LE NUMÉRIQUE :
UNE MENACE POUR NOS DÉMOCRATIES
OU UNE FORMIDABLE OPPORTUNITÉ POUR LA FRANCE ET L'EUROPE ?

Dans cinq ans, serons-nous encore maîtres de notre destin ?

Le numérique n'est plus un sujet sectoriel. Il conditionne notre souveraineté, notre sécurité, notre économie et la confiance dans nos institutions, et l'intelligence artificielle accélère tout. Le prochain mandat présidentiel sera celui au cours duquel il sera déterminé si la France et l'Europe subissent ces bouleversements ou les orientent pour en tirer avantage.

Il y a urgence car dans cinq ans, si nous ne faisons rien ou pas assez :

Souveraineté : l'Europe sera restée dépendante des infrastructures de calcul et des modèles d'IA américains et chinois, et les grandes décisions technologiques qui nous impactent directement se prendront à Washington ou à Pékin.

Sécurité : un hôpital, une administration, un réseau électrique, une chaîne de supermarchés ou une banque aura subi une paralysie majeure ou une attaque, et lorsque les données des citoyens auront fuité, ces derniers n'auront toujours aucun recours effectif.

Société : une génération entière aura grandi sans garde-fou face à des algorithmes conçus pour capter son attention et manipuler les consciences.

Économie : la facture numérique européenne aura continué d'enfler, au prix d'une perte de valeur ajoutée estimée à 107 milliards d'euros et de 1,4 million d'emplois d'ici 2030.

Culture et information : les *deepfakes* seront devenus indiscernables du réel, et la confiance dans le processus démocratique sera durablement entamée.

IA augmentée : des agents autonomes travailleront dans nos administrations et nos métiers qualifiés sans cadre de responsabilité clair, et nous réglementerons dans l'urgence des pratiques déjà généralisées.

Mais rien n'est écrit, et l'Europe dispose d'atouts réels : une électricité décarbonée, des champions émergents, une puissance normative unique. Le choix d'un numérique porteur de nos valeurs reste ouvert, à condition de s'y préparer sans perdre davantage de temps.

Introduction

Le numérique a profondément recomposé le champ de l'action publique, économique, sociétale, culturelle, politique et géopolitique. Il redessine les équilibres géopolitiques, reconfigure les économies, transforme les sociétés, menace les libertés individuelles, ouvre des vecteurs inédits de désinformation et fragilise nos démocraties. Mais il constitue tout autant un formidable levier de puissance, de croissance et de progrès pour qui saura s'en saisir. L'Europe dispose d'atouts réels pour transformer cette dépendance subie en un numérique choisi, porteur des valeurs démocratiques européennes ; la France doit y jouer un rôle de premier rang.

Tout cela évolue vite, très vite. Ces sujets sont éminemment complexes et imbriqués entre eux, et la vitesse avec laquelle évolue l'ensemble des technologies numériques ainsi que l'accélération liée à l'intelligence artificielle rendent encore plus périlleuse la préparation de l'exercice du pouvoir.

Chacun des six grands champs thématiques que nous présentons fait l'objet d'une transformation structurelle que les programmes présidentiels ne peuvent ignorer.

La généralisation de l'intelligence artificielle s'inscrit désormais dans un contexte de polarisation idéologique globale : le mouvement MAGA aux États-Unis a développé une techno-structure radicalisée, mobilisant des outils de surveillance, d'analyse comportementale et de ciblage politique de masse. Palantir, entreprise fondée par Peter Thiel, figure emblématique de cette nébuleuse, illustre comment des technologies d'exploitation des données peuvent être mises au service d'agendas politiques extrêmes, en équipant aussi bien des agences gouvernementales que des campagnes électorales. L'IA promue par MAGA est une IA fermée (« boîte noire ») que seuls les concepteurs connaissent.

De l'autre côté du monde, la Chine développe une IA tout aussi performante, mais en faisant depuis peu le pari d'une IA ouverte (*open weight*) et en rassemblant autour d'elle un ensemble d'une trentaine de pays dans une alliance : l'Organisation de coopération mondiale sur l'intelligence artificielle (WAICO).

L'ingérence politique est devenue une réalité documentée : manipulation de l'opinion, production industrielle de fake news, micro-ciblage émotionnel des électeurs via l'IA générative, autant de pratiques qui exigent désormais une réponse réglementaire urgente, notamment sur la déclaration obligatoire de l'utilisation de l'IA dans les comptes de campagne électorale, afin de garantir la transparence du financement et des moyens employés. Cette menace est désormais reconnue au plus haut niveau de l'État : le Premier ministre Sébastien Lecornu a présenté aux partis politiques les risques d'ingérences étrangères pesant sur la présidentielle de 2027, soulignant qu'aucun pays européen n'y échappe depuis 2024.

