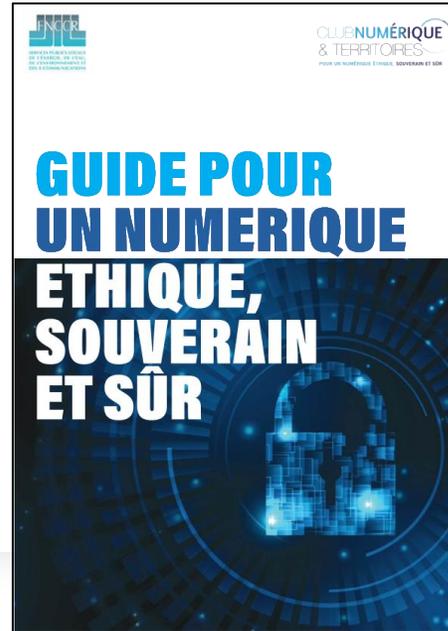


RESTITUTION DU GUIDE POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR



11 février 2025, FNCCR

Bilan 2024 – perspectives 2025 du Club

LE CLUB NUMÉRIQUE & TERRITOIRES

- Lancé en 2016 en lien avec la Commission Supérieure du Numérique & des Postes et des fédérations du secteur
- Objectif : Faire avancer les solutions en faveur du numérique 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 engagées.

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 porteurs 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**



LES 5 PILIERS DE L'ACTION DE LA FNCCR

- 1/ Infrastructures de communications électroniques
- 2/ Données territoriales et information géographique
- 3/ Usages, services et inclusion numériques
- 4/ Territoires connectés et durables
- 5/ Cybersécurité



SERVICES PUBLICS LOCAUX
DE L'ÉNERGIE, DE L'EAU,
DE LA GESTION DES DÉCHETS,
DES TÉLÉCOMMUNICATIONS
ET DE L'ENVIRONNEMENT

LA FNCCR

Le numérique, transverse à l'ensemble des secteurs, est une compétence à part entière de la FNCCR. Derrière le terme « numérique », deux compétences distinctes :

Services publics de communications électroniques

La FNCCR regroupe des collectivités locales, départements, agglomérations, syndicats mixtes et syndicats d'énergie, impliqués dans le déploiement de réseaux d'initiative publique (RIP) visant à garantir un accès à très haut débit fixe et mobile dans leur territoire. Elle œuvre pour la rationalisation des dépenses nécessaires au développement de ces réseaux, pour l'essentiel en fibre optique, par la gestion et la valorisation des infrastructures d'accueil (canalisations souterraines, points hauts, objets connectés, appuis aériens, etc.) propriétés des collectivités, la mutualisation des travaux de génie civil notamment avec d'autres services publics locaux (eau, énergie, ...). Elle milite pour la mise en place de systèmes de péréquation à l'échelon régional voire national, ainsi que pour la défense et la viabilité économique des RIP.

Mutualisation informatique et e-administration (MIEA)

La FNCCR regroupe des structures de mutualisation informatique, métropoles, agglomérations, syndicats ou associations publiques, qui, très tôt, ont pris conscience de la nécessité de produire en commun des services informatiques pour les besoins propres des collectivités, en particulier les plus petites, lesquelles ne disposent ni des moyens ni des ressources en la matière. Ces services informatiques visent la bureautique, la cartographie, les moyens internet, dont les plates-formes de stockage des données et applications. La FNCCR œuvre au sein des instances nationales pour la mise en œuvre de la dématérialisation et de la e-administration dans l'intérêt des collectivités, pour toujours plus d'efficacité au bénéfice des citoyens.

Le département numérique organise régulièrement des groupes de travail et des colloques ouverts aux non-adhérents.

OBJECTIFS DU GUIDE

- **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



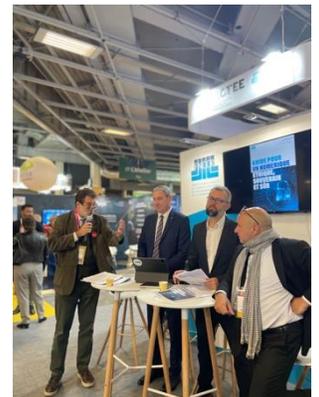
SERVICES PUBLICS LOCAUX
DE L'ÉNERGIE, DE L'EAU,
DE LA GESTION DES DÉCHETS,
DES TÉLÉCOMMUNICATIONS
ET DE L'ENVIRONNEMENT

CLUB **NUMÉRIQUE**
& TERRITOIRES

POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR

LE GUIDE EN QUELQUES MOTS

- **Fruit de 3 ateliers de travail en 2024 réunissant adhérents du club et de la FNCCR :**
 - Atelier 1 10/06/24 : présentation des enjeux, pourquoi avancer vers un numérique éthique, souverain et sûr ?
 - Atelier 2 01/09/24 : Souveraineté numérique & cybersécurité
 - Atelier 3 30/09/24 : Vie privée et protection des données
- **15 contributions & recommandations de décideurs publics – privés sur les enjeux soulevés**
- **1 évènement de restitution au salon des Maires et des collectivités locales le 21/11/24**
- **Un envoi à 4000 destinataires publics ciblés concernés – Janvier 2025**



AUTRES RENCONTRES DU CLUB

- 12 juin 2024 « **Quels leviers pour accélérer la mise en place d'un numérique de confiance ?** »

Avec les participations de

- Michel Cadic, Délégué ministériel adjoint aux industries de sécurité et à la lutte contre les cybermenaces, Ministère de l'Intérieur
- Jean-Luc Sallaberry, Chef du Département Numérique, FNCCR



- 5 novembre 2024 « **Compétitivité, autonomie stratégique, cyber...quels leviers pour accélérer le développement d'un numérique éthique, souverain et sûr ?** »

Invité d'honneur :

- Philippe Latombe, Député de la Vendée, Vice-président du groupe d'études sur la souveraineté numérique

Avec les participations de

- François Bonneau, Sénateur de la Charente
- Jean-Luc Sallaberry, Chef du Département Numérique, FNCCR
- Thierry Vinçon, Administrateur de l'État, Direction des Entreprises et Partenariats de Sécurité et des Armes (DEPSA), ministère de l'Intérieur



ENSEIGNEMENTS

- **I- Souveraineté numérique et cybersécurité**
 - Des défis pour notre autonomie stratégique, jusqu'au cœur des territoires
 - De vrais enjeux concurrentiels : rééquilibrer le rapport de force
- **II- Ethique**
 - La protection des libertés individuelles, un impératif pour la confiance des citoyens envers les institutions publiques
 - Impact environnemental du numérique
- **III- Commande publique : le levier des territoires pour structurer un numérique éthique, souverain et sûr**

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.

- 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.
- 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.
- 12 Faciliter l'accès des entreprises locales à la commande publique**
- 13 Élaborer des cahiers des charges avec une vision claire et précise dès la phase de conception** des projets publics.
- 14 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.
- 15 Favoriser la création de consortiums européens** en encourageant les entreprises à s'unir pour atteindre une masse critique et offrir des solutions intégrées compétitives.
- 16 Financement de la transition numérique**
- 17 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.
- 18 Proposer des incitations fiscales aux investisseurs privés soutenant les entreprises locales,** notamment dans le domaine du cloud computing.
- 19 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





PPL RESILIENCE INFRASTRUCTURES CRITIQUES ET RENFORCEMENT DE LA CYBERSECURITE

- **Commission spéciale au Sénat présidée par Olivier Cadic, Sénateur Français hors de France**
 - **Michel Canévet, Sénateur du Finistère, Co-Rapporteur**
 - **Catherine Morin Dessailly, Sénatrice de la Seine-Maritime, Secrétaire**

- **Prochaines réunions de la commission spéciale**
 - 11/02 : Tables rondes avec autorités de regulation financières & cyberdéfense
 - 4/03 : examen du rapport en commission
 - 11/03 : examen des amendements en commission
 - 11-12/03 : examen en séance publique

PERSPECTIVES 2025

Trump – Guerre en Ukraine – Deepseek - Europe : un contexte géopolitique qui démontre chaque jour l'importance des enjeux numériques

Transposition de la directive NIS 2:

- PPL Résiliences infrastructures critiques & renforcement de la cybersécurité
- Les données essentielles des collectivités à protéger : développer la souveraineté numérique et se protéger contre les cyberattaques
- Suivi réglementaire : arrêtés & décrets
- Comment accompagner cette nécessaire transition sur le plan financier ?

Commande publique :

- Diffusion du guide : quelles actions exemplaires aujourd'hui à diffuser ?
- Quelles évolutions à porter pour accélérer les nécessaires mutations ?

Evènements et sensibilisation :

- Dans les territoires, avec l'organisation de Rencontres Régionales Numérique & territoires avec l'appui de la FNCCR
- "SAV" guide & financement de la transposition NIS 2

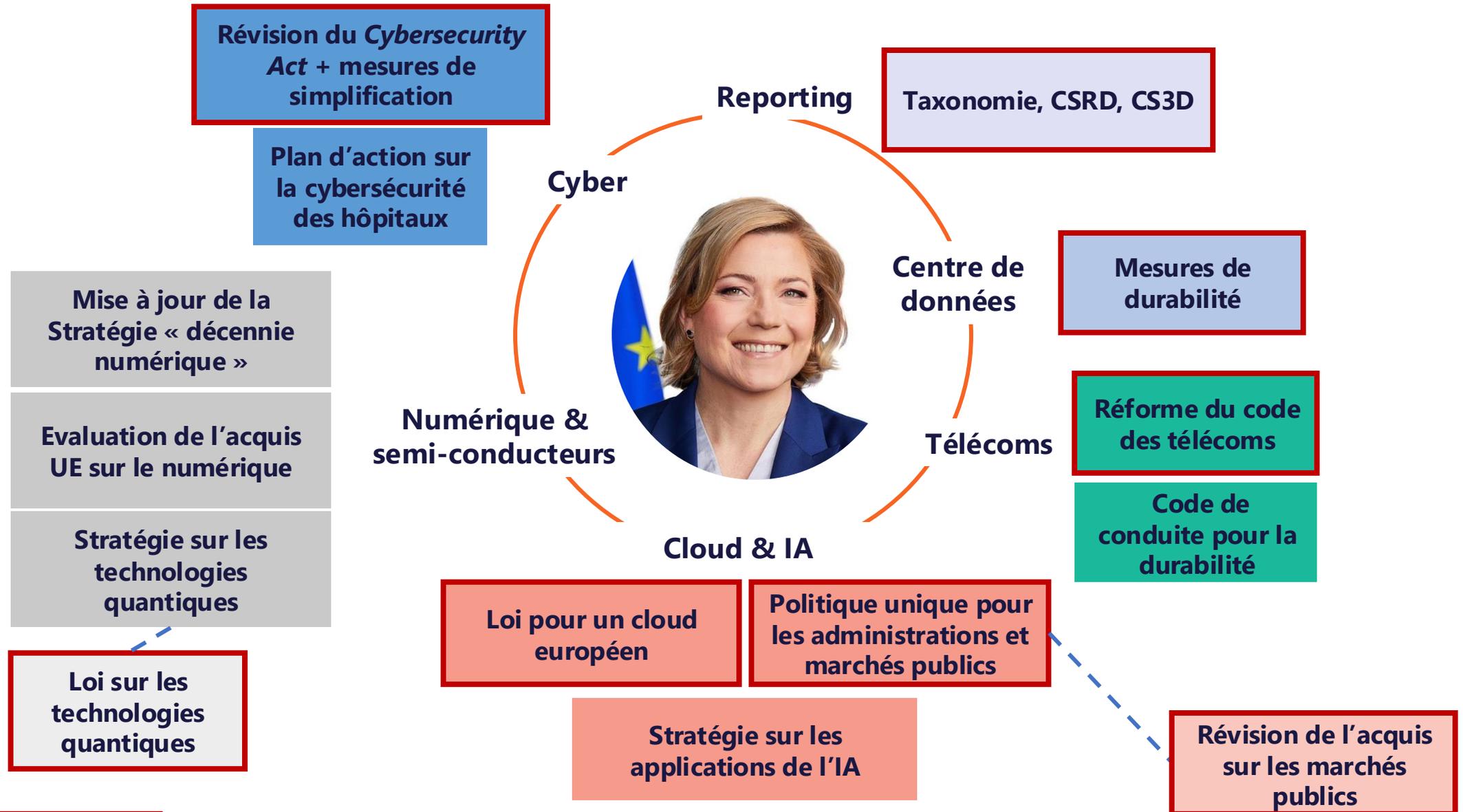


SERVICES PUBLICS LOCAUX
DE L'ÉNERGIE, DE L'EAU,
DE LA GESTION DES DÉCHETS,
DES TÉLÉCOMMUNICATIONS
ET DE L'ENVIRONNEMENT

CLUBNUMÉRIQUE
& TERRITOIRES

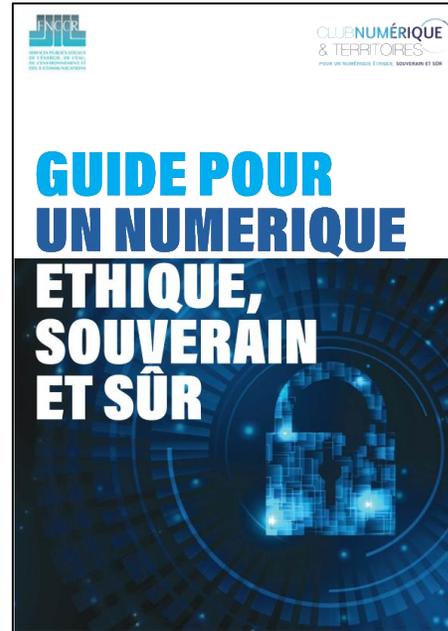
POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR

LES PRIORITÉS DE LA NOUVELLE COMMISSION



Réglementaire / contraignant

RESTITUTION DU GUIDE POUR UN NUMÉRIQUE ÉTHIQUE, SOUVERAIN ET SÛR



11 février 2025, FNCCR

Bilan 2024 – perspectives 2025 du Club