# Maîtriser nos dépendances numériques

## Vers une autonomie numérique choisie et gouvernée

**MARS 2026**

IN CYBER FORUM EUROPE

*en partenariat avec le*

CESIN

# Sommaire

# Dépendances : la face opérationnelle de la souveraineté numérique



**Guillaume TISSIER**
**Directeur général du Forum INCYBER - Europe**

En 2013, la 5e édition du Forum INCYBER portait un titre qui, à l'époque, pouvait sembler presque excessif : « Le cyberespace, enjeu de souveraineté et de sécurité ». Nous étions alors relativement seuls à parler de souveraineté numérique. La mondialisation paraissait encore fluide, presque irréversible. La Russie de Vladimir Poutine commandait à la France des BPC. L'universalisme américain n'était ni véritablement questionné de l'intérieur, ni contesté de l'extérieur. L'espace numérique était perçu comme un champ technique – rarement comme un champ stratégique.

Pourtant, les signaux faibles existaient déjà. Nous pressentions que souveraineté et sécurité formaient un continuum, et que le numérique en deviendrait l'un des principaux terrains de friction. L'histoire nous a depuis rattrapés. 13 ans plus tard, le mot souveraineté est partout. Il structure les discours publics, irrigue les politiques industrielles, nourrit les stratégies nationales et européennes. Et pourtant, cette omniprésence est trompeuse.

Car le débat sur la souveraineté numérique reste trop souvent abstrait, incantatoire, ou instrumentalisé à des fins politiques. On parle de valeurs, rarement de réalités. De principes, plus que de capacités. D'observatoires davantage que de programmes d'action. La souveraineté est convoquée comme un horizon stratégique, rarement interrogée comme une contrainte opérationnelle. Elle devient un mot-valise, un label rassurant, parfois un slogan, mais trop rarement un objet de pilotage concret.

C'est précisément pour cette raison que nous avons fait le choix de parler de dépendances. Car derrière les grands récits sur la souveraineté se cache sa réalité la plus concrète, la plus opérationnelle – et souvent la plus inconfortable : celle de nos dépendances technologiques et numériques.

Nous avons également fait ce choix parce que les dépendances se situent à l'intersection du continuum sécurité–souveraineté, là où ces deux notions convergent pour produire de la résilience, sans pour autant se confondre. Les solutions que nous utilisons peuvent être sécurisées et souveraines, sécurisées mais non souveraines, souveraines mais fragiles – ou parfois ni l'un ni l'autre.

C'est aussi à cette même intersection que les dépendances peuvent avoir un impact direct sur la disponibilité, le D du triptyque DICT, trop souvent relégué derrière la confidentialité et l'intégrité, alors qu'il conditionne pourtant l'ensemble du système.

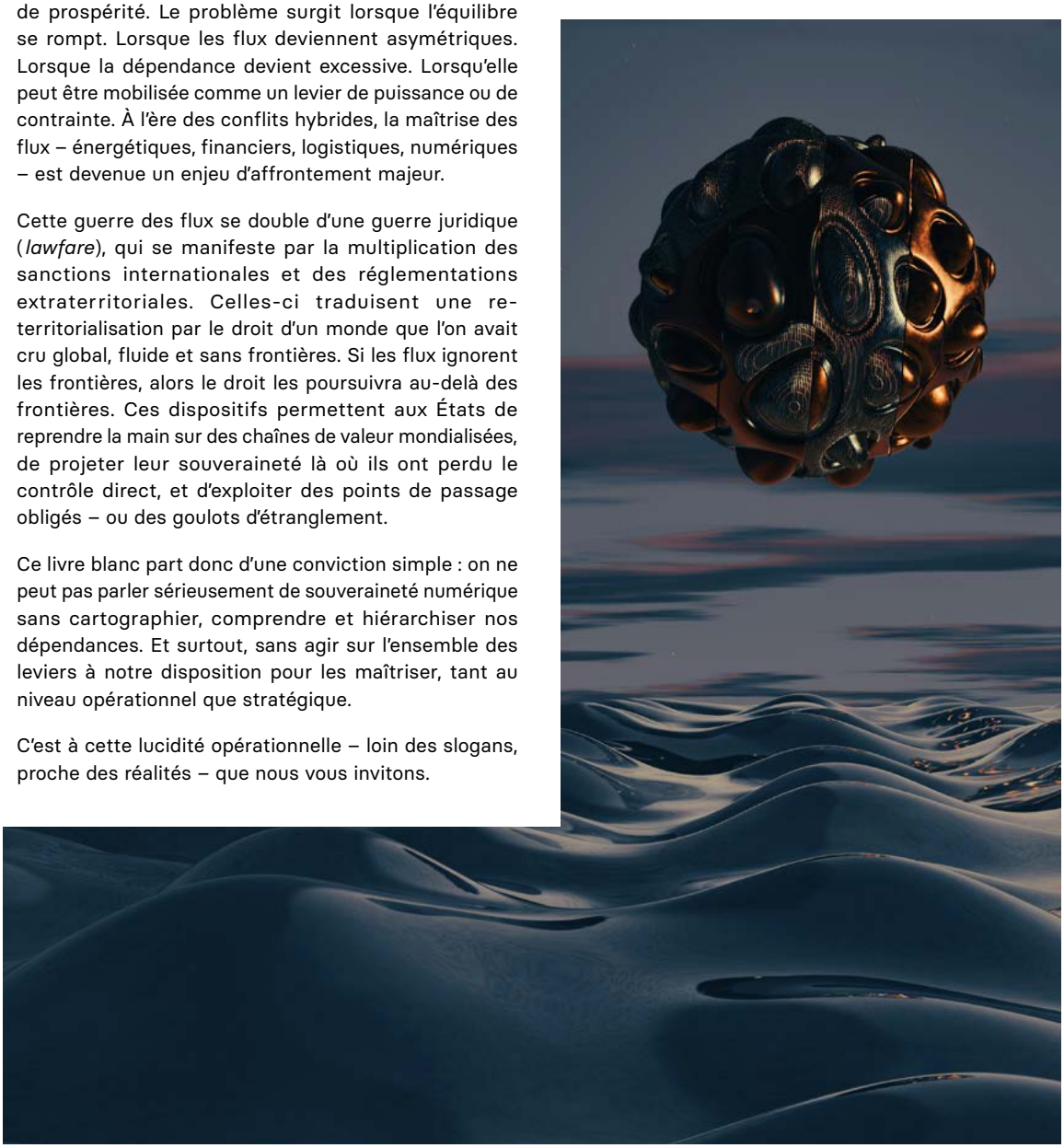
Les dépendances constituent ainsi la face la plus tangible de notre non-souveraineté – ou, plus exactement, de notre souveraineté nécessairement imparfaite dans une économie qui demeure largement globalisée, malgré les soubresauts de la mondialisation et la fragmentation géopolitique à l'œuvre.

Soyons clairs : la dépendance n'est pas en soi un problème. L'interdépendance – la dépendance mutuelle – est même un moteur de paix, selon le doux commerce cher à Montesquieu, en même temps qu'un puissant facteur de prospérité. Le problème surgit lorsque l'équilibre se rompt. Lorsque les flux deviennent asymétriques. Lorsque la dépendance devient excessive. Lorsqu'elle peut être mobilisée comme un levier de puissance ou de contrainte. À l'ère des conflits hybrides, la maîtrise des flux – énergétiques, financiers, logistiques, numériques – est devenue un enjeu d'affrontement majeur.

Cette guerre des flux se double d'une guerre juridique (*lawfare*), qui se manifeste par la multiplication des sanctions internationales et des réglementations extraterritoriales. Celles-ci traduisent une re-territorialisation par le droit d'un monde que l'on avait cru global, fluide et sans frontières. Si les flux ignorent les frontières, alors le droit les poursuivra au-delà des frontières. Ces dispositifs permettent aux États de reprendre la main sur des chaînes de valeur mondialisées, de projeter leur souveraineté là où ils ont perdu le contrôle direct, et d'exploiter des points de passage obligés – ou des goulots d'étranglement.

Ce livre blanc part donc d'une conviction simple : on ne peut pas parler sérieusement de souveraineté numérique sans cartographier, comprendre et hiérarchiser nos dépendances. Et surtout, sans agir sur l'ensemble des leviers à notre disposition pour les maîtriser, tant au niveau opérationnel que stratégique.

C'est à cette lucidité opérationnelle – loin des slogans, proche des réalités – que nous vous invitons.



# Préface du CESIN

**Alain BOUILLÉ**
**Délégué Général du CESIN**

Les questions de souveraineté numérique ou d'autonomie stratégique ont longtemps été cantonnées aux seuls aspects juridiques incarnés par les nombreuses lois dites extraterritoriales étrangères dont l'objectif premier était souvent de traiter des questions de sécurité intérieure des pays auteurs de ces textes dont les États-Unis restent l'acteur majoritaire compte-tenu de son hégémonie en Europe. Ces textes, souvent antérieurs aux offres numériques actuelles, sont devenus au fil des ans de véritables permis d'espionner dont beaucoup d'entreprises et de dirigeants ont été la cible par le passé et le sont encore aujourd'hui. Cette première prise de conscience des questions de souveraineté a été plus récemment exacerbée par les sujets de continuité dans la délivrance des services numériques proposés par des puissances étrangères. Ce risque depuis longtemps identifié dans les cartographies des risques numériques des entreprises les plus matures, a été avéré à plusieurs reprises depuis quelques années. Que ça soit au moment du Covid-19 où Microsoft sous injonction gouvernementale (déjà signée par Trump à l'époque !) avait diminué le niveau de service de certains pays européens afin de satisfaire à la fameuse règle de « l'*America first* » où lors d'incident retentissant comme celui de la malheureuse mise à jour de Crowstrike ayant mis à genoux des hôpitaux, des aéroports et autres services stratégiques juste parce que cette opération avait affecté le cœur même de l'OS de Microsoft.

À cela est venu se greffer depuis Trump2 les menaces de coupure de service pouvant peser sur un pays, une entreprise voire un simple individu en cas de désaccord portant sur des questions géopolitiques ou autres.

Du coup ces questions de dépendance ont dépassé les cercles des spécialistes pour éclater au grand jour et enfin être pris au sérieux par le plus grand nombre.

Le baromètre 2026 du CESIN reflète bien cette prise de conscience :

À la question « Dans un contexte géopolitique en tension, comment jugez-vous l'évolution de la menace d'origine étatique sur votre entreprise ? » 53% des répondants juge cette menace en augmentation.

En ce qui concerne plus précisément le sujet de souveraineté, près de 2 entreprises sur 3 se sentent concernées par les enjeux de souveraineté et de *Cloud* de confiance, un constat en augmentation de 11 points depuis l'an dernier.

Cela démontre que ces questions font désormais parties de l'agenda de beaucoup de RSSI et que les risques systémiques induits par notre extrême dépendance aux solutions étrangères doivent être désormais à l'agenda des COMEX.

Ce livre blanc permet de clarifier les différents aspects d'un sujet qui au premier abord peut paraître comme une montagne infranchissable. C'est malheureusement souvent au pied du mur que l'on réagit face à des défis paraissant insurmontables. Les sujets sont posés, les solutions proposées alors comme dit l'adage : quand on veut, on peut !

# Préambule

**Eric SINGER**
**CISO, membre du CESIN**

Pour la 18ème édition du Forum INCYBER 2026, le thème retenu est « Maîtriser nos dépendances numériques ». Ce choix s'inscrit dans un contexte marqué par l'accélération de la transformation numérique, la concentration des acteurs technologiques, la montée des tensions géopolitiques et l'émergence de nouvelles formes de vulnérabilités systémiques. Il traduit une volonté claire : dépasser une lecture exclusivement technique de la cybersécurité pour s'interroger sur les dépendances structurelles qui conditionnent désormais la résilience, la capacité de décision et la souveraineté des organisations comme des États.