Par ailleurs, la mainmise des GAFA sur les infrastructures numériques européennes constitue une dépendance structurelle, chiffrée avec précision par les travaux menés pour le CIGREF.[1] Cette captation de valeur affaiblit la compétitivité européenne et expose nos données stratégiques à des législations extraterritoriales comme le Cloud Act ou le FISA américains.

Face à cela, trois atouts européens méritent d'être posés dès l'introduction, car ils fondent la possibilité d'un choix plutôt que d'une seule résignation : une électricité largement décarbonée, atout majeur pour héberger des centres de calcul souverains et bas-carbone ; des champions émergents (Mistral AI, OVHcloud, Scaleway, ChapsVision, Atea…ASML aux Pays-Bas et StackIT en Allemagne) sur lesquels bâtir plutôt que repartir de zéro en les aidant à passer à l'échelle ; et une puissance normative unique (RGPD, DMA, DSA, AI Act) qui permet à l'Europe d'exporter ses règles au-delà de ses frontières, bien qu'aujourd'hui battu en brèche aux États-Unis depuis juillet 2026 : le président Trump a le droit de nommer les chefs des instances indépendantes chargées de vérifier la bonne transcription des règles RGPD…

[1] Voir supra, I) 4).

I. Contexte et enjeux : un monde recomposé par le numérique

1. Enjeux géopolitiques : la souveraineté en question

La rivalité sino-américaine constitue le rapport de force structurant du XXIe siècle numérique. Les États-Unis dominent les plateformes, les modèles d'intelligence artificielle et les systèmes d'exploitation ; la Chine contrôle des pans entiers de la chaîne de production électronique et des réseaux 5G via Huawei, projette son influence numérique à l'échelle mondiale et continue à surprendre les observateurs par la puissance des IA proposées face aux modèles américains.

Le déploiement d'un grand modèle d'IA de frontière illustre l'ampleur de ces montants : le coût d'entraînement d'un seul modèle de pointe se compte déjà en centaines de millions de dollars et pourrait atteindre le milliard, voire davantage, dans les prochaines années, sur des clusters de dizaines de milliers de GPU aujourd'hui très majoritairement fournis par Nvidia. Pour donner un ordre de grandeur comparatif au niveau public : le plan « InvestAI » de la Commission européenne mobilise jusqu'à 200 milliards d'euros d'ici 2030, dont 20 milliards pour quatre à cinq « gigafactories IA » de plus de 100 000 puces chacune ; la candidature française portée par le consortium AION (Ardian, Bull, Capgemini, EDF, Iliad, Orange, Scaleway, entre autres) avance un investissement de l'ordre de 10 milliards d'euros ; et une note récente évoque, à titre prospectif, un effort pouvant atteindre plusieurs centaines de milliards de dollars sur trois ans pour doter la France d'un laboratoire d'IA de frontière pleinement compétitif. Ces chiffres donnent la mesure de l'écart entre l'ambition affichée et les moyens aujourd'hui mobilisés. La souveraineté numérique ne peut donc se construire qu'à l'échelle européenne, par une mutualisation des investissements, une politique industrielle commune, des entreprises qui changent d'échelle et une réglementation ambitieuse.

Au-delà de la dépendance, il existe un risque systémique lié à la concentration : une poignée de grands modèles d'IA généralistes servent aujourd'hui de socle à presque tous les usages. Cette concentration fait peser un risque majeur : si l'un d'eux vient à défaillir (panne, changement de conditions, coupure d'accès), ce sont des pans entiers de l'économie et de l'administration qui peuvent s'arrêter d'un coup.

Dans cinq ans, si nous ne faisons rien ou pas assez : l'Europe ne parviendra pas à rattraper son retard industriel. Elle demeurera structurellement dépendante des infrastructures de calcul et des modèles d'IA américains et chinois et se retrouvera exposée aux décisions unilatérales de Washington ou de Pékin (restrictions à l'export de puces, coupures d'accès à des services critiques). Notre autonomie stratégique, militaire, industrielle, diplomatique, deviendrait alors un vœu pieux, chaque grande décision technologique se prenant hors de nos frontières.

