RIGST — *Revue Internationale de Gouvernance, Stratégie et Territoires*

Institut Européen de Gouvernance et de Stratégie Internationale

revue@iegsi.eu · www.iegsi.eu · © 2026 IEGSI

NOTE STRATÉGIQUE

Référence : RIGST-NS-2026-001

Classification : Diffusion publique

Date : Juin 2026

Souveraineté numérique : enjeux de gouvernance globale

Analyse prospective des cadres réglementaires émergents, des stratégies de souveraineté technologique et de leurs implications pour les institutions publiques et les opérateurs économiques

Auteure : Sophie Ngamba Mbeki

Qualité : Directrice du Pôle Diplomatie Économique et Numérique, IEGSI

Institution : IEGSI — Institut Européen de Gouvernance et de Stratégie Internationale

Référence : RIGST-NS-2026-001

Date de publication : Juin 2026

Évaluation : Revue par le Comité scientifique et stratégique IEGSI

Mots-clés : *souveraineté numérique ; gouvernance de l'internet ; réglementation technologique ; intelligence artificielle ; données personnelles ; géopolitique du numérique ; cloud souverain ; RGPD ; DMA ; DSA*

RÉSUMÉ EXÉCUTIF

SYNTHÈSE ANALYTIQUE DE LA NOTE STRATÉGIQUE

La souveraineté numérique est devenue, au cours des cinq dernières années, l'un des enjeux les plus structurants de la géopolitique mondiale et de la gouvernance institutionnelle contemporaine. Ce qui n'était encore, au début des années 2010, qu'un concept émergent dans les cercles académiques spécialisés est devenu aujourd'hui une priorité stratégique explicitement affichée par les grandes puissances mondiales, un vecteur de compétition internationale entre blocs technologiques rivaux et une contrainte opérationnelle majeure pour les institutions publiques comme pour les opérateurs économiques de toutes tailles.

Cette note stratégique analyse les dynamiques de fond qui ont propulsé la souveraineté numérique au sommet des agendas politiques et institutionnels, cartographie les cadres réglementaires émergents à l'échelle mondiale, décrypte les stratégies de souveraineté technologique déployées par les grandes puissances et les blocs géopolitiques, et propose une analyse prospective de leurs implications pour les institutions publiques et les opérateurs économiques à l'horizon 2030.

Trois conclusions majeures structurent notre analyse. La souveraineté numérique ne constitue pas un phénomène conjoncturel lié à des tensions géopolitiques passagères : elle représente une reconfiguration structurelle et durable de l'architecture de gouvernance de l'espace numérique mondial, dont les effets se feront sentir pendant plusieurs décennies. La fragmentation réglementaire et technologique en cours — conceptualisée dans cette note sous le terme de trilemme de la gouvernance numérique — impose aux acteurs institutionnels et économiques des arbitrages stratégiques fondamentaux pour lesquels la majorité d'entre eux n'est pas encore suffisamment préparée. Enfin, les acteurs qui parviendront à construire des stratégies de souveraineté numérique cohérentes et proactives bénéficieront d'avantages compétitifs et institutionnels considérables dans le monde numérique multipolaire qui se dessine.

POINTS CLÉS DE CETTE NOTE STRATÉGIQUE

- **La fragmentation irréversible de l'espace numérique mondial**

  Le « splinternet » — la division de l'internet mondial en espaces numériques distincts gouvernés par des règles, des normes et des acteurs différents — n'est plus un scénario prospectif mais une réalité en cours de consolidation. Les acteurs institutionnels et économiques doivent intégrer cette réalité dans leurs stratégies numériques à moyen et long terme.

- **L'Union européenne comme puissance réglementaire mondiale**

  Avec le RGPD, le DSA, le DMA et l'AI Act, l'UE a établi le corpus réglementaire numérique le plus complet et le plus ambitieux du monde. L'effet Bruxelles — la diffusion mondiale des normes européennes par capillarité — fait de la réglementation européenne un instrument de souveraineté technologique à part entière.

- **Le trilemme de la gouvernance numérique**

  Les acteurs institutionnels et économiques font face à un trilemme insoluble entre efficacité opérationnelle, conformité réglementaire multi-juridictionnelle et souveraineté des données. La gestion stratégique de ce trilemme constitue le défi de gouvernance numérique central de la prochaine décennie.

- **L'intelligence artificielle comme nouveau front de souveraineté**

La gouvernance de l'IA représente le prochaine bataille de la souveraineté numérique mondiale. Celui qui définit les normes et les standards de l'IA souveraine — l'UE avec l'AI Act, les États-Unis avec leurs executive orders, la Chine avec ses règlements sectoriels — définit les règles du jeu pour des décennies à venir.

Les recommandations stratégiques de l'IEGSI

Cette note formule douze recommandations opérationnelles à destination des institutions publiques, des régulateurs nationaux et des opérateurs économiques pour naviguer dans la complexité du nouveau paysage de souveraineté numérique.

