/PME, face aux concurrents américains et européens. Cependant, en France, cette commande est sous-utilisée, atteignant seulement 30 %, contre 60 % en Allemagne. Pour remédier à cette situation, il est crucial d'activer plusieurs leviers.
Tout d'abord, les collectivités doivent se poser la question de la localisation et de l'utilisation de leurs données, car l'indépendance géographique, technologique et financière est primordiale. Il sera toujours plus simple de négocier l'obtention d'un code avec une entreprise plus locale, car les discussions seraient directes par exemple, chose difficile avec les grands acteurs extraterritoriaux.
Mais comment faire ? Il est en premier lieu possible de mobiliser le levier de l'empreinte environnementale, mais ce sujet peut être subjectif et encore difficilement mesurable.

Afin d'encourager plus globalement l'accélération d'un écosystème privé plus local, les appels d'offre importants pourraient notamment encourager davantage la création de groupements d'acteurs français, comme cela se fait dans le secteur du BTP, afin de créer une synergie face aux grands acteurs. En parallèle, pourquoi ne pas privilégier les entreprises qui mettent leur code à disposition, garantissant ainsi l'indépendance des collectivités en cas de défaillance d'un fournisseur ? En effet, une disposition du code des marchés publics stipule qu'en cas d'investissements conséquents ou de continuité dans les investissements, il est possible d'inclure des clauses de dépôt de code source dans un tiers lieu garanti. J'ignore néanmoins si les sociétés américaines s'y plient. Cette clause pourrait donc être favorable à une entreprise plus locale.

Commande publique : Quelles priorités au niveau national ?

Au niveau national, la présence d'une garantie de marché me semble nécessaire pour motiver les investissements sur le secteur. Une décision politique ferme sur ce sujet permettrait sans aucun doute de générer des investissements. En outre, il est impératif que l'Europe, et la France en particulier, développent leurs compétences en intelligence économique pour protéger les TPE et PME, souvent plus vulnérables que les grands groupes. Enfin, et c'est tout le sens des discussions autour de la transposition en cours de la directive européenne dite NIS 2, la classification des données selon leur valeur et leur sensibilité peut s'avérer un enjeu stratégique. Un des objectifs majeurs de la mesure est d'identifier les services essentiels ainsi que les données qui leur sont associées. Cette démarche permettra non seulement de mieux sécuriser les informations critiques, mais également d'accélérer l'adoption de solutions numériques plus souveraines, en garantissant que les données « essentielles » soient traitées avec le niveau de protection requis.

LES RECOMMANDATIONS DE PATRICK CHAIZE :

1. Établir un choix politique clair en matière de sécurité des données.
2. En complément du SecNumCloud, proposer un système de labellisation dédié afin de garantir la souveraineté des infrastructures et des différents processus utilisés.
3. S'appuyer sur la transposition de NIS 2 pour identifier les services essentiels et les données qui leur sont associées afin de leur garantir un plus haut niveau de sécurisation et ainsi favoriser des solutions plus souveraines.
4. Promouvoir une sensibilisation collective sur les enjeux de la souveraineté numérique à tous les niveaux (UE, État, collectivités) pour faciliter des échanges et des discussions plus larges au-delà du cercle des experts.
5. Activer les leviers de la commande publique pour renforcer la compétitivité des acteurs locaux, nationaux et européens face aux concurrents, dans les appels d'offres publics notamment :
   - Mobiliser le levier de l'empreinte environnementale.
   - Promouvoir la création de groupements d'acteurs français pour répondre à de gros appels d'offres.
   - Intégrer des clauses de dépôt de code source dans les marchés publics pour garantir l'indépendance des collectivités en cas de défaillance d'un fournisseur.
   - Motiver les investissements par une garantie de marché.
   - Développer les compétences des collectivités et des entreprises en intelligence économique.

> *« LA PROCHAINE TRANSPOSITION DE LA DIRECTIVE NIS2 CONSTITUERA UN VÉRITABLE DÉFI POUR LES COLLECTIVITÉS*

Gaëtan PONCELIN de RAUCOURT,
Sous-Directeur Stratégie de l'ANSSI

Quelle est votre définition du numérique éthique, souverain et sûr ?

Si ce n'est pas un objectif assigné l'action de l'ANSSI, par substance, participe néanmoins d'un numérique éthique.
Nous évoluons dans un monde où plus la société et l'économie se numérisent, plus elles s'exposent aux risques inhérents à ces technologies. Dans ce contexte, la mission principale de l'agence, en tant qu'autorité nationale de cybersécurité et de cyberdéfense, est de construire et d'organiser la protection de la Nation face aux cyberattaques.
A ce titre, elle agit afin de s'assurer que nous gardions en main des atouts essentiels tels que, parmi d'autres, la maîtrise des technologies et des compétences ou le levier réglementaire afin de sécuriser notre économie et notre société dans le respect des droits fondamentaux et des libertés publiques.

Quels liens faites-vous entre souveraineté numérique et cybersécurité ?

Il y a quelque chose de consubstantiel entre l'un et l'autre car la souveraineté numérique de la Nation est intrinsèquement liée à sa capacité à se protéger et à être résiliente face à la menace cyber, quelles que soient sa forme et son origine.
Ces menaces évoluent et s'intensifient. L'ANSSI a vu le nombre des incidents significatifs augmenter de 30 % l'an passé et la courbe ne fléchit pas en 2024. Les menaces stratégiques s'étendent désormais à la chaîne de valeurs, où se trouvent prestataires et sous-traitants. Et les menaces systémiques, à caractère criminel ou activiste, affectent de plus en plus d'entités sensibles tels que les hôpitaux, les médias, les acteurs du domaine social, l'enseignement supérieur et la recherche, les entreprises et les collectivités territoriales.
L'ANSSI adresse ainsi de nombreux secteurs d'activités régulés et s'apprête à étendre son champ d'action auprès des collectivités et des moyennes entreprises.
Car la cybersécurité est un pilier essentiel de la souveraineté numérique. Il n'y a ni durabilité ni confiance dans les systèmes d'informations et les usages numériques sans la sécurité et la résilience de ces derniers.

Quels sont, selon vous, les risques associés à l'utilisation de solutions qui protègent insuffisamment les libertés individuelles, la souveraineté et la sécurité des données ? L'ANSSI apporte-t-elle des solutions ?

L'une des actions de l'ANSSI est de favoriser le développement d'une offre de confiance.

Celle-ci se fonde sur l'évaluation de la robustesse des solutions face aux cyberattaques les plus courantes.
Une évolution notable est l'adoption de lois extraterritoriales, qui imposent aux entreprises soumises à cette juridiction de transmettre à leurs autorités les données de leurs clients.
Dans ce contexte, l'ANSSI a notamment fait évoluer son référentiel « SecNumCloud », qui permet d'identifier des offres de confiance assurant une protection face à ces lois et qui comprend aujourd'hui un premier vivier d'offres.
Cette présomption de sécurité est un élément important à l'heure où certaines collectivités territoriales se posent légitimement la question du stockage de leurs données.
Ce n'est d'ailleurs pas un hasard si l'ANSSI a conduit un travail conjoint avec la CNIL sur ce référentiel.

Dans ce contexte quels sont les enjeux pour les collectivités territoriales ?

Pour l'autorité nationale, l'enjeu est d'adapter la réponse en matière de cyberdéfense à une massification des attaques à laquelle n'échappent pas les communes, les intercommunalités ni les syndicats territoriaux qui assument des missions parfois très sensibles comme celles liées, par exemple, à l'adduction et la distribution de l'eau potable.
Et les compromissions des systèmes d'information n'affectent pas que les grandes entités car, désormais, il ne s'agit plus d'être une cible pour devenir une victime.
La future loi « Résilience » vise, dans son volet cybersécurité, à renforcer le niveau de maturité des tissus économique et administratif.
18 secteurs d'activité seront concernés, dont les collectivités territoriales en fonction de leur statut et certains de leurs établissements en fonction de la sensibilité de leurs activités.
C'est un temps fort pour l'agence que de préparer et d'accompagner ce changement d'échelle qui concerne les grands acteurs territoriaux, sachant de surcroît qu'ils ne partent pas tous du même degré de maturité en matière de cybersécurité.

Disposez-vous d'une vision des freins et des accélérateurs de cette montée en maturité ?

Dans le cadre des derniers plans de relance de l'État, l'ANSSI s'est vu confier des moyens pour accompagner les parcours de cybersécurité de plus de 700 collectivités volontaires. On trouve dans leurs rangs les plus importantes démographiquement mais aussi des communautés de communes et quelques communes.
C'est un laboratoire exceptionnel pour l'agence et une source d'informations inédites sur la manière dont les collectivités abordent leur montée en maturité cyber, les différentes marches techniques, l'implication des agents et, peut-être le plus décisif, l'engagement des gouvernances de ces collectivités dans la définition et la mise en œuvre de ces parcours.
Nous étudions actuellement les résultats de cette campagne d'envergure nationale à l'heure où près de 2 500 collectivités, établissements de coopération et syndicats techniques s'apprêtent à devenir des entités régulées au titre de la directive NIS2.
Je n'ignore pas que pour répondre à cette exigence de sécurité au sein des collectivités, disposer de collaborateurs formés, de prestataires qualifiés et en nombre suffisants ou d'opérateurs publics de services numériques est une des clefs de la réussite. L'action des campus cyber régionaux ou encore des centres régionaux de réponses aux incidents dans le développement des écosystèmes cyber territorialisés constituent une première réponse engageante pour l'avenir.

> *« NOUS PROPOSONS DES SOLUTIONS DE SENSIBILISATION ACCESSIBLES POUR LES COLLECTIVITÉS*

Séverine REYNAUD,
Vice-présidente Numérique, département de la Loire

La transformation numérique des collectivités soulève des enjeux cruciaux de souveraineté. Le Schéma Directeur d'Aménagement Numérique (SDAN) du département de la Loire établit un cadre essentiel pour cette transition, visant à optimiser les services publics tout en garantissant la maîtrise des données et la sécurité des infrastructures. Cette approche permet aux élus et aux services de mieux comprendre les défis technologiques actuels et de développer des solutions éthiques et souveraines adaptées aux besoins locaux.

Un SDAN au profil des transitions énergétiques et sociales

Le SDAN, établi en 2015, a permis à notre territoire d'être reconnu comme un espace connecté, intelligent et durable, dans le cadre de France 2030. Notre principal objectif est de déployer à grande échelle des expérimentations innovantes dans des domaines tels que l'éclairage public intelligent et la gestion de l'eau, en exploitant les infrastructures existantes, notamment la fibre optique professionnelle. Nous nous engageons également à répondre aux défis liés au vieillissement de la population et aux revenus modestes des habitants, ce qui nécessite la mise en place de solutions visant à réduire les charges énergétiques des logements sociaux.
Pour ce faire, nous avons établi des partenariats avec des startups locales, telles qu'URBS, qui offrent un soutien essentiel à la prise de décision. Parallèlement, la société QARNOT, avec ses chaudières numériques, contribue de manière significative à l'optimisation énergétique des bâtiments. Ces initiatives témoignent de notre volonté de développer des solutions durables et adaptées aux besoins spécifiques de notre territoire.

Un Hyperviseur en local pour plus de souveraineté et de sécurité

Le département de la Loire a pris la décision stratégique de créer son propre hyperviseur afin d'assurer la maîtrise de ses données, en dépit des offres attrayantes émises par de grands opérateurs, qui semblaient particulièrement intéressés par l'exploitation des données du territoire. Dans le cadre de la révision du SDAN en 2022, qui comprend 16 fiches actions, une attention particulière a été accordée à la gestion des données et des data centers. Des sondages ont été réalisés pour identifier les besoins des communes en matière de services numériques. Deux pistes de développement de data centers ont été envisagées : un data center public avec des espaces disponibles et un data center du Groupe Casino. L'objectif est d'exploiter ces deux infrastructures pour garantir une maîtrise optimale des données locales.
Parallèlement, le réseau LOTIM, qui est en délégation de service public jusqu'en juillet 2025, sera repris en régie personnalisée par le département, permettant ainsi de conserver le contrôle sur ses opérations et de générer des recettes qui seront réinvesties dans des services à haute valeur ajoutée pour les collectivités. Ce choix privilégie une approche locale, efficace et durable, en favorisant la proximité des prestataires et le partage vertueux des données relatives aux bâtiments.
Un autre enjeu majeur est notre refus du modèle américain en matière d'intelligence artificielle (IA), qui repose sur une collecte massive de données. Pour le département, la protection des données personnelles est primordiale, en particulier dans un contexte de solidarité humaine. C'est pourquoi nous favorisons la recherche d'entreprises locales ou nationales qui, bien que moins avancées, offrent des solutions d'IA moins énergivores et mieux adaptées aux besoins spécifiques des collectivités, contrairement à des plateformes comme ChatGPT. L'IA doit être orientée par des

besoins clairement définis, et les élus doivent établir des limites, car, à l'instar du clonage, il est essentiel de tracer des frontières claires quant à ce qui peut être réalisé.
En intégrant des acteurs locaux et en mettant l'accent sur les besoins spécifiques de notre territoire, nous veillons à ce que la transformation numérique profite véritablement à l'ensemble de la population, tout en préservant notre souveraineté.

Une ambition forte : Faire des collectivités des actrices proactives de leur transformation numérique

La transformation numérique des collectivités constitue désormais une priorité stratégique, soutenue par la Direction des Systèmes d'Information (DSI) et la Direction de la Transformation Numérique (DTN). Nos échanges avec les collectivités mettent en évidence l'importance cruciale de l'acculturation des élus et des services aux enjeux liés aux données et à la souveraineté numérique. En l'absence d'une compréhension adéquate de ces problématiques, les collectivités risquent de se retrouver mal préparées à évoluer dans un environnement numérique complexe.
Elles sont confrontées à des défis majeurs, notamment en matière de cybersécurité. Pour faire face à ces défis, nous avons initié des expérimentations en partenariat avec des entreprises locales innovantes telles que Serenicity. Ces initiatives ont conduit à un déploiement sur les 323 communes volontaires et au SDIS, financé par l'ANSSI dans le cadre de l'appel à projet «Dispositif d'acquisition de produits et licences mutualisés pour les collectivités territoriales» et par le département de la Loire, offrant ainsi une gratuité pendant trois ans.
Notre système, incluant un observatoire dédié, permet de suivre les cyberattaques, et la visualisation des attaques bloquées constitue un outil clé pour sensibiliser les acteurs locaux à l'importance d'une cybersécurité préventive. Nous organisons également des sessions d'information pour expliquer les terminologies et les enjeux associés. Il est essentiel que le message soit clair et accessible, afin d'éviter toute résistance à l'adoption de ces technologies.
En définitive, notre approche vise à garantir que les collectivités ne se contentent pas d'être de simples réceptacles technologiques, mais qu'elles deviennent des actrices engagées et autonomes de leur transformation numérique, prenant ainsi le contrôle de leur avenir numérique sans dépendre de modèles externes.