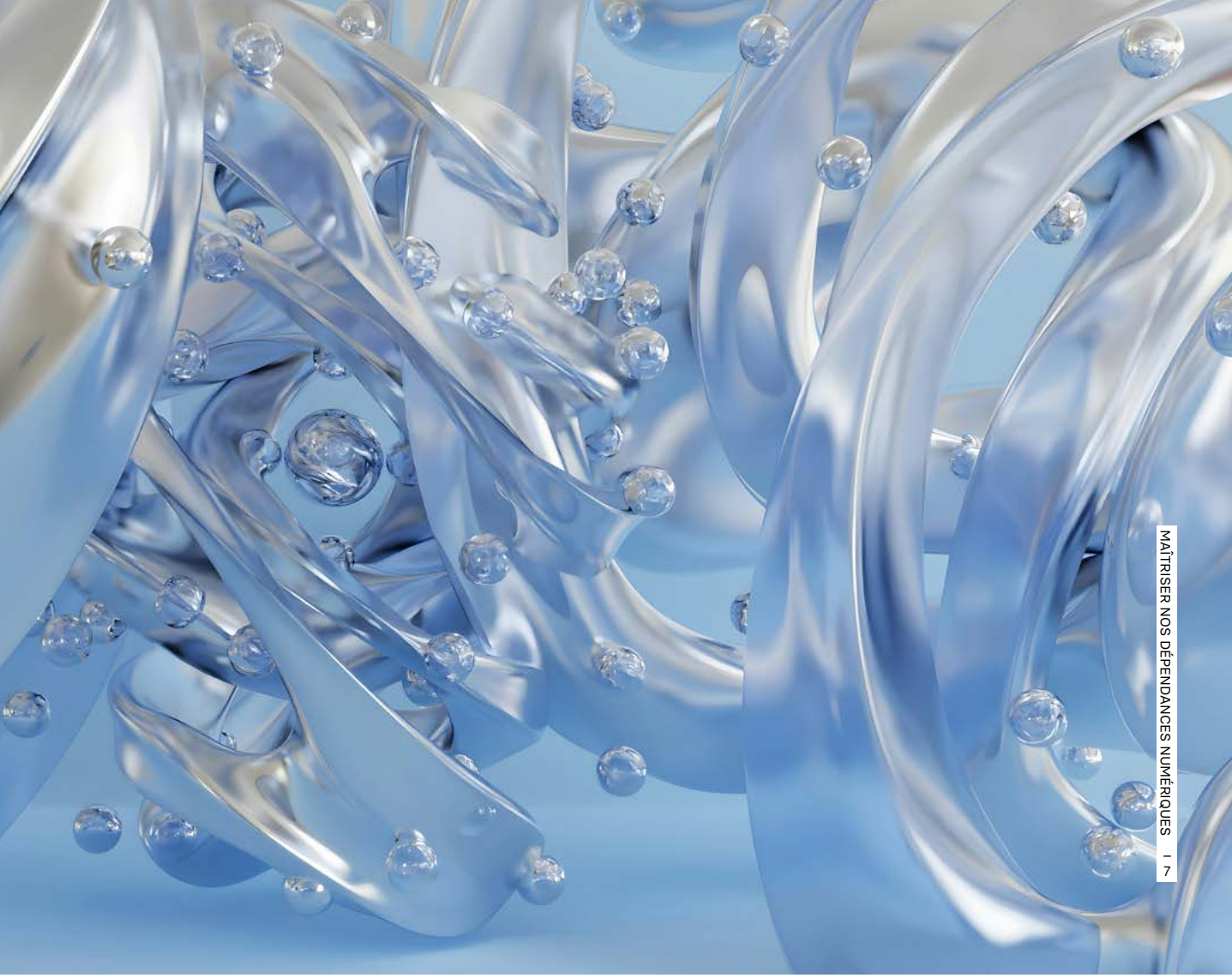
Représentant les responsables francophones de la cybersécurité, le CESIN s'est naturellement associé au Forum INCYBER pour la réalisation de ce livre blanc intitulé Maîtriser nos dépendances numériques. Cette initiative vise à proposer une lecture pragmatique, opérationnelle et ancrée dans le réel de la dépendance numérique, en s'appuyant sur les retours d'expérience concrets de RSSI et de responsables sécurité confrontés quotidiennement à ces enjeux dans leurs organisations.

Un sondage mené auprès des membres du CESIN, ayant recueilli près de 150 réponses, est venu nourrir cette réflexion. Il met en lumière les enjeux majeurs, les difficultés rencontrées, mais aussi les leviers d'action identifiés face aux dépendances numériques. Cette enquête confirme une prise de conscience croissante : la dépendance ne se limite pas aux technologies elles-mêmes, mais concerne tout autant les architectures, les fournisseurs, les compétences, les cadres juridiques et les choix stratégiques de long terme.

Ce livre blanc a été particulièrement structuré par l'implication déterminante de Guillaume Tissier, Alain Bouillé et Fabrice Bru. Leurs apports ont joué un rôle central dans la définition de l'orientation, de la cohérence et de la profondeur de l'analyse proposée. Leur engagement a permis de relier les problématiques très opérationnelles des RSSI aux enjeux plus larges de gouvernance, de souveraineté et de résilience numérique.

Les travaux ont également bénéficié d'éclairages stratégiques essentiels apportés par Arno Pons, co-fondateur du *think-do-tank Digital New Deal.*

En complément de cette étude et de ces contributions structurantes, de nombreux membres, partenaires et sponsors du CESIN, ainsi que des experts reconnus de la cybersécurité et du numérique, ont activement participé à l'élaboration de ce livre blanc. La diversité de leurs points de vue, la richesse de leurs retours de terrain et la qualité des échanges ont été déterminantes pour proposer une analyse équilibrée, concrète et directement exploitable.





Je tiens à exprimer toute ma gratitude à l'ensemble de ces contributeurs engagés :

- David BIZEUL (Sekoia)
- Gabriel de BROSSES (Tevarua conseil)
- Julien COULET (Tenacy)
- Eric DOMAGE (PAC Analyst)
- Nicolas FERNANDEZ (Thales)
- Pascal FORTIN (Cybereco Canada)
- Emmanuel GARNIER (Orano)
- Olivier HERSON (Kudelski Security)
- Maxime de JABRUN (Headmind Partners)
- Thierry LELÉGARD (SiPearl)
- Arnaud MARTIN (Caisse des Dépots)
- Frederick MEYER (Auchan)
- Emmanuel ORLANDO (Dassault Systèmes)
- Lucile PHILIBERT-COUPEZ (Essilor Luxitica)
- Orion RAGOZIN (CESIN)
- Franck ROUXEL (Expert Cybersécurité)
- Loïs SAMAIN (Groupe RATP)
- Petra SEVCIKOVA (Ingenico)
- Olivier STASSI (CESIN)
- Eric VAUTIER (Groupe ADP)

Ce livre blanc est structuré en plusieurs chapitres complémentaires. Il propose d'abord un cadrage des dépendances numériques et de leurs impacts, avant de développer des pistes de solutions opérationnelles à l'échelle des organisations, puis des leviers stratégiques au niveau des États et de la société. Cette double lecture, micro et macro, constitue le fil conducteur de l'ouvrage.

Pensé comme un outil accessible et pragmatique, ce livre blanc a vocation à accompagner les RSSI, les dirigeants et les décideurs publics dans leurs réflexions et leurs arbitrages. Il ne propose pas de solutions toutes faites, mais un cadre d'analyse, un vocabulaire commun et des pistes d'action pour transformer une dépendance souvent subie en un objet de gouvernance maîtrisé.

Je vous souhaite une excellente lecture et espère que ce livre blanc saura vous apporter les éléments de compréhension et de réflexion nécessaires pour aborder les dépendances numériques avec lucidité, méthode et ambition.



# Synthèse exécutive

La dépendance numérique est devenue un facteur structurant de la résilience des organisations et des États. Longtemps perçue comme une conséquence naturelle de la transformation numérique, elle s'est installée progressivement au cœur des systèmes d'information, des processus métiers et des chaînes de valeur, jusqu'à constituer une vulnérabilité potentiellement systémique. Elle ne se limite pas à une problématique technologique ou de cybersécurité : elle affecte la continuité d'activité, la protection des données, la capacité de décision, la soutenabilité économique et, plus largement, la souveraineté des organisations et des États.

Ce livre blanc, porté par le CESIN et le Forum INCYBER, propose une lecture structurée et opérationnelle de la dépendance numérique, fondée sur les retours d'expérience de RSSI, un sondage réalisé auprès des membres du CESIN, ainsi que des contributions d'experts issus de la cybersécurité, de la gouvernance et des relations internationales. Il vise à dépasser une approche exclusivement centrée sur l'incident cyber pour analyser les dépendances structurelles qui se construisent dans le temps, souvent de manière implicite, par l'accumulation de choix rationnels.

L'ouvrage définit la dépendance numérique comme la situation dans laquelle une organisation, une collectivité ou un État ne peut plus assurer ses missions essentielles sans recourir à des technologies, des plateformes ou des services sur lesquels il ne dispose ni d'une maîtrise suffisante, ni d'une capacité réaliste d'arbitrage ou de substitution. Il distingue cette notion de l'interdépendance, inhérente à l'économie numérique globale. Le risque n'est pas de dépendre, mais de dépendre sans visibilité, sans hiérarchisation et sans capacité de reprise en main.

Le livre blanc identifie plusieurs formes de dépendances numériques : technologiques (*Cloud*, SaaS, infrastructures réseau, composants matériels), économiques et industrielles (concentration des marchés, captation de valeur), juridiques et contractuelles (exposition à des droits extraterritoriaux, clauses déséquilibrées), géopolitiques, mais aussi liées aux compétences, aux savoir-faire et aux cadres cognitifs induits par les outils et les plateformes. Ces dépendances se combinent et s'amplifient, créant des points de concentration critique et des effets de *blast radius*, où un incident isolé peut produire des impacts transverses à grande échelle.

Les risques associés sont analysés sous plusieurs angles : opérationnels, juridiques, financiers, réputationnels, sociaux et politiques. Le document montre que la dépendance numérique se manifeste moins par des ruptures brutales que par une érosion progressive des marges de manœuvre, une rigidification des architectures, une perte de capacité de négociation et une exposition accrue aux décisions unilatérales de tiers. À l'échelle sociétale, ces dépendances interrogent la résilience des services essentiels, la protection des libertés fondamentales et la capacité des États à exercer pleinement leurs missions régaliennes.