TABLE DES MATIÈRES

INTRODUCTION

Il est des moments dans l'histoire des technologies où une bifurcation s'opère non pas progressivement, par accumulation de petites transformations imperceptibles, mais brutalement, sous l'effet conjugué de ruptures technologiques, de chocs géopolitiques et de prises de conscience institutionnelles dont la soudaineté contraste avec la profondeur des transformations qu'elles engagent. La montée en puissance de la souveraineté numérique comme enjeu central de la gouvernance globale constitue précisément une telle bifurcation. En moins d'une décennie, le paradigme dominant de l'internet mondial, fondé sur la libre circulation des données, l'universalisme des standards techniques et la gouvernance multi-parties prenantes d'inspiration libérale, a cédé la place à un nouveau paradigme fragmenté, conflictuel et profondément géopolitisé, dans lequel la maîtrise des données, des infrastructures et des standards numériques constitue un enjeu de puissance aussi stratégique que le contrôle des ressources énergétiques ou des arsenaux militaires.

Cette transformation n'est pas le produit du hasard ni le résultat d'une planification concertée entre acteurs aux intérêts convergents. Elle est le fruit d'une conjonction de facteurs hétérogènes dont la combinaison a produit des effets systémiques que peu d'observateurs avaient anticipés dans leur ampleur. Les révélations Snowden de 2013 sur les programmes de surveillance massive de la NSA ont constitué le premier choc majeur, en révélant aux gouvernements du monde entier la vulnérabilité de leurs communications et de leurs données aux ingérences d'une puissance étrangère, fût-elle alliée. Les scandales successifs autour des grandes plateformes numériques, de Cambridge Analytica aux soupçons d'ingérence électorale en passant par les controverses autour de TikTok, ont ensuite démontré que les risques liés à la dépendance numérique ne se limitaient pas à la surveillance étatique mais touchaient également à l'intégrité démocratique et à la souveraineté des décisions politiques. La pandémie de Covid-19 a révélé avec une acuité particulière la dimension critique des infrastructures numériques et la vulnérabilité stratégique que représente la concentration des capacités technologiques entre les mains d'un petit nombre d'acteurs privés majoritairement localisés en dehors des frontières européennes.

C'est dans ce contexte d'une complexité et d'une urgence croissantes que l'IEGSI propose cette analyse prospective de la souveraineté numérique. Notre ambition n'est pas de produire une recension exhaustive de l'abondante littérature académique et institutionnelle sur le sujet, mais de fournir aux décideurs publics et aux opérateurs économiques un cadre analytique cohérent pour comprendre les dynamiques en jeu, anticiper leurs évolutions et formuler des stratégies adaptées aux contraintes et aux opportunités du nouveau paysage de gouvernance numérique.

I. Anatomie d'un concept révolutionnaire : la souveraineté numérique en question

1.1 Généalogie et évolution sémantique

Le concept de souveraineté numérique est apparu dans le débat académique et politique au cours des années 2010, porté initialement par des juristes et des politologues européens préoccupés par les implications de la dépendance numérique vis-à-vis des grandes plateformes américaines et des législations extraterritoriales, au premier rang desquelles le CLOUD Act de 2018. Sa signification originelle était essentiellement défensive : il s'agissait de préserver la capacité des États à exercer leur autorité juridictionnelle sur les données de leurs citoyens et de leurs entreprises, à l'abri des intrusions d'acteurs étrangers, étatiques ou privés. Cette conception défensive, bien que toujours pertinente, s'est considérablement enrichie depuis lors, au point que la souveraineté numérique désigne aujourd'hui un ensemble pluridimensionnel de capacités que les États, les organisations régionales et les institutions cherchent à préserver ou à reconquérir dans l'espace numérique.

On peut en distinguer au moins cinq dimensions analytiquement distinctes, même si elles sont dans la pratique profondément interdépendantes. La souveraineté des données constitue la dimension la plus immédiatement accessible et la plus avancée sur le plan réglementaire : elle désigne la capacité d'un acteur à contrôler la collecte, le stockage, le traitement et la transmission des données qui lui sont relatives ou qui transitent par son territoire. Le RGPD européen en constitue l'expression réglementaire la plus aboutie. La souveraineté des infrastructures renvoie au contrôle des couches physiques et logiques sur lesquelles repose l'espace numérique, notamment les câbles sous-marins, les satellites, les centres de données et les réseaux de télécommunications de cinquième génération. La souveraineté technologique désigne la capacité à maîtriser les technologies numériques critiques sans dépendance excessive vis-à-vis d'acteurs étrangers susceptibles d'exercer une coercition en cas de détérioration des relations diplomatiques. La souveraineté normative renvoie à la capacité à influer sur la définition des standards qui régissent l'espace numérique mondial, domaine dans lequel celui qui définit les normes définit les règles du jeu pour l'ensemble des acteurs. La souveraineté algorithmique, enfin, désigne la capacité à comprendre, à auditer et à orienter les systèmes d'intelligence artificielle qui médiatisent de manière croissante l'ensemble des décisions de nos sociétés.

