



OBSERVER. COMPRENDRE. CONSTRUIRE.

PÔLE BLEU

VÉRITÉ & COMMANDEMENT

NUMÉRIQUE FRANÇAIS, DONNÉES, IA ET SOUVERAINETÉ TECHNOLOGIQUE

PROGRAMME COMPLET • VERSION V4

DJILALI HAKIKI • FONDATEUR DE LPE

OBSERVER. COMPRENDRE. CONSTRUIRE.

02

ARCHITECTURE DU PROGRAMME

Ministère n°02

NUMÉRIQUE FRANÇAIS, DONNÉES, IA ET SOUVERAINETÉ TECHNOLOGIQUE



Pôle	PÔLE BLEU — VÉRITÉ & COMMANDEMENT
Fonction du pôle	Le Bleu révèle.
Place du document	02 / 21 — NUMÉRIQUE

Le Bleu révèle. Le Blanc conçoit. Le Rouge réalise.

SOMMAIRE

Lecture structurée du diagnostic à l'exécution, puis aux annexes et instruments de contrôle.

PRÉAMBULE DOCTRINAL - NE PAS TRAHIR L'HÉRITAGE

PRINCIPE TRANSVERSAL — DISCRIMINATION ZÉRO

- 1. IDENTITÉ**
- 2. PREUVES D'ENTRÉE — VERSION CHIFFRÉE ET DOCTRINALE**
- 3. AUJOURD'HUI**
- 4. CE QUI A ÉTÉ FAIT JUSQU'ICI**
- 5. CE QUE NOUS CHANGEONS**
- 6. CADRAGE ET AUTORITÉ**
- 7. COMPÉTENCES TERRITORIALES**
- 8. ARCHITECTURE PUBLIC / PRIVÉ / MUTUALISÉ / CAPITALISÉ**
- 9. RESPONSABILITÉ CITOYENNE**
- 10. BASE JURIDIQUE**
- 11. MOYENS ET MÉTIERS**
- 12. PLAN DES 100 JOURS**
- 13. EXÉCUTION ANNÉE 1 À 5 + HORIZON 10-15 ANS**
- 14. PREUVE PERMANENTE, RISQUES ET CONTRÔLE**
- 15. DONNÉES**
- 16. COORDINATION**
- 17. DÉPENDANCES**
- 18. PUBLICS CONCERNÉS**
- 19. ENNEMIS STRUCTURELS**
- 20. CONDITIONS DE VICTOIRE**
- 21. COÛT POLITIQUE — VERSION CHIFFRÉE**
- 22. IRRÉVERSIBILITÉ**
- 23. PROFIL DU MINISTRE / COMMANDANT**
- 24. TABLEAU DE BORD PUBLIC**
- 25. RISQUES DE DÉRIVE ET GARDE-FOUS**
- 26. ATTAQUES / RÉPONSES**
- 27. TROIS NIVEAUX DE LECTURE**
- 28. SIMULATEURS LIÉS**
- 29. ARTICLES LIÉS**
- 30. QUIZ LIÉS**
- 31. SONDAGES LIÉS**
- 32. LEXIQUE LIÉ**
- 33. INFOS PRATIQUES**
- 34. MATÉRIEL DE CAMPAGNE**
- 35. RÉSULTAT POLITIQUE**

PRÉAMBULE DOCTRINAL — NE PAS TRAHIR L'HÉRITAGE NUMÉRIQUE

Nos anciens ont construit des routes, des écoles, des hôpitaux, des administrations, des services publics et des repères communs.

Ils n'ont pas tout transmis parfait.

Mais ils ont transmis un pays où l'on pouvait encore comprendre à qui parler, où déposer un dossier, où demander un droit, où contester une décision, où trouver un guichet, où serrer la main d'un agent, où être reconnu comme personne avant d'être traité comme numéro.

Le numérique aurait dû prolonger cet héritage.

Il aurait dû alléger la vie.

Il aurait dû libérer du temps.

Il aurait dû rendre l'État plus simple, plus rapide, plus proche, plus juste.

Mais trop souvent, il a transformé la paperasse en formulaire en ligne, l'attente en bug, le guichet en mot de passe perdu, la relation humaine en ticket automatique, et la souveraineté nationale en dépendance technique.

LPE refuse cette inversion.

Le numérique ne doit pas revendre au citoyen ce que l'État devrait déjà lui garantir : accès aux droits, simplicité, sécurité, continuité, dignité, contrôle et accompagnement humain.

Le numérique français doit réparer le lien entre l'État et le peuple.

Il doit protéger les données sans enfermer les citoyens.

Il doit simplifier sans surveiller.

Il doit former sans abandonner.

Il doit créer des outils sans créer de dépendance.

Il doit produire des imaginaires français au lieu de laisser nos enfants grandir uniquement dans les mondes numériques des autres.

Le ministère n°2 existe pour une raison simple :

faire du numérique un outil de transmission, de souveraineté et de liberté retrouvable.

Formule :

Nous ne voulons pas entrer dans l'Histoire pour qu'on se souvienne de nous. Nous voulons simplement que ceux qui viennent après nous puissent dire : ils n'ont pas laissé tomber.

PRINCIPE TRANSVERSAL — DISCRIMINATION ZÉRO NUMÉRIQUE

Le numérique ne doit jamais devenir une machine froide qui reproduit, accélère ou cache les discriminations.

Aucune personne ne doit être exclue d'un droit, d'un service, d'un emploi, d'une formation, d'un logement, d'un soin, d'un crédit, d'une orientation ou d'une démarche parce qu'un formulaire, un algorithme, une plateforme, une base de données, un prestataire ou une administration l'a traitée injustement.

La discrimination numérique peut être visible ou invisible.

Elle peut venir :

- d'un algorithme biaisé ;
- d'un formulaire mal conçu ;
- d'une donnée fausse ;
- d'un nom ou d'une origine supposée ;
- d'un handicap non pris en compte ;
- d'une adresse stigmatisée ;
- d'un âge ;
- d'une situation familiale ;
- d'un niveau social ;
- d'un manque d'équipement ;
- d'un manque de compétence numérique ;
- d'une interface inaccessible ;
- d'une décision automatisée non vérifiée.

LPE refuse que la modernisation serve à masquer l'injustice.

Règle :

Tout outil numérique public ou financé par l'argent public doit être auditable, contestable, accessible, non discriminatoire et humainement réversible.

En cas de discrimination numérique établie :

- instruction rapide ;
- correction de la donnée ou de l'algorithme ;
- réparation de la victime ;
- suspension de l'usage fautif si nécessaire ;
- sanction de l'opérateur ou du prestataire ;
- publication statistique ;
- contrôle renforcé ;
- recours effectif.

Formule courte :

Argent public, service public, algorithme public : discrimination zéro, recours humain obligatoire.

1. IDENTITÉ

Pôle : Pôle Bleu — Vérité, Commandement, Puissance.

Formule du pôle : *La France qui voit clair, compte juste, commande, sécurise et pèse dans le monde.*

Formule courte : *La France qui pèse.*

Classement : Ministère n°2.

Nom complet : Ministère du Numérique français, des Données, de l'IA et de la Souveraineté technologique.¹

Fonction : Construire la colonne vertébrale numérique souveraine de l'État, protéger les données françaises, simplifier l'administration, sécuriser les services publics, former la population, maîtriser l'IA, réduire les dépendances technologiques, protéger les mineurs, défendre les libertés publiques, garantir un recours humain, prévenir les discriminations algorithmiques, soutenir la filière numérique française,

¹ Capacité à maîtriser les infrastructures, données, logiciels et technologies indispensables aux décisions nationales.

développer les jeux vidéo stratégiques, organiser les alliances européennes utiles et faire du numérique un outil de confort, de puissance, de protection, de continuité nationale, de production française et de création culturelle.

Mission courte : Faire du numérique un système nerveux national simple, sûr, souverain, utile au peuple, protecteur des libertés et incapable de devenir une machine de surveillance sociale.

Mesure centrale : Bâtir une architecture numérique souveraine, progressive, contrôlée et exécutable : FranceConnect sécurisé et complété, ERP d'État modulaire, coffre numérique citoyen limité d'abord aux documents administratifs simples, doctrine nationale de la donnée, accès par statuts strictement autorisés, journalisation de toute consultation, historique visible par le citoyen, droit de retrait pour situations sensibles, contrôle indépendant, IA publique uniquement comme outil d'accompagnement, cloud souverain lorsque possible et cloud maîtrisé lorsque nécessaire, cybersécurité territoriale, réserve cyber citoyenne et experte, protection des mineurs, formation numérique nationale, souveraineté progressive des paiements, open data utile, réversibilité fournisseurs, réduction des dépendances logicielles, contribution de consolidation de filière réinvestie dans le secteur, filière française du jeu vidéo structurée comme puissance culturelle, technologique, cognitive, médicale, industrielle et exportatrice, projet UNIVERS FRANCE comme grande licence numérique culturelle française, et tableau permanent coût / retour / risque / délai pour tous les grands projets numériques.

Doctrine : Le numérique doit servir la France, pas la rendre dépendante.

Il doit simplifier la vie, protéger les données, former les citoyens, sécuriser les services publics, augmenter la puissance productive, défendre les libertés publiques, créer des imaginaires français et libérer les Français de la paperasse.

Il ne doit jamais devenir :

- une surveillance sociale ;
- un fichier général de la population ;
- une décision automatique sans humain ;
- une barrière contre les personnes fragiles ;
- un accélérateur de discriminations ;
- une dépendance technique déguisée en modernité.

Ligne centrale validée :

Simplifier, protéger, souverainiser, former, créer, sans surveiller.

Slogan :

Le numérique doit servir la France, pas la rendre dépendante.

Règle d'or :

Tout outil numérique public doit supprimer plus de complexité qu'il n'en ajoute.

Phrase de souveraineté :

Une nation qui ne maîtrise pas ses données, ses logiciels, ses paiements, son IA et ses systèmes critiques ne commande plus totalement son destin.

Phrase de liberté :

L'État LPE organise les données pour supprimer la paperasse, pas pour surveiller la population.

Phrase culturelle numérique :

Le numérique français ne doit pas seulement protéger nos données. Il doit aussi produire nos imaginaires.

Phrase d'exécution :

Le numérique LPE ne sacralise pas les grands projets. Il sacralise le résultat.

2. PREUVES D'ENTRÉE — VERSION CHIFFRÉE

La France est déjà un pays numérisé.

Le sujet n'est plus de savoir si le numérique existe.

Il existe déjà dans les démarches administratives, les paiements, l'école, la santé, le travail, la recherche d'emploi, les impôts, les transports, les achats, les réseaux sociaux, les entreprises, la sécurité, les loisirs et les relations familiales.

Selon le Baromètre du numérique présenté en 2025, 94 % de la population est internautes, 84 % se connecte tous les jours, 73 % accomplit des démarches administratives en ligne et 33 % utilise l'intelligence artificielle Baromètre du numérique - economie.gouv.fr.

FranceConnect constitue déjà une porte d'entrée massive : la DINUM indique que FranceConnect a franchi le cap des 40 millions de citoyens connectés en juin 2024 et qu'il est utilisé par plus de 43 millions d'utilisateurs DINUM - FranceConnect.

Mais numériser ne signifie pas simplifier.

Une démarche en ligne peut rester une humiliation administrative si elle oblige le citoyen à chercher, scanner, recommencer, comprendre seul, attendre, relancer et prouver dix fois ce que l'État possède déjà.

La France ne souffre donc pas seulement d'illectronisme.

Elle souffre aussi de paperasse numérisée.

En 2021, 15,4 % des personnes de 15 ans ou plus étaient en situation d'illectronisme : 13,9 % n'avaient pas utilisé Internet dans les trois derniers mois et 1,5 % l'avaient utilisé sans posséder les compétences numériques de base. 28 % des internautes avaient des capacités numériques faibles. Chez les 75 ans ou plus, l'illectronisme atteignait 61,9 % ; dans les DOM, 20 % contre 15 % en métropole INSEE - Illectronisme 2021.