Mais la souveraineté ne se limite pas au rattrapage. Trois leviers peuvent être activés dès aujourd'hui : faire de l'électricité décarbonée française un avantage compétitif pour héberger des centres de calcul souverains ; soutenir les modèles ouverts auditables (open source / open weight) ; et amplifier les champions existants, plutôt que de partir de zéro, en leur facilitant l'accès à des marchés.

2. Enjeux sécuritaires : infrastructures, individus et défense

La sécurité numérique se joue sur deux fronts simultanés. D'un côté, les infrastructures critiques — hôpitaux, réseaux électriques, systèmes bancaires, administrations — sont exposées à des cyberattaques d'ampleur croissante, souvent pilotées par des acteurs étatiques. De l'autre, les citoyens sont les victimes directes de vols de données massifs, portés par une criminalité galopante permettant aussi des escroqueries et agressions dans le monde réel.

L'ampleur du phénomène est désormais bien documentée. Selon le Panorama de la cybermenace 2025 de l'ANSSI, l'agence a traité 3 586 événements de sécurité et confirmé 1 366 incidents en 2025 ; l'éducation et la recherche, les collectivités et ministères, la santé et les télécommunications concentrent à eux seuls les trois quarts des incidents. Du côté des citoyens, la CNIL a enregistré 5 629 notifications de violations de

données en 2024, soit une hausse de 20 % en un an. Malgré l'adoption du RGPD, les fuites de données personnelles (de santé, bancaires, biométriques) se multiplient, tandis que la directive NIS 2 n'est toujours pas transposée en droit français. Les citoyens ne disposent pas des outils réels pour exercer leurs droits, faute de moyens des autorités de contrôle et de sanctions suffisamment dissuasives, alors que nombre de ces affaires relève de la « négligence » des organisations, donc du pénal.

Un volet est trop souvent absent de ces débats : celui de la défense et du double usage technologique, qui est actuellement l'une des clefs de l'innovation dans les conflits. Outre la cyber et la guerre informationnelle, l'IA militaire employable en matière de commandement, de renseignement, de ciblage, de coordination de dispositifs de drones autonomes et de capteurs font pourtant partie intégrante de l'autonomie stratégique, au même titre que la protection des infrastructures civiles.

Dans cinq ans, si nous ne faisons rien ou pas assez : les cyberattaques contre nos infrastructures vitales se seront multipliées et complexifiées, aidées par des IA offensives capables d'identifier les vulnérabilités, voire de générer des attaques automatisées et personnalisées à grande échelle. Un hôpital, un réseau électrique régional ou un système bancaire subira une paralysie majeure, avec des conséquences humaines directes. Les citoyens, dont les données biométriques et de santé auront continué de fuiter, n'auront toujours aucun recours réellement effectif, alimentant une défiance durable envers le numérique et les institutions.

La France dispose d'une filière cyber reconnue autour de l'ANSSI, de quelques grands industriels comme Thalès, Airbus ou Orange, et de quelques ETI…. Le reste du tissu industriel est plutôt constitué de PME ; voire de TPE, innovantes certes mais n'arrivant pas à passer à l'échelle par manque de financements européens et de marchés, et soumis à une concurrence et à un lobbying effréné des acteurs américano-israéliens.

Disposer d'une base industrielle capable de sécuriser les organisations et entreprises européennes est aussi un élément essentiel de l'autonomie stratégique.

3. Enjeux sociétaux : la majorité numérique et la protection des mineurs

Le numérique reconfigure en profondeur les liens sociaux, les modes d'apprentissage et les équilibres psychologiques, en particulier pour les générations les plus jeunes. Les algorithmes de recommandation, optimisés pour la captation maximale de l'attention, sont devenus des instruments de manipulation comportementale.

TikTok expose quotidiennement des millions d'enfants à des contenus préjudiciables (troubles alimentaires, violences, idéologies extrêmes) sans que les parents disposent des moyens effectifs d'intervention. La question de la majorité numérique, soit l'âge à partir duquel un mineur peut accéder seul aux réseaux sociaux, est devenue un enjeu politique et sanitaire de premier ordre. Les indicateurs suivis par Santé publique France et les organismes internationaux de référence font état d'une dégradation continue de la santé mentale des adolescents (anxiété, troubles alimentaires, exposition à des contenus extrêmes) et d'un temps d'écran quotidien très élevé chez les plus jeunes.
Deux risques émergents doivent être ajoutés à ce constat : les IA de compagnie (chatbots affectifs), auxquelles des mineurs peuvent s'attacher et confier des données intimes, avec un risque de conseils dangereux ; et la dépendance cognitive, c'est-à-dire la perte progressive de compétences (lecture, calcul, esprit critique) chez des jeunes qui délèguent trop tôt et sans formation à l'IA.