CONCEPT CLEF — LE TRILEMME DE LA GOUVERNANCE NUMÉRIQUE

Le trilemme de la gouvernance numérique postule qu'aucun acteur institutionnel ou économique ne peut simultanément satisfaire trois objectifs également désirables : l'efficacité opérationnelle maximale, c'est-à-dire l'utilisation des meilleurs outils disponibles sur le marché mondial quelle que soit leur origine géographique ; la conformité réglementaire complète dans toutes les juridictions dans lesquelles il opère ou avec lesquelles il interagit ; et la souveraineté intégrale de ses données et de ses

systèmes d'information. Toute stratégie de gouvernance numérique implique nécessairement de sacrifier partiellement l'un de ces trois objectifs au profit des deux autres, et le choix des arbitrages à opérer constitue la décision stratégique fondamentale à laquelle sont confrontés les dirigeants institutionnels et économiques dans le contexte actuel.

1.2 Le trilemme de la gouvernance numérique

Pour rendre compte des contraintes structurelles auxquelles font face les acteurs institutionnels et économiques dans leur gestion de la souveraineté numérique, l'IEGSI propose le concept de trilemme de la gouvernance numérique, qui s'inspire du trilemme de Mundell en économie internationale et du trilemme politique développé par Rodrik dans ses travaux sur la mondialisation. Ce trilemme postule qu'un acteur opérant dans l'espace numérique mondial ne peut simultanément satisfaire trois objectifs également désirables : l'efficacité opérationnelle maximale, la conformité réglementaire complète dans toutes les juridictions pertinentes, et la souveraineté intégrale des données et des systèmes d'information. Toute stratégie de gouvernance numérique implique nécessairement de sacrifier partiellement l'un de ces trois objectifs, et le choix des arbitrages à opérer constitue la décision stratégique fondamentale des dirigeants institutionnels et économiques.

II. La géopolitique de la souveraineté numérique : trois modèles en compétition

2.1 Le modèle européen : la réglementation comme instrument de souveraineté

L'approche européenne de la souveraineté numérique repose sur un pari intellectuellement audacieux et historiquement inédit : utiliser la réglementation non pas seulement comme un instrument de protection des droits fondamentaux et du marché intérieur, mais comme un vecteur d'influence normative mondiale capable de transformer les pratiques des acteurs technologiques à l'échelle globale. Ce pari s'appuie sur l'effet Bruxelles, la tendance des entreprises à aligner leurs pratiques mondiales sur les standards européens pour éviter la complexité de la gestion de multiples régimes de conformité, que Bradford (2020) a documenté de manière systématique dans ses travaux pionniers sur la puissance réglementaire de l'Union européenne.

Le corpus réglementaire numérique européen construit depuis 2016 est d'une ampleur et d'une cohérence sans équivalent dans le monde. Le Règlement Général sur la Protection des Données de 2018, pionnier dans sa conceptualisation de la vie privée comme droit fondamental opposable aux acteurs économiques les plus puissants, a provoqué une onde de choc réglementaire mondiale dont les effets continuent de se diffuser. Le Digital Services Act et le Digital Markets Act de 2022, qui encadrent respectivement la responsabilité des

plateformes numériques et les pratiques anticoncurrentielles des contrôleurs d'accès, constituent une rupture radicale avec l'approche permissive qui avait prévalu depuis les origines de l'internet commercial. L'AI Act de 2024, premier règlement mondial dédié à la gouvernance de l'intelligence artificielle, établit une approche fondée sur les risques qui pourrait bien devenir le standard de référence mondial pour la régulation de l'IA.

Cette stratégie réglementaire présente cependant des limites importantes que les institutions européennes commencent à reconnaître explicitement. La réglementation peut contraindre les comportements des acteurs technologiques déjà établis, mais elle ne peut pas seule engendrer les capacités technologiques souveraines qui manquent à l'Europe dans les domaines des semi-conducteurs de pointe, des grands modèles de langage ou des services cloud hyperscalers. La prise de conscience de cette limite a conduit à une évolution significative de la stratégie européenne depuis 2022, avec l'adoption du Chips Act et les investissements massifs dans les projets d'infrastructure cloud souveraine.

L'EFFET BRUXELLES EN CHIFFRES

Le RGPD a conduit 145 pays à adopter une législation sur la protection des données personnelles entre 2018 et 2026, contre 40 pays en 2000. Selon les données de l'IAPP publiées au premier trimestre 2026, 78 % des entreprises multinationales ont aligné leurs pratiques mondiales de traitement des données sur les standards européens pour éviter la gestion de multiples régimes de conformité. L'amende de 1,3 milliard d'euros infligée à Meta en 2023 a constitué un signal mondial sur la capacité de l'Union européenne à faire respecter ses règles par les plus grands acteurs technologiques.

2.2 Le modèle américain : souveraineté de marché et sécurité nationale

L'approche américaine de la souveraineté numérique est fondamentalement différente de l'approche européenne dans ses fondements doctrinaux, ses instruments et ses objectifs. Elle repose sur une combinaison de deux impératifs que les administrations successives ont cherché à articuler avec des succès variables : la préservation du leadership technologique américain et de la compétitivité mondiale des géants numériques américains, conçus comme des vecteurs de l'influence et de la puissance nationale ; et la protection de la sécurité nationale contre les ingérences numériques étrangères, en particulier chinoises, dont l'ampleur et la sophistication croissantes ont conduit à une réaction de plus en plus musclée de la part de l'exécutif américain.