La cybermenace confirme l'urgence.

En 2024, l'ANSSI a traité 4 386 événements de sécurité, soit +15 % par rapport à 2023, avec 3 004 signalements et 1 361 incidents ANSSI - Panorama de la cybermenace 2024.

Les hôpitaux, communes, écoles, PME, associations et citoyens vulnérables ne peuvent pas être laissés seuls face à cette pression.

Le numérique hospitalier est un cas d'école : multiplicité des applications, équipements obsolètes, budgets SI insuffisants, attaques par rançongiciel, pertes d'activité et délais de reconstruction parfois considérables. Les chiffres détaillés doivent être consolidés dans la data room, mais le constat est clair : une cyberattaque n'est pas seulement un problème informatique ; c'est une rupture de soins, d'organisation et de continuité nationale.

L'IA est déjà entrée dans la vie quotidienne, mais la confiance reste fragile.

Elle peut aider à comprendre, trier, résumer, traduire, détecter, simuler, orienter.

Mais elle peut aussi décider sans expliquer, reproduire des biais, invisibiliser des erreurs, produire des faux, surveiller, discriminer ou remplacer le jugement humain.

La donnée devient une infrastructure nationale.

Les données administratives, fiscales, sociales, médicales, scolaires, territoriales, économiques et environnementales peuvent améliorer les politiques publiques.

Mais elles posent des questions vitales :

- confidentialité ;
- finalité ;
- proportionnalité ;
- accès ;
- recours ;
- traçabilité ;
- contrôle démocratique ;
- interdiction de la surveillance sociale.

Les paiements sont aussi une infrastructure stratégique.

La France doit renforcer CB, Wero et les solutions européennes sans brutaliser les usages existants ni couper les Français de Visa et Mastercard.

Le jeu vidéo est une filière stratégique sous-estimée.

La base LPE retient environ 700 studios en 2021, 1 350 jeux en production, une majorité de créations originales et une forte part d'export. Ces données doivent être conservées mais classées À ACTUALISER dans la data room si une source sectorielle plus récente est disponible.

Le jeu vidéo n'est pas seulement un loisir.

C'est :

- logiciel ;
- moteur 3D ;
- simulation ;
- IA ;
- graphisme ;
- narration ;
- formation ;
- santé cognitive ;
- motricité ;
- mémoire ;
- tourisme ;
- patrimoine ;
- export ;
- souveraineté culturelle.

La France ne doit pas seulement consommer les grands univers numériques américains ou japonais.

Elle doit produire son propre grand univers numérique mondial : UNIVERS FRANCE.

Formule :

La France a déjà numérisé massivement ses usages. LPE doit maintenant rendre ce numérique simple, souverain, humain, contrôlé, sécurisé, productif, mesurable, non discriminatoire et créateur d'imaginaire.

3. AUJOURD'HUI

Aujourd'hui, la France a numérisé une partie de son administration, mais elle n'a pas encore supprimé la logique de paperasse.

Le citoyen ne voit pas toujours la différence entre un dossier papier et un dossier en ligne.

Dans les deux cas, il doit souvent :

- répéter ;
- télécharger ;
- scanner ;
- prouver ;
- attendre ;
- relancer ;
- recommencer.

La France dispose pourtant d'atouts :

- ingénieurs ;
- chercheurs ;
- développeurs ;
- experts cyber ;
- administrations capables ;
- start-up utiles ;
- studios de jeu vidéo ;
- laboratoires ;
- industriels ;
- écoles ;
- talents publics et privés.

Mais cette puissance reste dispersée.

Le numérique actuel produit huit fractures.

Première fracture : la fracture administrative. Les citoyens se perdent dans les portails, mots de passe, justificatifs, délais, erreurs, interfaces différentes et demandes répétées.

Deuxième fracture : la fracture territoriale. Une métropole ou un grand CHU peut mieux se protéger qu'une petite commune, un petit hôpital, une école rurale, une PME ou un artisan.

Troisième fracture : la fracture générationnelle. Les enfants sont très exposés mais pas toujours formés. Les adultes utilisent beaucoup les outils sans toujours comprendre les risques. Les personnes âgées sont plus vulnérables aux arnaques.

Quatrième fracture : la fracture stratégique. Des fonctions vitales françaises reposent encore sur des technologies, plateformes, logiciels, clouds, paiements, composants ou standards que la France ne maîtrise pas assez.

Cinquième fracture : la fracture mentale. L'écran peut instruire, former, organiser, soigner, relier et aider. Mais il peut aussi distraire, isoler, exciter, polariser, harceler, voler l'attention et fragiliser les enfants.

Sixième fracture : la fracture productive. La France produit des talents numériques, mais trop de valeur part ailleurs : plateformes étrangères, clouds dominants, logiciels captifs, moteurs propriétaires, composants critiques, standards internationaux et dépendances contractuelles.

Septième fracture : la fracture culturelle numérique. La France possède un patrimoine immense, des territoires magnifiques, des récits puissants, des Outre-mer, des métiers, des paysages, des villes, des campagnes, des ports, des montagnes, de la gastronomie, de l'histoire et de la création. Pourtant, elle n'a pas encore bâti un grand univers numérique populaire, mondial, exportable et souverain.

Huitième fracture : la fracture discriminatoire invisible. Un système numérique mal conçu peut exclure sans insulter, refuser sans expliquer, trier sans assumer, discriminer sans laisser de visage. LPE refuse cette injustice froide.

Le ministère du Numérique doit donc tenir une ligne claire :

- oui au numérique utile ;
- non au numérique qui abîme ;
- oui à l'IA utile ;
- non à l'IA qui décide ;
- oui aux données organisées ;
- non à la surveillance sociale ;
- oui au confort administratif ;
- non au flicage ;
- oui aux outils pour les métiers ;
- non à la dépendance ;
- oui aux jeux vidéo utiles, culturels, cognitifs et exportables ;
- non aux plateformes qui captent l'attention sans responsabilité ;
- oui aux alliances européennes utiles ;
- non à la dilution de la souveraineté française ;
- oui à l'imaginaire numérique français ;
- non aux grands projets qui survivent seulement parce qu'ils ont déjà coûté cher.

Formule :

La France ne doit pas choisir entre paperasse et Big Brother. Elle doit construire un État numérique simple, cloisonné, contrôlé, humain, sanctionnable en cas d'abus et capable de produire ses propres mondes numériques.

4. CE QUI A ÉTÉ FAIT JUSQU'ICI

La France n'est pas partie de rien.

Des efforts réels ont été engagés :

- FranceConnect ;
- France Identité ;
- services publics en ligne ;
- démarches simplifiées ;
- RGPD ;
- CNIL ;
- ANSSI ;
- DINUM ;
- initiatives cyber ;
- stratégie cloud ;
- Mon espace santé ;
- France Num ;
- soutien à la French Tech ;
- programmes d'inclusion numérique ;
- réglementation européenne sur les plateformes, les données et l'intelligence artificielle.

Ces outils montrent qu'une base existe.

Mais l'État a souvent ajouté des couches numériques sans supprimer l'architecture ancienne.

Il a créé des portails sans toujours unifier les données.

Il a lancé des démarches sans toujours simplifier les règles.

Il a financé de l'innovation sans toujours organiser la commande publique pour faire grandir des champions souverains.

Il a régulé les plateformes sans toujours construire d'alternative.

Il a protégé juridiquement sans maîtriser matériellement.

Il a parfois dépendu de grands prestataires, de logiciels captifs, de contrats lourds, de migrations mal préparées ou de systèmes trop complexes pour être repris facilement.

La cybersécurité existe, mais les territoires restent fragiles.

La donnée est protégée, mais pas toujours sanctuarisée.

Les plateformes sont régulées, mais encore trop puissantes.

L'IA progresse, mais la souveraineté reste à construire.

Les paiements évoluent, mais la dépendance demeure.

Le jeu vidéo français existe, mais il est trop peu pensé comme filière culturelle, technologique, pédagogique, cognitive, industrielle et exportatrice.

La formation numérique existe, mais elle reste trop inégale.

L'accompagnement humain existe, mais il n'est pas garanti partout.

L'Europe est présente dans les textes, mais pas toujours assez dans les projets industriels concrets.

Le numérique français existe en morceaux.

Il doit devenir une colonne vertébrale.

Formule :

LPE ne casse pas ce qui fonctionne. LPE sécurise, complète, relie, contrôle, rend souverain et transforme la puissance numérique en puissance française.

5. CE QUE NOUS CHANGEONS

Nous faisons du numérique un ministère de souveraineté, de confort administratif, de protection mentale, de formation populaire, de puissance technologique, de libertés publiques, d'imaginaire culturel et d'exécution mesurable.

Nous arrêtons :

- les portails administratifs redondants ;
- les justificatifs répétés inutilement ;
- les achats numériques dispersés ;
- les logiciels critiques non audités ;
- les données vitales mal maîtrisées ;
- la dépendance naïve aux plateformes ;
- la complexité numérique vendue comme modernité ;
- la confusion entre simplification et surveillance ;
- l'exposition des enfants aux écrans sans cadre éducatif solide ;
- la formation numérique réservée aux initiés ;
- les outils professionnels inaccessibles aux petits métiers ;
- l'IA utilisée comme décisionnaire ;
- les contrats captifs ;
- les migrations numériques irréalistes ;
- le jeu vidéo traité comme un simple divertissement ;
- la contribution de filière perçue comme une taxe punitive alors qu'elle revient au secteur ;
- l'Europe utilisée comme alibi ;
- l'absence d'un grand univers numérique français ;
- les grands projets numériques sans clause d'arrêt ;

- les algorithmes publics non audités ;
- les discriminations numériques invisibles.

Nous créons :

- FranceConnect sécurisé, renforcé et complété ;
- ERP d'État modulaire, progressif, auditable, gouverné et stoppable ;
- coffre numérique citoyen limité d'abord aux documents administratifs simples ;
- doctrine nationale de la donnée ;
- statuts de confidentialité et d'accès par métier ;
- traçabilité obligatoire de toute consultation ;
- historique citoyen des accès ;
- droit de retrait et de blocage pour situations sensibles ;
- IA publique utile, auditée, encadrée et classée par criticité ;
- cloud souverain lorsque possible et maîtrisé lorsque nécessaire ;
- clause de non-migration automatique des données anciennes vers le coffre ;
- pilote de migration contrôlée ;
- plan cyber territorial phasé ;
- réserve cyber citoyenne et experte ;
- formation numérique progressive de toute la population ;
- protection renforcée des mineurs ;
- doctrine anti-deepfakes ;
- stratégie française et européenne des paiements ;
- outils numériques simples pour chaque métier ;
- filière française du jeu vidéo structurée ;
- stratégie composants critiques, semi-conducteurs et souveraineté logicielle ;
- doctrine open data pour les données publiques non personnelles ;
- clause de réversibilité dans les contrats numériques publics sensibles ;
- accompagnement humain garanti pour les services essentiels ;
- indice de confiance dans le numérique public ;
- fonds de consolidation de la filière numérique française ;
- cinq alliances européennes prioritaires ;
- projet UNIVERS FRANCE ;
- tableau coût / retour / risque / délai ;
- clause anti-usine à gaz ;
- audit anti-discrimination des algorithmes publics.

Règle IA :

Aucune décision publique individuelle ne doit être prise par l'IA. L'IA accompagne, trie, alerte, résume, simule, aide et accélère ; elle ne décide jamais à la place de l'humain.

Règle coffre numérique :

Le coffre numérique commence par des documents simples. Il ne commence jamais par la santé, la justice, l'enfance protégée, les violences conjugales, le handicap sensible ou les données sociales intimes.

Règle discrimination numérique :

Toute décision automatisée ou semi-automatisée qui affecte un droit doit être explicable, contestable et révisable par un humain.

Formule :

Un projet numérique public n'a pas le droit de survivre uniquement parce qu'il a déjà coûté cher.

6. CADRAGE ET AUTORITÉ

Le numérique devient une fonction régaliennne.