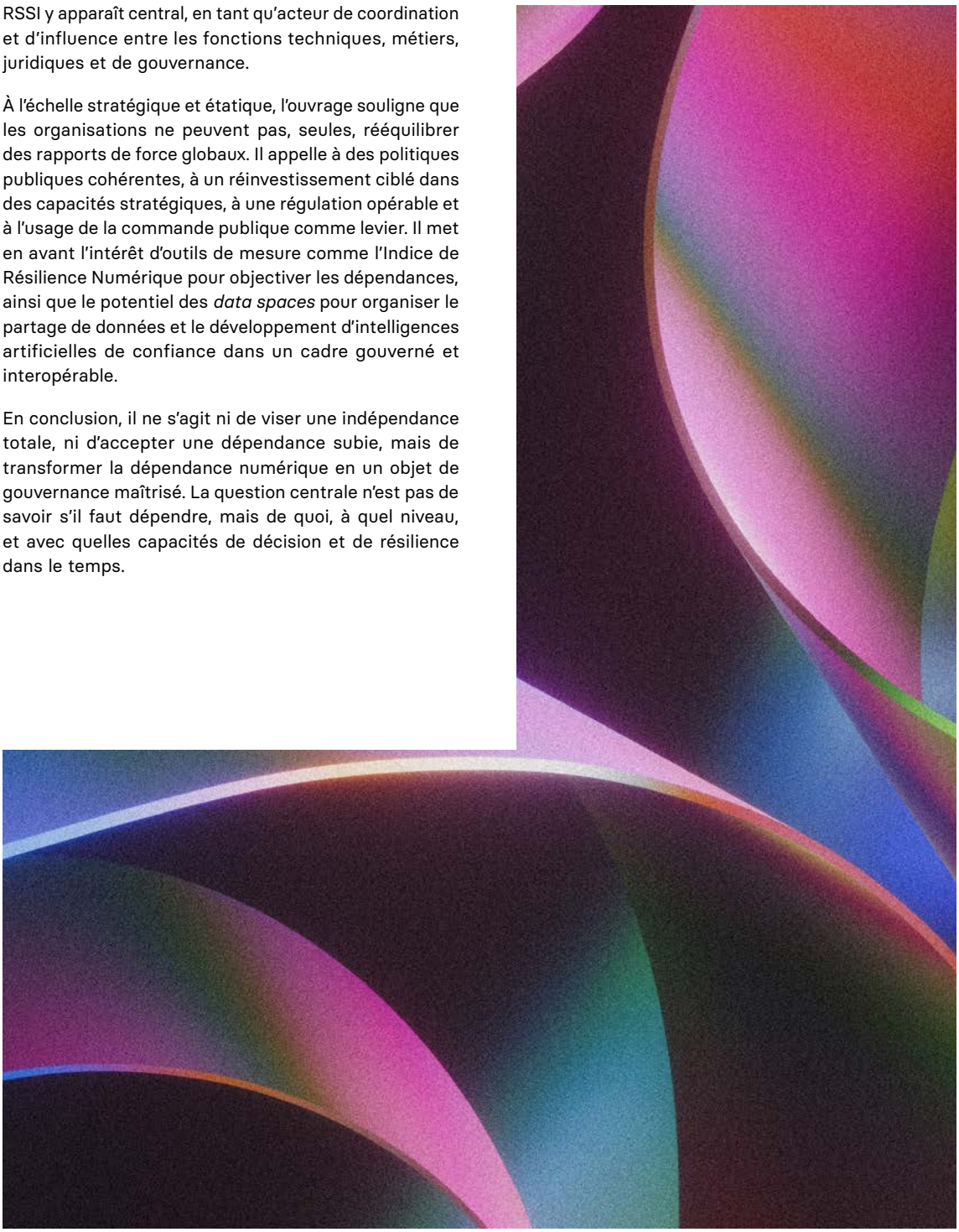
L'intelligence artificielle occupe une position singulière dans cette analyse. Elle apparaît simultanément comme un accélérateur des dépendances existantes – du fait de la concentration des capacités de calcul, de l'opacité des modèles, des biais qu'ils véhiculent et du transfert progressif des savoirs et savoir-faire des organisations – et comme un outil potentiel de reconquête de maîtrise. Les modèles ouverts, par exemple, ainsi que l'analyse automatisée des dépendances à travers des approches telles que les BOM *(Bill of Materials),* permettent d'identifier rapidement des vulnérabilités ou des points de concentration critiques. L'IA contribue également au renforcement des capacités de détection et de réponse aux incidents, à l'automatisation des politiques de

sécurité, aux tests d'intrusion et à d'autres mécanismes avancés de résilience opérationnelle.

Sur le plan opérationnel, le livre blanc propose une démarche pragmatique pour les organisations : nommer la dépendance numérique comme un objet de gouvernance, rendre visibles les chaînes de dépendance à partir des processus métiers critiques, analyser et hiérarchiser les dépendances, intégrer la réversibilité dans les architectures, les contrats et les politiques d'achat, et investir durablement dans les compétences. Le rôle du RSSI y apparaît central, en tant qu'acteur de coordination et d'influence entre les fonctions techniques, métiers, juridiques et de gouvernance.

À l'échelle stratégique et étatique, l'ouvrage souligne que les organisations ne peuvent pas, seules, rééquilibrer des rapports de force globaux. Il appelle à des politiques publiques cohérentes, à un réinvestissement ciblé dans des capacités stratégiques, à une régulation opérable et à l'usage de la commande publique comme levier. Il met en avant l'intérêt d'outils de mesure comme l'Indice de Résilience Numérique pour objectiver les dépendances, ainsi que le potentiel des *data spaces* pour organiser le partage de données et le développement d'intelligences artificielles de confiance dans un cadre gouverné et interopérable.

En conclusion, il ne s'agit ni de viser une indépendance totale, ni d'accepter une dépendance subie, mais de transformer la dépendance numérique en un objet de gouvernance maîtrisé. La question centrale n'est pas de savoir s'il faut dépendre, mais de quoi, à quel niveau, et avec quelles capacités de décision et de résilience dans le temps.



# INTRODUCTION
# Pourquoi parler de « dépendance numérique » aujourd'hui ?

En quelques années, les organisations ont basculé dans un monde où leurs activités, leurs relations avec leurs clients, leurs employés, leurs chaînes de valeur et même une partie de leurs décisions reposent sur des infrastructures, des logiciels, des plateformes et des données numériques liées souvent aux même entreprises, situées dans des pays qui possèdent des lois différentes. Dans un contexte géopolitique en pleine évolution, il questionne l'autonomie de fonctionnement, de résilience métier et de préservation de la confidentialité des données et des échanges.

Pour les RSSI, cette réalité se traduit très concrètement dans **la gestion quotidienne des risques**. Elle se manifeste lorsqu'un incident affectant un *hyperscaler* perturbe simultanément plusieurs activités métiers, révélant une concentration excessive des dépendances. Elle apparaît également à travers des évolutions unilatérales de modèles de licence ou de tarification, susceptibles de déséquilibrer brutalement les budgets. À cela s'ajoute la pression croissante des directions métiers pour adopter rapidement des plateformes d'intelligence artificielle générative hébergées à l'étranger, souvent sans évaluation approfondie des impacts en matière de sécurité des données, de conformité ou de réversibilité. Enfin, ces dépendances se cristallisent dans des contrats où les mécanismes de sortie existent davantage sur le papier que dans la réalité opérationnelle, limitant la capacité de l'organisation à reprendre la main en cas de rupture.

**DÉFINITION**

Un *hyperscaler* est un fournisseur *Cloud* mondial qui met à disposition des capacités de calcul et de stockage massives, avec une scalabilité quasi illimitée. Quelques exemples : Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud.

**RAPPEL DE FAITS**

Les 20 et 29 octobre 2025, des pannes majeures chez Amazon Web Services et Microsoft Azure ont paralysé pendant plusieurs heures des services numériques essentiels : messageries, outils professionnels, télécommunications, transport aérien et services publics.

Dans les deux cas, une erreur technique isolée a suffi à déclencher des effets en cascade à l'échelle mondiale, révélant le haut niveau d'interdépendance du *Cloud*.

Ces incidents rappellent que la concentration de services critiques chez quelques acteurs mondiaux crée une dépendance structurelle, dont les impacts dépassent largement la sphère technologique.[1]

Pour un État ou une collectivité, le constat est tout aussi direct. De nombreuses infrastructures critiques reposent aujourd'hui sur des équipements, des logiciels ou des services *Cloud* exposés à des cadres juridiques extraterritoriaux. L'espace public numérique lui-même dépend largement de quelques grandes plateformes privées, qui structurent les usages, les flux d'information et une part croissante de l'activité économique et sociale. Dans ce contexte, les autorités publiques se heurtent à une difficulté croissante à enquêter, juger, réguler ou même comprendre des systèmes devenus opaques, hautement complexes et intrinsèquement globaux.

**Maîtriser les dépendances numériques ne signifie pas, pour autant, revenir en arrière** ni poursuivre une illusoire autarcie technologique. Il s'agit plutôt de restaurer des marges de manœuvre, de réduire les vulnérabilités excessives et de mieux articuler les choix d'entreprise avec des enjeux collectifs tels que la souveraineté, la résilience et la protection des libertés publiques.

Ce livre blanc s'appuie sur une démarche collective et ancrée dans le terrain. Il est le fruit d'une participation collégiale de professionnels du domaine, d'un corpus d'entretiens menés auprès de RSSI et de responsables sécurité de grands groupes, ainsi que de plusieurs séances de travail réunissant des acteurs directement concernés par ces enjeux.

Il propose une lecture à deux niveaux. **À l'échelle micro**, il s'attache à comprendre comment une organisation peut identifier, piloter et réduire des dépendances susceptibles de fragiliser sa résilience, sa sécurité, sa conformité ou sa capacité d'évolution. **À l'échelle macro**, il analyse la manière dont l'agrégation de ces choix individuels façonne la souveraineté, la compétitivité et les libertés publiques au niveau national et européen.

L'ambition est double : **offrir aux entreprises un cadre d'analyse**, un vocabulaire commun et des pistes d'action pour traiter la dépendance numérique comme un risque à part entière, **et nourrir le débat public d'une vision opérationnelle**, fondée sur les arbitrages concrets auxquels les organisations sont confrontées au quotidien.

1 https://www.thousandeyes.com/blog/aws-outage-analysis-october-20-2025
https://www.thousandeyes.com/blog/microsoft-azure-front-door-outage-analysis-october-29-2025

# 1. Qu'est-ce que la dépendance numérique ?

## 1.1. Une définition de travail

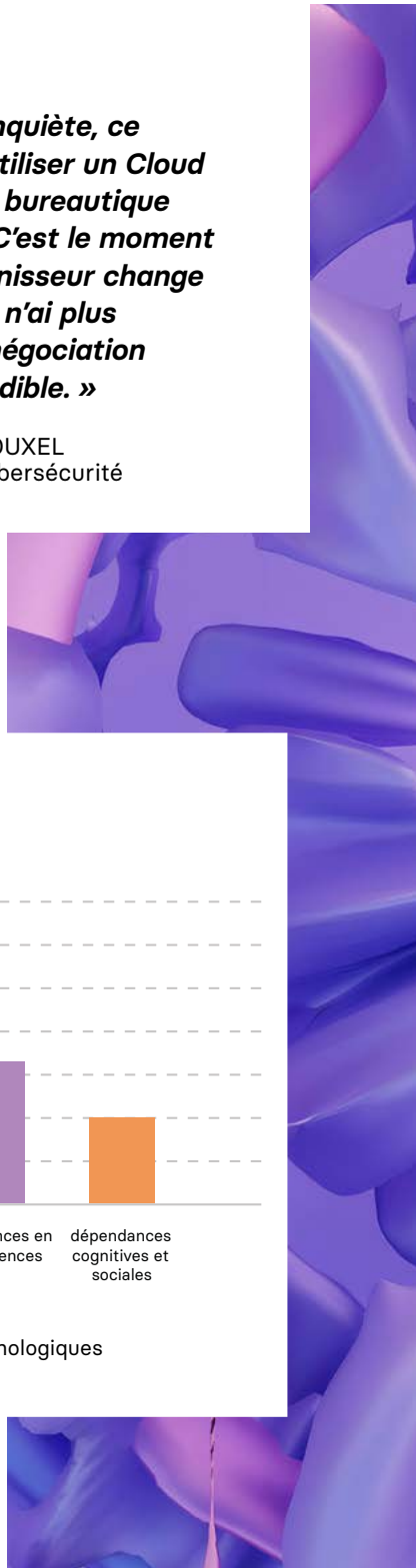
Les échanges au sein du groupe de travail ont permis de converger vers la définition suivante :

**La dépendance numérique est la situation dans laquelle une organisation, une collectivité ou un État ne peut plus assurer ses missions essentielles sans recourir à des technologies, des plateformes ou des services numériques sur lesquels elle n'a ni la maîtrise suffisante, ni la capacité réaliste d'arbitrage ou de substitution.**

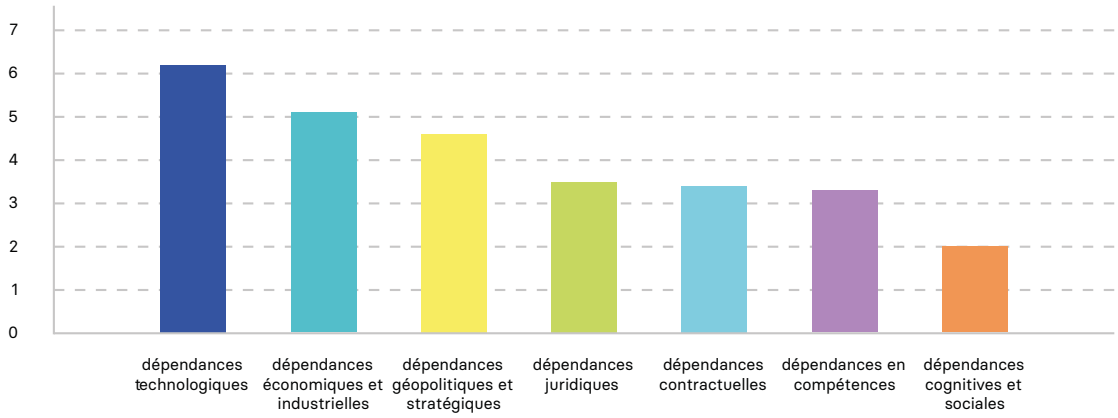
Les stratèges naviguent désormais dans un environnement à forte incertitude : fragmentation géopolitique, révolution IA ultra rapide. La dépendance numérique pose les questions de disponibilité opérationnelle, de maîtrise des coûts futurs, de protection des savoir différentiant de l'organisation voir de conservation de ses savoir-faire.