Cette tension entre ces deux impératifs explique l'ambivalence caractéristique de la politique numérique américaine. Les États-Unis ont simultanément promu la libre circulation des données à l'échelle mondiale comme principe de gouvernance libérale de l'internet, et déployé un arsenal de restrictions à l'exportation de technologies sensibles sans précédent depuis la Guerre froide. L'Export Administration Regulations renforcé, les

restrictions visant Huawei dans les réseaux 5G alliés et les tentatives d'interdiction de TikTok illustrent la dimension protectionniste-sécuritaire d'une politique qui continue pourtant d'afficher une rhétorique de liberté numérique.

2.3 Le modèle chinois : souveraineté totale et exportation d'un paradigme

La Chine a développé, au fil de trente ans d'expérimentation et d'une cohérence doctrinale remarquable, le modèle le plus radical de souveraineté numérique qui soit, désigné sous les termes de cyberespace souverain ou de sécurité de l'information. Ce modèle repose sur trois piliers indissociables : le contrôle territorial de l'espace numérique national incarné par le Grand Pare-feu ; le développement d'un écosystème technologique national intégré et autosuffisant, porté par des champions industriels comme Huawei, Alibaba, Tencent et ByteDance ; et l'exportation active du modèle de gouvernance numérique souveraine à destination des pays en développement à travers les Routes de la Soie Numériques.

L'ambition exportatrice de la Chine dans le domaine de la gouvernance numérique représente peut-être la dimension géopolitiquement la plus significative de ce modèle. À travers le déploiement d'infrastructures numériques dans les pays partenaires, notamment des centres de données, des réseaux 5G construits par Huawei, des systèmes de surveillance urbaine et des plateformes de paiement numérique, la Chine construit une dépendance technologique qui lui confère une influence stratégique durable, difficile à remettre en cause une fois les infrastructures déployées et les habitudes numériques installées.

FOCUS — LES ROUTES DE LA SOIE NUMÉRIQUES

L'initiative des Routes de la Soie Numériques lancée en 2015 a permis le déploiement d'infrastructures numériques dans 138 pays. Selon les données compilées par l'IEGSI, Huawei a déployé des réseaux 4G et 5G dans 70 pays africains, Alibaba Cloud opère des centres de données dans 25 pays émergents, et les solutions de surveillance urbaine d'entreprises chinoises équipent plus de 60 villes à travers le continent africain. La question de la souveraineté des données dans ces écosystèmes numériques opérés par des entreprises soumises à la législation chinoise sur la sécurité nationale représente un enjeu stratégique de première importance pour les gouvernements et les institutions africains.

2.4 Les autres acteurs : entre alignement, autonomie et instrumentalisation

Au-delà des trois grands blocs technologiques, une série d'acteurs plus modestes mais stratégiquement importants développent leurs propres approches de la souveraineté numérique, souvent en cherchant à tirer parti de la compétition entre les grandes puissances pour maximiser leurs marges de manœuvre stratégiques. L'Inde représente le cas le plus intéressant de construction d'une voie spécifique. Forte de sa position de troisième

utilisateur mondial d'internet et de son écosystème technologique national en pleine croissance, New Delhi développe une approche qui aspire à l'indépendance vis-à-vis des deux blocs dominants sans renoncer aux bénéfices de l'intégration dans l'économie numérique mondiale.

L'Afrique se trouve dans une position particulièrement délicate. Massivement dépendante d'infrastructures numériques construites et contrôlées par des acteurs étrangers, elle risque de voir la bataille pour la souveraineté numérique mondiale se jouer sur son territoire sans disposer des capacités institutionnelles et technologiques nécessaires pour peser sur son issue. La Convention de Malabo de l'Union Africaine sur la cybersécurité et la protection des données personnelles, encore insuffisamment ratifiée, et les initiatives de la Zone de Libre-Échange Continentale Africaine dans le domaine numérique constituent des tentatives prometteuses mais encore fragiles de construction d'une souveraineté numérique africaine collective.

III. Les cadres réglementaires émergents : anatomie d'une révolution normative

3.1 L'écosystème réglementaire européen : complexité, cohérence et rayonnement

La compréhension précise de l'écosystème réglementaire européen dans le domaine numérique est devenue une compétence stratégique indispensable pour tout acteur institutionnel ou économique opérant dans l'espace européen ou en relation avec des partenaires européens. Cet écosystème est structuré autour d'une architecture à plusieurs niveaux dont la cohérence interne, bien qu'imparfaite sur certains points, est remarquable au regard de la complexité des enjeux traités.