Une nation qui ne maîtrise pas son numérique ne maîtrise plus complètement :

- son économie ;
- sa santé ;
- sa défense ;
- sa justice ;
- ses paiements ;
- son information ;
- son administration ;
- ses données ;
- ses infrastructures ;
- sa démocratie.

Le ministère du Numérique reçoit donc une autorité transversale.

Il fixe les normes d'interopérabilité.

Il classe les données vitales.

Il impose les règles d'accès.

Il audite les logiciels critiques.

Il coordonne l'ERP d'État.

Il encadre l'IA publique.

Il protège les mineurs.

Il organise la cyberdéfense civile.

Il réduit les dépendances critiques.

Il pilote l'accompagnement humain numérique.

Il structure la réserve cyber.

Il soutient la filière du jeu vidéo stratégique.

Il pilote le projet UNIVERS FRANCE en coordination avec Culture et Patrimoine.

Il établit le tableau coût / retour / risque / délai des grands projets numériques.

Il impose la clause anti-usine à gaz.

Il impose l'audit anti-discrimination des algorithmes publics.

Principes d'autorité :

- l'ERP d'État doit être modulaire, progressif, auditable et phasé sur 10 à 15 ans ;
- les données vitales doivent être classées, cloisonnées et protégées ;
- l'accès aux données dépend d'un statut, d'une mission et d'une finalité ;
- toute consultation doit être journalisée ;
- le citoyen doit pouvoir consulter l'historique d'accès à ses données ;
- toute consultation abusive doit être sanctionnée ;
- l'IA publique ne décide jamais seule ;

- les mineurs doivent être protégés des plateformes addictives, frauduleuses, pornographiques, violentes, manipulateurs ou destructrices ;
- la formation numérique doit être progressive ;
- le numérique ne doit jamais remplacer les guichets humains nécessaires ;
- les données publiques non personnelles doivent être ouvertes par défaut sauf exception motivée ;
- tout contrat numérique sensible doit prévoir une réversibilité ;
- toute centralisation technique doit être compensée par un contrôle démocratique plus fort ;
- les données anciennes ne sont pas automatiquement migrées vers le coffre citoyen ;
- la stratégie européenne est intégrée lorsque l'Europe augmente la puissance française ;
- UNIVERS FRANCE doit être une licence culturelle ouverte à la création, pas un outil de propagande officielle ;
- tout grand projet numérique public doit publier son coût, son délai, son retour attendu, son risque et sa clause d'arrêt.

Clause de réversibilité :

Tout marché public numérique sensible au-dessus d'un seuil à définir comporte une clause obligatoire de réversibilité :

- formats ouverts ;
- documentation technique ;
- API ;
- schémas ;
- dépendances ;
- interfaces ;
- modalités d'export ;
- droits d'usage sur les adaptations spécifiques développées pour l'État ;
- procédures de transfert ;
- délais de sortie ;
- continuité de service ;
- transfert de compétence ;
- coûts de sortie ;
- sanctions contractuelles en cas de refus de coopération.

Gouvernance de l'ERP d'État :

L'ERP d'État est piloté par une instance interministérielle associant :

- ministère du Numérique ;
- Budget ;
- Intérieur ;
- Justice ;
- Armée ;
- Santé ;
- Éducation ;
- DINUM ;
- ANSSI ;
- CNIL ;
- Cour des comptes ;
- experts techniques indépendants ;
- représentants citoyens selon un cadre légal.

Critères du cloud maîtrisé :

Un cloud est maîtrisé s'il répond à six critères :

- données hébergées dans l'Union européenne ou cadre juridiquement compatible avec les intérêts français ;
- droit français ou européen applicable ;
- capacité d'audit ;
- réversibilité réelle ;
- accès journalisés et contrôlés ;
- maintenance par équipes habilitées et contrôlées.

Formule juridique centrale :

L'État LPE organise les données pour supprimer la paperasse, pas pour surveiller la population.

7. COMPÉTENCES TERRITORIALES

L'État décide :

- doctrine de souveraineté numérique ;
- architecture de l'ERP d'État ;
- règles du coffre numérique citoyen ;
- classification des données vitales ;
- normes d'interopérabilité ;
- statuts d'accès ;
- journalisation obligatoire ;
- doctrine IA publique ;
- grille IA par criticité ;
- exigences cyber ;
- stratégie cloud ;
- souveraineté des paiements ;
- protection des mineurs ;
- lutte contre les deepfakes ;
- commande publique numérique ;
- réduction des dépendances critiques ;
- doctrine open data ;
- règles de réversibilité fournisseurs ;
- charte du numérique libre et protecteur ;
- stratégie jeu vidéo et simulation ;
- projet UNIVERS FRANCE ;
- contribution de consolidation de filière ;
- alliances européennes utiles ;
- clause anti-usine à gaz ;
- audit anti-discrimination numérique.

L'État finance :

- ERP d'État ;
- coffre numérique citoyen pilote ;
- cloud souverain ou maîtrisé ;
- IA publique critique ;
- cybersécurité territoriale ;
- outils numériques mutualisés ;

- réserve cyber citoyenne ;
- formation numérique nationale ;
- infrastructures stratégiques ;
- outils métiers prioritaires ;
- cyberprotection des hôpitaux, citoyens vulnérables, communes, écoles et services publics ;
- filière jeu vidéo française ;
- UNIVERS FRANCE ;
- participation aux alliances européennes utiles.

L'État contrôle :

- conformité des accès ;
- usage des données ;
- audits cyber ;
- logiciels critiques ;
- plateformes ;
- protection des mineurs ;
- deepfakes ;
- fraudes numériques ;
- prestataires sensibles ;
- dépendances cachées ;
- respect des libertés publiques ;
- réversibilité des contrats ;
- ouverture des données publiques non personnelles ;
- indice de confiance numérique ;
- non-migration automatique des données anciennes vers le coffre ;
- conformité anti-discrimination des outils publics.

La région planifie :

- infrastructures numériques régionales ;
- data centers utiles ;
- formation numérique professionnelle ;
- filières IA ;
- filières cyber ;
- filières jeu vidéo ;
- liens avec l'industrie ;
- composants critiques ;
- reconversion numérique ;
- pôles régionaux de soutien aux PME ;
- cartographie régionale pour UNIVERS FRANCE.

Le département accompagne :

- inclusion numérique ;
- personnes âgées ;
- handicap ;
- publics fragiles ;
- travailleurs sociaux ;
- protection des familles ;
- aide aux démarches ;
- formation des aidants ;
- prévention des arnaques ;

- usages numériques adaptés à la mémoire, à la motricité et à la cognition.

La commune identifie :

- vulnérabilités cyber ;
- besoins de sauvegarde ;
- logiciels critiques ;
- urgences numériques ;
- écoles à protéger ;
- PME et commerces fragiles ;
- besoins d'accompagnement humain ;
- espaces de formation locale ;
- citoyens vulnérables face aux arnaques ;
- patrimoine local et récits pouvant alimenter UNIVERS FRANCE.

Le citoyen dispose de droits :

- ne plus fournir plusieurs fois les mêmes documents ;
- savoir qui consulte ses données ;
- être protégé contre les fraudes ;
- bénéficier d'une administration plus simple ;
- refuser les usages non nécessaires ;
- obtenir un recours en cas d'accès abusif ;
- demander un blocage en situation sensible ;
- conserver un accompagnement humain ;
- être formé à l'hygiène numérique ;
- contester une décision algorithmique.

Le citoyen a aussi des devoirs :

- protéger ses accès ;
- adopter une hygiène numérique de base ;
- ne pas harceler ;
- ne pas diffuser de deepfakes malveillants ;
- signaler les fraudes ;
- respecter la protection des mineurs ;
- former ses enfants à un usage sain des écrans ;
- respecter la dignité numérique d'autrui.

8. ARCHITECTURE PUBLIC / PRIVÉ / MUTUALISÉ / CAPITALISÉ

Public ou sous contrôle public direct :

- ERP d'État ;
- coffre numérique citoyen ;
- données régaliennes ;
- données de santé critiques ;
- données fiscales ;
- données judiciaires ;
- identité numérique ;
- normes d'interopérabilité ;

- IA publique critique ;
- statuts d'accès ;
- journalisation ;
- cyberdéfense civile ;
- protection des mineurs ;
- doctrine deepfakes ;
- décisions souveraines ;
- contrôle des accès ;
- open data public non personnel ;
- registre public des algorithmes ;
- indice de confiance numérique ;
- gouvernance de l'ERP ;
- tableau coût / retour / risque / délai ;
- clause anti-usine à gaz.

Privé sous contrôle strict :

- logiciels spécialisés ;
- certains services cloud ;
- outils IA non critiques ;
- outils métiers ;
- solutions cyber ;
- moteurs de jeu ;
- composants ;
- semi-conducteurs ;
- applications de paiement ;
- prestations de migration ;
- studios de jeu vidéo ;
- créateurs, auteurs, designers, artistes, historiens, géographes, architectes numériques, scénaristes, développeurs et équipes 3D d'UNIVERS FRANCE.

Condition :

Le privé peut produire, mais la France doit garder la maîtrise des données, des normes, des accès, de l'audit, de la réversibilité, de la continuité et du sens stratégique.

Mutualisé :

- outils numériques des administrations ;
- briques de cybersécurité ;
- systèmes de sauvegarde ;
- identités d'accès ;
- référentiels de données ;
- logiciels communs ;
- achats numériques ;
- protocoles de crise ;
- formations de base ;
- outils simples pour communes, écoles, hôpitaux, PME, artisans et agriculteurs ;
- briques 3D, cartographiques, patrimoniales et pédagogiques utiles à UNIVERS FRANCE.

Capitalisé :

- infrastructures cloud souveraines ou maîtrisées ;
- IA publique ;

- filières françaises du logiciel ;
- cybersécurité ;
- composants critiques ;
- semi-conducteurs ;
- jeu vidéo ;
- paiements souverains ;
- outils professionnels ;
- données publiques utiles ;
- formation nationale ;
- registre des algorithmes ;
- réserve cyber citoyenne ;
- jeux sérieux ;
- licence UNIVERS FRANCE ;
- moteurs 3D et simulation ;
- cartographie culturelle ;
- patrimoine numérique ;
- alliances européennes utiles.

Principe budgétaire :

On ne finance pas seulement des logiciels. On rachète de la dépendance, on réduit des risques, on supprime des doublons, on protège les données, on gagne du temps, on forme la population et on construit une infrastructure nationale.

Contribution de consolidation de filière :

Une contribution sectorielle peut être étudiée, calibrée juridiquement et économiquement, avec seuils de protection pour les petites structures, progressivité, prise en compte des marges et affectation intégrale au fonds de consolidation numérique.

Principe :

Ce que la filière verse revient à la filière.

9. RESPONSABILITÉ CITOYENNE

Le citoyen doit sortir de la position d'utilisateur perdu.

Il devient propriétaire moral de ses données, bénéficiaire du confort administratif et acteur de sa sécurité numérique.

Droits nouveaux :

- ne plus fournir dix fois les mêmes documents ;
- disposer d'un coffre numérique limité d'abord aux documents administratifs simples ;
- voir qui consulte ses données ;
- contester un accès abusif ;
- demander correction ;
- demander un blocage de certaines données en situation sensible ;
- bénéficier d'un accompagnement humain ;
- être protégé contre les fraudes ;
- être formé à l'hygiène numérique ;
- protéger ses enfants avec l'appui de l'État ;
- bénéficier d'outils numériques accessibles pour son métier ;

- accéder aux données publiques non personnelles utiles ;
- contester une décision algorithmique ;
- ne pas voir ses données anciennes automatiquement reversées dans le coffre numérique.

Droit de retrait et de protection sensible :

Tout citoyen peut demander, pour des motifs tenant à sa situation personnelle, que certaines catégories de données ne soient pas accessibles via le coffre numérique dans les usages ordinaires.

Cas concernés :

- violences conjugales ;
- harcèlement ;
- menace d'usurpation d'identité ;
- adresse protégée ;
- vulnérabilité particulière ;
- dossier médical sensible ;
- situation familiale à risque ;
- protection d'un mineur ;
- témoignage ou procédure judiciaire sensible.