LES RECOMMANDATIONS DE SÉVERINE REYNAUD :

1. **Proposer des solutions de sensibilisation accessibles et peu coûteuses pour les collectivités**
   - Mettre en place des observatoires pour suivre et visualiser en temps réel le blocage des cyberattaques, afin de sensibiliser les collectivités aux menaces numériques et à la cybersécurité préventive.
   - Organiser des sessions d'information régulières pour expliquer de manière claire les terminologies, les enjeux de la souveraineté numérique et les risques liés à la gestion des données.

2. Sur le modèle des initiatives en matière de cybersécurité, lancer des programmes de **formation et des actions de sensibilisation spécialement dédiés à la souveraineté numérique**, permettant aux collectivités locales de mieux comprendre l'importance de cet enjeu stratégique et les dangers liés à la dépendance numérique.

3. **Encourager le recours à des entreprises locales ou nationales** qui offrent des solutions technologiques moins énergivores et plus adaptées aux besoins spécifiques des collectivités territoriales, afin de promouvoir un numérique éthique et durable.

4. **Favoriser la création et l'utilisation de data centers locaux, publics ou privés**, pour garantir la souveraineté des données et offrir des services numériques sur mesure, adaptés aux besoins des collectivités et en adéquation avec les exigences de sécurité et de protection des données.

5. Mieux accompagner les collectivités dans la mise en place de solutions leur permettant de gérer elles-mêmes leurs infrastructures numériques et leurs données, pour éviter la dépendance à des prestataires extérieurs et renforcer leur résilience face aux menaces numériques.

6. Lors des appels d'offres publics, **intégrer des critères environnementaux, éthiques et souverains**, afin de sélectionner des partenaires technologiques qui partagent les mêmes valeurs de transparence, sécurité et durabilité.

Fabrice COUPRIE,
Advanced MedioMatrix

> ***« PROTECTION DES DONNÉES VIA DES DATA CENTERS SOUVERAINS : UNE PRIORITÉ STRATÉGIQUE DE SÉCURITÉ MAIS AUSSI DE CONFIANCE***

Rétablir protection et concurrence équitable face aux GAFAM

La souveraineté numérique est, en effet, devenue absolument essentielle pour protéger nos droits et nos libertés individuelles, ainsi que pour garantir la confidentialité de nos données personnelles. En pratique, cela signifie que nous devons assurer un contrôle français – ou au minimum européen – sur nos données et nos infrastructures. Que ce soit en termes de localisation des données ou de leur financement, ce contrôle est indispensable pour préserver l'indépendance, la sécurité et la résilience de nos systèmes, surtout face aux cyberattaques de plus en plus fréquentes.
Pour atteindre cet objectif, il est également primordial que nos institutions travaillent à rétablir des conditions de concurrence plus équitables face aux géants technologiques, les GAFAM. Leur position dominante limite souvent l'accès des entreprises européennes à des marchés publics majeurs et à des canaux de distribution comme l'UGAP, ce qui freine notre innovation locale.

Data centres souverains et durables : Deux exemples de partenariat fructueux avec des collectivités territoriales

Après 24 ans d'expérience dans la Défense, spécialisé dans la sécurisation des données, j'ai intégré le groupe Abalone en 2014 avant de lancer Advanced MedioMatrix pour proposer un hébergement de données de proximité, fiable, sûr et adapté via un data centre à Metz. Nous ne cessons de grandir depuis.
Dans ce cadre, nous avons récemment déployé une solution d'hébergement pour une plateforme de gestion des données urbaines pour une grande métropole de la région Grand-Est. Ce projet a notamment impliqué la mise en place d'une solution Cloud, le renforcement de la gestion des accès, ainsi qu'une solution de sauvegarde. En externalisant l'hébergement dans notre data centre de confiance, cette métropole a pu réduire ses investissements en infrastructure et optimiser sa consommation énergétique. Notre architecture redondante assure la continuité de service sans coupures d'électricité ni interruptions de réseau, ce qui garantit une meilleure qualité de service pour les administrés, tout en assurant une stricte conformité aux normes de protection des données.
Par ailleurs, nous hébergeons également la vidéosurveillance de communautés de communes. Grâce à une solution de cloud privé, ces données sont centralisées, sécurisées, et leur gestion est facilitée pour les différentes mairies impliquées. L'externalisation de ce type d'hébergement permet de réduire les coûts tout en garantissant un haut niveau de protection pour ces images sensibles.
Nous nous engageons également à assurer une veille constante sur les vulnérabilités (en lien avec le CERT et l'ANSSI), ce qui nous permet d'appliquer rapidement les mises à jour de sécurité nécessaires.

Aiguiller les collectivités vers les bonnes solutions et les bons prestataires

Les collectivités sont responsables des données qu'elles collectent. C'est une priorité stratégique aujourd'hui, pour une question de sécurité évidemment, mais aussi de confiance ! Du choix de leur hébergement dépendra aussi leur résilience face aux cybermenaces. Il est crucial de ne pas attendre une crise (via une attaque cyber) pour agir, mais de prendre des mesures proactives pour sécuriser leurs espaces numériques.
La création de vrais labels de confiance et de transparence pourrait être un premier pas.
Ils permettraient aux collectivités d'identifier plus facilement les fournisseurs offrant des solutions souveraines et éthiques en matière de numérique, là où les entreprises plus connues et influentes ne le sont pas toujours (GAFAM).
Une simplification administrative pourrait aussi permettre un accès plus simple des TPE et PME à la commande publique : abaissement des seuils d'appel d'offres, référencement plus simple à l'UGAP. Ce sont actuellement de véritables freins à l'accès aux marchés publics.
Enfin, pourquoi ne pas imaginer de nouveaux mécanismes de financements, comme le partage des coûts entre CAPEX et OPEX, pour permettre aux collectivités de mieux gérer ces investissements, qui peuvent être lourds.

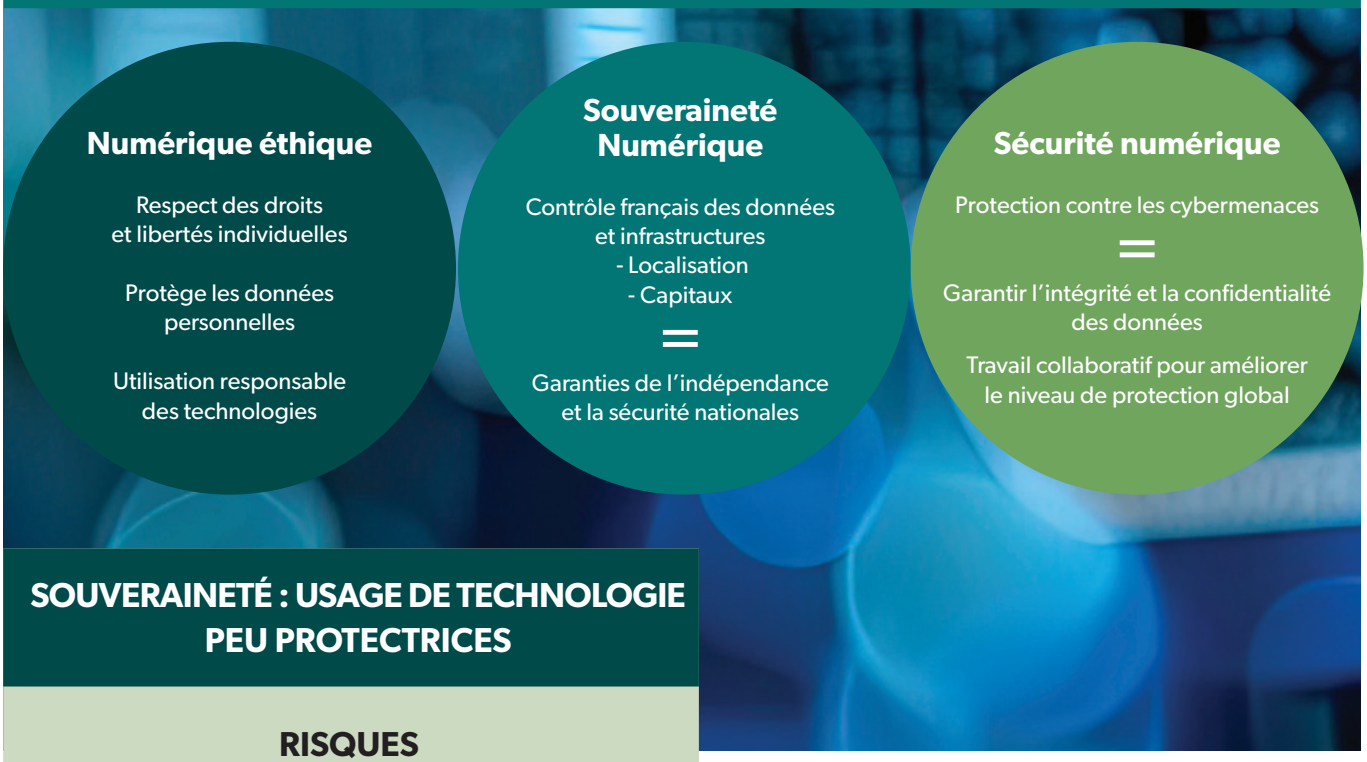
Transposition de NIS2 en cours : Les collectivités auront besoin de soutien pour mieux protéger leurs données

On peut légitimement se poser la question de la nécessité d'imposer une directive pour que des données essentielles soient mieux protéger. Pour autant, l'application de NIS2 permettra de mieux protéger les infrastructures critiques et de garantir la continuité des services publics. Oui, cette directive va imposer des obligations de sécurité accrues, et cela est d'autant plus pertinent pour les collectivités à mon sens : elles gèrent des données sensibles et des services essentiels pour les citoyens. Les collectivités auront besoin de soutien pour se conformer aux exigences tout en conservant une efficacité opérationnelle.

LES RECOMMANDATIONS DE FABRICE COUPRIE :

1. Promouvoir un contrôle français (ou européen) des données et des infrastructures en insistant notamment sur l'origine de leur financement et leur localisation.
2. Créer des labels permettant aux collectivités de repérer facilement les prestataires de solutions numériques souveraines et éthiques.
3. Réduire les seuils d'appels d'offres et simplifier le référencement à l'UGAP pour favoriser la commande publique auprès des petites et moyennes entreprises françaises.
4. Mettre en place des mécanismes de financement, par exemple via un partage des coûts entre CAPEX et OPEX, pour aider les collectivités à gérer les investissements nécessaires pour sécuriser leurs infrastructures.
5. Fournir un accompagnement accru pour aider les collectivités à se conformer aux obligations de sécurité de la directive NIS2.

MIEUX COMPRENDRE LE NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR



SOUVERAINETÉ : USAGE DE TECHNOLOGIE PEU PROTECTRICES

RISQUES

- Vol/perte/utilisation frauduleuse de données personnelles (divers exemples dans l'actualité)
- ingérence extra-territoriale, application de règlementations qui ne protègent pas les données personnelles
- Absence de contrôle et de transparence

CONSÉQUENCES

- Perte de confiance des utilisateurs
- Perte d'indépendance nationale
- Possibles abus de pouvoir et de pratiques discriminatoires

DONNÉES CLÉS SUR MEDIOMATRIX

Advanced MedioMatrix propose des solutions de data centres souverains hautement sécurisés :

- Une multitude de certifications stratégiques : **Tier 3** (Sur les **270 data centers** en France, seulement 4 détiennent cette certification), **ISO 50001, 14001, 9001, 27001 et HDS**.
- **Signataire du programme Data Center Neutral** (pour une consommation électrique moins énergivore et transparente) et **du Code of Conduct des data centers de l'UE.**
- Un data centre **détenu à 100% par des fonds européens**. Il fait partie des 5-6 data centres dans ce cas en France.
- **Un ancien militaire en charge de la sécurisation des données** de la Défense à la tête de l'entreprise.

« *LA DONNÉE QUESTIONNE NOS VALEURS FONDAMENTALES ET NOTRE AUTONOMIE STRATÉGIQUE. QUELLE SOCIÉTÉ VOULONS-NOUS CONSTRUIRE ?*

Catherine MORIN-DESAILLY,
Sénatrice de la Seine-Maritime, Membre du collège CNIL

L'essor du numérique questionne nos valeurs fondamentales : prendre la mesure de ce qui se joue

Le numérique n'a pas fini de transformer le monde. Il impacte l'ensemble de l'activité humaine, modifie nos façons de communiquer et de s'informer, de travailler, de commercer et de nous distraire, bouleversant même notre vision du monde. C'est une innovation de rupture qui pose quantité de défis : économiques et culturels, juridiques et politiques, sociaux et démocratiques. L'Internet est devenu le nouveau terrain d'affrontement mondial pour la domination du monde par l'économie et la connaissance, donc un espace d'hyper vulnérabilité, théâtre de cyber attaques en tous genre et de plus en plus sophistiquées.
Les menaces sont aujourd'hui aussi importantes que la perspective de progrès. L'IA nous fait prendre conscience que, selon les usages, les nouvelles technologies peuvent porter atteinte à nos libertés. La question est de savoir si le progrès continuera à servir l'homme ou s'il l'asservira : l'humain restera-t-il au cœur de ces transformations ou deviendra-t-il l'esclave d'algorithmes qui décideront de tout pour lui. C'est ainsi que doit se poser la question d'un numérique éthique et de confiance.
A la notion de numérique éthique doit s'ajouter la notion d'un numérique durable. En effet, les technologies consomment beaucoup d'énergie et contribuent donc aux émissions de gaz à effet de serre. Nos choix technologiques doivent ainsi faire l'objet de questionnements responsables face au défi du changement climatique.