Le RGPD constitue la fondation de cet édifice réglementaire. Entré en application en mai 2018, il a profondément transformé les pratiques de collecte et de traitement des données personnelles à l'échelle mondiale, grâce à son mécanisme d'application extraterritoriale. Ses principes cardinaux, protection des données dès la conception, minimisation des données, limitation de finalité, transparence et droit à l'oubli, ont redéfini les relations entre les organisations et les données personnelles qu'elles détiennent, avec des implications opérationnelles considérables pour l'ensemble des secteurs économiques.

Le Digital Services Act et le Digital Markets Act de 2022 représentent la deuxième vague majeure de la révolution réglementaire européenne, ciblant spécifiquement les plateformes numériques de grande taille. Le DSA impose aux très grandes plateformes en ligne des obligations renforcées en matière de modération des contenus illicites, de transparence algorithmique et d'accès aux données pour les chercheurs. Le DMA, de son côté, s'attaque aux pratiques anticoncurrentielles des contrôleurs d'accès, en leur imposant des obligations d'interopérabilité et d'accès aux données qui visent à rétablir une

concurrence effective dans l'écosystème numérique européen. L'AI Act, entré en vigueur en 2024, constitue la troisième révolution normative : son approche fondée sur les risques est conceptuellement ambitieuse mais génère une incertitude juridique considérable pour les organisations qui développent ou déploient des systèmes d'intelligence artificielle.

PANORAMA DE L'ÉCOSYSTÈME RÉGLEMENTAIRE NUMÉRIQUE EUROPÉEN

Le RGPD (2018) établit la protection des données personnelles comme droit fondamental avec une portée mondiale extraterritoriale, des sanctions pouvant atteindre 4 % du chiffre d'affaires mondial et 1 750 décisions rendues par les CNIL nationales entre 2018 et 2025.

Le DSA (2022) encadre la responsabilité des plateformes numériques en matière de modération des contenus, de transparence algorithmique et d'accès aux données pour la recherche. Dix-neuf Very Large Online Platforms et deux Very Large Search Engines sont désignés.

Le DMA (2022) vise les marchés numériques et impose aux contrôleurs d'accès, à savoir Alphabet, Amazon, Apple, ByteDance, Meta et Microsoft, des obligations d'interopérabilité et l'interdiction de pratiques anticoncurrentielles spécifiées.

L'AI Act (2024), premier règlement mondial sur l'intelligence artificielle, adopte une approche fondée sur les risques avec interdiction des IA présentant des risques inacceptables et obligations strictes pour les IA à haut risque.

3.2 Au-delà de l'Europe : cartographie des régimes réglementaires mondiaux

La prolifération des régimes réglementaires nationaux dans le domaine numérique constitue l'un des défis opérationnels les plus complexes auxquels font face les opérateurs économiques internationaux. Selon les données de l'International Association of Privacy Professionals compilées au premier trimestre 2026, 145 pays disposent aujourd'hui d'une législation sur la protection des données personnelles, contre seulement 40 en 2000. Cette multiplication des régimes nationaux, dont les exigences sont souvent partiellement contradictoires, crée une complexité de conformité croissante que seuls les acteurs disposant de ressources juridiques et de gouvernance considérables peuvent gérer efficacement.

Trois familles de régimes réglementaires peuvent être distinguées. La famille des régimes d'inspiration européenne regroupe les pays qui ont adopté des législations directement inspirées du RGPD, permettant des flux transfrontaliers de données sur la base de décisions d'adéquation de la Commission européenne, et comprenant l'essentiel des pays d'Amérique latine, plusieurs pays africains comme le Maroc, la Tunisie et le Kenya, ainsi que certains pays d'Asie-Pacifique. La famille des régimes de type américain regroupe les approches sectorielles et fragmentées, sans législation nationale unifiée sur la protection des données, mais avec des régimes sectoriels spécifiques complétés par des législations étatiques dont la CCPA californienne constitue l'exemple le plus ambitieux. La famille des régimes de souveraineté stricte, enfin, regroupe les pays qui imposent des exigences de

localisation des données sur leur territoire et des restrictions aux transferts transfrontaliers d'une sévérité variable, notamment la Russie, la Chine et l'Inde dans certains secteurs.

IV. Implications stratégiques pour les institutions publiques et les opérateurs économiques

4.1 Le nouveau paradigme de la conformité numérique

La transformation du paysage réglementaire numérique impose aux institutions publiques comme aux opérateurs économiques une révolution dans leur approche de la conformité. Le paradigme traditionnel, fondé sur une approche réactive, sectorielle et essentiellement juridique des obligations légales, est profondément inadapté au nouveau contexte de prolifération et de fragmentation réglementaire. Ce que l'IEGSI désigne comme la conformité stratégique repose sur quatre principes fondamentaux.