Dans cinq ans, si nous ne faisons rien ou pas assez : une génération entière aura grandi sans aucun garde-fou réel face à des algorithmes toujours plus efficaces pour capter et orienter son attention. Les indicateurs de santé mentale des adolescents continueront de se dégrader, sans que les familles ni l'école ne disposent de leviers d'action concrets. La question de la majorité numérique, non tranchée, se sera imposée dans le débat public par la crise plutôt que par l'anticipation politique.

Mais l'IA peut aussi être un atout éducatif : tutorat personnalisé, remédiation scolaire, outils souverains de contrôle parental et de vérification d'âge respectueux de la vie privée. L'enjeu pour les responsables politiques sera de financer et de labelliser des solutions européennes plutôt que de subir celles imposées par les plateformes.

4. Enjeux économiques : la valeur captée hors d'Europe

L'économie numérique génère des rentes considérables, captées presque exclusivement par des acteurs américains et asiatiques. L'Europe paie chaque année des dizaines de milliards d'euros en licences logicielles, en services cloud et en accès aux plateformes d'IA, sans disposer d'alternatives compétitives à la hauteur. La transition vers l'IA transforme profondément les marchés du travail et exige une politique d'accompagnement ambitieuse.

Pour donner la mesure de cette « facture numérique » : les entreprises et administrations françaises consacrent aujourd'hui environ 66 milliards d'euros par an au cloud et au logiciel (400 milliards à l'échelle de l'Union), une dépense qui croît de 8,7 % par an et pourrait dépasser 700 milliards d'euros à l'échelle européenne d'ici 2030, pour un surcoût annuel projeté de 140 milliards d'euros et une perte de valeur ajoutée de l'ordre de 107 milliards d'euros et 1,4 million d'emplois pour l'économie européenne.[2] Ce déficit doit désormais être mis en regard avec les montants publics engagés pour le résorber : de l'ordre de 200 milliards d'euros au niveau européen d'ici 2030 via InvestAI, dont une fraction seulement, de l'ordre de quelques dizaines de milliards, est aujourd'hui fléchée vers des projets français.

Dans cinq ans, si nous ne faisons rien ou pas assez : la facture numérique européenne (cloud, licences, IA) continuera de croître de manière incontrôlée, aggravant notre déficit commercial dans les services numériques. Les emplois et talents les plus qualifiés continueront d'être attirés par les écosystèmes américains, faute de champions européens compétitifs. Les métiers bouleversés par l'automatisation et l'IA n'auront pas bénéficié d'un accompagnement suffisant, creusant les inégalités entre travailleurs qualifiés capables de tirer parti de l'IA et ceux laissés sur le bord du chemin.

Il ne faut pas s'y tromper : ce qui se passe aujourd'hui avec l'IA suit la même trajectoire que Google avec Booking. Au départ, ce n'est pas cher, et ensuite cela capte une part croissante de la valeur créée, sans qu'on puisse en sortir facilement, sauf à s'organiser pour « vivre à part », à la façon du groupe Accor. Ceux qui en doutent n'ont qu'à se demander comment les milliers de milliards d'euros investis par les géants de l'IA pourront rétribuer leurs bailleurs de fonds sans faire, à terme, payer très cher leurs services.

Trois leviers de reconquête de valeur méritent d'être explorés : des marchés réglementés orientés vers les solutions européennes ; un levier fiscal (taxation effective des géants et conditionnalité des aides) ; et l'accompagnement de l'inclusion numérique — la lutte contre l'illectronisme, qui touche environ 13 millions de Français et constitue à la fois un enjeu social et un marché à part entière.
La commande publique seule ne suffira pas à changer la donne et l'Etat a besoin de performances qu'on ne trouve pas forcément, aujourd'hui, dans les solutions européennes. Ce sont bien les entreprises qu'il faut convaincre, par des mesures réglementaires pour les secteurs essentiels et des mesures d'incitation pour tous, car ce sont les grandes entreprises qui peuvent faire plier leurs fournisseurs vers des solutions conciliant le meilleur de la performance et le meilleur de la souveraineté.