Attention à ne pas confondre protectionnisme et autonomie stratégique

Nos démocraties européennes reposent sur une certaine idée de l'homme et le respect d'un certain nombre de fondamentaux. Entre le néo-libéralisme américain à la solde des big tech, détenues par une élite technologique qui veut imposer sa vision du monde, et l'autoritarisme étatique de la Chine avec son modèle de crédit social, il y a la place pour un autre modèle humaniste européen. Se pose alors la question de notre souveraineté numérique. Il ne s'agit pas de protectionnisme, mais comme pour les questions de défense, de souveraineté alimentaire ou encore pour les médicaments, d'autonomie stratégique. Pour cela, il est crucial que nous nous libérions de nos dépendances technologies, servant les seuls intérêts d'entreprises monopolistiques menaçant à terme nos propres modèles culturels, économiques et politiques.
La stratégie de ces acteurs aujourd'hui plus puissants que les états nations est claire : éradiquer toute forme de concurrence et préempter un marché en plein développement, celui du cloud (informatique en nuage) et de l'IA.
Leur capacité de lobbying et de séduction est immense, entretenant le dénigrement de nos propres entreprises, que nos gouvernements n'ont pas su assez soutenir et promouvoir ces quinze dernières années. Par exemple pourquoi systématiquement avoir recours aux trois mêmes « fournisseurs d'informatique en nuage » Google, AWS et Microsoft pour l'hébergement et le traitement des données de nos administrations y compris les plus sensibles et stratégiques ?
J'ai toujours plaidé pour un Small Business Act, ou un buy European act, permettant d'orienter la commande publique, dans le respect des règles de concurrence, vers nos propres entreprises certifiées Secnumcloud et garantissant la protection de nos données. C'est ce que font les Américains, les Russes et les Chinois ! Il est regrettable que nous continuions de donner une forme de monopole à des acteurs économiques qui ne paient pas ou peu d'impôts en Europe plutôt que de valoriser des consortiums locaux. Il aura fallu un énorme travail de pression de quelques parlementaires pour que la circulaire sur la doctrine d'utilisation de l'informatique en nuage par l'État soit finalement signée et envoyée à chaque ministère, et ce pour rappeler qu'il est des données sensibles qui nécessitent un niveau de protection stratégique. Jusqu'alors, aucune instruction ministérielle n'était en place sur ces sujets.

La donnée, c'est l'or noir du numérique

Si par le passé la manne mondiale était le pétrole, aujourd'hui, c'est la donnée qui crée la richesse. Elle est donc devenue un actif stratégique majeur qui conditionne le développement de l'économie, donc de l'emploi. Protéger nos données c'est aussi assurer notre sécurité. Ce n'est pas un hasard si les cyberattaques envers les établissements de santé ou établissements publics se multiplient, derrière celles-ci il y a des ingérences étrangères qui visent à nous affaiblir.
Heureusement, il existe des autorités administratives indépendantes de contrôle, comme la CNIL, l'ANSSI ou encore des services spécialisés de gendarmerie, présents sur tous les territoires. Certaines régions ont mis en place des CSIRT. Aujourd'hui; tous ces acteurs publics comme privés travaillent à structurer la réponse à la menace cyber. En effet la synergie entre tous est indispensable tant la menace est devenue hybride et sophistiquée. La directive NIS 2 bientôt transposée en droit français devrait apporter des réponses aux entreprises et administrations.

Les collectivités territoriales en première ligne

Toute notre administration est aujourd'hui dématérialisée, les collectivités territoriales, de la plus grande entité, la région, à la plus petite entité communale, ont dû et doivent continuer à s'adapter. Les plus petites collectivités, disposant de peu de moyens sont en premier ligne face aux cyberattaques. Dans leur cas, les conséquences tant pour les administrations que pour les administrés sont très préjudiciables (interruption voire blocages des services, perte ou violation des données, perte de recettes financières…)
Pour anticiper ou résoudre ces crises, il y un fort besoin d'acculturation des élus et des agents territoriaux. En 2018,

déjà, mon rapport « Reprendre en main notre destin numérique l'urgence de la formation » recommandait que la montée en compétence de tous soit déclarée grande cause nationale. Selon une étude de cybermalveillance.gouv.fr, 64% des élus et des agents des communes de moins de 25 000 habitants sont en demande de sensibilisation. Je conseillerais aux associations d'élus d'accélérer et d'amplifier leurs programmes dans ce sens.

Comment réussir cette transition vers un numérique éthique, souverain et sûr ?

De manière générale, dans les prochaines années, il est nécessaire que l'apprentissage des bonnes pratiques numériques fasse partie intégrante de la formation de tous.
Il faut aussi mieux sensibiliser les élus et agents aux risques de cyberattaques. Les collectivités sont encore trop peu conscientes de la menace cyber et d'un besoin de résilience en cas d'attaque. Elles doivent être accompagnées dans la mise en place d'une politique globale de sécurité informatique et savoir à qui s'adresser pour obtenir aide et conseils.
Sur un bassin de vie, qui peut être celui de l'intercommunalité, il est important aussi de mutualiser les moyens, d'organiser des réseaux de référence en matière de cybersécurité, par exemple en nommant un référent sécurité informatique. Ce référent pourrait devenir l'interface entre la collectivité et les autorités compétentes, ce qui renforcerait la cyber-résilience.
Enfin, pour promouvoir un numérique éthique, la question du choix des prestataires est primordiale. En matière d'hébergement et de gestion des données, par exemple, il est important de choisir des prestataires apportant des solutions respectueuses de l'environnement et garantissant la sécurisation complète des données. En parallèle, il faut encourager les entreprises européennes à se regrouper en consortium pour développer des offres de cloud multi-localisé, par exemple, et éviter de centraliser toutes nos données dans un même système. Encore une fois, un Small Business Act européen permettrait également de protéger les données sensibles, comme celles de l'éducation, des acteurs extérieurs à l'Europe.

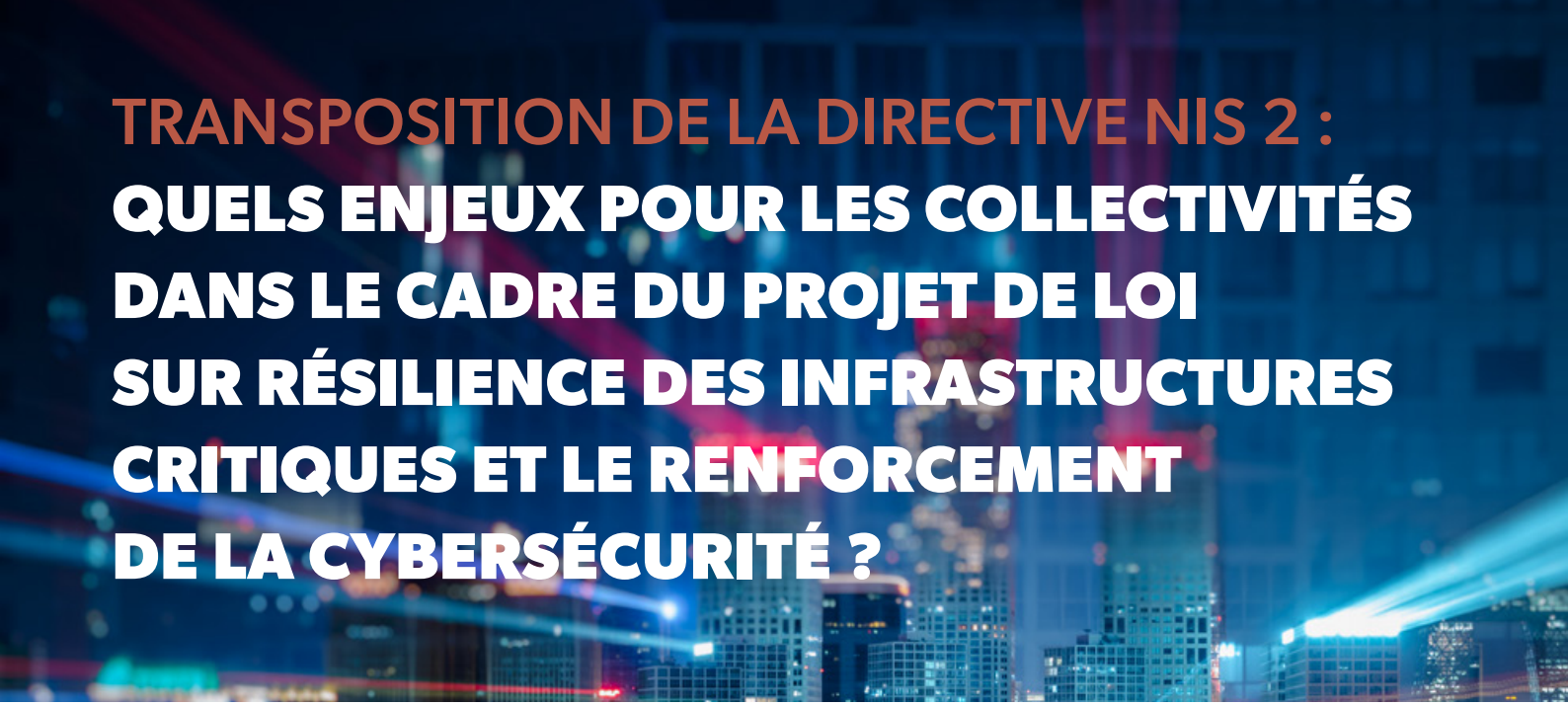
L'ENJEU STRATÉGIQUE D'UN SMALL BUSINESS ACT EUROPÉEN

« Dans les années 50, les Américains ont défini quelles étaient, selon eux, les structures vitales et les données sensibles sur leur territoire. Cette démarche leur a permis de prendre des dispositions législatives et fiscales qui ont orienté la commande publique vers des entreprises maison à travers un « Small Business Act ». Il faudrait donc aller vers plus d'équité sur le sujet de la concurrence dans les négociations internationales. Je pense que la question de la protection contre les lois extraterritoriales doit devenir primordiale. Le Small Business Act européen permettrait de sanctuariser ces notions. Toutefois, nous sommes inégalement positionnés sur ce sujet en Europe. C'est regrettable car certaines de nos entreprises fournisseurs de solutions souveraines du territoire français sont contraints de s'orienter vers l'Allemagne pour obtenir des contrats, car aucune commande publique ne leur est passée en France ».

LES RECOMMANDATIONS DE CATHERINE MORIN-DESAILLY :

1. **S'interroger collectivement sur le modèle de société que nous souhaitons :** Place de l'humain et de la machine, respect des valeurs fondamentales européennes, de notre souveraineté, etc.,
2. **Mettre en place un Small Business Act européen :** À l'image du modèle américain, cet outil permettrait de protéger les données sensibles en Europe et de soutenir la compétitivité des entreprises locales dans la commande publique,
3. Commande publique : **Encourager nos entreprises françaises et européennes à se constituer en consortiums** pour atteindre une masse critique et offrir des solutions intégrées,
4. **Établir un réseau de référents en cybersécurité :** Nommer un référent numérique pour chaque bassin de vie, pour servir d'interface entre les collectivités territoriales et les autorités,
5. **Lister l'ensemble de leurs initiatives et actions pour les faire connaître des collectivités,** pour lesquelles les choix de traitement et d'hébergement de nos données, de celles des administrations et des entreprises, doivent être éclairés,
6. **Faire davantage connaître le dispositif de cyberprotection publique qui s'articule autour de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et d'un réseau de CERT (Computer Emergency Response Team),** organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ce sont des centres d'alerte et de réaction aux attaques informatiques, dont les informations sont accessibles à tous,
7. **Faire de la formation aux élus et administrations une grande cause nationale** pour accélérer leur acculturation,
8. **S'assurer des bonnes compréhension et application de la circulaire sur l'utilisation du cloud dans le secteur public,** pour encadrer la gestion et la sécurité des données sensibles,
9. **Adopter une stratégie multicloud :** Diversifier les prestataires de cloud pour éviter la concentration des données auprès d'un seul acteur, assurant ainsi une meilleure sécurité et indépendance des données,
10. **Instaurer des incitations fiscales et des labels verts** pour promouvoir les solutions numériques respectueuses de l'environnement et protectrices de la vie privée.

3 - CYBERSÉCURITÉ



TRANSPOSITION DE LA DIRECTIVE NIS 2 : QUELS ENJEUX POUR LES COLLECTIVITÉS DANS LE CADRE DU PROJET DE LOI SUR RÉSILIENCE DES INFRASTRUCTURES CRITIQUES ET LE RENFORCEMENT DE LA CYBERSÉCURITÉ ?

QU'EST-CE QUE NIS 2 ?

La directive NIS 2 (Network and Information Security), adoptée par l'Union européenne, a été mise en place par la Commission européenne dans le cadre de sa stratégie de cybersécurité pour améliorer la résilience des infrastructures critiques et renforcer la sécurité des réseaux et systèmes d'information au sein de l'UE. Elle vient compléter et développe la première directive NIS publiée en 2016[1]. La directive a été votée le 10 novembre 2022, publiée au JO de l'UE[2] le 27 décembre 2022 avant d'entrer en vigueur le 17 janvier 2023. La France soutient la directive et s'affirme consciente de l'importance d'une mise en œuvre significative dans les États membres.

LES MESURES PHARES

Dans un contexte de hausse des cyberattaques, la directive vise à renforcer la sécurité de nombreuses entités afin de préserver les données des citoyens et faciliter le fonctionnement d'une société numérique sûre et sécurisée. Dans ce cadre, elle élargit le champ des entités et secteurs concernés.