***« Ce qui m'inquiète, ce n'est pas d'utiliser un Cloud ou une suite bureautique dominante. C'est le moment où, si le fournisseur change les règles, je n'ai plus ni levier de négociation ni plan B crédible. »***

— Franck ROUXEL
Expert Cybersécurité



**Quels sont les principaux types de dépendances liées au numérique ?**
**SONDAGE CESIN (150 RÉPONSES)**




Une hierarchisation des dépendances numériques dominée par les dépendances technologiques

*(1 = moins important, sans ex aequo, 7 = plus important)*

## 1.2. Dépendance, interdépendance et vulnérabilité

Dans un monde numérique globalisé, aucune organisation ne peut prétendre à une autonomie totale. Nous sommes tous **interdépendants** : rares sont les acteurs capables d'exploiter seuls leurs infrastructures, de concevoir leurs propres composants matériels, ou de développer l'ensemble des briques logicielles – qu'il s'agisse d'outils de gestion, de moteurs de recherche ou de modèles d'intelligence artificielle. L'interdépendance est donc un état de fait, inhérent au fonctionnement même de l'économie numérique.

## 1.3. Micro vs macro : deux focales complémentaires

La dépendance numérique peut être analysée selon **2 focales complémentaires : micro et macro,** indissociables l'une de l'autre.

À l'échelle des organisations, pour un RSSI ou un DSI, elle se traduit d'abord par des enjeux très concrets de **résilience opérationnelle, de cybersécurité et de gouvernance des fournisseurs**. Il s'agit d'identifier les points de fragilité : que se passe-t-il si un prestataire critique devient indisponible, modifie ses conditions d'usage, augmente brutalement ses prix ou se retrouve soumis à des décisions juridiques ou géopolitiques ? La dépendance n'est alors plus théorique, elle devient un risque direct pour la continuité d'activité et la maîtrise des données.

À l'échelle de l'État et de la société, la question change de nature mais pas de fond. La dépendance numérique touche à la **souveraineté, à la compétitivité économique et aux libertés fondamentales** : capacité à maintenir des services essentiels, à protéger les données des citoyens, à faire respecter ses propres lois dans l'espace numérique.

Ces deux niveaux sont étroitement liés : Sans organisations lucides et résilientes, il n'existe pas de souveraineté numérique réelle ; sans politiques publiques cohérentes, les efforts des acteurs restent isolés, parfois contradictoires, et insuffisants face aux enjeux collectifs.

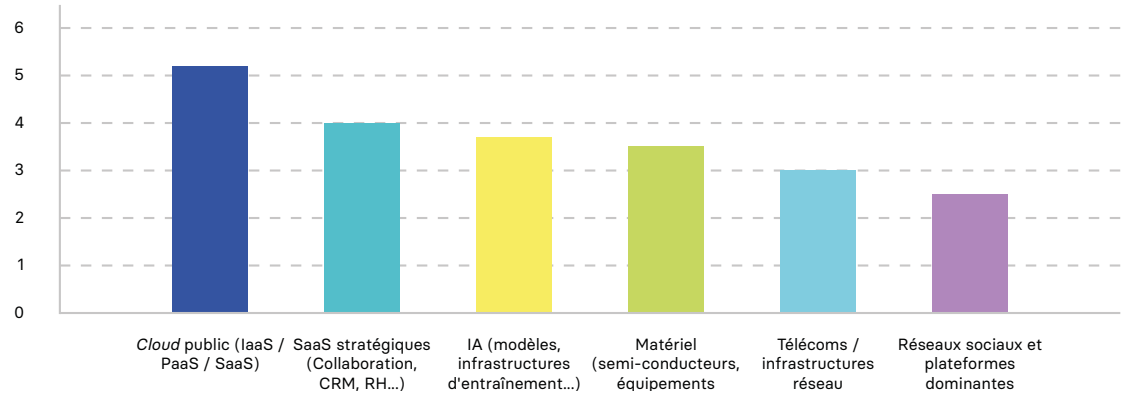
# 2. Les différentes formes de dépendances numériques

Les dépendances numériques prennent des formes multiples, souvent imbriquées et parfois invisibles. Les distinguer permet aux organisations d'identifier leurs fragilités réelles et aux pouvoirs publics de mieux comprendre les dynamiques de concentration à l'œuvre.

***« Quand trop de fonctions critiques reposent sur une même plateforme, le confort d'usage se paie par une perte de liberté de choix. »***

— Arnaud MARTIN
Caisse des Dépôts

**Quelles sont les technologies numériques qui créent le plus de dépendances ?**
**SONDAGE CESIN (150 RÉPONSES)**




**Le *Cloud* public est perçu comme apportant le plus de dépendances numériques.**

*(1 = moins important, 6 = plus important)*

# 2.1. Dépendances technologiques

Ce sont les plus visibles pour les équipes IT et sécurité. On peut ainsi considérer :

## Logiciels systémiques

Systèmes d'exploitation (Windows, iOS, Android), hyperviseurs, suites bureautiques, solutions de cybersécurité. Ces briques de base sont essentielles au fonctionnement de l'ensemble des systèmes d'information. Leur contrôle par un nombre restreint d'acteurs rend les organisations extrêmement dépendantes.

Un défi majeur est la **plateformisation** (Microsoft 365, Google Workspace, Palo Alto Networks PAN OS, etc.) qui concentre des usages multiples au sein d'écosystèmes fermés et accroît mécaniquement la dépendance, y compris en incluant des solutions de cybersécurité.

**PLATEFORMISATION ET CONCENTRATION DES DÉPENDANCES**

La plateformisation des systèmes d'information constitue un facteur de dépendance technologique. Des environnements tels que **Microsoft 365, Google Workspace** ou les plateformes intégrées de **Palo Alto Networks** concentrent, au sein d'écosystèmes fermés, un nombre croissant de fonctions critiques : messagerie, collaboration, gestion des identités, sécurité, supervision et mécanismes de mise à jour.

Cette intégration renforce la cohérence fonctionnelle et la simplicité d'exploitation, mais elle **accroît mécaniquement la dépendance** en réduisant les capacités de dissociation et de substitution des briques technologiques. Lorsque plusieurs fonctions structurantes reposent sur un même acteur, une défaillance technique, une évolution contractuelle ou une contrainte juridique peut avoir un impact transversal sur l'ensemble du système d'information.

L'intégration des fonctions de cybersécurité au cœur de ces plateformes renforce encore cette concentration. La sécurité devient alors elle-même dépendante d'un écosystème unique, limitant la diversification des contrôles et la capacité à remettre en cause certaines décisions techniques. Dans ce contexte, la plateformisation transforme des choix d'outillage en **dépendances structurelles**, qui relèvent des enjeux de résilience et de gouvernance du risque.

***« La dépendance numérique ne se manifeste pas toujours là où on l'imagine. Elle s'installe discrètement dans des briques banales, mutualisées, que le temps et l'usage ont rendues invisibles ».***

— Emmanuel GARNIER
Orano

Cette concentration de fonctions critiques (identité, messagerie, sécurité, mises à jour, collaboration) chez un nombre limité d'acteurs accroît le périmètre d'impact systémique d'un incident. Lorsqu'un composant central devient défaillant ou compromis, l'impact peut se diffuser simultanément à l'ensemble des organisations qui en dépendent.

Plus un système est concentré, mutualisé ou interconnecté, plus ce périmètre d'impact – souvent désigné par le terme anglo-saxon *blast radius* – est étendu.

À la différence de l'effet domino, qui décrit une propagation séquentielle d'un dysfonctionnement, le blast radius renvoie avant tout à l'ampleur structurelle de l'impact liée à la concentration des dépendances.

## *Cloud* et infrastructures

Les grands *Clouds* publics sont devenus le socle de milliers d'applications. Une forte concentration des infrastructures (*hyperscalers*, grands CDN, registres DNS, etc.) crée des points de défaillance uniques à très large impact potentiel. Ils sont aujourd'hui opérés principalement par des acteurs américains (AWS, Microsoft Azure, Google Cloud) ou chinois (Alibaba Cloud, Huawai Cloud, Tencent Cloud). Les acteurs européens ne sont pas exempts de risques : l'incendie de **OVHCloud** en 2021 a montré qu'un incident physique peut provoquer une perte massive de services et de données. Quelle que soit l'origine, la concentration amplifie le *blast radius* et impose des stratégies de résilience et de réversibilité. Ces dépendances sont renforcées par l'essor de l'IA, qui repose sur d'énormes capacités de calcul et de stockage. Une panne ou une défaillance de ces grands offreurs peut rapidement impacter de nombreuses entreprises ou des services en ligne à grande échelle.