5. Enjeux culturels et manipulation de l'information, évolution des métiers

Les industries culturelles européennes sont affaiblies par la domination des plateformes de distribution, qui captent la valeur au détriment des créateurs. Parallèlement, la désinformation est devenue une arme stratégique : infox, deepfakes, campagnes d'influence coordonnées exploitent la viralité des plateformes pour déstabiliser les démocraties, fracturer les débats publics et manipuler les scrutins électoraux. L'IA vient déstabiliser de nombreux métiers

[2] Étude du cabinet Asterès pour le CIGREF, mai 2026.

Un sujet amont est trop souvent absent de ces débats : celui de la propriété intellectuelle et des données d'entraînement. Sur quelles œuvres les modèles d'IA sont-ils entraînés, avec quel consentement et quelle rémunération des créateurs, des artistes et de la presse ? C'est le pendant, en amont, de la « juste rémunération » évoquée dans la partie consacrée à l'action politique.

Dans cinq ans, si nous ne faisons rien ou pas assez : les deepfakes et les campagnes de désinformation générées par IA seront devenus indiscernables du réel pour une large part des électeurs, y compris à l'approche d'échéances majeures comme la présidentielle de 2027. Les créateurs et médias européens, toujours privés d'une juste rémunération, auront continué de perdre en indépendance financière. La confiance dans l'information et dans le processus démocratique lui-même en sera durablement fragilisée.

Face à la désinformation, des leviers concrets existent : soutenir les standards de provenance et de marquage des contenus (traçabilité, filigrane numérique) ; investir dans l'éducation aux médias ; et développer des outils civiques (vérification, démocratie délibérative) qui font de la technologie un appui pour le débat public plutôt qu'une menace.

Cela passe aussi par une formation massive à réaliser auprès des professeurs et des élèves bien sûr, mais aussi dans le cadre des formations continues. Il faut apprendre à maitriser ces technologies afin de ne pas les subir ; de nombreux métiers vont être ou sont déjà touchés.

6. Enjeux liés à l'IA augmentée : des pratiques bouleversées plus vite que la régulation

Une nouvelle génération d'IA dites « augmentées », agentiques ou encore « frontière », capables d'agir de manière autonome, d'enchaîner des tâches complexes et de prendre des décisions avec une supervision humaine réduite, commence à transformer en profondeur les pratiques professionnelles : médecine, droit, administration, éducation, journalisme. Ces systèmes soulèvent des questions inédites de responsabilité, de fiabilité et de contrôle, à un rythme que les cadres juridiques et techniques nationaux peinent à suivre.

Cette inquiétude n'est plus l'apanage des seuls défenseurs d'une régulation stricte : même l'administration américaine, pourtant engagée dans une ligne résolument dérégulatrice sur l'IA, commence à exprimer des réserves sur ces sujets et encourage les acteurs privés à s'autoréguler, faute de cadre étatique capable d'évoluer à la vitesse de la technologie. Ce constat, venant d'un acteur peu suspect de vouloir freiner l'innovation, doit alerter les responsables politiques français et européens sur l'urgence d'anticiper ces bouleversements plutôt que de les subir.

Un agent d'IA autonome intégré aux systèmes d'une administration ou d'une entreprise peut aujourd'hui traiter des dossiers, engager des dépenses ou produire des recommandations sans qu'un cadre clair ne définisse qui est responsable en cas d'erreur, de biais ou de dérive. L'autorégulation privée, en l'absence de norme publique, laisse aux seuls acteurs technologiques, principalement américains et chinois, le soin de fixer les limites de leurs propres outils.

Dans cinq ans, si nous ne faisons rien ou pas assez : des pans entiers de métiers qualifiés (juridique, médical, administratif) fonctionneront avec des IA agentiques largement autonomes, déployées sans cadre de responsabilité clair ni contrôle démocratique réel. Les incidents (erreurs de décision, biais discriminatoires, dérives incontrôlées, piratage de prompts) se seront multipliés, révélés après coup plutôt qu'anticipés. La France et l'Europe, prises de vitesse, se retrouveront à réguler dans l'urgence des pratiques déjà généralisées, plutôt qu'à en avoir fixé les règles du jeu en amont.

Il faut également anticiper le risque de « désintermédiation » des professionnels (médecins, juristes, enseignants) qui délèguent progressivement leur jugement à des agents autonomes, avec des enjeux de sécurité et de qualité, et pas seulement d'emploi : la supervision humaine effective doit rester la règle. L'IA

agentique est aussi, à l'inverse, une opportunité pour l'État lui-même : modernisation et gains de productivité des services publics, appui à la santé et à la recherche.