Plusieurs nouvelles mesures sont ainsi prévues :

- Introduction d'un **mécanisme de proportionnalité** selon **deux types d'entités différenciées en fonction de leur niveau de criticité, à savoir les entités essentielles et les entités importantes.**
- **Prise en charge des incidents de sécurité et la gestion des crises** pouvant en résulter :
  - Définition de plusieurs niveaux d'alertes.
  - Les entités doivent disposer d'un cadre de gestion des incidents (Incident Management Framework) robuste et veiller à la continuité des opérations en cas d'incident majeur et à la maitrise des risques liés aux tiers.
- **Obligation de mise en place d'un véritable écosystème dédié à la cybersécurité** avec la formation des collaborateurs aux risques qui en découlent.
  - Mise en place d'une **équipe de gestion des incidents cyber dans chaque entité**. Les pouvoirs de supervision et de sanction de l'ANSSI vont augmenter.
  - **Obligation de sécurisation des réseaux et systèmes d'informations de l'entité,** par plusieurs moyens tels que la cryptographie et le chiffrement des données, le contrôle des accès aux systèmes ou encore des solutions d'authentification à plusieurs facteurs. Les entités auront également l'obligation de partager certaines informations mises à jour. Elles devront également mettre en place des mesures juridiques, techniques et organisationnelles pour gérer les risques qui menacent la sécurité de leurs réseaux et de leurs systèmes d'information et signaler à l'autorité nationale désignée leurs incidents de sécurité. Enfin, les entités devront fournir des rapports concernant l'évolution de la situation.
- Pour aider les entités dans ces démarches, l'ANSSI a créé le service numérique « MonEspaceNIS2 »[3] dont la vocation est d'accompagner les entités régulées dans leur mise en conformité à la directive. Des consultations sont également mises en place entre les fédérations professionnelles, les associations d'élus locaux et les ministères concernés par NIS 2 sont en cours depuis l'automne 2023 afin d'échanger avec les représentants des futures entités régulées.

1 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L1148
2 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555
3 https://monespacenis2.cyber.gouv.fr/directive

IMPACT SUR LES COLLECTIVITÉS ET LES AUTRES ACTEURS PUBLICS

Cette directive vise à renforcer la protection des collectivités territoriales gérant les « entités essentielles » nommées ainsi en raison de leur rôle fondamental dans la gestion des services critiques. Les collectivités sont considérées comme des entités essentielles.

ENTITÉS ESSENTIELLES :

Il s'agit de **secteurs d'activité dont le service fourni est essentiel au maintien d'activités sociétales ou économiques critiques.** La perturbation de ce service aurait un impact dramatique sur le bon fonctionnement de l'État.

En bref, les secteurs concernés :

- Les administrations publiques, dont les collectivités ;
- Les eaux potables ;
- Le eaux usées ;
- Les énergies ;
- L'Espace ;
- La gestion des services Technologies de l'Information et de la Communication (interentreprises) ;
- Les infrastructures des marchés financiers ;
- Les infrastructures numériques ;
- La santé ;
- Le secteur bancaire ;
- Les transports.

ENTITÉS IMPORTANTES :

Les entités importantes, quant à elles, concernent des secteurs d'activité « critiques ».

En bref, les secteurs concernés :

- La fabrication, la production et la distribution de produits chimiques ;
- Les fournisseurs numériques ;
- La gestion des déchets ;
- L'industrie manufacturière ;
- La production, la transformation et la distribution de denrées alimentaires ;
- La recherche ;
- Les services postaux et d'expédition.

LA TRANSPOSITION DE LA DIRECTIVE EN FRANCE

Le processus de transposition est encore en cours. La transposition devait être réalisée avant la date limite d'octobre 2024 mais la procédure a été **retardée du fait de la dissolution**. Le projet de loi d'Antoine Armand, ministre de l'Économie, des finances et de l'industrie et de Patrick Hetzel, ministre de l'Enseignement supérieur et de la recherche **relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité**[4] a été déposée au Sénat le 15 octobre 2024. A date, aucun rapporteur n'a encore été désigné.

Une commission parlementaire spéciale a été créée pour examiner le texte. Sa réunion constitutive s'est tenue le 12 novembre dernier.

La transposition adaptera le cadre existant de protection des infrastructures critiques (SAIV) en intégrant les nouvelles exigences européennes.

4 https://www.senat.fr/dossier-legislatif/pjl24-033.html

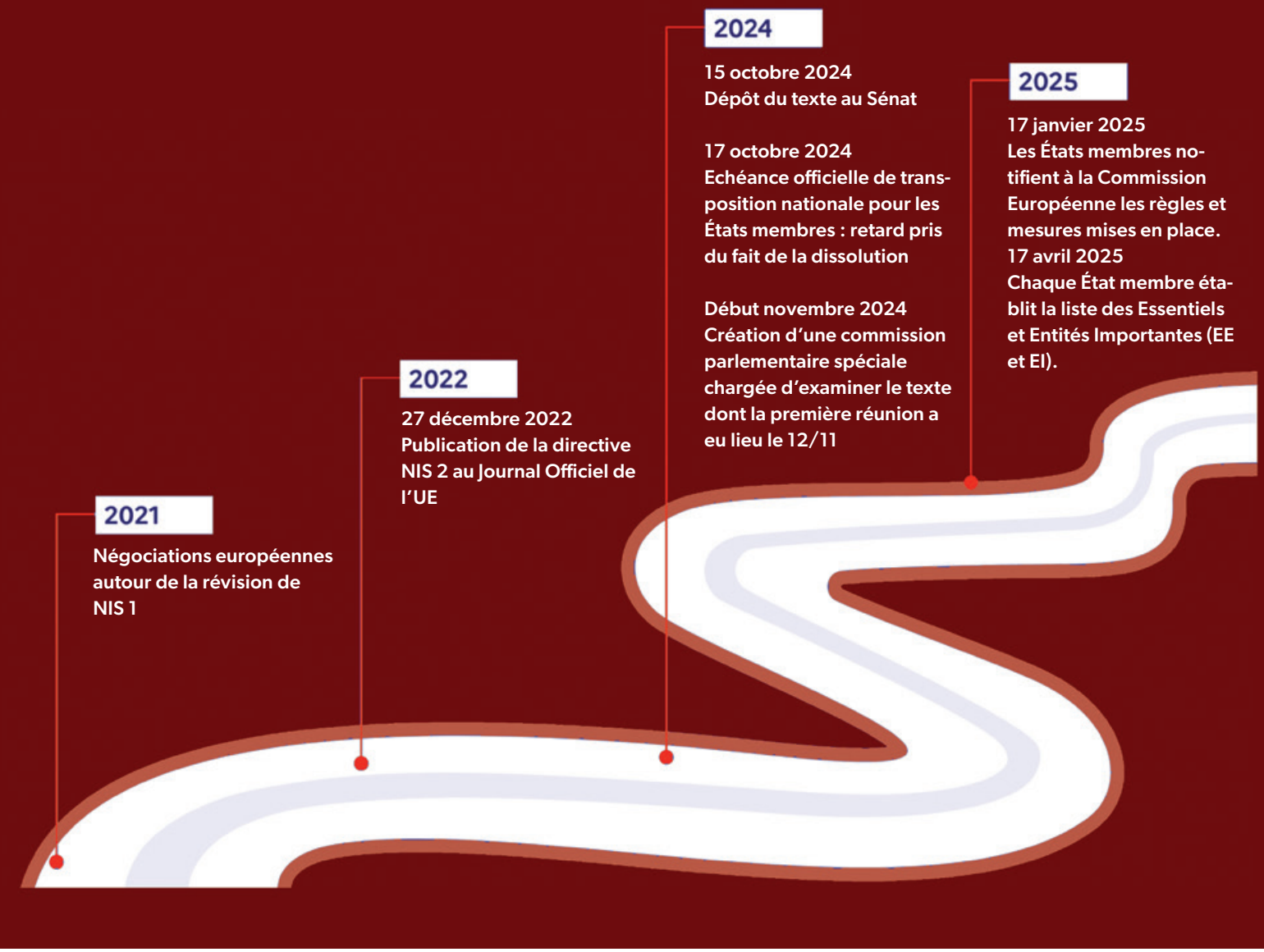
LES AUTRES DIRECTIVES CONCERNÉES PAR LA TRANSPOSITION

Le projet de loi fait allusion à deux autres directives qui viennent en appui à la directive NIS 2 :

- La directive **Résilience des entités critiques (REC)**[5] a pour objet d'améliorer la fourniture, au sein de l'Europe, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales. Cette directive **renforce la résilience des infrastructures considérées comme critiques** par les pays européens dans plusieurs secteurs d'activité.
- **Digital Operational Resilience Act (DORA)**[6] vise à améliorer les exigences liées à l'encadrement des risques induits par l'emploi des technologies de l'information et de la communication (TIC) dans le secteur financier. Par exemple, pour les banques, le respect de la directive NIS 2 passe par le règlement DORA.

LES PROCHAINES ÉTAPES

Les étapes de la transposition



5 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2557
6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

> ***« FINISTÈRE SMART CONNECT, UNE INFRASTRUCTURE MUTUALISÉE ET SOUVERAINE AU SERVICE DES COLLECTIVITÉS FINISTÉRIENNES***

Antoine COROLLEUR,
Président du SDEF, Maire de Plourin

Le Syndicat Départemental d'Énergie et d'Équipement du Finistère (SDEF) accorde une importance primordiale au développement d'un numérique éthique, souverain et sûr, en étroite collaboration avec les collectivités locales. Cette démarche s'inscrit dans une volonté politique forte, visant à garantir que les territoires, en particulier les zones rurales, bénéficient des mêmes opportunités numériques que les métropoles. Le SDEF met aussi l'accent sur la souveraineté des données, qui doivent rester sous le contrôle des collectivités, ainsi que sur la sécurisation des infrastructures numériques, grâce à des initiatives telles que le projet Finistère Smart Connect.

Finistère Smart Connect : Réduire la fracture numérique entre zones urbaines et rurales

Une volonté politique forte est indispensable pour la réussite et la pérennité de projets numériques éthiques, souverains et sûrs. Les élus jouent un rôle clé dans la promotion des solutions et dans leur adoption par les collectivités.
Le projet Finistère Smart Connect a été mis en place par le SDEF pour permettre à des collectivités de tailles variées, y compris des petites communes, d'accéder à des services d'objets connectés, les premières initiatives ayant été souvent initiés par les métropoles. Cette initiative pionnière en France vise à proposer un service de territoire connecté sur l'ensemble du département, à l'exception du territoire de Brest Métropole, non adhérent au SDEF. En proposant un partenariat avec les communautés de communes afin de co-financer la couverture radio, nécessaire pour mettre à disposition les services d'objets connectés, l'objectif est de disposer et mettre à disposition, des services d'objets connectés à moindre coût, pour optimiser les politiques publiques en réseau et dans le domaine de l'efficacité énergétique. L'initiative permet ainsi d'apporter une offre à toutes les collectivités finistériennes. Ainsi, les collectivités peuvent engager, par exemple, l'installation de compteurs d'eau connectés, permettant une gestion plus efficace en réduisant les déplacements pour la relève manuelle. Dans le domaine des déchets, l'installation de capteurs de mesure du remplissage des colonnes d'apport volontaire vise à optimiser les tournées. Autre illustration : nous améliorons la gestion des systèmes de chauffage, la ventilation et la surveillance des niveaux de CO_2 grâce aux capteurs installés dans les bâtiments publics.

Un projet emblématique qui incarne des valeurs d'efficience, d'éthique et de souveraineté

Le projet Finistère Smart Connect met un accent particulier sur la maîtrise des données, en garantissant qu'elles soient stockées

localement et demeurent la propriété des collectivités. Ainsi, les serveurs sont hébergés dans un data center situé dans la région. La collectivité possède également une plateforme permettant de visualiser les données ainsi que d'un système de gestion de bases de données brute. Elle maîtrise aussi le réseau de transport des données. Chaque partenaire finance ses propres capteurs, ce qui garantit la souveraineté du transport et du stockage des données brutes. Bien que le SDEF gère ses infrastructures, il ne travaille pas uniquement en régie. Le SDEF fait appel à des prestataires externes pour fournir des solutions sur mesure en segmentant les différentes briques du projet : infrastructure de cœur de réseau, plateforme d'hypervision, réseau radio, capteurs. Cela permet de mieux évaluer la qualité des solutions proposées, même si cela demande un suivi important et le développement d'une expertise interne. En terme de souveraineté sur la donnée, si le choix actuel a été d'être propriétaire des serveurs, l'utilisation de solutions SaaS peut être pertinente, à condition que les données soient stockées dans des serveurs locaux sécurisés par des acteurs européens. Le critère géographique permet aussi de s'assurer d'une continuité dans l'accès aux données, particulièrement pour des services publics comme la facturation de l'eau, qui est stratégique. Un autre point important consiste dans l'organisation des prestataires, avec une attention particulière à la proximité des équipes, qui doivent être accessibles, avec un délai d'intervention de moins de deux heures. Enfin, il est essentiel de formaliser la réversibilité des solutions et de s'assurer que celles-ci soient maîtrisées. Par ailleurs, les cyberattaques, de plus en plus fréquentes, mettent en lumière la nécessité de sécuriser ces données au sein d'une infrastructure adaptée, surtout que toutes les collectivités ne disposent pas forcément des outils pour faire face à de telles menaces. En tant que structure départementale, le SDEF se doit de garantir un niveau de sécurité maximal.

Maîtrise et anonymisation des données, réversibilité des solutions : établir des critères précis dès la conception du projet

Nous nous engageons à élaborer un cahier des charges qui corresponde fidèlement à nos besoins, même si nous ne recevons pas toujours des réponses adéquates de la part des prestataires. L'expérience acquise depuis 2019, notamment lors du renouvellement de certains marchés, a été précieuse pour clarifier nos attentes et améliorer nos outils. Cette approche proactive nous permet de sélectionner les solutions et les prestataires les plus appropriés dès les premières étapes. Par exemple, nous nous attachons à conserver au maximum la souveraineté sur nos infrastructures et nos réseaux, tout en offrant à nos partenaires la flexibilité nécessaire pour répondre à leurs besoins, notamment en visualisation des données. Notre but n'est pas d'imposer des solutions à nos collectivités adhérentes, mais de travailler en collaboration étroite avec elles, en veillant demeurer indépendant pour assurer la continuité et l'indépendance de nos projets. L'un des principaux défis réside dans la montée en compétence au niveau technique, de l'ensemble des acteurs, que ce soient les prestataires où les personnels des collectivités. Le passage à l'échelle de ce type de solutions nécessite des expertises fortes et multiples en matière de radio, de développement informatique, de gestion de la donnée, de cybersécurité etc.
Parallèlement, notre priorité demeure la mutualisation de l'infrastructure. Par exemple sur un territoire, le SDEF va s'appuyer sur le réseau radio LoRa pour assurer la télégestion de l'éclairage public, une commune pour le suivi des consommations d'énergie de ses bâtiments, la communauté de communes pour la télérelève de ses compteurs d'eau.