La prospective réglementaire constitue le premier de ces principes : la vitesse d'évolution des cadres normatifs dans le domaine numérique impose d'anticiper les obligations futures plutôt que de se contenter de satisfaire les exigences actuelles. Les organisations qui ont intégré les principes du RGPD avant son entrée en vigueur ont bénéficié d'un avantage compétitif considérable, tout comme celles qui préparent aujourd'hui leurs architectures techniques et organisationnelles aux exigences de l'AI Act avant même que ses obligations les plus contraignantes ne soient applicables. L'intégration systémique constitue le deuxième principe : la conformité numérique ne peut plus être gérée comme une fonction spécialisée, confinée aux équipes juridiques, mais doit être intégrée dans l'ensemble des processus de décision stratégique, de conception des produits et de déploiement des systèmes d'information. L'intelligence réglementaire constitue le troisième principe, désignant le suivi systématique des évolutions réglementaires dans toutes les juridictions pertinentes comme une fonction stratégique à part entière, comparable à l'intelligence économique ou à la veille concurrentielle. L'engagement proactif, enfin, renvoie à la participation active aux processus consultatifs qui précèdent l'adoption des textes réglementaires, en contribuant à façonner des normes compatibles avec les modèles opérationnels.

LES QUATRE PILIERS DE LA CONFORMITÉ STRATÉGIQUE

La prospective réglementaire vise à anticiper les obligations futures avec un avantage de dix-huit à vingt-quatre mois sur l'entrée en vigueur des textes, afin d'adapter les systèmes et les processus dans des délais raisonnables sans subir les coûts de mise en conformité d'urgence.

L'intégration systémique suppose d'inscrire la conformité numérique dans l'ensemble des processus de décision stratégique, de conception des produits et de déploiement des systèmes d'information, et non de la déléguer à une équipe juridique spécialisée opérant en silo.

L'intelligence réglementaire constitue une fonction stratégique à part entière, comparable à la veille

concurrentielle, couvrant l'ensemble des juridictions pertinentes pour l'activité de l'organisation.

L'engagement proactif dans les consultations publiques précédant l'adoption des textes réglementaires permet de façonner des normes compatibles avec les réalités opérationnelles et de positionner la conformité anticipée comme un avantage compétitif.

4.2 La souveraineté numérique comme avantage compétitif

Il serait erroné de réduire les enjeux de souveraineté numérique à une contrainte réglementaire supplémentaire pesant sur les marges de manœuvre des organisations. Pour les acteurs capables de les appréhender dans toute leur complexité, ils constituent au contraire une source d'avantages compétitifs structurels considérables. Les organisations qui parviennent à construire et à démontrer de manière crédible une maîtrise souveraine de leurs données et de leurs systèmes d'information bénéficient d'un avantage de confiance croissant auprès de clients, partenaires et parties prenantes de plus en plus sensibilisés aux risques numériques.

Dans les marchés publics européens, dont la valeur annuelle dépasse 2 000 milliards d'euros selon les données de la Commission européenne, les critères de souveraineté numérique et de conformité réglementaire sont devenus des facteurs de sélection explicites pour de nombreux types de marchés impliquant le traitement de données sensibles. Les opérateurs qui anticipent ces exigences et construisent leurs offres en intégrant nativement les impératifs de souveraineté numérique se positionnent favorablement sur un segment de marché dont la croissance est assurée pour la prochaine décennie.

4.3 Le cas spécifique des institutions publiques

Les institutions publiques occupent une position particulièrement complexe et particulièrement responsabilisante dans le paysage de la souveraineté numérique. Complexe, parce qu'elles sont simultanément régulateurs des pratiques numériques d'autres acteurs, utilisateurs massifs de technologies et de services numériques souvent fournis par des acteurs privés dont la souveraineté n'est pas garantie, et garants des droits fondamentaux de leurs citoyens face aux risques numériques. Responsabilisante, parce que leur capacité à incarner dans leurs propres pratiques numériques les exigences de souveraineté qu'elles imposent aux acteurs privés conditionne la crédibilité de leur action régulatrice et la confiance des citoyens dans les institutions numériques de l'État.

Le défi de la souveraineté numérique pour les institutions publiques se décline en plusieurs problématiques concrètes dont deux méritent une attention particulière. La question des achats de solutions numériques est sans doute la plus immédiate : dans quelle mesure les institutions publiques peuvent-elles continuer à recourir aux grands services

cloud américains pour leurs applications sensibles, à l'heure où le CLOUD Act américain permet aux autorités judiciaires des États-Unis d'exiger l'accès aux données stockées par ces fournisseurs, y compris lorsque celles-ci sont hébergées en Europe ? La question du déploiement des agents conversationnels et des systèmes d'intelligence artificielle dans les administrations publiques est également d'une acuité croissante : comment concilier les gains d'efficacité offerts par les grands modèles de langage avec les exigences de souveraineté, de transparence et de responsabilité qui caractérisent l'action publique ?

V. Analyse prospective : trois scénarios à l'horizon 2030

L'analyse prospective des dynamiques de souveraineté numérique à l'horizon 2030 conduit à distinguer trois scénarios contrastés dont la probabilité relative dépend d'un ensemble de variables-clés que nous identifions ci-après.