En cas d'urgence, le blocage doit pouvoir être immédiat, sous contrôle ultérieur.

Formule :

La simplification administrative ne doit jamais mettre en danger une personne fragile.

Devoirs citoyens :

- protéger ses mots de passe ;
- utiliser l'authentification forte ;
- ne pas diffuser de faux contenus ;
- signaler arnaques et deepfakes ;
- respecter la dignité numérique d'autrui ;
- protéger les mineurs ;
- ne pas utiliser l'anonymat pour harceler ;
- accepter que certains accès professionnels soient tracés.

Formation nationale :

Avant la maîtrise de l'écriture, de la lecture, du langage, du geste, de l'attention et des bases relationnelles, le numérique ne doit pas devenir un refuge permanent.

À l'école, le numérique commence comme outil ludique, maîtrisé, pédagogique et limité.

Il ne remplace pas :

- l'écriture ;
- le professeur ;
- le livre ;
- la mémoire ;
- le sport ;
- la relation ;
- le réel.

Pour les adultes, la formation couvre :

- démarches ;

- cybersécurité ;
- IA ;
- protection des enfants ;
- fraude ;
- deepfakes ;
- outils métiers ;
- données personnelles ;
- paiements ;
- sauvegardes.

Pour les personnes âgées, l'objectif est double :

- protection contre les arnaques ;
- possibilité, pour les volontaires, de devenir transmetteurs d'hygiène numérique.

Objectifs LPE :

- tendre vers 0 % d'illectronisme chez les moins de 50 ans ;
- réduire fortement l'illectronisme chez les plus de 50 ans ;
- garantir qu'aucun service public essentiel ne devienne 100 % numérique sans alternative humaine.

Formule :

Un pays qui numérise ses droits doit former son peuple. Sinon, le numérique devient une barrière sociale.

10. BASE JURIDIQUE

La réforme repose sur une loi de souveraineté numérique, de protection informationnelle, de simplification administrative, de continuité numérique de l'État, de garanties fondamentales des libertés publiques et de non-discrimination algorithmique.

Charte du numérique libre et protecteur :

Elle repose sur dix engagements opposables :

1. L'État ne crée pas de fichier unique de tous les citoyens. 2. Nul ne peut accéder à une donnée sans motif légal, finalité précise, habilitation et traçabilité. 3. Chaque citoyen peut consulter l'historique des accès à ses données, sauf exception légale strictement encadrée. 4. Tout accès abusif à une donnée sensible est sanctionné. 5. Aucune décision publique individuelle n'est prise par l'IA. 6. Les personnes éloignées du numérique conservent un accompagnement humain. 7. Le coffre numérique citoyen est expérimenté, évalué et généralisé seulement après débat et vote. 8. Les données publiques non personnelles sont ouvertes par défaut dans des formats réutilisables. 9. La réserve cyber citoyenne est civile, volontaire, formée et encadrée. 10. Toute modification substantielle de cette charte fait l'objet d'un débat parlementaire renforcé.

La loi encadre :

- ERP d'État ;

- coffre numérique citoyen ;
- expérimentation territoriale ;
- interopérabilité obligatoire ;
- protection des données stratégiques ;
- statuts d'accès ;
- journalisation ;
- droit de retrait ;
- IA publique critique ;
- registre public des algorithmes ;
- cloud souverain ou maîtrisé ;
- cybersécurité ;
- réserve cyber ;
- obligations des plateformes ;
- protection des mineurs ;
- deepfakes ;
- fraudes numériques ;
- paiements ;
- commande publique numérique ;
- open data ;
- réversibilité fournisseurs ;
- contrôle indépendant ;
- indice de confiance ;
- fonds de consolidation de filière ;
- non-migration automatique des données anciennes ;
- UNIVERS FRANCE ;
- clause anti-usine à gaz ;
- audit anti-discrimination algorithmique.

Le système interdit explicitement :

- surveillance sociale généralisée ;
- scoring citoyen ;
- croisement massif sans finalité ;
- consultation de curiosité ;
- accès non tracé ;
- accès global par défaut ;
- partage commercial des données publiques personnelles ;
- utilisation politique des données individuelles ;
- décision automatique publique ;
- fichage idéologique, religieux, syndical, ethnique ou politique hors cadre légal strict ;
- algorithme discriminatoire fondé sur des critères protégés ;
- utilisation du coffre numérique pour constituer un fichier général de surveillance.

Contrôle indépendant :

LPE crée une autorité de contrôle des accès aux données publiques sensibles, associant :

- CNIL ;
- Parlement ;
- Cour des comptes pour les coûts et contrats ;
- Défenseur des droits ;
- représentants de la Justice ;
- experts cyber indépendants ;

- représentants citoyens selon cadre légal.

Cette autorité contrôle :

- accès abusifs ;
- journaux de consultation ;
- dérives de finalité ;
- demandes massives ;
- algorithmes publics ;
- décisions automatisées ;
- cybersécurité ;
- fournisseurs sensibles ;
- clauses de réversibilité ;
- incidents de données ;
- sanctions appliquées ;
- conformité anti-discrimination.

Formule juridique centrale :

Le numérique souverain n'est légitime que s'il rend l'État plus contrôlable par le citoyen, jamais le citoyen plus contrôlable par l'État.

11. MOYENS ET MÉTIERS

Moyens principaux :

- ERP d'État modulaire ;
- coffre numérique citoyen pilote ;
- cloud souverain ou maîtrisé ;
- IA publique souveraine ou maîtrisée selon criticité ;
- registre public des algorithmes ;
- état-major numérique souverain ;
- réserve cyber citoyenne et experte ;
- doctrine nationale de la donnée ;
- cellule deepfakes ;
- programme de cybersécurité territoriale ;
- programme outils métiers ;
- programme jeu vidéo stratégique ;
- programme UNIVERS FRANCE ;
- cellule souveraineté des paiements ;
- plan composants critiques ;
- centre national d'audit des logiciels publics ;
- plateforme de formation numérique populaire ;
- autorité de contrôle des accès ;
- programme open data ;
- programme réversibilité fournisseurs ;
- indice de confiance numérique ;
- fonds de consolidation de la filière numérique française ;
- cellule alliances européennes utiles ;
- cellule gouvernance ERP ;
- cellule coût / retour / risque / délai ;
- cellule anti-usine à gaz ;
- cellule anti-discrimination algorithmique.

Métiers critiques :

- architectes systèmes d'État ;
- ingénieurs IA ;
- experts cloud ;
- spécialistes cyber ;
- développeurs ERP ;
- ingénieurs data ;
- juristes numériques ;
- analystes fraude ;
- experts paiements ;
- spécialistes deepfakes ;
- experts accessibilité ;
- experts UX publique ;
- producteurs de jeux vidéo ;
- game designers ;
- développeurs moteurs ;
- techniciens simulation ;
- formateurs numériques ;
- experts protection de l'enfance numérique ;
- spécialistes outils agricoles ;
- spécialistes outils santé ;
- spécialistes outils PME et artisans ;
- spécialistes jeux sérieux ;
- experts vieillissement cognitif ;
- experts droit européen ;
- scénaristes de mondes ouverts ;
- historiens du patrimoine numérique ;
- cartographes 3D ;
- designers de territoires virtuels ;
- auditeurs coût / retour / risque / délai ;
- auditeurs de biais algorithmiques.

Réserve cyber :

Trois cercles :

Cercle 1 — Citoyens formés. Hygiène numérique, signalement, aide locale simple, prévention des arnaques.

Cercle 2 — Talents validés. Personnes compétentes, parfois sans parcours classique, testées, formées, encadrées et habilitées progressivement.

Cercle 3 — Experts mobilisables. Crises, audits, soutien hôpitaux, communes, écoles, PME, associations utiles, services publics.

Garde-fous :

- contrôle du casier judiciaire ;
- conflits d'intérêts ;
- risques de compromission ;
- habilitation progressive ;
- missions limitées ;
- traçabilité ;

- supervision publique.

Formule :

La France ne doit pas gâcher ses talents cachés, mais aucun talent ne doit entrer dans la cybersécurité publique sans contrôle strict.

12. PLAN DES 100 JOURS

Les 100 jours ne livrent pas l'ERP.

Ils livrent la doctrine, l'audit, la loi-cadre, les priorités, les garde-fous et le récit public.

Jours 1 à 30 : doctrine et audit

- installation de l'état-major numérique souverain ;
- audit national des dépendances numériques ;
- cartographie des données vitales de l'État ;
- identification des systèmes publics redondants ;
- plan cyber d'urgence pour hôpitaux, citoyens vulnérables, communes, écoles et services publics vulnérables ;
- doctrine : numérique souverain sans surveillance sociale ;
- cadrage juridique du coffre numérique citoyen ;
- préparation du débat public sur le coffre ;
- cadrage de l'expérimentation dans deux territoires volontaires ;
- cadrage du fonds de consolidation de filière ;
- cellule alliances européennes utiles ;
- non-migration automatique des données anciennes ;
- critères du cloud maîtrisé ;
- cadrage initial d'UNIVERS FRANCE ;
- cellule coût / retour / risque / délai ;
- clause anti-usine à gaz.

Jours 31 à 60 : règles et prototypes

- cadre de l'ERP d'État modulaire ;
- gouvernance de l'ERP ;
- doctrine nationale de la donnée ;
- statuts d'accès ;
- journalisation obligatoire ;
- réserve cyber citoyenne et experte ;
- doctrine IA d'accompagnement ;
- grille IA par criticité ;
- doctrine plateformes, mineurs, deepfakes et fraude numérique ;
- audit paiements ;
- formation numérique nationale ;
- open data ;
- réversibilité fournisseurs ;
- indice de confiance numérique ;
- programme jeu vidéo stratégique ;
- programme jeux vidéo seniors, mémoire, motricité et cognition ;
- cadrage d'UNIVERS FRANCE ;
- cinq alliances européennes prioritaires ;
- sept premiers cahiers des charges outils métiers.

Jours 61 à 100 : loi-cadre et visibilité

- présentation de la loi de souveraineté numérique ;
- annonce des premières migrations prioritaires ;
- lancement programme outils métiers simples ;
- lancement programme jeu vidéo stratégique ;
- étude de préproduction UNIVERS FRANCE ;
- plan d'éducation numérique progressive ;
- tableau de bord public ;
- charte "confort administratif sans surveillance sociale" ;
- doctrine cloud souverain / cloud maîtrisé ;
- calendrier de débat public sur le coffre ;
- budget prévisionnel sur 10 ans par scénarios ;
- calendrier d'interopérabilité ;
- principe de contribution de filière réinvestie ;
- règle de non-migration automatique ;
- tableau coût / retour / risque / délai des dix projets prioritaires ;
- clause anti-usine à gaz.

Formule :

Les 100 jours ne construisent pas toute la souveraineté numérique. Ils empêchent qu'elle reste un slogan.

13. EXÉCUTION ANNÉE 1 À 5 + HORIZON 10-15 ANS

Année 1 : installation

- audit complet des dépendances ;
- loi de souveraineté numérique ;
- lancement ERP modulaire ;
- cadrage coffre citoyen ;
- débat public ;
- choix des territoires pilotes ;
- pilote documents simples ;
- doctrine nationale de la donnée ;
- statuts d'accès ;
- journalisation ;
- cyber urgence ;
- réserve cyber pilote ;
- doctrine IA ;
- registre public des algorithmes ;
- plan plateformes, mineurs et deepfakes ;
- phase stricte protection des mineurs ;
- audit paiements ;
- plan outils métiers ;
- plan jeu vidéo stratégique ;
- open data ;
- réversibilité ;
- autorité de contrôle ;
- fonds de consolidation ;
- préproduction UNIVERS FRANCE ;

- tableau coût / retour / risque / délai.