LES RECOMMANDATIONS D'ANTOINE COROLLEUR :

1. Élaborer des cahiers des charges porteurs d'une vision claire et adaptés aux besoins spécifiques, dès la phase de conception des projets.
2. Mettre un accent particulier sur la maîtrise des données par les collectivités : garantir leur stockage local tout en permettant une flexibilité aux partenaires pour la visualisation des données. Deux options sont envisageables :
   - Conserver un maximum de propriété sur les infrastructures et réseaux en hébergeant les serveurs dans un data center propre.
   - Considérer l'utilisation de solutions SaaS et de data centers externes, sous réserve qu'elles soient européennes et que les données soient stockées sur des serveurs locaux sécurisés.
3. Assurer une continuité dans l'accès aux données en intégrant des clauses de réversibilité solides dans les cahiers des charges.
4. Exiger des prestataires des délais d'intervention courts afin d'assurer un service efficace et agile.
5. Intégrer l'anonymat des données dès la conception des projets afin de renforcer la confiance des administrés.
6. Promouvoir une prise de conscience des thématiques liées à la souveraineté numérique au sein des administrés et de l'écosystème économique.
7. Favoriser la mutualisation des ressources pour garantir l'usage de solutions les plus souveraines, éthiques et sécurisées possibles, tout en maintenant un coût maîtrisé.

> *« UNE PLATEFORME D'ACHAT AU SERVICE D'UN NUMÉRIQUE SOUVERAIN ET SÛR : SANS DOUTE UN MODÈLE UNIQUE EN FRANCE*

Jean-Pierre SABIO,
GIGALIS

Répondre à une demande croissante de nos partenaires publics en matière de souveraineté

Chez Gigalis, la souveraineté numérique est au cœur de notre engagement envers les collectivités et les acteurs publics. Notre approche repose sur une maîtrise complète et sécurisée de chaque étape du cycle de la donnée. À travers notre réseau propriétaire, nous assurons un accès sécurisé et intégral aux données, permettant ainsi aux collectivités de maintenir le contrôle de leurs informations sensibles dans un environnement entièrement sécurisé, sous gestion publique.
En 2025, nous franchirons une étape décisive avec l'intégration d'un data center sous bail emphytéotique administratif de longue durée, renforçant notre indépendance et notre ancrage territorial. Contrairement aux data centers détenus par des fonds de pension ou des entreprises étrangères, ce data center sera intégralement maîtrisé par une structure publique régionale, assurant ainsi aux collectivités locales une véritable souveraineté numérique, « du sol au plafond ».
Ce data center, en complément de nos infrastructures d'hébergement actuelles, a été conçu pour répondre aux normes les plus exigeantes en matière d'efficacité énergétique. Il sera exemplaire dans sa gestion de l'empreinte carbone, démontrant ainsi notre engagement pour un numérique responsable et durable, tout en garantissant une sécurité maximale des données. Avec ces initiatives, Gigalis réaffirme sa mission de partenaire de confiance pour un numérique souverain, éthique et responsable, au service de l'autonomie stratégique de nos territoires.

Privilégier les partenariats locaux

Chez Gigalis, nous accordons une importance croissante aux partenariats locaux, en recherchant un juste équilibre entre les collaborations avec des grands groupes et les PME de proximité. Cette stratégie nous permet de renforcer notre agilité opérationnelle tout en soutenant le développement de l'écosystème numérique territorial.
Un exemple concret de cet engagement est le choix récent d'un partenaire de taille moyenne basé à Castres pour la gestion de notre réseau, après un appel d'offres rigoureux. Ce nouvel acteur a été sélectionné parmi cinq intégrateurs en raison de sa réactivité et de sa capacité à répondre efficacement à nos exigences, confirmant la valeur ajoutée d'une proximité géographique et d'une connaissance approfondie du territoire.
Au printemps 2025, nous lancerons un nouvel appel d'offres structuré en plusieurs lots afin de couvrir de façon optimale les besoins en services des collectivités, notamment sur les volets critiques de cybersécurité et d'intelligence artificielle. Ces lots seront attribués de manière multi-attributaire, permettant à la fois aux grands groupes et aux PME/TPE de se positionner comme prestataires de référence au sein de notre centrale d'achat. Cette démarche garantit une complémentarité de compétences et favorise l'accès des petites entreprises aux marchés publics, renforçant ainsi l'autonomie et la résilience numérique des territoires.
En privilégiant ces partenariats locaux, Gigalis réaffirme son rôle d'acteur stratégique pour un numérique de proximité, sécurisé et souverain, en réponse aux attentes croissantes des entités publiques.

Nos leviers pour assurer la cybersécurité de nos partenaires publics

Gigalis s'engage activement à protéger les collectivités et acteurs publics face aux cybermenaces en développant des solutions innovantes et adaptées aux enjeux actuels. Notre approche de la cybersécurité se distingue par des technologies de pointe et un soutien opérationnel direct pour assurer une protection optimale des données et des infrastructures publiques.
Dès 2025, nous introduirons le chiffrement optique de notre réseau, une avancée rare dans le secteur public, qui permettra d'assurer une protection de bout en bout des données échangées. Ce procédé sécurise les informations en transit et protège leur intégrité, assurant aux collectivités un contrôle renforcé et une fiabilité sans faille de leurs communications.
En matière de défense contre les attaques par déni de service (DDoS), Gigalis a lancé en juin 2024 une solution dédiée qui filtre le trafic en amont, empêchant les cyberattaques d'atteindre les infrastructures de nos clients. Cette solution, fournie gracieusement à nos adhérents, renforce à la fois la sécurité et la continuité des services numériques publics, garantissant une accessibilité maximale des réseaux.

Nous avons également mis en place un contrôle strict d'accès aux URL dans les lycées publics des Pays de la Loire. Ce dispositif empêche l'accès à des contenus inappropriés, assurant ainsi un environnement numérique sécurisé pour les lycéens lors de leur présence en établissement. Notre supervision, effectuée directement par les équipes de Gigalis, intègre une analyse approfondie de millions de logs chaque semaine, garantissant une détection proactive et une réaction rapide face aux risques potentiels.
En cas d'incidents, notre engagement s'étend au-delà des solutions préventives : Gigalis assure un accompagnement de proximité auprès de ses adhérents en période de crise. Par exemple, lors d'une cyberattaque survenue en octobre dernier, nous avons pu intervenir immédiatement pour soutenir une structure publique touchée, démontrant notre réactivité et notre engagement dans la gestion des cybermenaces.
Avec ces initiatives, Gigalis confirme sa volonté d'être un partenaire de confiance pour les acteurs publics, en assurant un environnement numérique sûr et résilient, à la hauteur des défis de la cybersécurité moderne.

Une initiative phare : notre plateforme d'achat de confiance

La transformation de Gigalis, de syndicat mixte public en Groupement d'Intérêt Public (GIP) au 1er janvier 2025, illustre notre engagement à fédérer le maximum d'entités publiques. Ce GIP permettra à de nouveaux acteurs publics, comme les centres hospitaliers, les universités ou d'autres GIP, d'évoluer dans un cadre entièrement sécurisé et géré de manière agile par des institutions publiques, en proposant des solutions clé en main : connectivité, cybersécurité, cloud et hébergement. Il se distinguera en étant financé uniquement par les abonnements aux services, sans subventions ni cotisations. C'est sans doute un modèle unique en France. En optimisant nos coûts de fonctionnement, nous sommes en mesure d'offrir des services de haute qualité à des tarifs compétitifs, ce qui attire de plus en plus de collectivités et d'établissements publics.
Notre vision est claire : d'ici cinq ans, nous visons un écosystème numérique régional robuste et souverain, où chaque acteur public peut évoluer en toute confiance, avec un contrôle total sur sa souveraineté et sa cybersécurité.

Aller au-delà de la simple logique des cahiers des charges : Faire confiance aux intermédiaires publics pour une commande adaptée

Chez Gigalis, nous encourageons les collectivités à dépasser la logique purement administrative des cahiers des charges. Nous croyons en une démarche de co-construction, où les acteurs publics locaux et les collectivités travaillent en synergie pour affiner leurs besoins et concevoir des solutions sur mesure. En collaborant de manière proactive, nous pouvons réellement prendre en compte les spécificités de chaque territoire et proposer des réponses adaptées aux enjeux uniques de chaque collectivité. Cette approche ne se contente pas d'améliorer la compréhension des attentes locales : elle favorise également une concurrence saine et équitable entre les prestataires, permettant aux acteurs publics d'évaluer des offres diversifiées, adaptées à leurs priorités réelles. En collaborant ainsi, nous aidons les collectivités à surmonter leurs défis avec des solutions pertinentes, modernes et alignées sur les besoins de leur territoire.

Lever le quota des 20 % permettrait de mieux servir les collectivités

En tant que Groupement d'Intérêt Public (GIP), notre activité sera soumise à une contrainte réglementaire qui limite notre chiffre d'affaires à 20 % en faveur d'entités non adhérentes. Cette restriction freine notre capacité à offrir des solutions compétitives et adaptées à un plus grand nombre de collectivités, limitant ainsi notre contribution à l'intérêt général. En conséquence, certaines collectivités se voient privées d'offres plus avantageuses, les contraignant parfois à se tourner vers des centrales d'achat nationales, qui, en raison de leur taille, connaissent des coûts de structure plus élevés.
En levant cette limitation, nous pourrions élargir notre capacité d'action et proposer des offres plus compétitives et diversifiées aux collectivités territoriales. Cela renforcerait non seulement notre engagement envers l'intérêt général, mais également notre rôle en tant qu'opérateur public de référence dans le domaine des services numériques, permettant ainsi à chaque collectivité d'accéder à des solutions de qualité, adaptées à leurs besoins spécifiques.

LES RECOMMANDATIONS DE JEAN-PIERRE SABIO :

1. **Garantir un accès sécurisé aux données :** Assurer que les collectivités locales disposent d'un accès complet et sécurisé à leurs données grâce à des réseaux entièrement contrôlés par leurs soins.
2. **Promouvoir la mutualisation :** Encourager la collaboration entre acteurs locaux et nationaux lors des appels d'offres pour renforcer notre compétitivité face aux entreprises extraterritoriales.
3. **Développer des plateformes d'achat public :** Concevoir et mettre en place davantage de structures de type plateforme d'achat public, tout en respectant les règles de concurrence, afin d'accélérer la croissance des acteurs économiques nationaux.
4. **Favoriser les collaborations avec des tiers de confiance :** Inciter les collectivités à collaborer plus étroitement avec des opérateurs publics de confiance, comme Gigalis, pour mieux définir leurs besoins. Cela permettra d'assurer une adéquation optimale des solutions proposées et de garantir une mise en concurrence équitable.
5. **Revoir la limite de 20 % de chiffre d'affaires :** Augmenter ou supprimer le quota actuel de 20 % de chiffre d'affaires hors adhérents afin de permettre aux GIP de mieux servir un plus grand nombre de collectivités.

> *« NOTRE ENJEU EST DE PERMETTRE AUX COLLECTIVITÉS DE GARDER LA MAÎTRISE DE LEURS DONNÉES, MÊME SANS INGÉNIERIE SPÉCIALISÉE*

Alexandre DESROUSSEAUX,
Directeur Mission Transition Numérique de la Région Hauts-de-France

Clarifier la souveraineté numérique : un défi pour les collectivités locales face aux enjeux de données et de cybersécurité

Le point central de la souveraineté est la capacité des collectivités locales à être maîtresses de leurs données numériques. Or, la définition et les facettes de la souveraineté doivent être précisées, parce que chaque élu a la sienne. Malgré l'existence d'outils légaux et de labels, nous constatons que leur méconnaissance, même parmi les spécialistes, constitue un frein. Les réglementations, souvent techniques et en constante évolution, représentent en particulier un défi pour les petites structures. Notre mission vise aussi à fournir aux collectivités locales les outils et la formation nécessaires pour naviguer dans ces enjeux.

Un plan d'actions coordonnées pour une véritable prise de conscience des enjeux cyber

Sur la cybersécurité, nous nous appuyons notamment sur le plan régional de soutien aux collectivités, avec une contribution hebdomadaire d'une demi-journée dédiée à la sensibilisation. L'exemple de NIS 2 est parlant. Au départ, beaucoup de territoires pensaient que la directive n'était qu'une énième réglementation, une contrainte de plus à intégrer. Cependant, après neuf mois de tournée, au cours desquels nous avons organisé une vingtaine de rendez-vous autour de la cybersécurité, il est devenu évident que cette approche a permis de légitimement créer un sentiment d'urgence en incitant ainsi les collectivités à prendre des mesures proactives stratégiques pour leur avenir.
Nous avons également constaté que l'absence d'un délégué régional de l'ANSSI dans les Hauts-de-France a parfois entravé la diffusion de bonnes pratiques. La nomination d'un représentant a permis de dissiper certaines inquiétudes et d'engager une réflexion politique visant à sensibiliser les collectivités aux enjeux cyber. Depuis lors, nous avons créé un véritable écosystème en réunissant le cyber campus, l'ANSSI, la gendarmerie, la police et le CSIRT. Ensemble, nous avons conçu un diaporama commun et une plateforme dédiée pour les événements liés à la cybersécurité, sous la coordination de notre référent interne unique. Pour promouvoir l'emploi dans le numérique, nous avons également notamment organisé une tournée des sous-préfectures sous la forme d'un barnum itinérant couronnée de succès. Cette initiative vise à sensibiliser les collectivités locales et à faciliter les échanges sur les opportunités offertes dans le secteur numérique.

Créer des champions nationaux et européens capables d'offrir des solutions locales et de générer des emplois

Notre objectif premier est d'accompagner les collectivités locales dans l'adoption d'une stratégie numérique orientée vers les «Territoires intelligents» souverains et sécurisés.

Cette démarche implique un besoin accru d'outils adaptés. La mission de transition numérique de la région Hauts-de-France se positionne comme un financeur et conseiller.
Nous considérons qu'un numérique souverain implique un contrôle total sur l'hébergement et la gestion des données. Il est essentiel que le stockage et l'exploitation des données ne soient pas compromis par les logiciels utilisés.
Une autre question est l'impact économique territorial. La souveraineté est ainsi abordée sous l'angle de la filière. L'objectif est d'établir des champions nationaux ou européens, à l'échelle mondiale, pour être en capacité de proposer des solutions locales, créant des emplois territoriaux. Enfin, nous sommes particulièrement attentifs à la question de la réversibilité et de l'interopérabilité qui se pose en cas de changement de solution numérique et donc de prestataire.