Le premier scénario, désigné comme la fragmentation contrôlée, est le scénario de continuation des tendances actuelles. Il se caractérise par la consolidation des trois grands blocs technologiques, européen, américain et sino-asiatique, avec des passerelles de plus en plus restreintes entre eux, une prolifération continue des régimes réglementaires nationaux et une gestion au cas par cas des tensions entre les impératifs de compétitivité économique et les exigences de souveraineté. Dans ce scénario, les coûts de conformité continuent de croître pour les opérateurs multilatéraux, les inégalités numériques entre pays développés et pays en développement se creusent, et l'innovation numérique se concentre progressivement dans les espaces nationaux ou régionaux au détriment de la dynamique collaborative mondiale qui avait caractérisé l'internet de ses origines.

Le deuxième scénario, désigné comme la convergence normative partielle, suppose une reprise du dialogue multilatéral sur la gouvernance numérique mondiale, portée par la prise de conscience des coûts systémiques de la fragmentation. Il se caractérise par l'émergence d'un corpus de standards minimaux partagés dans des domaines ciblés, notamment la protection des données personnelles transnationales, la gouvernance des intelligences artificielles à usage général et la cybersécurité des infrastructures critiques, sans pour autant aboutir à une harmonisation complète des régimes réglementaires. Ce scénario, le plus favorable à la fois pour la prospérité économique mondiale et pour les droits fondamentaux, est également le plus exigeant sur le plan de la coopération internationale.

Le troisième scénario, désigné comme la souveraineté fracturée, est le scénario de rupture. Il suppose une détérioration significative des relations entre les grandes puissances technologiques, conduisant à une déconnexion partielle ou totale entre des espaces numériques incompatibles. Dans ce scénario, la technologie n'est plus un bien mondial partiellement libre mais un attribut de souveraineté nationale ou de bloc strictement

contrôlé, avec des coûts économiques considérables pour l'ensemble des acteurs et des risques systémiques élevés pour la stabilité mondiale.

SYNTHÈSE PROSPECTIVE — VARIABLES DÉTERMINANTES À L'HORIZON 2030

L'évolution vers l'un ou l'autre des trois scénarios dépend principalement de cinq variables-clés : l'état des relations diplomatiques sino-américaines et leur trajectoire dans le domaine technologique ; la capacité de l'Union européenne à construire une autonomie technologique réelle dans les secteurs critiques, au-delà de la seule puissance réglementaire ; le positionnement stratégique des grandes puissances émergentes, notamment l'Inde, le Brésil et l'Indonésie, dont le choix d'alignement sera déterminant pour l'équilibre global ; l'évolution de la gouvernance de l'intelligence artificielle, dont les standards définissent des règles du jeu pour plusieurs décennies ; et la capacité du multilatéralisme numérique à produire des accords contraignants dans des délais compatibles avec la vitesse des transformations technologiques.

VI. Recommandations stratégiques

À la lumière de l'analyse développée dans cette note, l'IEGSI formule douze recommandations stratégiques opérationnelles à l'attention des institutions publiques, des régulateurs nationaux et internationaux, et des opérateurs économiques. Ces recommandations sont organisées selon les deux catégories d'acteurs auxquelles elles s'adressent prioritairement, tout en reconnaissant que nombre d'entre elles présentent une pertinence transversale.

Pour les institutions publiques et les régulateurs

Recommandation 1

Élaborer une stratégie nationale de souveraineté numérique intégrée articulant les dimensions réglementaire, industrielle et diplomatique, avec des indicateurs de suivi mesurables, des responsabilités institutionnelles clairement désignées et des mécanismes de coordination inter-ministérielle dédiés à la transversalité des enjeux numériques.

Recommandation 2

Investir massivement dans les compétences numériques souveraines au sein des administrations publiques, en combinant formations internes, recrutements spécialisés et partenariats avec les établissements d'enseignement supérieur et les centres de recherche dans les domaines de la cybersécurité, de la gouvernance des données et de l'intelligence artificielle.

Recommandation 3

Réviser systématiquement les politiques d'achats publics numériques pour y intégrer des critères explicites et contraignants de souveraineté, de conformité réglementaire et de réversibilité

technologique, en particulier pour les applications traitant des données sensibles ou jouant un rôle dans les décisions affectant les droits des administrés.

RECOMMANDATION 4

Renforcer la participation aux instances de gouvernance numérique mondiale en y déployant des équipes qualifiées capables de peser substantiellement sur la définition des normes et des standards numériques internationaux, et de résister aux tentatives d'appropriation de ces espaces normatifs par des acteurs poursuivant des objectifs incompatibles avec les valeurs démocratiques.

Pour les opérateurs économiques

RECOMMANDATION 5

Conduire un audit complet de souveraineté numérique permettant d'identifier les dépendances technologiques critiques, les flux de données transfrontaliers à risque et les expositions réglementaires multi-juridictionnelles, afin d'établir une cartographie précise des vulnérabilités stratégiques en matière de gouvernance numérique.

RECOMMANDATION 6

Développer une architecture de gouvernance des données fondée sur le principe de souveraineté par conception, extension du privacy by design à l'ensemble des dimensions de la souveraineté numérique, intégrant nativement les exigences réglementaires dans la conception des systèmes d'information plutôt que de les y adjoindre après coup à grands frais.

