

GRAND DOSSIER • DONNÉES, CYBERSÉCURITÉ ET LIBERTÉ

Souveraineté numérique

Tenir ses données, donc son destin

Le numérique est devenu le système nerveux de la Nation. Une France qui ne maîtrise ni ses données, ni ses infrastructures, ni la formation de sa population délègue une part de sa liberté.

LA DOCTRINE

Le numérique doit étendre notre liberté, pas organiser notre dépendance.

01 — POURQUOI

Un territoire aussi réel que nos frontières

Les données de santé, de justice, d'éducation, d'énergie, de sécurité, de recherche et de solidarité forment la mémoire active du pays. Les réseaux, centres de données, logiciels et algorithmes constituent désormais un territoire stratégique.

Ce qui est vital pour la Nation ne peut dépendre entièrement d'un droit étranger, d'un fournisseur unique ou d'une infrastructure que nous ne contrôlons pas.

02 — DIAGNOSTIC

Trois dépendances à réduire

Données vitales Hébergement et traitements soumis à des droits ou prestataires étrangers.	Infrastructures Cloud, composants, réseaux et logiciels insuffisamment maîtrisés.
Compétences Pénurie de profils, culture numérique inégale et dépendance aux solutions fermées.	Décision Algorithmes opaques et concentration privée du pouvoir d'orienter l'attention.

03 — DÉFINITION

Les fondations souveraines

Cloud national Héberger sous droit français les données publiques et stratégiques, avec migration progressive des services vitaux.	Réseaux résilients Sécuriser fibre, centres de données, liaisons critiques, satellites et continuité en cas de crise.
Cyberdéfense 24 h/24 Relier État, armées, collectivités, hôpitaux, recherche et entreprises stratégiques.	Cryptographie Développer chiffrement, authentification et protections adaptées aux technologies présentes et futures.
Interopérabilité Faire communiquer les services autorisés sans multiplier saisies et fichiers contradictoires.	Filière industrielle Soutenir composants, serveurs, logiciels ouverts, robotique, IA et cybersécurité.

04 — CHOIX DÉMOCRATIQUE

Une identité protégée, pas une surveillance généralisée

La carte biométrique interopérable peut lutter contre l’usurpation, fiabiliser l’ouverture des droits et simplifier les services publics. Sa légitimité dépend de garde-fous inscrits dans la loi et contrôlés.

Nécessité Collecter uniquement les données indispensables à une finalité définie par la loi.	Transparence Permettre à chacun de connaître, corriger et suivre les accès à ses informations.
Contrôle indépendant Audits réguliers, sanctions effectives et révocation immédiate en cas d’incident.	Séparation Interdire le rapprochement généralisé des fichiers et les usages hors mission.
Sécurité Chiffrer les échanges et compartimenter strictement les accès.	Présence humaine Maintenir accueil physique et recours pour qu’aucun citoyen ne soit abandonné.

05 — INTELLIGENCE ARTIFICIELLE

Augmenter l'intelligence collective sans remplacer la décision humaine

Une intelligence artificielle nationale, sécurisée et ouverte à la recherche peut améliorer les services publics, accélérer la science et soutenir l'industrie. Elle ne doit ni manipuler l'attention ni rendre une décision publique impossible à comprendre ou à contester.

Algorithmes publics vérifiables Documentation, tests, audits, objectifs publiés et explication compréhensible.	Usages sensibles certifiés Évaluation indépendante dans l'éducation, la santé, la justice, la police et l'administration.
Décision humaine responsable Aucune machine ne devient l'alibi d'une décision sans auteur, recours ou responsabilité.	Attention protégée Encadrer les recommandations et combattre la manipulation, notamment des mineurs.

06 — INVESTISSEMENTS ET COMPÉTENCES

Former, produire et relier les territoires

École et esprit critique Vie privée, sources, images truquées, code, données et IA sans surexposition aux écrans.	Métiers numériques Cloud, réseaux, maintenance, électronique, robotique, cybersécurité et médiation.
Recherche et industrie Laboratoires, commandes publiques, logiciels ouverts, composants et coopération européenne.	Médiation de proximité Professionnels et lieux accessibles dans les départements, communes, quartiers et Outre-mer.
Budget 2028-2037 Programmer Cloud, cybersécurité, formation et équipements en distinguant investissement et fonctionnement.	Fonds souverains Mobiliser l'épargne longue pour les actifs numériques stratégiques et les filières françaises.

**RÈGLE
BUDGÉTAIRE**

Chaque investissement doit afficher son coût complet, son calendrier, ses risques, les dépendances évitées et la valeur économique ou publique créée.

07 — INTERACTIONS

Une souveraineté au service de toutes les autres

Santé et solidarité Protéger les données, garantir la continuité des soins et fiabiliser les droits.	Défense et sécurité Renseignement, cybersécurité, communications résilientes et infrastructures critiques.
Éducation et travail Former dès l'école et permettre la reconversion sans repartir de zéro.	Industrie et énergie Maîtriser automatismes, composants, réseaux, données et outils de production.

08 — TRAJECTOIRE 2028-2037

Auditer, sécuriser, former, puis reconstruire

Années 1 et 2 Cartographie des données et dépendances, audit des algorithmes publics, plan cyber et formation des agents.	Années 2 à 5 Cloud national progressif, interopérabilité prioritaire, filières de formation et premières commandes industrielles.
Années 5 à 10 Consolidation des composants, logiciels, centres de données, IA et capacités de recherche.	Évaluation annuelle Disponibilité, incidents, délais de rétablissement, données protégées, audits, personnes formées et emplois pourvus.

INDICATEURS PUBLICS

Vérifier pour corriger

Part des données vitales hébergées sous droit français ; disponibilité des services ; nombre et gravité des incidents ; délais de rétablissement ; systèmes sensibles audités ; compétences formées ; postes pourvus ; part des commandes bénéficiant aux filières nationales et européennes.

LA RÈGLE
COMMUNE

Une démocratie qui n'éduque pas l'esprit confie son avenir à ceux qui savent le manipuler. Protéger la mémoire du pays, c'est rendre à la Nation la capacité de décider.