Vers une commande publique adaptée et une approche responsable du numérique

Si la cybersécurité, bien identifiée comme un risque, bénéficie d'un soutien politique à travers notre appréhension de la commande publique, la souveraineté numérique, quant à elle, nécessite encore une véritable stratégie à l'échelle territoriale.
Nous intégrons également l'éthique dans nos réflexions autour d'un numérique durable, sobre, inclusif et responsable. Malgré les premières initiatives en faveur d'un numérique sobre, nous avons constaté que les tentatives d'introduire des fresques du numérique ont souvent été perçues comme culpabilisantes et peu productives pour favoriser une réelle prise de conscience, à l'image des consultations citoyennes sur ces sujets. La commande publique est clairement identifiée comme un levier important, mais la mise en place de clauses standardisées adaptées aux différents territoires reste un défi complexe à relever.

LES RECOMMANDATIONS D'ALEXANDRE DESROUSSEAUX :

1. S'assurer que l'hébergement et la maîtrise des données sont sous contrôle local, en évitant les dépendances excessives aux logiciels tiers.
2. Fédérer les acteurs nationaux et européens : Collaborer avec des partenaires pour créer des solutions locales tout en développant des champions nationaux et européens.
3. Pour surmonter le manque d'ingénierie locale, former les élus et les responsables locaux sur les bonnes pratiques en matière de souveraineté numérique et de cybersécurité : webinaires, plateformes dédiées, demi-journées de sensibilisation régulières, etc.
3. Créer un guichet unique pour la souveraineté numérique et la cybersécurité, servant de point central d'accès aux ressources et informations.
4. Veiller à ce que les actions de sensibilisation, comme les fresques du numérique, ne soient pas culpabilisantes, mais constructives et adaptées aux réalités locales.
5. Assurer réversibilité et interopérabilité : Veiller à ce que les solutions numériques permettent un changement de prestataire sans perte de contrôle des données.

« ÉTHIQUE, SOUVERAINETÉ NUMÉRIQUE ET NUMÉRIQUE SOUTENABLE : LA FEUILLE DE ROUTE DE L'ARCEP

©Brigitte Baudesson - ARCEP

Laure de La Raudière,
Présidente de l'ARCEP

Quelle est la définition de l'Arcep d'un numérique éthique, souverain et sûr ?

La numérisation de notre société est une révolution : elle transforme profondément toutes nos activités économiques ou sociales, elle bouleverse nos démocraties, elle crée de nouvelles opportunités et de nouvelles menaces… Ces changements doivent être conduits dans un univers de confiance permettant une liberté de choix des consommateurs, la liberté d'entreprendre et d'innover, et les mêmes principes de sécurité et d'éthique que dans le monde « physique ». Cela nécessite des infrastructures numériques ouvertes, offrant un service de qualité, à des prix raisonnables, et résilientes. Cela nécessite aussi d'avoir des services numériques respectant des règles pour garantir à la fois le développement des innovations et de la concurrence, mais aussi la préservation de nos valeurs démocratiques essentielles.

Quels sont, selon vous, les risques associés à l'utilisation de solutions qui protègent insuffisamment les libertés individuelles, la souveraineté et la sécurité des données ? Quelles sont les opportunités offertes par des technologies alignées avec nos valeurs européennes ?

L'Arcep est un régulateur technico-économique des infrastructures numériques dont la mission est de favoriser l'émergence d'une concurrence loyale et le développement de l'innovation au bénéfice du plus grand nombre. Elle a conscience des enjeux qu'induit le numérique sur le respect des libertés individuelles, la souveraineté, la sécurité… Toutefois, ces thèmes relèvent des missions d'autres autorités en France (CNIL, ANSSI, …) avec lesquels l'Arcep travaille pour apporter son expertise.
L'Arcep s'efforce à son niveau de promouvoir un cadre ouvert et loyal d'accès de toutes les infrastructures numériques, que ce soit les télécommunications, les services du cloud ou toutes autres services structurants pour le développement d'acteurs économiques compétitifs, innovants et résilients en France et en Europe. Cela permet de rendre possible l'émergence de solutions alternatives aux modèles dominants, qui porteront les valeurs européennes.

Comment l'Arcep participe-t-elle à la mise en place d'un modèle vertueux du numérique ?

Maillage et sécurisation des réseaux : un enjeu de souveraineté stratégique

Le déploiement de nouvelles infrastructures de réseaux de communications électroniques (fibre optique, 5G) nécessite une résilience accrue en raison de leur importance pour les citoyens et les entreprises. Ces technologies améliorent la connectivité mais

sont complexes à sécuriser, notamment à cause de la diversité des acteurs impliqués. L'Arcep en a conscience et adapte son action pour prendre en compte l'émergence d'une chaîne de valeur fragmentée, avec de nombreux acteurs pour le déploiement de la fibre, l'externalisation de la gestion des pylônes ou la virtualisation des réseaux. Pour approfondir ces enjeux, l'Arcep, au-delà de ses compétences formelles, a lancé un cycle de travail sur la résilience des réseaux dans le cadre de sa démarche « Réseaux du futur » fin 2023.

Garantir un comportement des opérateurs agissant sur le territoire national comme « opérateurs d'importance vitale »

La question de la définition du service universel et de sa mise en œuvre ne relève pas de la compétence de l'Arcep. Pour autant, apporter le très haut débit, fixe et mobile, partout, pour tous, et de qualité, est un objectif prioritaire de l'Arcep. C'est essentiel pour l'attractivité de tous les territoires.
Le plan « France très haut débit » vise la généralisation du FttH grâce aux investissements des opérateurs privés, des collectivités territoriales et de l'Etat, et s'appuie sur les dispositions du cadre réglementaire défini par l'Arcep. Au 30 juin 2024, près de 90% des locaux sont rendus raccordables à la fibre en France.
Le programme « New Deal Mobile » a priorisé l'aménagement numérique du territoire plutôt que le critère financier pour l'attribution des fréquences, a favorisé la mutualisation d'infrastructures entre opérateurs et a associé les collectivités dans l'identification des zones à couvrir.
Ces deux politiques publiques ont permis de réduire considérablement la fracture territoriale numérique. L'Arcep rend compte de leur avancement par la publication d'observatoires et d'outils cartographiques (monreseaumobile.fr ; maconnexioninternet.fr).

Promouvoir un numérique soutenable d'un point de vue environnemental

Depuis 2019, l'Arcep a fait de la réduction de l'empreinte environnementale du numérique, un nouveau chapitre de sa régulation. Elle conduit des travaux, aux côtés d'autres institutions pour améliorer les connaissances sur l'empreinte environnementale du numérique : étude prospective réalisée avec l'ADEME en 2023 ; collectes de données réalisées auprès des acteurs du secteur et présentées dans l'enquête « Pour un numérique soutenable » de l'Arcep… Ainsi, l'Arcep alimente le débat public de données fiables pour orienter les décisions des parties prenantes.
Parallèlement, elle soutient la mobilisation du secteur avec des actions concrètes, comme par exemple la migration du réseau cuivre vers la fibre optique ou la mutualisation des infrastructures là où cela est pertinent. L'Arcep promeut aussi le développement de services numériques sobres : elle a publié en mai 2024 avec l'Arcom, l'ADEME et d'autres partenaires, le Référentiel Général de l'Écoconception des Services Numériques[1] pour inciter les acteurs à s'emparer de cet enjeu.

Quelles recommandations adressez-vous aux collectivités pour réussir leur transition vers un numérique éthique, souverain et sûr ? Pouvez-vous citer des initiatives territoriales que vous souhaitez mettre en lumière ?

Les collectivités territoriales jouent un rôle essentiel dans le déploiement et l'exploitation des réseaux de communications électroniques. Nul doute que leur implication sera tout aussi importante pour assurer la transition vers un numérique éthique, souverain et sûr.
Certains syndicats mixtes d'aménagement numérique pionniers ont mis en œuvre des actions pour améliorer la résilience des réseaux, en application d'un schéma local de résilience (SLR) élaboré à partir du guide établi par l'ANCT.
Par ailleurs, pour orienter la conception de leurs services numériques vers des choix plus soutenables, les collectivités peuvent utiliser le Référentiel général de l'écoconception des services numérique (cf ci-dessus). De façon générale, tous les travaux conduits dans notre démarche « Pour un numérique soutenable » ont vocation à alimenter les réflexions pour l'élaboration de la stratégie numérique responsable des collectivités (obligatoire pour toutes les communes et intercommunalités de plus de 50 000 habitants).

1 https://www.arcep.fr/mes-demarches-et-services/entreprises/fiches-pratiques/referentiel-general-ecoconception-services-numeriques.html

LE GUIDE POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR

EN DEUX PAGES

NOTRE AMBITION

La FNCCR, en collaboration avec le Club Numérique & Territoires de Com'Publics, a coconstruit un guide pratique pour accompagner les collectivités territoriales dans le choix de leurs solutions technologiques.
Élaboré à partir de trois ateliers et de nombreux entretiens, ce guide repose sur trois piliers : la souveraineté numérique, la protection des libertés individuelles et la cybersécurité.
Il propose des recommandations concrètes, notamment pour une commande publique au service des entreprises européennes et respectueuses de nos valeurs.

NOTRE CONSTAT

I-Souveraineté numérique et cybersécurité

Des défis pour notre autonomie stratégique, jusqu'au cœur des territoires
Face aux tensions géopolitiques croissantes et à l'influence dominante des géants technologiques (GAFAM, BATX), la souveraineté numérique s'impose comme une priorité stratégique. Bien que des initiatives européennes telles que le Digital Markets Act (DMA) ou le Data Privacy Framework marquent des progrès, les collectivités restent trop peu conscientes des dangers liés à l'usage de solutions non souveraines.
Par exemple, des lois extraterritoriales comme le Cloud Act permettent dans certaines conditions aux autorités étasuniennes d'accéder aux données traitées par les entreprises américaines, même hébergées en Europe, tandis que les cyber-espionnages orchestrés par des puissances comme la Chine ou la Russie menacent la sécurité de nos informations sensibles. Dans ce contexte, la transposition de la directive NIS 2 et la montée du protectionnisme américain, incarnée par un Donald Trump de nouveau au pouvoir, soulignent l'urgence de garantir la protection de nos données.

De vrais enjeux concurrentiels : rééquilibrer le rapport de force
Par ailleurs, la domination des géants du numérique constitue un frein majeur à l'émergence de solutions européennes. Ces entreprises bénéficient d'une concentration de marché exceptionnelle, limitant la capacité des acteurs locaux à exister, alors que certaines ne paient que peu d'impôts en Europe et ne jouent pas toujours le jeu de nos valeurs européennes.

II – Éthique

La protection des libertés individuelles, un impératif pour la confiance des citoyens
Dans un monde interconnecté où les données personnelles alimentent l'économie et le pilotage de nos politiques publiques, et où la méfiance envers la sphère publique va crescendo, le mauvais usage des données personnelles menace la confiance des citoyens et avec elle, la transition numérique apaisée souhaitée par tous.
Il est impératif de prendre conscience que les données personnelles sont devenues si stratégiques que des abus par certaines entreprises ou acteurs publics sont inévitables sans encadrement. L'argument «je n'ai rien à cacher» ne justifie pas que nos vies deviennent transparentes : des sociétés de vidéosurveillance, par exemple, vendent déjà des plaques d'immatriculation à des assureurs, permettant des ajustements de primes selon les cas. Des solutions de vidéoprotection utilisées dans le cadre de Territoires intelligents sont parfois détournées par des acteurs en collectivité pour suivre des individus ou groupe d'individus dans la rue ou repérer des SDF.
Il est donc essentiel de concevoir des technologies intégrant dès leur conception le principe de proportionnalité, afin que les données collectées soient strictement limitées à la finalité prévue. Il est à préciser que les solutions utilisées légitimement à des fins de sécurité publique par les forces de l'ordre ne sont pas concernées par nos recommandations (vs Smart city).

III - La commande publique :

le levier des territoires pour structurer un numérique éthique, souverain et sûr
La commande publique représente un outil stratégique puissant pour soutenir le développement d'un numérique propre à nos valeurs. En imposant des critères stricts dans les appels d'offres, les acteurs publics peuvent contribuer à protéger nos citoyens tout en accompagnant le développement de nos entreprises.

SYNTHESE DES RECOMMANDATIONS

Parmi la totalité des propositions formulées tout au long du guide, une vingtaine de recommandations font l'unanimité auprès de l'ensemble de nos contributeurs.

Souveraineté numérique, cybersécurité et commande publique

1. **Appliquer strictement les mesures prévues par la directive NIS2** en cours de transposition, afin de renforcer la cybersécurité et la cyber résilience des collectivités.
   - La directive prévoit la qualification de nouveaux domaines comme essentiels, nécessitant un renforcement de la sécurité et de la souveraineté des données concernées.
2. **Privilégier des infrastructures et solutions souveraines :**
   - **Favoriser des infrastructures (data centers) et des solutions logicielles ou cloud localisées en Europe** (publics ou privés), financées par des **capitaux européens ou nationaux.**
   - **Exclure autant que possible les équipements non européens** susceptibles de présenter des vulnérabilités et soumis à des réglementations extraterritoriales.
   - **Envisager le stockage de données en on-premise** (en local) pour garantir un contrôle maximal.
3. **Adopter une stratégie multicloud :** Diversifier les prestataires de cloud pour éviter une concentration excessive des données chez un seul acteur.
   - **Promouvoir des solutions garantissant interopérabilité, réversibilité, et une intervention rapide** des équipes techniques (moins de deux heures).
4. **Mettre en place un dispositif de labellisation :** Compléter le dispositif SecNumCloud avec un label garantissant la souveraineté des infrastructures et des processus utilisés, incluant une immunité aux lois extraterritoriales.
5. **Intégrer des critères environnementaux** dans les cahiers des charges :
   - Insister sur la recyclabilité et la production locale des équipements.
   - Privilégier des infrastructures (data centers) moins énergivores et localisées au plus près des utilisateurs.
6. **Pour autant, distinguer souveraineté et protectionnisme :**
   - Accepter des technologies étrangères (ex. couches logicielles) si elles sont intégrées dans des infrastructures locales et contrôlées.
7. **Créer un guichet unique pour la souveraineté numérique et la cybersécurité :** Fournir un point d'accès centralisé pour accompagner les collectivités dans leurs démarches et l'accès aux ressources nécessaires.