Année 2 : expérimentation

- premiers pilotes ERP ;
- expérimentation coffre ;
- premiers accès par statut ;
- premiers historiques visibles ;
- premiers transferts cloud maîtrisé ;
- premiers outils IA publics non sensibles ;
- cyber territorial ;
- formation hygiène numérique ;
- prototypes outils métiers ;
- premiers jeux de données non personnelles ouverts ;
- premiers droits de retrait testés ;
- premiers projets jeu vidéo / santé cognitive / formation ;
- premières alliances européennes utiles ;
- prototype UNIVERS FRANCE.

Année 3 : consolidation

- extension ERP ;
- évaluation publique coffre ;
- objectif 5 000 réservistes opérationnels ;
- accompagnement de structures prioritaires ;
- réduction logiciels redondants ;
- accélération cloud maîtrisé ;
- protection informationnelle ;
- paiements souverains européens ;
- filière jeu vidéo structurée ;
- IA publique auditée ;
- formation adulte renforcée ;
- premiers outils métiers adaptés ;
- sanctions d'accès abusifs si cas constatés ;
- premier indice de confiance ;
- version bêta UNIVERS FRANCE ;
- premières décisions d'arrêt ou correction de projets numériques.

Année 4 : maturité intermédiaire

- ERP stabilisé sur plusieurs fonctions majeures ;
- IA maîtrisée auditée ;
- protection mineurs renforcée ;
- PME et collectivités accompagnées ;
- commande publique numérique réorganisée ;
- outils métiers dans plusieurs secteurs ;
- formation numérique intégrée aux parcours de vie ;
- jeu vidéo relié à formation, culture, simulation, export, santé cognitive ;
- premières souverainetés européennes tangibles ;
- lancement public progressif UNIVERS FRANCE ;
- revue annuelle coût / retour / risque / délai.

Année 5 : colonne vertébrale consolidée

- colonne numérique consolidée sur périmètres prioritaires ;
- objectif 15 000 réservistes ;
- dépendances critiques réduites ;
- réserve cyber opérationnelle ;
- cloud maîtrisé sur périmètres vitaux ;
- IA publique encadrée ;
- paiements souverains progressant ;
- coffre utilisé sur démarches validées après évaluation et débat ;
- statuts d'accès contrôlés ;
- formation nationale installée ;
- open data non personnelle réflexe administratif ;
- réversibilité intégrée aux marchés sensibles ;
- UNIVERS FRANCE installé comme projet national de filière ;
- dix projets prioritaires réévalués : continuer, corriger, réduire, fusionner ou arrêter.

Horizon 10 ans :

- administration largement interopérable ;
- objectif 50 000 réservistes formés ou mobilisables ;
- données stratégiques maîtrisées ;
- IA publique souveraine ou maîtrisée selon criticité ;
- citoyens formés ;
- cyberdéfense territoriale solide ;
- paiements moins dépendants ;
- filières françaises numériques renforcées ;
- jeu vidéo français filière d'excellence ;
- outils métiers accessibles ;
- protection mentale des enfants intégrée ;
- UNIVERS FRANCE licence culturelle mondiale.

Horizon 15 ans :

- maturité complète de la colonne vertébrale numérique ;
- réduction profonde des dépendances logicielles ;
- interopérabilité stabilisée ;
- réversibilité fournisseurs devenue norme ;
- open data utile installé ;
- IA publique mature ;
- culture nationale d'hygiène numérique ;
- souveraineté numérique transmise aux générations formées.

Formule :

La souveraineté numérique ne se proclame pas. Elle se migre, se teste, se sécurise, se contrôle et se transmet.

14. PREUVE PERMANENTE, RISQUES ET CONTRÔLE

Indicateurs :

- part des données stratégiques hébergées dans un cadre maîtrisé ;

- doublons administratifs supprimés ;
- temps moyen de traitement des démarches ;
- justificatifs évités ;
- taux d'interopérabilité ;
- cyberattaques réussies contre services publics ;
- hôpitaux, communes, écoles et structures prioritaires couverts ;
- logiciels critiques audités ;
- commande publique numérique souveraine ou maîtrisée ;
- citoyens formés ;
- taux d'illectronisme par âge ;
- réservistes cyber ;
- consultations de données tracées ;
- accès abusifs sanctionnés ;
- filière jeu vidéo ;
- dépendance aux paiements extra-européens ;
- outils métiers déployés ;
- satisfaction citoyenne ;
- contrats avec clause de réversibilité ;
- jeux de données non personnelles ouverts ;
- algorithmes publics audités ;
- confiance citoyenne ;
- droits de retrait instruits ;
- contribution de filière réinvestie ;
- projets européens utiles ;
- avancement UNIVERS FRANCE ;
- projets continués, corrigés, réduits, fusionnés ou arrêtés ;
- écarts coût / délai ;
- taux d'adoption terrain ;
- cas de discrimination algorithmique détectés et corrigés.

Risques :

- ERP usine à gaz ;
- coûts sous-estimés ;
- résistance administrative ;
- surveillance perçue ;
- dépendances cachées ;
- fuite des talents ;
- réaction des plateformes ;
- faiblesse européenne ;
- atteinte aux libertés publiques ;
- fracture numérique aggravée ;
- substitution du numérique à l'humain ;
- exposition excessive des enfants ;
- IA décisionnaire ;
- accès abusifs ;
- réversibilité fictive ;
- cloud maîtrisé trop flou ;
- contribution de filière perçue comme taxe punitive ;
- réserve cyber mal encadrée ;
- UNIVERS FRANCE caricaturé ;

- grands projets maintenus par inertie.

Parades :

- architecture modulaire ;
- audits indépendants ;
- phasage 10-15 ans ;
- transparence des coûts ;
- journalisation ;
- recours citoyen ;
- sanctions ;
- formation massive ;
- accompagnement humain ;
- coopération européenne utile ;
- arrêt des outils qui compliquent ;
- contrôle indépendant ;
- clauses de réversibilité ;
- open data non personnelle ;
- débat public avant généralisation du coffre ;
- expérimentation territoriale ;
- indice de confiance ;
- affectation intégrale de la contribution de filière ;
- gouvernance créative indépendante d'UNIVERS FRANCE ;
- clause anti-usine à gaz ;
- audit anti-discrimination.

Règles de contrôle :

Tout outil numérique public doit supprimer plus de complexité qu'il n'en ajoute. Toute donnée consultée doit laisser une trace. Toute décision publique reste humaine. Tout algorithme public affectant un droit doit être auditable et contestable. Tout grand projet numérique public doit pouvoir être corrigé, réduit, fusionné ou arrêté.

15. DONNÉES — DATA ROOM NUMÉRIQUE

Le fichier numerique_data devra intégrer les données suivantes avec statuts.

Statuts obligatoires :

- OFFICIELLE_BRUTE
- CALCULÉE
- À AUDITER
- PROJECTION_PROGRAMME
- À ACTUALISER

A. USAGES NUMÉRIQUES

population_internaute

Type : OFFICIELLE_BRUTE Référence : 94 % selon Baromètre du numérique. Usage : diagnostic d'usage.

internet_quotidien

Type : OFFICIELLE_BRUTE Référence : 84 %. Usage : intensité d'usage.

demarches_administratives_ligne

Type : OFFICIELLE_BRUTE Référence : 73 %. Usage : poids du numérique public.

usage_ia_population

Type : OFFICIELLE_BRUTE Référence : 33 %. Usage : diffusion IA.

franceconnect_usagers

Type : OFFICIELLE_BRUTE Référence : plus de 40 millions connectés juin 2024 ; plus de 43 millions d'usagers. Usage : base d'identité.

B. ILLECTRONISME

illectronisme_total_2021

Type : OFFICIELLE_BRUTE Référence : 15,4 %. Usage : fracture numérique.

non_usage_internet_2021

Type : OFFICIELLE_BRUTE Référence : 13,9 %. Usage : non-accès.

competences_numeriques_faibles

Type : OFFICIELLE_BRUTE Référence : 28 % des internautes. Usage : formation.

illectronisme_75_plus

Type : OFFICIELLE_BRUTE Référence : 61,9 %. Usage : seniors.

illectronisme_dom

Type : OFFICIELLE_BRUTE Référence : 20 %. Usage : Outre-mer.

C. CYBER

evenements_anssi_2024

Type : OFFICIELLE_BRUTE

Référence : 4 386. Usage : pression cyber.

signalements_anssi_2024

Type : OFFICIELLE_BRUTE Référence : 3 004. Usage : signalements.

incidents_anssi_2024

Type : OFFICIELLE_BRUTE Référence : 1 361. Usage : incidents.

vulnerabilites_certfr_2024

Type : OFFICIELLE_BRUTE / À ACTUALISER Usage : vulnérabilités.

cout_cyber_hopital

Type : À AUDITER Usage : coût évité santé.

D. IA

registre_algorithmes_publics

Type : PROJECTION_PROGRAMME Usage : transparence.

ia_niveau_1_2_3_4

Type : PROJECTION_PROGRAMME Usage : criticité.

decisions_publiques_ia_seule

Type : PROJECTION_PROGRAMME Objectif : zéro. Usage : garde-fou.

biais_algorithmiques_detectes

Type : CALCULÉE / À AUDITER Usage : discrimination zéro.

E. SOUVERAINETÉ

dependance_cloud

Type : CALCULÉE / À AUDITER

dependance_logicielle

Type : CALCULÉE / À AUDITER

dependance_paiements_extra_europeens

Type : CALCULÉE / À AUDITER

contrats_reversibilite

Type : PROJECTION_PROGRAMME

donnees_hebergees_cadre_maitrise

Type : CALCULÉE

F. FILIÈRE ET UNIVERS FRANCE

studios_jeu_video_france

Type : OFFICIELLE_BRUTE / À ACTUALISER

jeux_production

Type : OFFICIELLE_BRUTE / À ACTUALISER

emplois_jeu_video

Type : OFFICIELLE_BRUTE / À ACTUALISER

fonds_consolidation_numerique

Type : PROJECTION_PROGRAMME

univers_france_phase_1

Type : PROJECTION_PROGRAMME

univers_france_phase_2

Type : PROJECTION_PROGRAMME

G. GRANDS PROJETS

cout_erp_etat

Type : PROJECTION_PROGRAMME

cout_coffre_numerique

Type : PROJECTION_PROGRAMME

cout_cyber_territorial

Type : PROJECTION_PROGRAMME

tableau_cout_retour_risque_delai

Type : PROJECTION_PROGRAMME

projets_arretes_ou_corrige

Type : OFFICIELLE_BRUTE / PROJECTION_PROGRAMME

Règle :

Toute donnée non validée doit porter son statut : À SOURCER, À AUDITER ou À ACTUALISER.

16. COORDINATION

Le ministère du Numérique est transversal.

Il n'est pas un silo.

Il est le système nerveux de l'État.

Avec Budget n°1 : coûts, contrats, économies, Fonds Productif, contribution de filière, grands projets SI, mutualisation, réversibilité, financement d'UNIVERS FRANCE, tableau coût / retour / risque / délai.

Avec Santé n°9 : données de santé, hôpitaux, cybersécurité sanitaire, IA médicale, jeux cognitifs, mémoire, motricité, vieillissement.

Avec Communications / Mobilités n°7 : réseaux, alertes, flux, cartographie, transports intelligents.

Avec Éducation n°8 : formation numérique progressive, protection mentale des enfants, modules pédagogiques d'UNIVERS FRANCE.

Avec Travail n°10 : outils métiers, formation continue, télétravail encadré, discrimination algorithmique dans l'emploi.

Avec Natalité n°11 : dossier parental simplifié, protection des parents, limitation des écrans pour la petite enfance.

Avec Handicap n°12 : accessibilité numérique, dossier unique, outils adaptés.

Avec Retraite n°13 : protection contre les arnaques, jeux cognitifs seniors, lien social.

Avec Culture n°14 : médias, deepfakes, jeu vidéo, création numérique, esprit critique, UNIVERS FRANCE.

Avec Industrie n°15 : composants, semi-conducteurs, data centers, IA industrielle, moteurs 3D.

Avec Logement n°16 : données foncières, plateformes logement, discrimination locative numérique.

Avec Agriculture n°17 : outils agricoles, capteurs, simplification, traçabilité.

Avec Commerce n°18 : paiement, cybersécurité, stocks, visibilité territoriale.