RECOMMANDATION 7

Construire une veille réglementaire internationale systématique couvrant l'ensemble des juridictions pertinentes pour l'activité de l'organisation, dotée des ressources humaines et technologiques nécessaires pour anticiper les évolutions normatives avec une avance minimale de douze à dix-huit mois.

RECOMMANDATION 8

Développer des stratégies de négociation contractuelle avec les grands fournisseurs de technologies numériques intégrant explicitement des clauses de souveraineté relatives à la localisation des données, aux droits d'audit, aux garanties d'interopérabilité, aux conditions de réversibilité et aux limitations d'usage extraterritorial.

RECOMMANDATION 9

Investir dans des solutions de cloud souverain et de technologies numériques européennes ou nationales pour les applications les plus sensibles, en traitant les surcoûts éventuels comme un investissement stratégique dans la résilience et l'indépendance opérationnelle à long terme, et non comme une simple dépense de conformité réglementaire.

RECOMMANDATION 10

Former et sensibiliser l'ensemble des collaborateurs aux enjeux de souveraineté numérique et aux comportements individuels qui contribuent à la protection ou à la vulnérabilité des actifs numériques de l'organisation, et non pas seulement les équipes techniques et juridiques directement concernées.

RECOMMANDATION 11

Participer activement aux travaux des organismes de normalisation et aux consultations publiques précédant l'adoption des textes réglementaires, pour faire valoir les contraintes opérationnelles des acteurs économiques et contribuer à façonner des normes efficaces et proportionnées aux réalités du terrain.

RECOMMANDATION 12

Engager un dialogue stratégique structuré avec les partenaires, fournisseurs et clients sur les enjeux de souveraineté numérique, pour construire des écosystèmes de confiance partagée qui renforcent collectivement la résilience numérique de l'ensemble des acteurs de la chaîne de valeur.

CONCLUSION

La souveraineté numérique n'est pas une mode passagère ni un concept idéologique sans prise sur les réalités opérationnelles des institutions et des entreprises. Elle est l'expression d'une transformation structurelle profonde du système international, dans lequel la maîtrise des données, des infrastructures et des standards numériques est devenue un attribut fondamental de la puissance et de l'autonomie stratégique, comparable en importance aux ressources énergétiques ou aux capacités militaires qui ont structuré les équilibres de puissance des siècles précédents.

Les acteurs, institutions publiques comme opérateurs économiques, qui auront su appréhender cette transformation dans sa profondeur, construire des stratégies cohérentes pour y faire face et investir suffisamment tôt dans les capacités de gouvernance numérique souveraine seront les mieux positionnés pour prospérer dans le monde multipolaire numérique qui se construit. Ceux qui se contenteront d'une conformité réactive aux obligations réglementaires immédiates, sans vision de long terme sur les enjeux de souveraineté, prennent le risque de se retrouver structurellement désavantagés dans une compétition où les règles du jeu continuent d'évoluer rapidement.

L'IEGSI continuera de suivre et d'analyser l'évolution des dynamiques de souveraineté numérique mondiale, et invite l'ensemble de ses partenaires institutionnels et économiques à contribuer à l'enrichissement collectif de la réflexion stratégique sur ces enjeux qui façonneront le monde des prochaines décennies.

IEGSI — Institut Européen de Gouvernance et de Stratégie Internationale

RIGST — Note Stratégique N° 001 · Juin 2026 · Diffusion publique

www.iegsi.eu · revue@iegsi.eu · © 2026 IEGSI

RÉFÉRENCES BIBLIOGRAPHIQUES

Les références suivantes respectent le style de citation APA 7e édition.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739.

Couture, S., & Toupin, S. (2019). What does the concept of sovereignty mean in digital, network and technological sovereignty? New Media & Society, 21(10), 2305-2322.

De Streel, A., & Renda, A. (2020). Why and how to fix the digital single market. CEPS Special Report.

Drezner, D. W. (2019). The Global Governance of the Internet: Bringing the State Back In. Political Science Quarterly, 119(3), 477-498.

European Commission. (2022). European Declaration on Digital Rights and Principles for the Digital Decade. COM(2022) 28 final.

European Parliament & Council. (2022). Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act). Official Journal of the European Union.

European Parliament & Council. (2022). Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act). Official Journal of the European Union.

European Parliament & Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369-378.

Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). Digital Citizenship in a Datafied Society. Polity Press.

IAPP. (2026). Global Privacy Law and DPA Directory. International Association of Privacy Professionals.

Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.

Mueller, M. L. (2017). Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. Polity Press.

OCDE. (2022). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Repnikova, M. (2022). Chinese Soft Power. Cambridge University Press.

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI & Society, 36(1), 59-77.

Rugge, F. (Ed.). (2018). Confronting an Axis of Cyber? China, Iran, Russia, North Korea and the New Cyber-threat Landscape. ISPI.

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. Third World Quarterly, 39(5), 821-837.

Scott, M., & Cerulus, L. (2018). Europe's new data protection rules export privacy standards worldwide. POLITICO.

UNCTAD. (2024). Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future. United Nations.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.