Éthique, vie privée et commande publique

8. **Intégrer des critères éthiques dès la conception** visant à garantir que les technologies respectent les droits et libertés individuelles.
9. **Renforcer la transparence.** Par exemple :
   - Instaurer des registres et logs pour assurer une gestion responsable et transparente.
   - Informer les citoyens sur les données collectées, leur finalité, leur durée de conservation et leur localisation.
   - Déployer des outils simples, comme des QR codes sur les équipements, pour expliquer les usages des données collectées et renforcer la confiance publique.
10. **Mettre en œuvre des systèmes de traçabilité des données personnelles** pour permettre de suivre les accès, modifications et utilisations des données.
11. **Respecter le principe de proportionnalité :**
    - Collecter uniquement les données strictement nécessaires à l'usage attendu.
    - Mettre en œuvre un traitement localisé pour réduire les risques de fuites.
    - Réduire la qualité des images captées (image dégradée by design) pour limiter l'intrusion, plutôt que de flouter après coup.
    - Supprimer les données une fois leur finalité atteinte.

Faciliter l'accès des entreprises locales à la commande publique

12. **Élaborer des cahiers des charges avec une vision claire et précise dès la phase de conception** des projets publics.
13. **Mettre en place un Small Business Act européen** inspiré du modèle américain qui vise à soutenir la compétitivité des entreprises locales en leur accordant la priorité dans la commande publique.
14. **Favoriser la création de consortiums européens** en encourageant les entreprises à s'unir pour atteindre une masse critique et offrir des solutions intégrées compétitives.

Financement de la transition numérique

15. Mettre en place diverses incitations au niveau national pour les acteurs territoriaux :
    - **Rééquilibrer les budgets entre Capex et Opex** pour répondre aux contraintes budgétaires des collectivités.
    - **Adapter les clés de répartition pour une meilleure adéquation** avec les besoins locaux.
16. Proposer des **incitations fiscales aux investisseurs privés soutenant les entreprises locales,** notamment dans le domaine du cloud computing.
17. **Créer une agence nationale inspirée de la DARPA** américaine, qui soutient activement les acteurs locaux en fournissant des financements adaptés via un guichet unique.

Retrouvez l'intégralité de notre Guide en scannant ce QR Code

LISTE DES RECOMMANDATIONS

LES RECOMMANDATIONS DE PHILIPPE LATOMBE :

1. Encourager les collectivités à **inclure des critères éthiques dès la phase de conception de leurs cahiers des charges**, afin de s'assurer que les technologies respectent les droits et libertés individuelles.

2. **Fixer des standards stricts pour les fournisseurs**, incluant la conformité aux principes éthiques relatifs à la protection de la vie privée.

3. **Instaurer systématiquement des mesures de traçabilité des accès aux systèmes**, via des logs et des registres, pour assurer une gestion transparente et responsable.
   - Possiblement, connecter directement les équipements de surveillance à un réseau filaire reliant les infrastructures locales aux autorités, comme les préfectures, afin d'assurer un contrôle optimal.

4. **A l'image du comité Vigouroux, mettre en place dans la mesure du possible un comité éthique** pour encadrer l'utilisation des technologies de surveillance, incluant des techniciens, des experts en sciences humaines et des fonctionnaires.

5. **Assurer que les données et les outils de surveillance restent sous un contrôle juridique strict** pour faciliter la responsabilité en cas de mauvaise utilisation :
   - **Privilégier l'utilisation de matériel fabriqué et localisé en France ou en Europe**, en évitant les équipements non européens susceptibles de présenter des vulnérabilités (solutions non soumises aux règles extraterritoriales) ;
   - **Favoriser le stockage de données en *on-premise*** pour garantir un contrôle accru ;
   - **Labelliser les solutions cloud européennes pour assurer sécurité et souveraineté**, en complément du SecNumCloud.

6. Sur le modèle des Etats-Unis, **renforcer la mise en œuvre de sanctions aux acteurs en cas de non-conformité** avec les réglementations en vigueur.

7. Mettre en place des incitations au niveau national pour aider les acteurs souverains à se protéger contre les règles extraterritoriales européennes :
   - **Réévaluer la répartition des budgets (Capex/Opex)**
   - **Revoir le partage des clés de dotation.**

LES RECOMMANDATIONS DE MIROSLAV SVIEZENY :

1. **Sensibiliser les plus hauts niveaux de l'État à l'importance stratégique de développer des infrastructures françaises** afin de susciter un engagement fort.

2. **Stimuler l'investissement public et privé dans les technologies et les acteurs nationaux pour prévenir leur départ** à l'étranger, où ils trouvent un écosystème d'investissement plus favorable.
   - Offrir **des incitations fiscales attractives** pour les investisseurs privés qui soutiennent les entreprises locales dans le cloud computing.
   - **Créer une agence nationale inspirée de la DARPA américaine** qui a vu naître les grands acteurs technologiques actuels : Mettre en place une structure dédiée pour soutenir les acteurs locaux, offrant des financements adaptés via un guichet unique pour les infrastructures physiques notamment.

3. **Soutenir davantage les entreprises développant des solutions de calcul intensif.**

4. **Renforcer les aides aux entreprises qui adoptent des modèles énergétiques circulaires** et qui mettent en œuvre des solutions de récupération de chaleur.

LES RECOMMANDATIONS DE DIDIER ARZ :

1. **Encourager la réappropriation des données par les collectivités** : Permettre aux élus de piloter et d'adapter les données aux besoins spécifiques de leurs territoires en développant un langage commun pour faciliter la compréhension et la prise de décision.

2. Au-delà de l'approche par la donnée, **assurer une valeur ajoutée tangible pour les collectivités** : Construire des services intuitif et utiles, générant des donnés facilement exploitables et valorisables pour renforcer la perception positive des territoires sur les nouvelles technologies.

3. **Privilégier des capteurs protecteur de la vie privée pour une collecte de données éthique** : Installer des capteurs de comptage (piétons, parking) garants du privacy by design.

4. **Proposer une charte d'interopérabilité** : Construire une charte pour garantir la protection, le stockage, et la gestion sécurisée des données, permettant la transparence, la réversibilité, et la traçabilité.

5. **Repenser les modèles de financement en faveur du CAPEX** afin de répondre aux contraintes budgétaires des collectivités et soutenir le pilotage économique des équipements.

6. **Intégrer des critères éthiques et environnementaux dans la commande publique** : Insister sur la production locale, la recyclabilité des matériaux, et la sécurité des données dans le choix des prestataires.

7. **Explorer des solutions comme le stockage local des données**, via des partenariats avec les communes pour une infrastructure souveraine et durable, **telle que le projet Morbihan Teradata.**

LES RECOMMANDATIONS DE JEAN-BAPTISTE POLJAK

1. **Vision politique : guider chaque choix technique et infrastructurel par une stratégie de souveraineté et de transparence claire.**

2. **Distinguer souveraineté et protectionnisme** en acceptant des technologies étrangères (ex : couches logicielles) dans le cadre d'infrastructures locales contrôlées, garantissant ainsi la sécurité sans isolation technologique.

3. **Garantir,** en revanche, **que les infrastructures numériques (serveurs, data centers, etc.) soient sous le contrôle de capitaux publics ou européens** pour éviter toute soumission aux lois extraterritoriales étrangères.

4. **Promouvoir l'éthique par la transparence et la traçabilité :**
   - **Informer clairement les citoyens sur les types de données collectées**, leur finalité, leur durée de conservation et leur localisation, afin d'encourager la confiance dans les services publics numériques.
   - **Déployer des outils d'information des citoyens** à travers des outils simples et visibles, comme des QR codes sur les équipements, pour expliquer l'utilisation des données et renforcer la perception de transparence.
   - **Mettre systématiquement en place des systèmes de traçabilité des données personnelles** permettant de suivre l'accès, les modifications, et les utilisations pour plus de transparence et de sécurité.

5. **Appliquer le principe de proportionnalité** (Charte de l'UE, RGDP) :
   - **Minimiser la collecte de données personnelles par défaut :** Développer des technologies «privacy by design» qui limitent automatiquement l'accès aux informations personnelles, afin d'éviter tout besoin de «confiance aveugle».
   - Dans le cadre des territoires intelligents : Adopter des capteurs et des algorithmes sans possibilité de reconnaissance des individus.

6. Lorsque nécessaire, **confier le processus d'anonymisation à des acteurs publics avant toute transmission à des entreprises privées**, comme le fait la ville d'Amsterdam.

7. **Établir des audits stricts de protection des données** pour évaluer les risques avant de travailler avec des technologies impliquant des données sensibles.

LES RECOMMANDATIONS DE PATRICK CHAIZE :

1. **Établir un choix politique** clair en matière de sécurité des données.
2. En complément du SecNumCloud, **proposer un système de labellisation dédié** afin de garantir la souveraineté des infrastructures et des différents processus utilisés.
3. **S'appuyer sur la transposition de NIS 2** pour identifier les services essentiels et les données qui leur sont associées afin de leur garantir un plus haut niveau de sécurisation et ainsi favoriser des solutions plus souveraines.
4. **Promouvoir une sensibilisation collective** sur les enjeux de la souveraineté numérique à tous les niveaux (UE, État, collectivités) pour faciliter des échanges et des discussions plus larges au-delà du cercle des experts.
5. **Activer les leviers de la commande publique** pour renforcer la compétitivité des acteurs locaux, nationaux et européens face aux concurrents, dans les appels d'offres publics notamment :
   - Mobiliser le levier de l'empreinte environnementale
   - Promouvoir la création de groupements d'acteurs français pour répondre à de gros appels d'offres.
   - Intégrer des clauses de dépôt de code source dans les marchés publics pour garantir l'indépendance des collectivités en cas de défaillance d'un fournisseur.
   - Motiver les investissements par une garantie de marché.
   - Développer les compétences des collectivités et des entreprises en intelligence économique

LES RECOMMANDATIONS DE SÉVERINE REYNAUD :

1. **Proposer des solutions de sensibilisation accessibles et peu coûteuses pour les collectivités**
   - Mettre en place des observatoires pour suivre et visualiser en temps réel le blocage des cyberattaques, afin de sensibiliser les collectivités aux menaces numériques et à la cybersécurité préventive.
   - Organiser des sessions d'information régulières pour expliquer de manière claire les terminologies, les enjeux de la souveraineté numérique et les risques liés à la gestion des données.
2. Sur le modèle des initiatives en matière de cybersécurité, lancer des programmes de **formation et des actions de sensibilisation spécialement dédiés à la souveraineté numérique**, permettant aux collectivités locales de mieux comprendre l'importance de cet enjeu stratégique et les dangers liés à la dépendance numérique.
3. **Encourager le recours à des entreprises locales ou nationales** qui offrent des solutions technologiques moins énergivores et plus adaptées aux besoins spécifiques des collectivités territoriales, afin de promouvoir un numérique éthique et durable.
4. **Favoriser la création et l'utilisation de data centers locaux, publics ou privés**, pour garantir la souveraineté des données et offrir des services numériques sur mesure, adaptés aux besoins des collectivités et en adéquation avec les exigences de sécurité et de protection des données.
5. Mieux accompagner les collectivités dans la mise en place de solutions leur permettant de gérer elles-mêmes leurs infrastructures numériques et leurs données, pour éviter la dépendance à des prestataires extérieurs et renforcer leur résilience face aux menaces numériques.
6. Lors des appels d'offres publics, **intégrer des critères environnementaux, éthiques et souverains**, afin de sélectionner des partenaires technologiques qui partagent les mêmes valeurs de transparence, sécurité et durabilité.

LES RECOMMANDATIONS DE FABRICE COUPRIE :

1. **Promouvoir un contrôle français (ou européen) des données et des infrastructures** en insistant notamment sur l'origine de leur financement et leur localisation.
2. **Créer des labels** permettant aux collectivités de repérer facilement les prestataires de solutions numériques souveraines et éthiques.
3. **Réduire les seuils d'appels d'offres et simplifier le référencement à l'UGAP** pour favoriser la commande publique auprès des petites et moyennes entreprises françaises.
4. **Mettre en place des mécanismes de financement**, par exemple via un partage des coûts entre CAPEX et OPEX, pour aider les collectivités à gérer les investissements nécessaires pour sécuriser leurs infrastructures.
5. **Fournir un accompagnement accru** pour aider les collectivités à se conformer aux obligations de sécurité de la directive NIS2

LES RECOMMANDATIONS DE CATHERINE MORIN-DESAILLY :

1. **S'interroger collectivement sur le modèle de société que nous souhaitons :** Place de l'humain et de la machine, respect des valeurs fondamentales européennes, de notre souveraineté, etc.
2. **Mettre en place un Small Business Act européen :** À l'image du modèle américain, cet outil permettrait de protéger les données sensibles en Europe et de soutenir la compétitivité des entreprises locales dans la commande publique,
3. Commande publique : **Encourager nos entreprises françaises et européennes à se constituer en consortiums** pour atteindre une masse critique et offrir des solutions intégrées,
4. **Établir un réseau de référents en cybersécurité :** Nommer un référent numérique pour chaque bassin de vie, pour servir d'interface entre les collectivités territoriales et les autorités,
5. **Lister l'ensemble de leurs initiatives et actions pour les faire connaître des collectivités,** pour lesquelles les choix de traitement et d'hébergement de nos données, de celles des administrations et des entreprises, doivent être éclairés,
6. **Faire davantage connaître le dispositif de cyberprotection publique qui s'articule autour de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et d'un réseau de CERT (Computer Emergency Response Team),** organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ce sont des centres d'alerte et de réaction aux attaques informatiques, dont les informations sont accessibles à tous,
7. **Faire de la formation aux élus et administrations une grande cause nationale** pour accélérer leur acculturation,
8. **S'assurer des bonnes compréhension et application de la circulaire sur l'utilisation du cloud dans le secteur public,** pour encadrer la gestion et la sécurité des données sensibles,
9. **Adopter une stratégie multicloud :** Diversifier les prestataires de cloud pour éviter la concentration des données auprès d'un seul acteur, assurant ainsi une meilleure sécurité et indépendance des données,
10. **Instaurer des incitations fiscales et des labels verts** pour promouvoir les solutions numériques respectueuses de l'environnement et protectrices de la vie privée.