Avec Écologie n°19 : données environnementales, recyclage, simulation écologique.

Avec Patrimoine n°20 : cartographie, tourisme, numérisation raisonnée, cœur patrimonial d'UNIVERS FRANCE.

Avec Mer n°21 : données maritimes, ports, ZEE, surveillance, Outre-mer.

Avec Armée n°5 : cyberdéfense, souveraineté technologique, composants critiques, simulation.

Avec Justice n°4 : libertés publiques, accès aux données, sanctions, deepfakes, cybercriminalité, recours citoyen.

Avec Intérieur n°3 : collectivités, identité numérique, crises, cybersécurité territoriale.

Avec Affaires étrangères n°6 : export numérique, alliances européennes utiles, francophonie numérique.

Formule :

Le numérique n'est pas un ministère qui ajoute des écrans. C'est le ministère qui relie les preuves, les droits, les alertes, les données, les métiers, les alliances utiles et la continuité de l'État.

17. DÉPENDANCES

Dépendances fortes :

- Budget ;
- Intérieur ;
- Justice ;
- Santé ;
- Armée ;
- Éducation ;
- Communications / Mobilités ;
- Industrie / Énergie ;
- Culture / Information / Jeunesse ;
- Patrimoine.

Dépendances critiques externes :

- cloud ;
- logiciels propriétaires ;
- plateformes ;
- composants électroniques ;
- semi-conducteurs ;
- IA ;
- paiements ;
- réseaux sociaux ;
- systèmes d'exploitation ;
- moteurs logiciels ;
- moteurs de jeu ;
- cyber-outils ;
- app stores ;
- câbles sous-marins ;
- satellites ;
- standards internationaux ;
- lois extraterritoriales.

Sans confiance, l'ERP devient suspect.

Sans talents, la souveraineté reste un slogan.

Sans formation, le peuple reste vulnérable.

Sans contrôle juridique, le confort administratif peut être perçu comme un danger.

Sans outils simples, le numérique continue de servir les initiés.

Sans financement de filière, le numérique français dépend toujours des autres pour grandir.

Sans culture numérique ambitieuse, la France consomme les imaginaires des autres.

Sans alliances européennes utiles, certaines souverainetés restent trop faibles.

Sans clause anti-usine à gaz, les grands projets deviennent des rentes administratives.

Sans lutte anti-discrimination algorithmique, la modernisation peut devenir une injustice silencieuse.

18. PUBLICS CONCERNÉS

Gagnants immédiats :

- citoyens ;
- familles ;
- parents ;
- mineurs ;
- citoyens vulnérables ;
- communes ;
- hôpitaux ;
- écoles ;
- PME ;
- artisans ;
- agriculteurs ;
- commerçants ;
- personnes âgées ;
- personnes handicapées ;
- agents publics ;
- victimes potentielles de fraude ;
- usagers perdus dans les démarches ;
- professionnels confrontés à des outils absurdes.

Gagnants à moyen terme :

- ingénieurs ;
- développeurs ;
- experts cyber ;
- experts IA ;
- studios de jeu vidéo ;
- entreprises cloud ;
- start-up utiles ;
- laboratoires ;
- formateurs numériques ;
- réservistes cyber ;
- écoles spécialisées ;
- acteurs open data ;
- PME numériques françaises et européennes ;
- créateurs d'UNIVERS FRANCE ;
- acteurs du tourisme ;
- historiens ;
- régions ;
- Outre-mer.

Publics protégés :

- mineurs ;
- seniors ;
- personnes éloignées du numérique ;
- victimes de cyberharcèlement ;
- victimes d'usurpation ;
- victimes de deepfakes ;

- citoyens en situation sensible ;
- personnes discriminées par un outil numérique ;
- usagers dépendants d'un guichet humain.

Acteurs à accompagner :

- petites communes ;
- hôpitaux ;
- écoles ;
- PME ;
- artisans ;
- agriculteurs ;
- associations utiles ;
- agents publics ;
- studios indépendants.

Acteurs à sanctionner :

- plateformes négligentes ;
- prestataires captifs ;
- auteurs d'accès abusifs ;
- producteurs de deepfakes malveillants ;
- opérateurs discriminants ;
- acteurs refusant la réversibilité ;
- porteurs de projets publics refusant l'évaluation.

19. ENNEMIS STRUCTURELS

Les ennemis structurels ne sont pas des personnes.

Ce sont des mécanismes :

- dépendance technologique ;
- paperasse numérisée ;
- logiciels captifs ;
- prestations opaques ;
- portails inutiles ;
- données dispersées ;
- accès non tracés ;
- cybercriminalité ;
- deepfakes ;
- fraudes numériques ;
- plateformes addictives ;
- protection insuffisante des mineurs ;
- adultes mal formés ;
- IA sans doctrine ;
- IA décisionnaire ;
- paiements dépendants ;
- achats publics dispersés ;
- complexité administrative ;
- contrats sans réversibilité ;
- souveraineté proclamée mais non réelle ;
- open data oublié ;

- jeu vidéo sous-estimé ;
- talents cachés gâchés ;
- seniors exclus des usages numériques utiles ;
- Europe fragmentée ;
- imaginaire numérique français abandonné ;
- métaverse spéculatif hors-sol ;
- copie servile des modèles étrangers ;
- grands projets maintenus par inertie ;
- discrimination algorithmique.

Réponse LPE :

Chaque outil créé doit supprimer plus de complexité qu'il n'en ajoute.

20. CONDITIONS DE VICTOIRE

La réussite dépendra :

- de la qualité du pilotage ERP ;
- de la doctrine nationale de la donnée ;
- de la capacité à protéger sans surveiller ;
- de la capacité à simplifier sans fragiliser ;
- de la clarté des statuts d'accès ;
- de la traçabilité des consultations ;
- de la confiance citoyenne ;
- de l'attractivité des métiers numériques souverains ;
- de la formation des citoyens ;
- de la baisse réelle de l'illectronisme ;
- de la protection réelle des mineurs ;
- de la coopération européenne utile ;
- de la capacité à contraindre les plateformes ;
- de la réorientation de la commande publique ;
- du chiffrage honnête ;
- du phasage réaliste ;
- du contrôle indépendant ;
- de la réversibilité fournisseurs ;
- de l'open data non personnelle ;
- de l'indice de confiance ;
- de sanctions appliquées en cas d'abus ;
- de la contribution de filière réinvestie ;
- de la qualité d'UNIVERS FRANCE ;
- de la capacité à arrêter les projets qui échouent ;
- de la correction des discriminations numériques.

Seuil minimal de succès :

- premiers doublons supprimés ;
- premières données vitales maîtrisées ;
- premiers hôpitaux et citoyens vulnérables sécurisés ;
- premières communes sécurisées ;
- premières consultations de données traçables ;
- premiers accès abusifs sanctionnés ;

- premiers résultats contre fraude et deepfakes ;
- premières démarches réellement simplifiées ;
- premières formations numériques adultes ;
- premiers outils métiers accessibles ;
- premières clauses de réversibilité imposées ;
- premières données publiques non personnelles ouvertes ;
- premier indice de confiance publié ;
- premier prototype UNIVERS FRANCE ;
- premier projet numérique corrigé ou arrêté par preuve.

Preuve populaire :

Le citoyen ne fournit plus dix fois les mêmes justificatifs.

Il sait qui a consulté ses données.

Il peut faire ses démarches plus simplement.

Il reste accompagné humainement s'il en a besoin.

Il sait que l'État n'a pas un droit général de fouiller sa vie.

Il voit que le numérique français produit aussi de la beauté, de la culture, des jeux, des métiers, de la mémoire et de l'export.

21. COÛT POLITIQUE

Coût médiatique : élevé.

Accusations possibles :

- Big Brother ;
- surveillance ;
- censure ;
- centralisation ;
- protectionnisme numérique ;
- ministère de contrôle ;
- taxe sur les start-up ;
- projet culturel d'État ;
- métaverse inutile ;
- usine à gaz.

Coût institutionnel : très élevé.

Il faut réorganiser des systèmes anciens, des contrats, des habitudes, des achats, des administrations entières.

Coût économique initial : élevé.

Cloud, ERP, IA, cybersécurité, formation, migration, audits, réserve cyber, composants critiques, outils métiers, filière jeu vidéo et UNIVERS FRANCE exigent un investissement massif.

Le ministère refuse une fourchette figée présentée comme promesse définitive.

Il fixe une logique :

- investissement public minimum ;
- phasage sur 10 à 15 ans ;
- mutualisation des achats publics ;
- réduction des contrats captifs ;
- contribution de consolidation de filière ;

- retour obligatoire dans le secteur numérique français ;
- logique d'actifs : logiciels, moteurs, données utiles, compétences, sécurité, export, licences culturelles ;
- tableau coût / retour / risque / délai ;
- clause d'arrêt.

La fourchette de travail de la base LPE doit être classée PROJECTION_PROGRAMME et confirmée par audit.

Réponse politique :

Le vrai danger n'est pas un numérique français contrôlé par la loi. Le vrai danger, c'est le désordre actuel : données dispersées, citoyens fraudés, enfants exposés, hôpitaux piratés, administrations captives, France dépendante, imagination numérique abandonnée aux autres et grands projets numériques jamais arrêtés malgré leurs échecs.

22. IRRÉVERSIBILITÉ

La réforme devient irréversible par :

- loi de souveraineté numérique ;
- charte du numérique libre et protecteur ;
- registre public des algorithmes ;
- historique citoyen des accès ;
- journalisation obligatoire ;
- sanctions en cas d'accès abusif ;
- clauses de réversibilité ;
- ouverture des données publiques non personnelles ;
- ERP modulaire ;
- coffre numérique expérimenté ;
- accompagnement humain garanti ;
- réserve cyber ;
- protection des mineurs ;
- souveraineté progressive des paiements ;
- fonds de consolidation de filière ;
- indice de confiance numérique ;
- formation populaire ;
- filière jeu vidéo stratégique ;
- non-migration automatique ;
- gouvernance de l'ERP ;
- critères du cloud maîtrisé ;
- alliances européennes utiles ;
- UNIVERS FRANCE ;
- clause anti-usine à gaz ;
- tableau coût / retour / risque / délai ;
- audit anti-discrimination algorithmique.

L'irréversibilité ne vient pas seulement du code.

Elle vient de la confiance.

Un outil numérique que le citoyen comprend, contrôle et utilise devient difficile à supprimer.

Une dépendance rendue visible devient difficile à reconduire.

Un fournisseur soumis à réversibilité ne peut plus posséder l'État.

Une donnée tracée ne peut plus être consultée en silence.

Une IA encadrée ne peut plus se déguiser en autorité.

Une grande licence culturelle numérique devient un actif national.

Formule :

Un numérique utile, contrôlé, compris, productif, culturel et mesuré devient très difficile à détruire.

23. PROFIL DU MINISTRE / COMMANDANT

Le ministre du Numérique ne doit pas être un vendeur de modernité.

Il doit être un architecte de souveraineté.

Il doit comprendre :

- systèmes d'information ;
- données ;
- libertés publiques ;
- administration ;
- cybersécurité ;
- collectivités ;
- hôpitaux ;
- écoles ;
- PME ;
- dépendances contractuelles ;
- paiements ;
- IA ;
- cloud ;
- plateformes ;
- jeux vidéo ;
- usages des enfants ;
- besoins des seniors ;
- conduite de grands projets publics ;
- institutions européennes ;
- alliances industrielles ;
- moteurs 3D ;
- économie des licences culturelles ;
- métiers créatifs ;
- contrôle coût / retour / risque / délai ;
- risques discriminatoires des algorithmes.

Il doit refuser :

- effet d'annonce ;
- numérique gadget ;
- ERP miracle ;
- cloud souverain de communication ;
- IA décisionnaire ;
- coffre numérique généralisé sans confiance ;
- abandon des guichets humains ;
- dépendance aux prestataires ;
- dépense informatique sans retour ;
- plateformes irresponsables ;
- outils qui compliquent la vie ;

- Europe comme alibi ;
- métaverse spéculatif ;
- culture officielle imposée ;
- grands projets intouchables.

Il doit imposer :

- simplicité ;
- preuve ;
- sécurité ;
- phasage ;
- réversibilité ;
- documentation ;
- audit ;
- protection des libertés ;
- formation ;
- souveraineté ;
- continuité ;
- contrôle citoyen ;
- retour sectoriel de la contribution de filière ;
- alliances européennes utiles ;
- gouvernance ERP ;
- liberté créative ;
- UNIVERS FRANCE ;
- clause anti-usine à gaz.

Sa phrase :

Je ne numérise pas pour moderniser l'apparence de l'État. Je numérise pour rendre l'État plus simple, plus sûr, plus souverain, plus productif et plus contrôlable par le peuple.

24. TABLEAU DE BORD PUBLIC

Le tableau de bord public publie :

- utilisateurs FranceConnect ;
- démarches réellement simplifiées ;
- temps moyen des démarches ;
- justificatifs évités ;
- satisfaction usager ;
- difficultés administratives en ligne ;
- illectronisme par âge ;
- citoyens accompagnés humainement ;
- hôpitaux sécurisés ;
- citoyens vulnérables accompagnés ;
- communes sécurisées ;
- écoles sécurisées ;
- PME / artisans / agriculteurs accompagnés ;
- incidents cyber ;
- signalements ;
- vulnérabilités traitées ;
- réservistes cyber ;
- talents cyber validés ;

- logiciels critiques audités ;
- contrats avec clause de réversibilité ;
- fournisseurs quittés sans coût abusif ;
- données vitales hébergées dans un cadre maîtrisé ;
- algorithmes publics enregistrés ;
- algorithmes audités ;
- usages IA par criticité ;
- décisions publiques prises par IA seule : objectif zéro ;
- accès aux données consultables par citoyen ;
- accès abusifs sanctionnés ;
- droits de retrait instruits ;
- niveau de confiance citoyenne ;
- progression CB / Wero / solutions européennes ;
- studios de jeu vidéo soutenus ;
- jeux sérieux financés ;
- fonds de consolidation ;
- projets numériques arrêtés ou corrigés ;
- alliances européennes utiles ;
- avancement UNIVERS FRANCE ;
- tableau coût / retour / risque / délai ;
- cas de discrimination algorithmique détectés et corrigés.

Quatre vues sont publiées :

Vue citoyenne : est-ce plus simple et plus sûr ? Vue territoriale : qui est protégé et où ? Vue expert : coûts, dépendances, audits, incidents, résultats. Vue culturelle : que produit la France dans le numérique au-delà de l'administration ?

Formule :

Le numérique public doit être contrôlable par ceux qu'il prétend servir.

25. RISQUES DE DÉRIVE ET GARDE-FOUS

Risque : Big Brother. Garde-fou : pas de fichier unique, accès par statut, finalité, journalisation, historique citoyen, contrôle indépendant, sanctions.

Risque : coffre numérique mal compris. Garde-fou : documents simples d'abord, expérimentation, débat public, vote, droit de retrait, accompagnement humain.

Risque : aspiration des données anciennes. Garde-fou : non-migration automatique, base légale, finalité, information, contrôle indépendant, pilote sur données simples.

Risque : IA décisionnaire. Garde-fou : aucune décision publique individuelle prise par IA ; validation humaine obligatoire ; registre public ; recours.

Risque : exclusion numérique. Garde-fou : aucun service public essentiel 100 % numérique sans alternative humaine ; formation ; objectifs illectronisme.

Risque : ERP usine à gaz. Garde-fou : modularité, phasage, périmètres prioritaires, audits indépendants, arrêt des modules inutiles.

Risque : coûts incontrôlés. Garde-fou : tableau de bord, publication des coûts, clauses de sortie, audit, mutualisation achats, clause anti-usine à gaz.

Risque : dépendance fournisseur. Garde-fou : réversibilité obligatoire, formats ouverts, documentation, transfert de compétence.

Risque : cyberréserve dangereuse. Garde-fou : casier judiciaire, conflits d'intérêts, habilitation progressive, supervision.

Risque : contribution de filière rejetée. Garde-fou : affectation intégrale au secteur, gouvernance transparente, retour visible.

Risque : cloud souverain de façade. Garde-fou : distinction cloud souverain / cloud maîtrisé, audit juridique et technique, réversibilité.

Risque : UNIVERS FRANCE perçu comme propagande. Garde-fou : liberté créative, gouvernance pluraliste, studios indépendants, régions, historiens, enseignants, artistes, auteurs.

Risque : discrimination algorithmique. Garde-fou : audit des biais, explicabilité, recours humain, suspension de l'algorithme, réparation de la victime.

Formule :

Le numérique LPE n'est légitime que s'il protège plus qu'il ne capte, simplifie plus qu'il ne complique, et rend l'État plus contrôlable qu'avant.

26. ATTAQUES / RÉPONSES

Attaque : vous construisez Big Brother. Réponse : Big Brother, c'est l'accès invisible, non tracé, dispersé, sous-traité et captif. LPE fait l'inverse : accès limité, finalité précise, journalisation, historique citoyen, contrôle indépendant, sanctions.

Attaque : votre coffre numérique est dangereux. Réponse : il commence par les documents administratifs simples, il est expérimenté, débattu, contrôlé, et le citoyen voit les accès. Il ne centralise pas toute la vie du citoyen.

Attaque : vous allez aspirer toutes les anciennes données de l'État. Réponse : non. Les données déjà détenues par l'État ne sont pas automatiquement intégrées au coffre numérique citoyen.

Attaque : votre IA va décider à la place des humains. Réponse : non. Aucune décision publique individuelle n'est prise par IA. L'IA aide, résume, alerte, simule. Elle ne décide pas.

Attaque : vous excluez les personnes âgées. Réponse : c'est l'inverse. Aucun service public essentiel ne devient 100 % numérique sans alternative humaine.

Attaque : votre réserve cyber est dangereuse. Réponse : elle est encadrée, habilitée progressivement, contrôlée par experts publics, avec vérification des risques.

Attaque : vous taxez les start-up françaises. Réponse : non. La contribution de consolidation revient dans leur propre secteur.

Attaque : vous allez couper Visa et Mastercard. Réponse : non. Les Français doivent continuer à pouvoir utiliser les solutions existantes. Mais la France et l'Europe doivent renforcer CB, Wero et les solutions européennes.

Attaque : vous voulez contrôler les enfants. Réponse : nous voulons protéger leur sommeil, leur attention, leur dignité, leur image, leur santé mentale et leur développement.

Attaque : le jeu vidéo n'est pas sérieux. Réponse : il est logiciel, image, IA, simulation, formation, culture, export, santé cognitive, mémoire, motricité et défense.

Attaque : UNIVERS FRANCE sera de la propagande d'État. Réponse : non. L'État impulse, finance, coordonne et protège ; les studios, artistes, auteurs, régions, historiens, enseignants, chercheurs et entreprises créent.

Attaque : vos algorithmes vont discriminer. Réponse : justement, LPE impose audit, explicabilité, recours humain, correction et réparation.

27. TROIS NIVEAUX DE LECTURE

Niveau populaire :

Le numérique doit rendre la vie plus simple, pas plus compliquée. Les Français ne doivent plus fournir dix fois les mêmes papiers. Ils doivent savoir qui consulte leurs données. Les personnes âgées doivent être accompagnées. Les enfants doivent être protégés. Les hôpitaux doivent être sécurisés. L'IA ne doit jamais décider à la place d'un humain. La France doit produire ses propres outils, ses propres protections et ses propres mondes numériques.

Niveau citoyen engagé :

LPE sécurise FranceConnect, crée un coffre limité d'abord aux documents simples, impose la traçabilité des accès, interdit l'IA décisionnaire, garantit un accompagnement humain, protège les hôpitaux et citoyens vulnérables, organise une réserve cyber, renforce CB/Wero/Europe, impose la réversibilité des contrats, structure le jeu vidéo, lance UNIVERS FRANCE, agit avec l'Europe quand cela renforce la maîtrise française, et soumet les grands projets numériques à une clause de résultat.

Niveau expert :

Architecture numérique souveraine fondée sur ERP modulaire, interopérabilité, classification des données vitales, statuts d'accès, journalisation, registre public des algorithmes, IA par criticité sans décision automatisée, cloud souverain ou maîtrisé, cyberpriorisation santé / citoyens vulnérables / collectivités / éducation / PME, réversibilité fournisseurs, open data non personnelle, souveraineté progressive des paiements, contribution de consolidation de filière, non-migration automatique vers le coffre, gouvernance ERP, alliances européennes utiles, UNIVERS FRANCE, audit anti-discrimination et clause anti-usine à gaz.

28. SIMULATEURS

Simulateurs à créer :

- simulateur coût ERP d'État ;
- simulateur coffre numérique citoyen ;
- simulateur justificatifs évités ;
- simulateur temps citoyen économisé ;
- simulateur réversibilité fournisseurs ;
- simulateur dépendance logicielle ;
- simulateur cloud souverain / cloud maîtrisé ;
- simulateur cyber hôpitaux ;
- simulateur cyber citoyens vulnérables ;
- simulateur cyber communes ;
- simulateur cyber écoles ;
- simulateur cyber PME / artisans / agriculteurs ;
- simulateur réserve cyber ;
- simulateur talents cachés cyber ;
- simulateur illettrisme ;
- simulateur formation numérique nationale ;
- simulateur IA publique par criticité ;
- simulateur registre des algorithmes ;
- simulateur accès aux données ;
- simulateur droit de retrait ;
- simulateur indice de confiance numérique ;

- simulateur protection des mineurs ;
- simulateur plateformes / deepfakes ;
- simulateur souveraineté paiements CB / Wero / Europe ;
- simulateur open data non personnelle ;
- simulateur contribution de filière numérique ;
- simulateur fonds de consolidation numérique ;
- simulateur jeu vidéo stratégique ;
- simulateur jeux vidéo seniors / mémoire / motricité / cognition ;
- simulateur coûts évités cyber santé ;
- simulateur coûts évités fraude numérique ;
- simulateur grands projets SI publics ;
- simulateur alliances européennes utiles ;
- simulateur UNIVERS FRANCE ;
- simulateur outils métiers ;
- simulateur anti-usine à gaz ;
- simulateur coût / retour / risque / délai ;
- simulateur discrimination algorithmique.

Formule :

Un simulateur numérique LPE ne sert pas à vendre du rêve. Il sert à éviter l'usine à gaz.

29. ARTICLES LIÉS

- FranceConnect : pourquoi la France a déjà une porte d'entrée numérique nationale.
- Pourquoi le numérique public ne doit pas devenir Big Brother.
- Coffre numérique : simplifier sans surveiller.
- IA publique : pourquoi l'IA doit aider mais jamais décider.
- Illectronisme : pourquoi l'accompagnement humain reste indispensable.
- Hôpitaux piratés : pourquoi la cybersécurité est une politique de santé.
- Cyberattaques : communes, écoles, PME, citoyens vulnérables, tous concernés.
- Réserve cyber : mobiliser les talents cachés sans danger.
- Réversibilité fournisseurs : ne plus laisser les prestataires posséder l'État.
- Cloud souverain ou cloud maîtrisé : sortir des slogans.
- CB, Wero, Europe : reconstruire la souveraineté des paiements sans brutalité.
- Jeu vidéo français : culture, logiciel, IA, simulation et export.
- Jeux vidéo et seniors : mémoire, motricité, cognition et lien social.
- Protection des mineurs : protéger sans paniquer.
- Deepfakes : défendre la vérité publique à l'ère des faux.
- Open data : ouvrir les données non personnelles sans livrer les citoyens.
- Contribution de filière : pourquoi le numérique français doit financer sa propre puissance.
- Grands projets SI : éviter les milliards dispersés.
- UNIVERS FRANCE : pourquoi la France doit créer son grand monde ouvert culturel.
- Discrimination algorithmique : pourquoi le recours humain est indispensable.