Enfin, l'empreinte environnementale et énergétique de l'IA — électricité, eau, foncier des centres de données — doit être traitée comme un enjeu à part entière plutôt que comme un angle mort. Elle est aussi, pour la France, une carte à jouer : la souveraineté énergétique, adossée à une électricité décarbonée, peut devenir un facteur de compétitivité pour l'hébergement de centres de calcul, à condition d'articuler cette ambition avec le défi de la transition climatique.

II. Ces grands axes méritent une action politique

Les six thèmes identifiés appellent des réponses politiques concrètes, ambitieuses et cohérentes. Voici les axes d'action sur lesquels nous souhaitons échanger avec vous.

1. Construire la souveraineté numérique à l'échelle européenne

- Aider les entreprises à répondre aux appels d'offres européens et à constituer des consortiums européens ;
- conditionner les marchés publics ou réglementés numériques à l'utilisation de solutions européennes dès lors qu'elles existent et sont performantes ou certifiées ;
- financer la formation et la recherche pour créer un vivier de talents européens capables de rivaliser avec la Silicon Valley ;
- bâtir une stratégie « énergie + calcul » adossée au parc nucléaire pour des centres de données souverains ;
- soutenir explicitement les modèles ouverts et les champions européens et français (Mistral, OVHcloud, Scaleway, Chapsvision….) ;
- utiliser la puissance normative européenne comme un instrument de souveraineté (« effet Bruxelles ») ;
- favoriser face aux approches « Cloud public » des architectures alliant le meilleur de la performance et le meilleur de la souveraineté via des partenaires étrangers mettant en œuvre des approches d'éditeur « on premise ».

2. Protéger les citoyens et sécuriser les infrastructures

- Renforcer les moyens et pouvoirs des autorités de régulation (CNIL, ANSSI) pour garantir l'effectivité du RGPD et la cybersécurité des opérateurs d'importance vitale ;
- conserver sa capacité d'influence et sa crédibilité en ne devenant pas le mauvais élève cyber de l'Europe (transposition de NIS 2 hors délai, multiplication des fuites de données) ;
- judiciariser les incidents cybers importants, notamment les fuites de données massives des citoyens, en les qualifiant d'infractions pénales non intentionnelles relevant de la négligence des directions ;
- légiférer sur la majorité numérique : instaurer une vérification effective de l'âge et un consentement parental renforcé pour l'accès des mineurs aux réseaux sociaux ;
- soutenir des outils souverains de vérification d'âge respectueux de la vie privée ;

- exiger la transparence algorithmique des plateformes et sanctionner les systèmes de recommandation nocifs pour les mineurs ;
- encadrer les ia de compagnie et les chatbots destinés aux mineurs ;
- appuyer les standards de provenance et de marquage des contenus pour lutter contre les deepfakes.

3. Rétablir une concurrence équitable et créer de la valeur en Europe

- Accélérer l'application du Digital Markets Act pour briser les rentes de situation des grandes plateformes et ouvrir le marché à des concurrents européens ;
- soutenir les PME et les territoires dans leur transformation numérique par des dispositifs d'accompagnement et de financement dédiés ;
- faciliter l'innovation et la création d'entreprise non par des subventions de projet technique, mais par de l'appui à la contractualisation avec les premiers clients ;
- faciliter et accompagner des levées de fonds pour permettre aux entreprises de grossir vite et arriver à avoir une taille significative, en mobilisant vers cet objectif les crédits européens ;
- activer le levier fiscal : taxation effective des plateformes et conditionnalité des aides publiques ;
- orienter la commande publique et celle de grandes entreprises vers les solutions européennes ;
- déployer un plan de lutte contre l'illectronisme pour ne laisser personne au bord du chemin.

4. Défendre la démocratie et la diversité culturelle

- Investir massivement dans l'éducation aux médias et à l'information numérique dès le primaire, pour former des citoyens résilients face à la désinformation ;
- garantir une juste rémunération des créateurs et des médias dans l'économie des plateformes ;
- fixer un cadre clair sur les données d'entraînement : consentement et rémunération des ayants droit et de la presse ;
- soutenir les standards de traçabilité et de marquage des contenus générés par IA ;
- développer des outils civiques au service du débat démocratique.

Comité de rédaction :
Amiral (2S) Arnaud Coustillière, Alexandre Malafaye
Avec le soutien de Marie Roisnel et de Marie Evrard
Contact :
Institut-synopia@synopia.fr et adjoint.international@pole-excellence-cyber.org