LES RECOMMANDATIONS D'ANTOINE COROLLEUR :

1. **Élaborer des cahiers des charges** porteurs d'une vision claire et adaptés aux besoins spécifiques, dès la phase de conception des projets.
2. **Mettre un accent particulier sur la maîtrise des données par les collectivités :** garantir leur stockage local tout en permettant une flexibilité aux partenaires pour la visualisation des données. Deux options sont envisageables :
   - Conserver un maximum de propriété sur les infrastructures et réseaux en hébergeant les serveurs dans un data center propre.
   - Considérer l'utilisation de solutions SaaS et de data centers externes, sous réserve qu'elles soient européennes et que les données soient stockées sur des serveurs locaux sécurisés.
3. **Assurer une continuité dans l'accès aux données** en intégrant des clauses de réversibilité solides dans les cahiers des charges.
4. **Exiger des prestataires des délais d'intervention courts** afin d'assurer un service efficace et agile.
5. **Intégrer l'anonymat des données** dès la conception des projets afin de renforcer la confiance des administrés.
6. **Promouvoir une prise de conscience des thématiques liées à la souveraineté numérique** au sein des administrés et de l'écosystème économique.
7. **Favoriser la mutualisation des ressources** pour garantir l'usage de solutions les plus souveraines, éthiques et sécurisées possibles, tout en maintenant un coût maîtrisé.

LES RECOMMANDATIONS DE JEAN-PIERRE SABIO :

1. **Garantir un accès sécurisé aux données :** Assurer que les collectivités locales disposent d'un accès complet et sécurisé à leurs données grâce à des réseaux entièrement contrôlés par leurs soins.
2. **Promouvoir la mutualisation :** Encourager la collaboration entre acteurs locaux et nationaux lors des appels d'offres pour renforcer notre compétitivité face aux entreprises extraterritoriales.
3. **Développer des plateformes d'achat public :** Concevoir et mettre en place davantage de structures de type plateforme d'achat public, tout en respectant les règles de concurrence, afin d'accélérer la croissance des acteurs économiques nationaux.
4. **Favoriser les collaborations avec des tiers de confiance :** Inciter les collectivités à collaborer plus étroitement avec des opérateurs publics de confiance, comme Gigalis, pour mieux définir leurs besoins. Cela permettra d'assurer une adéquation optimale des solutions proposées et de garantir une mise en concurrence équitable.
5. **Revoir la limite de 20 % de chiffre d'affaires :** Augmenter ou supprimer le quota actuel de 20 % de chiffre d'affaires hors adhérents afin de permettre aux GIP de mieux servir un plus grand nombre de collectivités.

LES RECOMMANDATIONS D'ALEXANDRE DESROUSSEAUX :

1. **S'assurer que l'hébergement et la maîtrise des données sont sous contrôle local**, en évitant les dépendances excessives aux logiciels tiers.
2. **Fédérer les acteurs nationaux et européens :** Collaborer avec des partenaires pour créer des solutions locales tout en développant des champions nationaux et européens.
3. Pour surmonter le manque d'ingénierie locale, **former les élus et les responsables locaux sur les bonnes pratiques en matière de souveraineté numérique et de cybersécurité :** webinaires, plateformes dédiées, demi-journées de sensibilisation régulières, etc.
4. **Créer un guichet unique pour la souveraineté numérique et la cybersécurité**, servant de point central d'accès aux ressources et informations.
5. **Veiller à ce que les actions de sensibilisation, comme les fresques du numérique, ne soient pas culpabilisantes, mais constructives et adaptées aux réalités locales**.
6. **Assurer réversibilité et interopérabilité :** Veiller à ce que les solutions numériques permettent un changement de prestataire sans perte de contrôle des données.

LES RECOMMANDATIONS DES INTERVENANTS

DE L'ATELIER : Comment garantir la confidentialité et la sécurité des données personnelles tout en tirant parti des innovations numérique dans des territoires de plus en plus connectés ?

1. **Respect du principe de proportionnalité :** S'assurer que la collecte de données soit strictement nécessaire aux objectifs définis au début du projet, sans excès.
2. **Distinguer les usages et développer des infrastructures dédiées :** Clarifier la différence entre les outils de la Safe City (sécuritaires et encadrés) et ceux des Smart Cities (territoires intelligents) qui ne nécessitent pas toujours de captation de données personnelles, et développer des infrastructures différentes
3. **Captation non intrusive :** Privilégier des méthodes de captation qui ne collectent pas de données personnelles, comme la réduction de la qualité des images dès la conception.
4. **Minimisation des données :** Collecter uniquement les informations nécessaires au projet et rien de plus.
5. **Limitation de la conservation des données :** Supprimer les données dès qu'elles ont été utilisées pour éviter toute conservation excessive.
6. **Traitement local des données :** Veiller à ce que les données soient traitées localement pour prévenir leur fuite, idéalement sans connexion internet.
7. **Transparence et traçabilité :** Proposer une présentation détaillée et ouverte des données collectées, par exemple via des QR codes, pour rassurer les citoyens sur le cheminement des données des solutions choisies.
8. **Renforcement de la CNIL :** Faire de la CNIL un guichet unique accessible pour obtenir des conseils et des sanctions, avec un élargissement de ses moyens et de son périmètre d'action.

LES RECOMMANDATIONS DES INTERVENANTS :

DE L'ATELIER : Numérique & Territoires : Quelles stratégies et leviers pour renforcer l'adoption de solutions garantissant la souveraineté des données ?

1 **Faire le choix d'infrastructures souveraines**

- Localisés en Europe, pour garantir une maîtrise des données et réduire les dépendances aux lois extraterritoriales.
- Exiger des garanties pour assurer la sécurité et l'interopérabilité des solutions de stockage de données.
  A noter : La certification SecNumCloud est un premier gage de sécurité mais, selon certains intervenants, ne constitue pas pour autant l'Alfa et l'Omega car elle permet une part minimale de capitaux extra-européens.
- Privilégier l'utilisation d'infrastructures supportées par des capitaux exclusivement européens
- S'assurer de la réversibilité des solutions pour permettre des transitions sans blocage.

2 **Encourager l'utilisation de logiciels souverains :**

- Éviter les solutions qui limitent le contrôle des données, comme certaines plateformes cloud qui réservent des droits d'utilisation des contenus (e.g., Adobe).
- Favoriser des logiciels développés par des acteurs locaux pour une maîtrise complète de la couche logicielle, réduisant les vulnérabilités liées à l'accès à Internet.

3 **Harmoniser la cybersécurité à travers la directive NIS 2 :**

- Anticiper les nouvelles exigences de cybersécurité et de souveraineté liées à l'élargissement de la qualification de «données essentielles» à certaines données traitées quotidiennement au sein des collectivités de toutes nature : archives, eau, énergie, transports…
- S'assurer qu'elles restent sous hébergement national ou européen.

4 **Améliorer la sensibilisation à tous les niveaux :**

- Mettre en place des formations continues et des simulations pour renforcer la prise de conscience des risques parmi tous les acteurs (collectivités, entreprises, citoyens).
- Engager une communication efficace pour surmonter le manque d'intérêt de certaines collectivités envers les enjeux numériques critiques.

5 **Faciliter la transition numérique avec une approche progressive :**

- Adopter une stratégie par étapes pour soutenir les collectivités de toutes tailles, en particulier les plus petites, afin d'éviter les choix bloquants et de garantir une adaptation en douceur aux nouvelles exigences.
- Ne pas exclure systématiquement les solutions non-européennes, mais garantir leur conformité avec des critères de souveraineté et de flexibilité / réversibilité.

6 **Créer un modèle exportable et compétitif :**

- Encourager les entreprises françaises à se démarquer sur le marché international en valorisant la sécurité et la durabilité de leurs solutions souveraines, adaptées aux exigences locales d'autres pays.
- Favoriser la mutualisation des PME pour qu'elles puissent rivaliser avec les grands groupes sur les marchés publics et renforcer leur pérennité par des collaborations territoriales.

7 **Indépendance financière des collectivités :**

- Promouvoir des initiatives d'autofinancement et de mutualisation au sein des collectivités pour réduire la dépendance aux subventions de l'État, notamment en mutualisant infrastructures et ressources entre départements et intercommunalités.

GLOSSAIRE

ANCT : Agence Nationale de la Cohésion des Territoires

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information, autorité française en charge de la cybersécurité

ARCEP : Autorité de Régulation des Communications Électroniques et des Postes

BATX : Acronyme des géants technologiques chinois : Baidu, Alibaba, Tencent, Xiaomi.

Backdoor : Accès secret contournant les sécurités numériques.

By design : Pensé / conçu dès l'origine

CAPEX / OPEX : CAPEX (Capital Expenditure) : Dépenses en investissements, achats d'actifs durables.

OPEX (Operational Expenditure) : Dépenses opérationnelles courantes pour maintenir l'activité.

CERT de l'ANSSI : Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, dédié à la gestion des incidents de cybersécurité en France.

CNIL : Commission Nationale de l'Informatique et des Libertés

CSIRT, Computer Security Incident Response Team : Équipe spécialisée dans la gestion des incidents de sécurité informatique.

DDoS : Distributed Denial of Service, attaque visant à rendre un service en ligne indisponible en saturant ses serveurs de trafic provenant de multiples sources.

DSI : Direction des Systèmes d'Information

DTN : Direction de la Transformation Numérique

HDS : Prestataires agréés en France pour héberger des données de santé conformément aux normes de sécurité et de confidentialité.

FFTH : Fiber To The Home (FIBRE OPTIQUE). Technologie de connexion internet où la fibre optique est installée directement dans le foyer de l'utilisateur.

France Très Haut Débit (THD) : Programme national de déploiement de la fibre optique.

GAFAM : Acronyme des cinq géants technologiques américains : Google, Apple, Facebook, Amazon, Microsoft.

HDS : Hébergement des données de santé

HPC (High-Performance Computing) : Calculs complexes à haute performance, utilisant des superordinateurs.

Hyperviseur : Logiciel permettant de gérer et virtualiser plusieurs systèmes d'exploitation sur une même machine.

In silico : Expérimentations ou simulations réalisées par ordinateur.

IoT : Internet des objets. Réseau d'objets connectés échangeant des données.

ISO, normes :
- ISO 50001 : Optimisation de l'efficacité énergétique.
- ISO 14001 : Réduction de l'impact environnemental.
- ISO 9001 : Garantie de qualité des produits/services.
- ISO 27001 : Garantie de la sécurité des informations.

On-Premise : Logiciel hébergé localement, en interne.

OIV : Opérateur d'Importance Vitale

PUE : Power Usage Effectiveness. Indicateur de l'efficacité énergétique d'un centre de données.

PSSI : Politique de Sécurité des Systèmes d'Information. Ensemble de règles et mesures définissant la sécurité des informations au sein d'une organisation.

QR Code : Code-barres lisible par smartphone.

RSSI : Responsable de la Sécurité des Systèmes d'Information

SDAN : Schéma Directeur d'Aménagement Numérique. Plan stratégique définissant l'organisation et l'évolution des systèmes d'information d'une organisation.
Service Départemental d'Incendie et de Secours (SDIS)

SAIV : Système d'alerte pour la protection des infrastructures critiques

Smart City : Ville intelligente. Ici, également « Territoires intelligents ».

SecNumCloud : Référentiel de sécurité délivré par l'ANSSI, certifiant les prestataires de services cloud répondant aux exigences de sécurité pour héberger des données sensibles.

SI : Système d'Information

Tier 3 : Certification garantissant une redondance des systèmes et 99,982% de disponibilité annuelle des data centers.

UGAP : Union des Groupements d'Achats Publics, Organisme public français d'achat groupé de biens et services pour les administrations et collectivités.

URL : Adresse web permettant d'accéder à une ressource sur Internet.

Vidéoprotection / surveillance algorithmique : Surveillance vidéo utilisant intelligence artificielle.

Safe City : Ville utilisant des technologies pour assurer la sécurité publique (Exemple : vidéosurveillance algorithmique)

LISTE DES CONTRIBUTEURS

REMERCIEMENTS

Nous tenons à exprimer notre gratitude à l'ensemble des contributeurs de ce guide :

Didier ARZ, Antoine COROLLEUR, Patrick CHAIZE, Cécile CHABRELE, Pascal CHEVALLOT, Fabrice COUPRIE, Arnaud MERCIER, Laurent DAUDE, Alexandre DESROUSSEAUX, Anne EUSEBE, Herinirina FANEVAMAMPIANDRA, Audrey LINKENHELD, Marc LOUIS-MARIE, Gabriela MARTIN, Jean-Christophe MIFSUD, Sophie METTE, Catherine MORIN-DESAILLY, Séverine REYNAUD, Gaëtan PONCELIN de RAUCOURT, Jean-Baptiste POLJAK, Gilles PIRMAN, Philippe PORTAL, Pierre QUINTARD, Miroslav SVIEZENY, Jonathan SIDGWICK, Nicolas SAINTHERANT, Jean-Pierre SABIO, Bertrand SERP, Louis TONDEUR, Fabrice LÉRIQUE, Magali ROGER, Philippe LATOMBE, Laure de LA RAUDIERE et l'équipe organisatrice.

Contacts FNCCR

Jean-Luc SALLABERRY,
Chef du département Numérique
jl.sallaberry@fnccr.asso.fr

Sandrine GUIRADO
Cheffe du service communication
s.guirado@fnccr.asso.fr

Contacts Club Numérique & Territoires

Linda SISSI
Déléguée
linda.sissi@compublics.com / 06 42 84 53 49

Guillaume METIVIER
Délégué collectivités
guillaume.metivier@compublics.com / 06 60 741 746

FNCCR
SERVICES PUBLICS LOCAUX DE L'ÉNERGIE, DE L'EAU, DE L'ENVIRONNEMENT ET DES E-COMMUNICATIONS

CLUB NUMÉRIQUE & TERRITOIRES
POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR