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