30. QUIZ LIÉS

- Savez-vous qui consulte vos données administratives ?
- Quelle différence entre coffre numérique et fichier unique ?
- Une IA peut-elle prendre une décision publique à la place d'un humain ?
- Qu'est-ce que l'illectronisme ?

- Pourquoi les plus de 75 ans sont-ils vulnérables numériquement ?
- Pourquoi les hôpitaux sont-ils des cibles cyber majeures ?
- Qu'est-ce qu'une clause de réversibilité fournisseur ?
- Pourquoi le cloud souverain n'est-il pas seulement une question de localisation ?
- Pourquoi CB, Wero et l'Europe sont-ils stratégiques ?
- Le jeu vidéo est-il seulement un loisir ?
- Qu'est-ce qu'un deepfake ?
- Qu'est-ce qu'un registre public des algorithmes ?
- Pourquoi la souveraineté numérique peut-elle avoir besoin d'alliances européennes utiles ?
- Qu'est-ce que la non-migration automatique vers le coffre numérique ?
- UNIVERS FRANCE est-il un jeu, un outil culturel ou une filière industrielle ?
- Pourquoi un projet numérique public doit-il pouvoir être arrêté ?
- Comment détecter une discrimination algorithmique ?

31. SONDAGES LIÉS

- Faut-il que chaque citoyen puisse voir qui consulte ses données ?
- Faut-il interdire toute décision publique prise uniquement par IA ?
- Faut-il garder un guichet humain pour tous les services essentiels ?
- Faut-il créer un coffre numérique limité d'abord aux documents simples ?
- Faut-il rendre obligatoire la réversibilité des contrats numériques publics ?
- Faut-il protéger prioritairement les hôpitaux contre les cyberattaques ?
- Faut-il créer une réserve cyber citoyenne et experte ?
- Faut-il renforcer fortement la protection des mineurs face aux plateformes ?
- Faut-il soutenir CB/Wero pour réduire la dépendance aux réseaux extra-européens ?
- Faut-il faire du jeu vidéo une filière stratégique française ?
- Faut-il qu'une contribution du secteur numérique soit réinvestie dans le secteur numérique ?
- Faut-il publier tous les grands projets numériques publics avec coûts, délais et résultats ?
- Faut-il ouvrir par défaut les données publiques non personnelles ?
- Faut-il lancer UNIVERS FRANCE comme grand monde ouvert culturel français ?
- Faut-il arrêter un projet numérique public qui ne prouve pas son utilité ?
- Faut-il auditer les algorithmes publics contre les discriminations ?

32. LEXIQUE LIÉ

FranceConnect : service d'identification permettant d'accéder à des services publics et privés via des comptes existants.

Coffre numérique citoyen : espace sécurisé où certains documents administratifs simples sont vérifiés une fois et réutilisables par les administrations autorisées.

ERP d'État : architecture numérique modulaire reliant progressivement les systèmes publics essentiels.

Interopérabilité : capacité de systèmes différents à communiquer sans ressaisie, doublon ou dépendance excessive.

Journalisation : enregistrement de toute consultation de donnée.

Historique citoyen des accès : interface permettant au citoyen de voir qui a consulté ses données, sauf exception légale.

Droit de retrait sensible : possibilité de bloquer certains accès ordinaires en cas de vulnérabilité ou de situation personnelle sensible.

IA d'accompagnement : IA qui aide, résume, trie, simule ou alerte sans décider.

Registre public des algorithmes : liste des systèmes algorithmiques publics avec finalité, criticité, audit et recours.

Cloud souverain : hébergement et services sous maîtrise nationale ou européenne forte.

Cloud maîtrisé : solution contractualisée, auditée, réversible et contrôlée selon critères précis.

Réversibilité fournisseur : capacité de quitter un prestataire sans perdre données, compétences ou continuité.

Illectronisme : situation d'une personne qui n'utilise pas Internet ou ne possède pas les compétences numériques de base.

Réserve cyber : réseau de citoyens formés, talents validés et experts mobilisables.

Deepfake : contenu audio, vidéo ou image falsifié par IA ou outils numériques.

Open data non personnelle : données publiques réutilisables ne contenant pas de données individuelles sensibles.

Contribution de consolidation de filière : contribution sectorielle réinvestie dans le numérique français.

Paiement souverain : capacité à payer et traiter les transactions via des infrastructures françaises ou européennes résilientes.

Non-migration automatique : principe selon lequel les données déjà détenues par l'État ne sont pas automatiquement intégrées au coffre.

UNIVERS FRANCE : grande licence numérique française en monde ouvert, mêlant jeu vidéo, patrimoine, territoires, Outre-mer, métiers, tourisme, éducation, culture, simulation, mémoire, export et création originale.

Clause anti-usine à gaz : mécanisme permettant de corriger, réduire, fusionner ou arrêter un projet numérique public qui ne prouve pas son utilité.

Discrimination algorithmique : traitement injuste produit ou amplifié par un système numérique.

33. INFOS PRATIQUES

Pour un citoyen : Démarches plus simples, moins de justificatifs répétés, historique des accès, recours en cas d'abus, accompagnement humain.

Pour une personne âgée : Protection contre les arnaques, guichet humain maintenu, formation adaptée, possibilité de jeux cognitifs et de lien social.

Pour un parent : Outils de protection des mineurs, formation aux écrans, signalement, contrôle des plateformes.

Pour un jeune : Formation numérique progressive, création, code, simulation, esprit critique, protection contre addiction et manipulation.

Pour un hôpital : Audit cyber, sauvegardes, réduction des applications obsolètes, procédures de crise, protection des données.

Pour une commune : Diagnostic cyber, sauvegarde, outils mutualisés, accompagnement, valorisation du patrimoine local dans UNIVERS FRANCE.

Pour une école : Protection des données, formation, outils pédagogiques limités et utiles, prévention cyberharcèlement.

Pour une PME / artisan / agriculteur : Outils simples, cybersécurité accessible, paiement, visibilité locale, aide contre fraude.

Pour une start-up numérique française : Contribution réinvestie, commande publique plus lisible, réversibilité, export, cloud, IA, cyber, jeux vidéo.

Pour un studio de jeu vidéo : Reconnaissance stratégique, accès à formation, export, simulation, culture, innovation, participation possible à UNIVERS FRANCE.

Pour une victime de discrimination numérique : Recours humain, audit, correction de donnée ou d'algorithme, réparation possible, contrôle indépendant.

34. MATÉRIEL DE CAMPAGNE

Slogans :

Le numérique doit servir la France, pas la rendre dépendante.

Simplifier, protéger, souverainiser, former, créer, sans surveiller.

La France ne doit pas choisir entre paperasse et Big Brother.

L'IA aide. L'humain décide.

Aucune décision publique ne doit être prise par une IA.

Un fournisseur qui sert l'État ne doit jamais devenir propriétaire de la dépendance de l'État.

Le coffre numérique n'est pas un œil de l'État. C'est un bouclier administratif du citoyen.

Une donnée consultée sans droit est une violation de confiance publique.

Un pays qui numérise ses droits doit former son peuple.

Aucun service public essentiel ne doit devenir 100 % numérique sans alternative humaine.

Si un hôpital tombe, ce sont des soins qui tombent.

La cyberdéfense commence aussi dans les communes, les écoles, les PME et les familles.

Protéger les mineurs, ce n'est pas refuser le numérique. C'est refuser qu'il les détruise.

Le jeu vidéo français peut divertir, former, soigner, stimuler et exporter.

La France ne doit pas seulement protéger ses données. Elle doit produire ses imaginaires.

Pas une copie de GTA. Une création française mondiale.

Un projet numérique public ne doit pas survivre uniquement parce qu'il a déjà coûté cher.

Algorithme public, recours humain obligatoire.

Phrase courte de meeting :

La France a déjà basculé dans le numérique. Notre devoir n'est pas d'ajouter des écrans, mais de rendre ce numérique simple, sûr, humain, souverain, productif, mesurable et contrôlable par le peuple.

Phrase anti-Big Brother :

Le numérique LPE rend l'État plus contrôlable par le citoyen, jamais le citoyen plus contrôlable par l'État.

Phrase IA :

L'IA peut aider l'administration. Elle ne doit jamais devenir l'administration.

Phrase UNIVERS FRANCE :

La France a inspiré les livres, les tableaux, les films et les monuments. Elle doit maintenant inspirer les grands mondes numériques du XXI^e siècle.

Phrase discrimination numérique :

Une décision numérique qui humilie sans expliquer est une injustice moderne. LPE impose le recours humain.

35. RÉSULTAT POLITIQUE

Le ministère n°2 transforme le numérique français en infrastructure de souveraineté, de liberté, de confort populaire, de puissance productive, de création culturelle et d'exécution mesurable.

Il ne crée pas un État de surveillance.

Il crée un État plus simple, plus sûr et plus contrôlable.

Il ne remplace pas l'humain par l'IA.

Il utilise l'IA pour aider l'humain à mieux travailler.

Il ne généralise pas brutalement un coffre numérique total.

Il commence par les documents administratifs simples, expérimente, contrôle, débat et protège.

Il ne laisse pas les personnes âgées ou fragiles derrière un écran.

Il garantit un accompagnement humain.

Il ne laisse pas les hôpitaux, communes, écoles, PME et citoyens vulnérables seuls face aux attaques.

Il organise une cyberdéfense territoriale, populaire et experte.

Il ne déclare pas une souveraineté numérique imaginaire.

Il audite, migre, documente, rend réversible, sécurise, forme et mesure.

Il ne coupe pas brutalement les moyens de paiement existants.

Il renforce progressivement CB, Wero et les solutions européennes.

Il ne traite pas le jeu vidéo comme un simple loisir.

Il en fait une filière de culture, logiciel, IA, simulation, formation, mémoire, motricité, cognition, santé, défense et export.

Il ne crée pas un fichier unique.

Il organise le cloisonnement, la journalisation, l'historique citoyen et le droit de retrait.

Il ne crée pas un métaverse spéculatif.

Il lance UNIVERS FRANCE : une grande licence numérique française, culturelle, éducative, touristique, productive et exportable.

Il ne sacralise pas les grands projets.

Il sacralise le résultat.

Il ne tolère pas les discriminations numériques invisibles.

Il impose audit, recours humain, correction, réparation et contrôle indépendant.

Résultat politique final :

La France reprend la maîtrise de son système nerveux numérique. Le citoyen fait moins de démarches, répète moins de justificatifs, voit mieux qui consulte ses données, garde un recours humain, protège ses enfants, sécurise ses droits et bénéficie d'un État plus simple. Les hôpitaux, communes, écoles, PME, citoyens vulnérables et services publics deviennent plus résistants. Les talents numériques français sont mieux mobilisés. La filière numérique française finance sa propre puissance. Les alliances européennes utiles renforcent la maîtrise française sans l'effacer. UNIVERS FRANCE donne à la France un grand monde numérique culturel, populaire et exportable. Les grands projets numériques

deviennent arbitrables, chiffrables, contrôlables et arrêtables. Le numérique cesse d'être une dépendance subie ; il devient une souveraineté utile, humaine, contrôlée, productive, imaginative, non discriminatoire et mesurée.

Formule finale :

Le numérique LPE n'est pas un ministère qui ajoute des écrans. C'est le ministère qui relie les preuves, les droits, les alertes, les données, les métiers, les alliances utiles, les territoires, l'imaginaire français et l'exécution mesurée, sans jamais transformer l'administration en machine de surveillance.



OBSERVER. COMPRENDRE. CONSTRUIRE.

LE BLEU RÉVÈLE.
LE BLANC CONÇOIT.
LE ROUGE RÉALISE.

MINISTÈRE N°02

NUMÉRIQUE FRANÇAIS, DONNÉES, IA ET SOUVERAINETÉ TECHNOLOGIQUE

Ce document présente le diagnostic, la doctrine, les instruments, les garde-fous et la trajectoire d'exécution du ministère dans l'architecture complète des vingt-et-un ministères LPE.



DJILALI HAKIKI

Fondateur de LPE

Document de travail • Version V4

OBSERVER. COMPRENDRE. CONSTRUIRE.