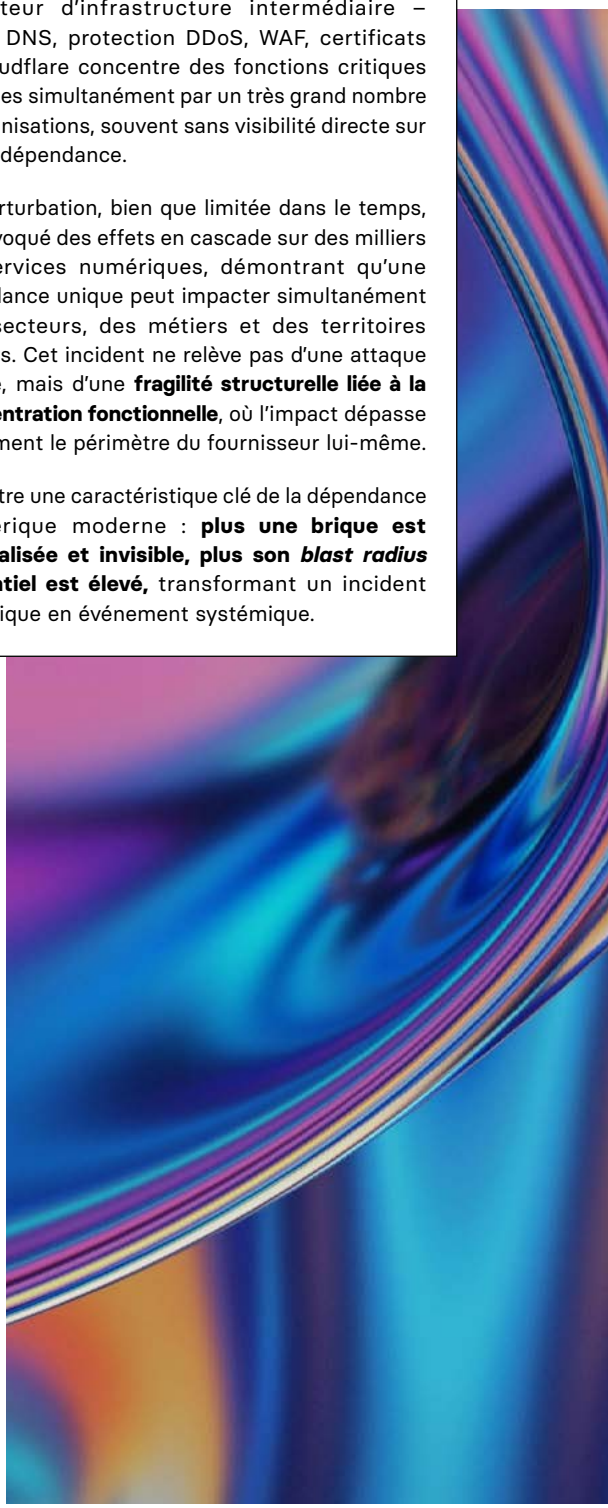
Le ***Shadow IT*** constitue une forme de dépendance numérique particulièrement insidieuse, car souvent invisible dans les cartographies officielles. Difficile à contrôler par la DSI, il est redouté par les RSSI tant il crée des angles morts majeurs en matière de sécurité. Mais au-delà du risque cyber, le *Shadow IT* génère une **dépendance opérationnelle cachée** : outils non contractualisés, services SaaS souscrits individuellement, automatisations maîtrisées par une seule personne. Problème ancien mais persistant, le *Shadow IT* illustre que la dépendance numérique ne se limite pas aux grands fournisseurs stratégiques : elle se niche aussi dans les usages informels, là où l'organisation a perdu la maîtrise sans même en avoir conscience.

**INCIDENT CLOUDFLARE (DÉCEMBRE 2025)**

L'incident survenu chez **Cloudflare** en décembre 2025 a illustré de manière concrète le *blast radius* des dépendances numériques. En tant qu'acteur d'infrastructure intermédiaire – CDN, DNS, protection DDoS, WAF, certificats – Cloudflare concentre des fonctions critiques utilisées simultanément par un très grand nombre d'organisations, souvent sans visibilité directe sur cette dépendance.

La perturbation, bien que limitée dans le temps, a provoqué des effets en cascade sur des milliers de services numériques, démontrant qu'une défaillance unique peut impacter simultanément des secteurs, des métiers et des territoires entiers. Cet incident ne relève pas d'une attaque ciblée, mais d'une **fragilité structurelle liée à la concentration fonctionnelle**, où l'impact dépasse largement le périmètre du fournisseur lui-même.

Il illustre une caractéristique clé de la dépendance numérique moderne : **plus une brique est mutualisée et invisible, plus son *blast radius* potentiel est élevé,** transformant un incident technique en événement systémique.



### Composants matériels critiques

La dépendance mondiale à **Taiwan Semiconductor Manufacturing Company (TSMC)** est un exemple de **dépendance numérique systémique, lié à des composants matériels critiques**. TSMC fabrique aujourd'hui l'essentiel des puces de dernière génération (5 nm, 3 nm et en dessous), indispensables aux smartphones, centres de données, systèmes d'IA, équipements militaires et infrastructures critiques. Des acteurs majeurs comme **Apple, NVIDIA** ou **AMD** dépendent directement de ses capacités industrielles. D'autre part, les États-Unis contrôlent des technologies clés de conception et de mémoire (via Micron), la Corée du Sud concentre une part majeure de la production mondiale de mémoire avec **Samsung Electronics** et **SK Hynix**, tandis que la Chine investit massivement dans les composants, batteries et capacités industrielles.

Cette concentration crée des **dépendances systémiques**, où une tension géopolitique ou industrielle peut avoir un impact mondial immédiat. Par exemple, un conflit dans le détroit de Taïwan, un blocus ou une perturbation industrielle majeure aurait des effets immédiats sur l'économie mondiale, bien au-delà du secteur technologique. La crise des semi-conducteurs de 2020-2022, causée par des tensions logistiques et sanitaires, a déjà montré comment une perturbation limitée pouvait paralyser l'automobile, l'électronique grand public et certaines industries critiques.

Contrairement à un risque cyber classique, cette dépendance combine **monoculture technologique, rareté industrielle et tension géostratégique**, rendant la diversification lente, coûteuse et politiquement sensible.

### Standards techniques et protocoles

Même lorsqu'ils sont formellement ouverts, de nombreux standards sont de facto façonnés par quelques grandes entreprises. Cela leur donne un avantage d'implémentation et la capacité de fixer les « règles du jeu » technique.

Par exemple, le protocole **QUIC**, à l'origine développé par **Google**, a largement façonné **HTTP/3**, donnant à Google un avantage naturel d'implémentation. De même, **Kubernetes**, initié par Google avant d'être confié à la **Cloud Native Computing Foundation**, reste principalement maîtrisé par les grands *hyperscalers*. Ces acteurs fixent ainsi les choix techniques structurants, obligeant l'écosystème à s'aligner pour rester interopérable et compétitif.

Imposer ses propres standards et référentiels comme dans les télécommunications est aussi une façon d'influencer ou de garder une maitrise industrielle.

## 2.2. Dépendances économiques et industrielles

Au-delà des choix purement techniques, **la structure même des marchés numériques** constitue un **facteur déterminant de dépendance**. Les dynamiques économiques à l'œuvre dans le numérique favorisent une concentration des acteurs, des données et des usages autour d'un nombre limité de plateformes mondiales. Moteurs de recherche, réseaux sociaux, places de marché applicatives, services publicitaires ou plateformes d'e-commerce s'imposent comme des infrastructures de fait, difficilement contournables pour les organisations comme pour les citoyens.

Cette concentration est renforcée par des **modèles d'innovation asymétriques.** La capacité à financer, incuber et faire croître rapidement de nouveaux acteurs se **concentre dans quelques écosystèmes géographiques** et financiers (Silicon Valley, Shenzhen, etc.). Les innovations issues de ces écosystèmes s'intègrent souvent dans des chaînes de dépendance existantes, plutôt que de constituer de véritables alternatives. Des start-ups, par exemple, reposent structurellement sur des API, des infrastructures *Cloud* tierces, ce qui fragilise leur durabilité et leur autonomie.

**L'économie de la donnée accentue encore ces phénomènes.** La capacité à collecter, agréger et valoriser de vastes volumes de données utilisateurs ou industrielles crée des effets d'échelle difficiles à reproduire. Ces effets renforcent les positions dominantes et réduisent progressivement l'espace concurrentiel, tout en rendant l'émergence d'alternatives économiquement viable de plus en plus complexe.

**Pour un RSSI,** ces dynamiques sont souvent perçues comme relevant du contexte macroéconomique ou réglementaire, et donc **hors de son périmètre direct.** Pourtant, elles conditionnent la capacité de négociation de l'organisation, la disponibilité d'alternatives en cas de rupture, et la résilience de l'écosystème de fournisseurs. Intégrer cette lecture de marché dans l'analyse des risques permet d'anticiper des dépendances qui ne sont ni techniques ni contractuelles, mais plutôt structurelles.

## 2.3. Dépendances géopolitiques et stratégiques

Le numérique est devenu un **terrain de puissance stratégique**, où technologies et infrastructures servent de leviers diplomatiques, économiques et sécuritaires. Les États exercent cette puissance par l'**extraterritorialité des lois** : aux États-Unis, le *Cloud Act*[2], le *Patriot Act*[3] , le FISA[4] peuvent contraindre un fournisseur à transmettre des données, y compris hébergées hors du territoire américain, souvent sans transparence pour le client concerné.

Cette logique n'est pas spécifique aux États-Unis : la Chine (*Cybersecurity Law, Data Security Law, National Intelligence Law*) ou la Russie (localisation des données, contrôle du Runet) disposent également de cadres juridiques permettant aux autorités d'imposer des contraintes fortes aux fournisseurs numériques, y compris au-delà de leurs frontières.

Les **sanctions et contrôles à l'export, comme la réglementation ITAR[5],** constituent un autre levier : l'interdiction de vendre des composants, logiciels ou services à certaines entreprises ou États peut provoquer des coupures brutales, comme l'ont montré plusieurs restrictions technologiques récentes.

Le numérique est aussi utilisé de manière **offensive** : surveillance de masse, espionnage industriel, campagnes de désinformation ou exploitation des dépendances techniques comme moyens de pression.

Dans ce contexte, la dépendance au *Cloud* crée des risques systémiques variables selon l'origine des fournisseurs : les *Cloud*s américains comme **Amazon Web Services** ou **Microsoft Azure** concentrent des fonctions critiques mais exposent à des dépendances juridiques extraterritoriales, tandis que les *Clouds* chinois, tels que **Alibaba Cloud**, ajoutent un risque géopolitique et réglementaire lié au contrôle étatique.

VUE MICRO : Pour le RSSI, cela se traduit par des risques parfois difficiles à appréhender : un fournisseur stratégique peut se retrouver du jour au lendemain sous le coup de sanctions ou soumis à des demandes légales incompatibles avec le droit européen.

VUE MACRO : Pour l'État, la question est plus frontale : comment protéger ses infrastructures, ses entreprises, ses citoyens, lorsqu'une part significative de l'écosystème

## 2.4. Dépendances juridiques et contractuelles

Les **dépendances juridiques et contractuelles** sont souvent sous-estimées dans les stratégies numériques, alors qu'elles conditionnent directement la capacité réelle de maîtrise des risques.

Le **choix du droit applicable** est central : une majorité de contrats *Cloud* et logiciels critiques sont soumis au droit d'un État étranger, fréquemment américain. Cela peut limiter les recours effectifs d'une organisation européenne et affaiblir certaines protections prévues par le droit de l'Union, notamment en matière de données personnelles.

Cette situation est aggravée par les **conflits de juridictions,** par exemple entre le RGPD et des lois extraterritoriales comme le *Cloud Act*, plaçant les entreprises dans des injonctions contradictoires difficiles à arbitrer.

À cela s'ajoutent des **clauses contractuelles déséquilibrées**, devenues quasi standard : fortes limitations de responsabilité, exclusions étendues, absence de garanties solides de réversibilité, coûts de sortie élevés, ou encore droit unilatéral du fournisseur de modifier les conditions de service.

Dans les contrats de grands acteurs comme **Amazon Web Services** ou **Microsoft Azure**, ces clauses traduisent un rapport de force asymétrique, renforçant une dépendance qui n'est pas seulement technique mais aussi juridique et économique. En cas de crise majeure, elles peuvent restreindre l'accès aux preuves, ralentir la reprise d'activité ou rendre toute action contentieuse illusoire.

VUE MICRO : Pour un RSSI, la dimension contractuelle est déterminante. Les contrats définissent la réalité opérationnelle : accès aux logs, niveaux d'assistance, responsabilités financières, garanties de continuité, délais de reprise et modalités concrètes de restitution des données dans un format exploitable.

VUE MACRO : À l'échelle étatique, ces dépendances contractuelles posent un enjeu de souveraineté. Elles conditionnent la capacité d'un pays à protéger ses données, à assurer la continuité de ses services essentiels et à ne pas subir de décisions juridiques étrangères sur des infrastructures critiques.

2. *Cloud Act : Clarifying Lawful Overseas Use of Data Act*
3. *USA Patriot Act : Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*
4. FISA : *Foreign Intelligence Surveillance Act*
5. ITAR : *International Traffic in Arms Regulations*

**UN CAS EMBLÉMATIQUE DE DÉPENDANCE JURIDICO-POLITIQUE : ÉCOLE POLYTECHNIQUE / MICROSOFT 365 (2025)**

**ACTE 1 – La décision (mars 2025)**

En mars 2025, l'École polytechnique annonce un projet de migration de certains services administratifs et de pilotage pédagogique vers Microsoft 365, afin de rationaliser un écosystème d'outils hétérogènes et largement contournés par les utilisateurs. Les autorités de tutelle rappellent que la solution est considérée comme conforme aux recommandations de l'ANSSI pour des données non sensibles.

**ACTE 2 – Le débat et les interrogations (mars–octobre 2025)**

Le projet suscite un débat juridique, académique et politique plus large. Plusieurs acteurs interrogent la compatibilité du projet avec les orientations nationales en faveur du logiciel libre dans l'enseignement public, ainsi qu'avec les exigences du RGPD et les enjeux liés à l'extraterritorialité du droit américain (notamment le *Cloud Act*). Dans le même temps, d'autres établissements poursuivent des démarches comparables, illustrant la complexité des arbitrages entre performance opérationnelle, conformité juridique, souveraineté numérique et contraintes budgétaires.

**ACTE 3 – La suspension et mise en réflexion (octobre 2025)**

Face à l'intensification du débat et aux incertitudes juridiques soulevées, le projet est suspendu à l'automne 2025 afin de permettre une réévaluation des conditions de déploiement et des alternatives possibles.

Cet épisode met en lumière une évolution majeure : les choix technologiques, notamment dans les secteurs sensibles comme l'éducation, la recherche ou la santé, ne sont plus seulement des décisions techniques ou budgétaires. Ils deviennent des arbitrages juridico-politiques exposés, intégrant des dimensions réglementaires, géopolitiques, symboliques et stratégiques.

# 2.5. Dépendances en matière de compétences et de savoir-faire

Les **dépendances en matière de compétences et de savoir-faire** constituent aujourd'hui un facteur critique de la dépendance numérique, souvent aussi structurant que la dépendance technologique elle-même. Les entretiens menés font apparaître un consensus fort : la **pénurie de talents**, combinée à l'externalisation massive et à la complexité croissante des systèmes, fragilise durablement les organisations. Les compétences rares – cybersécurité avancée, architectures *Cloud* complexes, exploitation d'environnements Kubernetes, ingénierie IAM ou intelligence artificielle – sont très recherchées et difficiles à recruter ou à fidéliser. Cette tension place les organisations dans une situation de dépendance vis-à-vis du marché et de quelques fournisseurs de services spécialisés.

Parallèlement, on observe une **érosion progressive des savoir-faire fondamentaux**. L'adoption généralisée de solutions *as-a-service (SaaS)* réduit la maîtrise interne de fonctions clés comme l'administration système, le réseau, l'exploitation ou le stockage. Lorsque l'infrastructure, la sécurité ou même l'identité sont entièrement opérées par des plateformes *Cloud*, les équipes internes perdent la capacité de comprendre finement les mécanismes sous-jacents, d'auditer les configurations, voire de reconstruire un environnement en cas d'indisponibilité. Cette perte de culture technique affaiblit la capacité de contrôle et de remise en question des choix effectués.

La conséquence principale de cette dépendance en compétences est une **réduction du choix réel**. Même lorsqu'il existe des alternatives techniques ou stratégiques, elles sont écartées faute de compétences pour migrer, opérer, maintenir ou faire évoluer les solutions. La dépendance n'est alors plus seulement subie : elle devient structurelle, limitant durablement l'autonomie et la capacité de décision de l'organisation.

VUE MICRO : Pour un RSSI, la dépendance en compétences est un risque opérationnel direct. Elle limite la capacité à challenger les fournisseurs, à s'assurer du niveau réel de sécurité des architectures, à détecter des dérives de configuration ou à piloter efficacement un incident complexe. Faute de savoir-faire interne, le RSSI devient dépendant des diagnostics et des priorités d'acteurs externes, parfois en situation de conflit d'intérêts. Cette dépendance fragilise la gouvernance de la sécurité, ralentit la prise de décision en crise et réduit la capacité à préparer des scénarios de sortie ou de réversibilité crédibles.

VUE MACRO : À l'échelle de l'État, la perte de compétences et de savoir-faire numériques pose un enjeu de souveraineté majeur. Elle réduit la capacité nationale à concevoir, auditer et opérer des infrastructures critiques, à réguler efficacement les grands acteurs technologiques et à faire émerger des alternatives industrielles crédibles. Une dépendance excessive à des expertises étrangères ou privées affaiblit la résilience collective, limite l'autonomie stratégique et expose les politiques publiques à des choix contraints, dictés moins par l'intérêt général que par la disponibilité des compétences sur le marché mondial.

# 2.6. Dépendances cognitives, sociales et épistémiques

Les **dépendances cognitives, sociales et épistémiques** sont parmi les plus subtiles, mais aussi les plus structurantes de la dépendance numérique. Elles agissent non sur les infrastructures, mais sur **les modes de perception, de raisonnement et de décision**. Les modèles économiques fondés sur la **captation de l'attention** – notifications permanentes, mécanismes de récompense, design persuasif – orientent les comportements individuels et collectifs. Le **filtrage algorithmique** renforce ce phénomène : ce que nous lisons, voyons ou recherchons est de plus en plus médié par des algorithmes opaques, qui priorisent certains contenus, signaux ou alertes au détriment d'autres.

Ces dépendances s'expriment aussi dans les outils professionnels. Un ERP (progiciel de gestion, intégrée – finance, achats, RH, logistique, ...), un outil de GRC (de gestion des risques, politiques et conformité) ou un modèle d'IA ne sont jamais neutres : ils **modélisent le monde**. Ils imposent des catégories, des seuils, des indicateurs et des hiérarchies. Comme l'ont souligné plusieurs RSSI lors des entretiens, choisir un outil revient à adopter une **vision du réel** : la manière de qualifier un incident, ce qui est mesuré ou ignoré dans un KPI, ou la façon dont une alerte est classée comme « critique » ou « mineure ». À force, l'outil ne soutient plus la décision, il la **préstructure**, parfois sans débat explicite.

À l'échelle sociétale, ces dépendances interrogent la **pluralité de l'information** et la formation de l'opinion. Lorsque les cadres de compréhension sont définis par quelques plateformes ou modèles dominants, la capacité à débattre sur des bases factuelles partagées s'érode. Le risque n'est pas seulement la désinformation, mais l'**uniformisation des grilles de lecture** du monde.

VUE MICRO : Pour le RSSI, la dépendance ne réside donc pas seulement dans l'usage d'une solution donnée, mais dans le risque de **confondre le cadre proposé par l'outil avec la réalité du risque**. Lorsque la gouvernance de la sécurité s'aligne trop étroitement sur les modèles, taxonomies et seuils imposés par des solutions, la capacité à détecter des signaux faibles, à challenger les priorités ou à construire une lecture autonome du risque peut s'avérer plus difficile.

VUE MACRO : Pour l'État, elles posent un enjeu démocratique et stratégique majeur : préserver la diversité des cadres cognitifs, la transparence des algorithmes et la capacité collective à comprendre et décider de manière autonome.

# 3. Enjeux sociétaux et impacts sur les libertés fondamentales

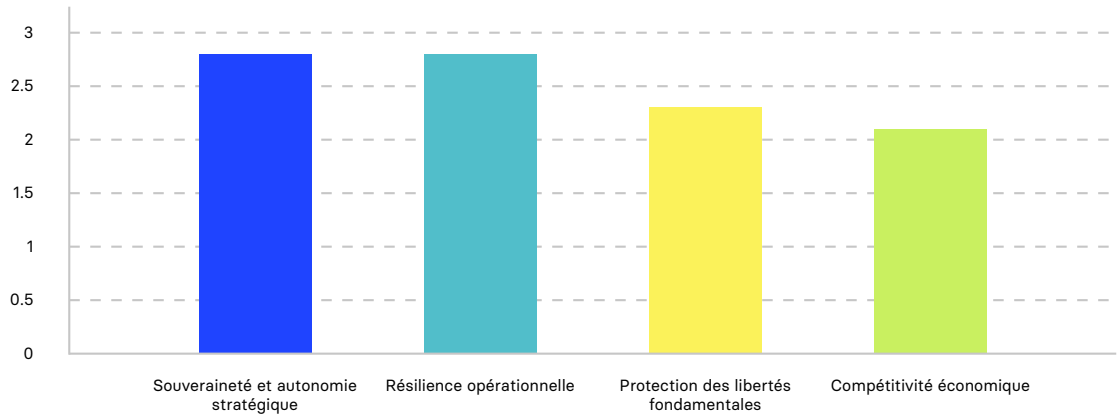
La **dépendance numérique** ne se limite pas à des choix techniques ou économiques : elle façonne en profondeur les **équilibres sociétaux**, les **libertés fondamentales** et la **capacité d'action collective**.

## 3.1. Souveraineté et autonomie stratégique

À l'échelle d'un État ou d'une union d'États, la souveraineté numérique se traduit d'abord par la capacité de **décider, d'agir et d'assurer la continuité** des fonctions régaliennes. Décider signifie pouvoir adopter des lois, des politiques publiques et des réglementations sans se heurter à des dépendances technologiques paralysantes. Agir implique enquêter, juger, réguler et protéger sans dépendre de services ou de données contrôlés par des puissances extérieures. Assurer la continuité suppose que les services essentiels – justice, sécurité, santé, finances publiques – puissent fonctionner même en cas de crise internationale majeure.

Or, lorsque les **systèmes de messagerie, de visioconférence ou de gestion documentaire** des administrations reposent sur des solutions étrangères, lorsque les **flux financiers** d'une économie transitent par quelques plateformes globales, ou lorsque les **services de sécurité et de défense** utilisent des solutions aux chaînes d'approvisionnement opaques, la souveraineté devient conditionnelle. Des décisions prises hors du contrôle démocratique national – qu'elles soient juridiques, commerciales ou géopolitiques – peuvent alors avoir des effets immédiats sur la capacité d'action publique

**Au-delà des aspects techniques, quels sont les principaux enjeux de la maîtrise des dépendances numériques ?**
**SONDAGE CESIN (150 RÉPONSES)**




**La souveraineté et la résilience sont perçues comme les enjeux les plus importants.**

*(1 = moins important, 4 = plus important)*

## 3.2. Résilience des services essentiels

La résilience numérique est devenue un enjeu sociétal majeur. La pandémie de Covid-19, les tensions géopolitiques et les grandes pannes de fournisseurs *Cloud* ont montré à quel point les dépendances numériques peuvent fragiliser la **santé** (hôpitaux, dossiers patients, chaînes logistiques de médicaments), l'**énergie** (SCADA, téléconduite), les **transports**, la **finance** et les **services publics** (portails administratifs, aides sociales, fiscalité). Lorsque des plateformes critiques sont indisponibles, l'impact dépasse largement les pertes financières : il touche directement les citoyens, avec des soins retardés, des aides non versées, des services de sécurité indisponibles.

Une dépendance excessive à un nombre réduit d'acteurs augmente le ***blast radius*** des incidents et réduit la capacité à opérer en mode dégradé.

> ***« Quand des plateformes critiques tombent, ce ne sont pas seulement des systèmes qui peuvent s'arrêter, mais des services essentiels à la population. La résilience numérique se mesure alors en impacts humains et sociaux, bien au-delà des indicateurs techniques. »***
>
> — Loïs Samain,
> Groupe RATP

**EXEMPLE**

L'attaque par déni de service distribué (DDoS) subie par La Poste entre le 22 décembre 2025 et début janvier 2026 illustre une dépendance numérique souvent sous-estimée : la dépendance à l'accessibilité des services en ligne. Sans compromission de données, l'indisponibilité partielle de plusieurs services numériques a suffi à perturber l'activité et la relation usagers.

Avec des pics atteignant **jusqu'à 2,5 milliards de paquets par seconde**, l'attaque a affecté l'accès à des systèmes opérationnels critiques : le site institutionnel et ses services transactionnels (notamment le suivi de colis), des services numériques connexes (coffre-fort numérique, services liés aux examens et codes), ainsi que certains services de banque en ligne et les centres d'appel, sans interrompre pour autant la distribution physique du courrier et des colis. L'incident a mis en évidence la dépendance à une chaîne d'accès élargie – connectivité Internet, infrastructures réseau, solutions de mitigation DDoS et coordination avec des acteurs tiers – largement hors du contrôle direct de l'organisation.

Selon le baromètre du CESIN 2026, les attaques par déni de service représentent **21 % des incidents détectés en France**. Elles rappellent que la dépendance numérique ne concerne pas seulement les données ou les applications métiers, mais aussi la capacité à rester accessible, condition essentielle de la continuité opérationnelle, économique et sociale.

# 3.3. Libertés fondamentales, État de droit et démocratie

Les dépendances numériques rejoignent directement plusieurs **libertés fondamentales** : le droit au respect de la vie privée et des données personnelles, la liberté d'expression et de communication, la liberté de conscience et le droit à un recours effectif. Lorsque les principaux espaces de débat public sont contrôlés par des plateformes privées globales, soumises à des logiques économiques et parfois politiques éloignées des valeurs démocratiques, une question centrale émerge : **qui gouverne réellement l'espace public numérique ?**

La hiérarchisation de l'information, la modération des contenus et la visibilité des opinions sont de plus en plus déterminées par des algorithmes opaques. Par ailleurs, lorsque les décisions publiques s'appuient sur des outils automatisés – notation de risques, orientation de politiques publiques, allocation de ressources – le citoyen peut perdre de vue qui décide réellement : le politique, le fournisseur ou l'algorithme. Cette opacité fragilise la confiance dans l'État de droit et complique l'exercice du droit au recours, pourtant essentiel dans une démocratie. La dépendance numérique devient alors un enjeu de **liberté politique**, autant que de performance technologique.

VUE MICRO : Le rôle du RSSI évolue : il ne s'agit plus seulement de sécuriser et de se conformer, mais aussi de **rendre visibles les limites structurelles induites par les dépendances**, d'éclairer les décideurs sur les zones de non-maîtrise et d'intégrer ces contraintes dans les arbitrages de gouvernance, de risque et de responsabilité. La dépendance numérique ne diminue donc pas l'action du RSSI ; elle **déplace son rôle vers un exercice de lucidité, de transparence et d'alerte stratégique**.

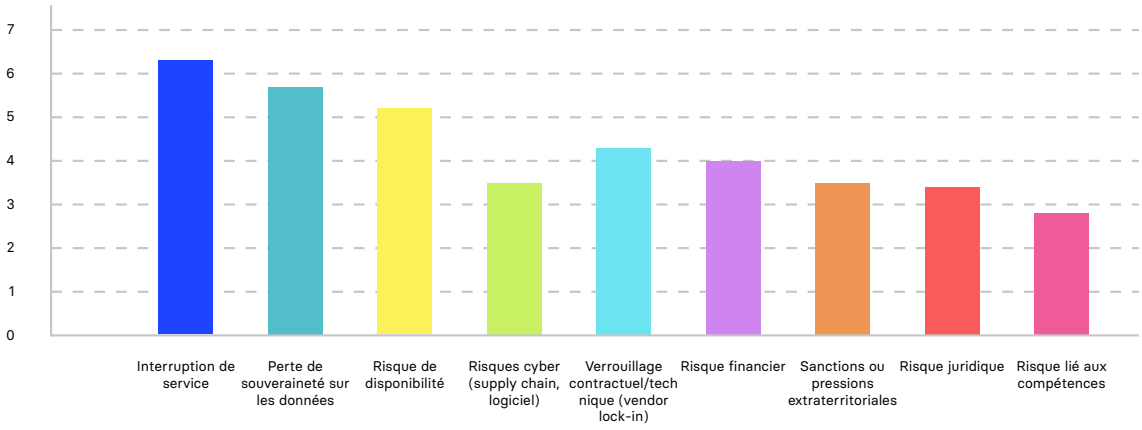
VUE MACRO : À l'échelle de l'État, la dépendance numérique pose une question centrale de **souveraineté démocratique**. Préserver les libertés fondamentales, garantir la résilience des services essentiels, soutenir l'innovation et maintenir l'autonomie stratégique exigent une politique cohérente : diversification des dépendances, régulation des acteurs dominants, investissement dans les compétences et la recherche, soutien aux écosystèmes locaux et transparence des choix technologiques. La maîtrise des dépendances numériques n'est pas un repli, mais une condition de la **liberté collective**, de la vitalité démocratique et de la capacité à construire un avenir numérique aligné avec les valeurs de la société.

# 4. Les risques associés aux dépendances numériques

Les RSSI interrogés convergent sur un point essentiel : *« ce n'est pas la dépendance en soi qui pose problème, mais l'absence de lucidité et de maîtrise sur les vulnérabilités qu'elle crée »*. Toute organisation dépend, par nature, de fournisseurs, de technologies et de services externes. Le risque apparaît lorsque ces dépendances deviennent **invisibles, subies ou irréversibles**, sans que leurs impacts opérationnels, cyber, juridiques, financiers ou sociétaux ne soient pleinement compris et pilotés.



**Quels sont les principaux impacts des dépendances numériques ?**
**SONDAGE CESIN (150 RÉPONSES)**




**L'interruption de service ou perte de disponibilité perçue comme le risque le plus prégnant.**

*(1 = moins important, 8 = plus important)*

## 4.1. Risques opérationnels : indisponibilité, continuité, performance

Les dépendances numériques exposent en premier lieu à des **risques opérationnels directs**. Une panne chez un fournisseur *Cloud*, un incident majeur sur un CDN, une attaque sur un opérateur d'importance vitale ou une défaillance d'un service d'authentification centralisé peuvent provoquer une **interruption brutale de service**. Plus une organisation concentre ses fonctions critiques chez un nombre réduit d'acteurs, plus l'impact potentiel est élevé (*blast radius*).

Au-delà de l'indisponibilité franche, la **dégradation de performance** constitue un risque souvent sous-estimé : saturation de services mutualisés, latence induite par des architectures imposées, limitations de quotas ou de capacités décidées unilatéralement par le fournisseur. Ces phénomènes peuvent affecter la qualité de service, la productivité des équipes et l'expérience client, sans qu'il soit toujours possible d'agir rapidement.

> ***« Les services numériques sont également devenus cœur de métier dans les environnements industriels. Quand l'un d'eux fait défaut, l'impact n'est pas virtuel : il est immédiat sur l'exploitation. »***
>
> — Emmanuel ORLANDO
> Dassault Systèmes

Enfin, certaines dépendances freinent la **capacité d'évolution** : une technologie dominante qui ne suit plus le rythme de l'innovation, ou dont la feuille de route ne correspond plus aux besoins métiers, peut devenir un facteur de rigidité structurelle. Pour un RSSI, ces risques, identifiées au travers des *Business Impact Analysis* (BIA), se traduisent en *Recovery Time Objective* (**RTO**), *Recovery Point Objective* (**RPO**) et en scénarios de crise. La dépendance numérique fait émerger des modes communs de défaillance : une même panne peut affecter plusieurs métiers, voire plusieurs secteurs simultanément, et plusieurs organisations peuvent dépendre du même sous-traitant sans en avoir conscience, révélant des **dépendances en cascade.**

## 4.2. Risques cyber et supply chain

Les chaînes logicielles et matérielles sont devenues un **vecteur d'attaque privilégié**. La compromission d'un fournisseur logiciel via une mise à jour piégée, les attaques sur des registres de paquets ou des dépôts open source, l'introduction de *backdoors* dans des équipements, ou encore la compromission d'un prestataire de services managés (MSP, MSSP) illustrent ces risques. Plus une organisation concentre des fonctions critiques chez un fournisseur, plus celui-ci devient une **cible de choix** pour les attaquants.

La complexité croissante des écosystèmes numériques amplifie ce phénomène. Bibliothèques tierces, services SaaS spécialisés, micro-SaaS, API externes : les **dépendances invisibles** se multiplient, rendant difficile une cartographie exhaustive de la surface d'attaque. Cette opacité complique la détection, la réponse à incident et la gestion de crise, tout en augmentant la probabilité d'un impact systémique.

> ***« Plus une organisation confie des fonctions critiques à ses fournisseurs, plus leurs vulnérabilités deviennent ses propres risques. »***
>
> — Frederick MEYER
> Auchan

## 4.3. Risques juridiques et réglementaires

Les dépendances numériques exposent également à **des risques juridiques et réglementaires significatifs**. Elles peuvent placer les organisations face à des **conflits de lois**, notamment lorsque les exigences du droit européen entrent en contradiction avec des législations extraterritoriales. En cas d'incident ou de transfert de données non conforme, les sanctions potentielles (RGPD, NIS 2, DORA, CRA etc.) peuvent être lourdes, tant financièrement qu'en termes d'image.

Au-delà des sanctions, l'incertitude juridique constitue un risque en soi. Il est souvent difficile d'anticiper ce qui se passera réellement en cas de conflit, d'enquête transfrontalière ou d'évolution réglementaire.

> ***« Les dépendances numériques ne créent pas seulement des risques techniques : elles exposent directement l'organisation à des conflits de lois, à des incertitudes juridiques et à des sanctions lourdes. La dépendance devient un risque de conformité à part entière. »***
>
> — Lucile PHILIBERT-COUPEZ
> Essilor Luxitica

## 4.4. Risques financiers et économiques

Les dépendances numériques comportent des **risques financiers majeurs**. Les hausses brutales de tarifs – modification de modèles de licence, facturation d'options auparavant incluses, changement de métriques (par utilisateur, par nombre de processeurs, par transaction), taxes ou de mesures douanières comme mesure de rétorsion ou anti-coercition liées à des tensions géopolitiques – peuvent avoir un impact immédiat sur les budgets IT. À cela s'ajoutent des **coûts de sortie élevés** : migrations complexes, frais de transfert de données, refonte d'architectures, formation des équipes.

Dans certains cas, l'organisation se retrouve dans une situation de **dépendance bloquée** : la solution est obsolète ou inadaptée, mais son remplacement est irréaliste à court ou moyen terme. À l'échelle macro, cette dépendance financière se traduit par une **captation de valeur** au profit d'acteurs dominants, souvent extra-européens, et par une difficulté à faire émerger et survivre des alternatives locales, pénalisées par des coûts de migration élevés et un rapport de force défavorable.

> ***« Une dépendance numérique mal maîtrisée peut faire exploser les coûts du jour au lendemain. Quand les règles tarifaires changent ou que la sortie devient irréaliste, le risque n'est plus technique, il devient financier et stratégique. »***
>
> — Olivier STASSI
> CESIN

## 4.5. Risques de réputation et de confiance

Les dépendances numériques peuvent exposer les organisations à des **risques réputationnels majeurs**, souvent disproportionnés par rapport à l'incident technique initial. Lorsqu'un incident met en lumière une **dépendance excessive à un fournisseur contesté** – par exemple en matière de protection des données, de pratiques de surveillance ou de localisation des services – l'organisation concernée peut apparaître comme imprudente, voire négligente, aux yeux de ses clients, partenaires ou autorités de régulation. L'incapacité à répondre rapidement et clairement à des questions pourtant fondamentales telles que *« où sont nos données ? »*, *« sont-elles sensibles »*, *« qui y a accès ? »* ou *« sous quel droit sont-elles protégées ? »* , *« ai-je une politique de rétention des données avec ce fournisseur »* fragilise immédiatement la crédibilité du discours de maîtrise et de gouvernance.

Ce risque est renforcé par un **manque de transparence** ou une communication mal préparée en situation de crise. Lorsque l'organisation dépend d'un fournisseur sur lequel elle n'a qu'une visibilité partielle, elle peut se retrouver dans l'incapacité de fournir des informations fiables, alimentant la défiance et les spéculations. Dans un contexte de sensibilité croissante aux enjeux de données personnelles, de souveraineté numérique et d'éthique, ces zones d'ombre sont de moins en moins acceptées.

## 4.6. Risques sociaux et politiques

À l'échelle sociétale, les dépendances numériques dépassent largement le cadre des organisations pour devenir des **facteurs de risques sociaux et politiques**. La concentration des canaux d'information et de communication sur quelques plateformes favorise la **manipulation de l'information**, qu'il s'agisse de campagnes de désinformation, d'amplification artificielle de certains discours ou de phénomènes de **bulles de filtre** qui fragmentent l'espace public. Lorsque les algorithmes déterminent ce qui est visible, crédible ou prioritaire, la capacité des citoyens à accéder à une information pluraliste et à se forger une opinion éclairée s'en trouve affaiblie.

Enfin, ces dépendances génèrent des **tensions politiques croissantes** lorsque les États peinent à réguler des plateformes dominantes ou à imposer leurs choix face à des acteurs disposant d'un pouvoir économique, technique et informationnel considérable, parfois adossé à des intérêts géopolitiques. La dépendance numérique devient alors un enjeu de **stabilité sociale, de souveraineté politique et de gouvernance démocratique**, conditionnant la capacité des sociétés à préserver le débat public, la cohésion et la confiance dans les institutions.

VUE MICRO : Pour le RSSI, ces risques se traduisent par une **complexité accrue de la gestion des risques**. Il ne s'agit plus seulement de sécuriser des systèmes, mais de comprendre et de piloter des dépendances multiples, souvent hors du contrôle direct de l'organisation. La lucidité sur ces dépendances, leur cartographie et leur intégration dans les analyses de risque conditionnent la capacité à préparer des scénarios crédibles, à dialoguer avec la direction et à arbitrer entre performance, sécurité et résilience.

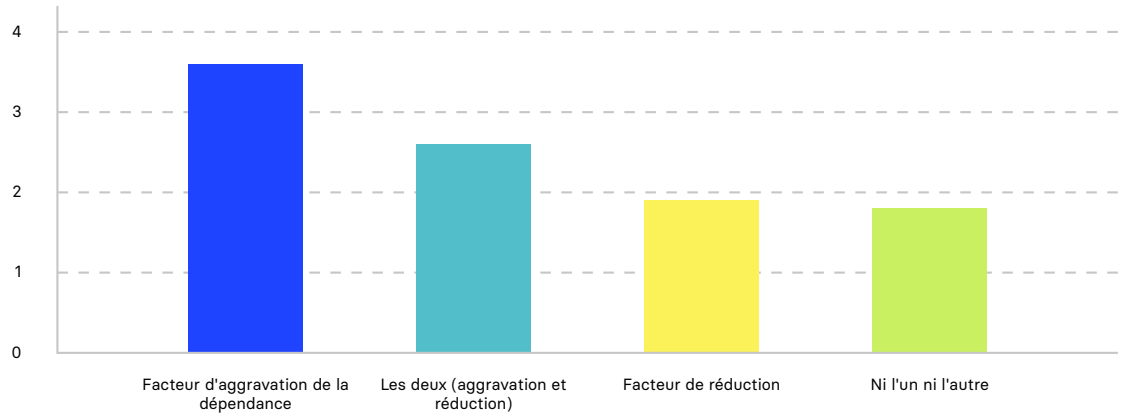
VUE MACRO : À l'échelle de l'État, les risques associés aux dépendances numériques interrogent la **souveraineté, la résilience et la cohésion sociale**. Ils appellent des politiques publiques capables de réduire les dépendances critiques, de renforcer la transparence des chaînes de valeur numériques et de préserver la capacité collective à décider et à agir. La maîtrise des dépendances numériques devient ainsi un enjeu stratégique majeur, au croisement de la sécurité, de l'économie et de la démocratie.

# 5. L'impact spécifique de l'intelligence artificielle : risques et opportunités

L'intelligence artificielle, et en particulier les **modèles d'IA générative**, agit aujourd'hui comme un **multiplicateur de dépendances numériques**. Là où le *Cloud*, les plateformes logicielles et les chaînes d'approvisionnement numériques avaient déjà concentré des pouvoirs techniques et économiques, l'IA ajoute une nouvelle couche de dépendance, plus profonde encore, car elle touche à la **production de connaissance, à la décision et au raisonnement**. Elle ne se contente pas d'automatiser des tâches : elle influence la manière dont les problèmes sont formulés, analysés et résolus.



**L'intelligence artificielle est-elle un facteur d'aggravation de la dépendance numérique ou au contraire un facteur de réduction ?**
**SONDAGE CESIN (150 RÉPONSES)**




**L'IA est perçue comme un facteur d'aggravation de la dépendance numérique.**

*(1 = moins important, 4 = plus important)*

# 5.1. Ce que l'IA change dans l'équation

Avec l'IA, plusieurs phénomènes se cumulent et s'amplifient.

D'abord, la **concentration des infrastructures**. Les grands modèles nécessitent des capacités massives de calcul, de stockage et de réseau, souvent basées sur des GPU (*Graphics Processing Unit* - processeur spécialisé conçu pour effectuer un très grand nombre de calculs en parallèle) spécialisés, des interconnexions à très haut débit et des centres de données hyperscale. Très peu d'acteurs disposent de ces capacités à l'échelle mondiale, ce qui crée une dépendance structurelle aux *hyperscalers*, qui contrôlent non seulement l'infrastructure, mais aussi l'accès aux modèles les plus performants..

Cette concentration pourrait toutefois être partiellement atténuée par l'essor de modèles spécialisés (*domain-specific language models* – DSLM), plus légers et optimisés pour des usages métier ciblés.

Ensuite, la **densité et la sensibilité des données**. L'IA consomme et produit des volumes considérables de données : conversations, documents internes, code source, journaux techniques, données métiers ou personnelles. Ces données sont souvent stratégiques, voire critiques. Leur centralisation dans des environnements IA accroît les risques de fuite, d'exploitation secondaire ou de réutilisation non maîtrisée.

Les grands modèles d'intelligence artificielle peuvent donner le sentiment d'être opaques : il n'est pas toujours facile d'expliquer précisément pourquoi ils produisent une réponse donnée. Cette difficulté complique l'audit, la conformité réglementaire, la justification des décisions ou la gestion d'un incident.

Toutefois, cette opacité diminue lorsque l'organisation utilise une architecture dite **RAG** (*Retrieval-Augmented Generation*). Concrètement, le RAG consiste à faire travailler le modèle d'IA à partir de documents internes identifiés (procédures, bases documentaires, référentiels), que l'on va rechercher automatiquement pour alimenter la réponse. Le modèle ne s'appuie alors plus uniquement sur son entraînement général, mais sur des sources maîtrisées et traçables.

l'IA introduit également un **effet de verrouillage culturel et épistémique**. Les modèles sont entraînés sur des corpus majoritairement anglo-saxons, avec des biais linguistiques, culturels et cognitifs qui influencent les exemples, les priorités, les raisonnements proposés. À cela s'ajoute des couches de gouvernance du modèle (filtres d'alignement, de sécurité et de modération) définies par les concepteurs reflétant leurs propres choix normatifs etjuridiques et culturels.

Un phénomène récent renforce cette dynamique : une part croissante des contenus en ligne est désormais produite par des modèles d'IA, tandis que les nouvelles versions sont entraînées sur des données issues d'Internet. Cette boucle peut amplifier les biais existants et homogénéiser progressivement les cadres de pensée. À grande échelle, l'IA ne génère pas seulement une dépendance technologique ou économique, mais aussi une dépendance cognitive et culturelle.

Enfin, le déploiement d'agents d'IA sur des processus métier clés peut entraîner une érosion progressive des savoir-faire internes. En automatisant des tâches structurantes de l'apprentissage, l'organisation prend le risque de fragiliser la montée en compétence des jeunes collaborateurs et d'affaiblir leur capacité de jugement critique face aux décisions produites par ces systèmes. La dépendance ne porte alors plus seulement sur la technologie, mais sur la compétence elle-même.

# 5.2. Opportunités de réduction de dépendance grâce à l'IA

Si l'intelligence artificielle est souvent perçue comme un **facteur d'amplification des dépendances numériques**, elle peut aussi devenir un **levier structurant d'autonomie et de résilience**, à condition d'être intégrée dans une démarche consciente et gouvernée. L'IA ne réduit pas mécaniquement la dépendance : elle offre des **capacités nouvelles** pour mieux la comprendre, la piloter et, dans certains cas, la diminuer.

Une première opportunité réside dans l'essor des **modèles ouverts**. L'émergence de modèles d'IA open source performants permet à des organisations – et potentiellement à des États – d'entraîner, d'adapter et d'héberger leurs propres modèles sur des **infrastructures maîtrisées**. Cette approche limite la dépendance aux modèles propriétaires opérés par des *hyperscalers*, réduit l'exposition juridique et renforce la transparence sur les données d'entraînement, les biais et les mécanismes internes. Elle favorise également des modèles mieux alignés avec les contextes métiers, linguistiques et réglementaires locaux.

L'IA peut également être mobilisée comme **outil central de cartographie des dépendances numériques**. Elle permet l'analyse automatisée des **SBOM**, **HBOM**, **CBOM** et désormais des **IA BOM** :

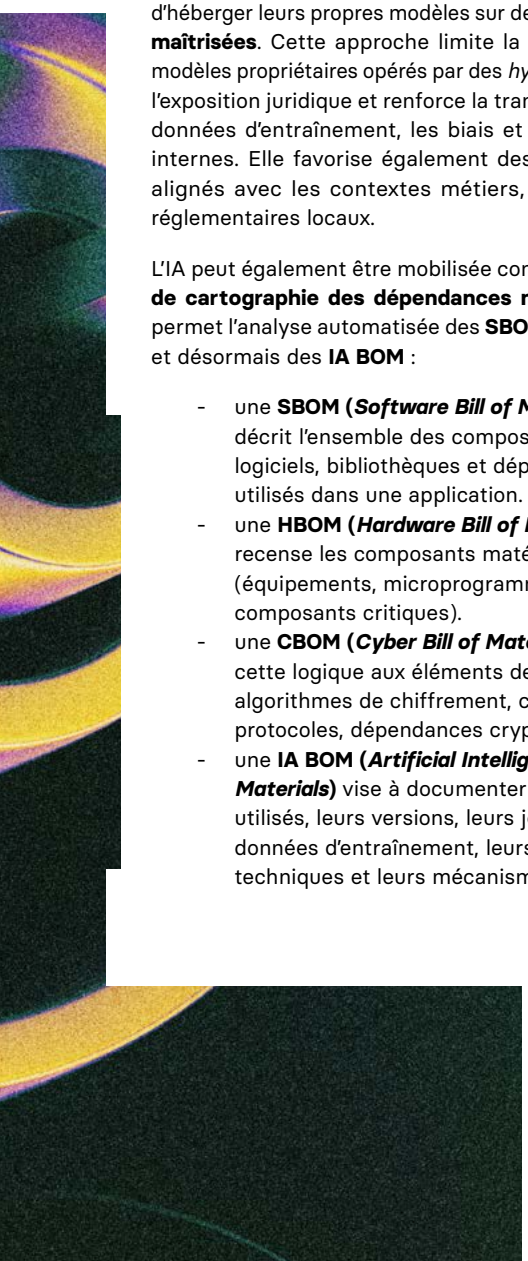
- une **SBOM (*Software Bill of Materials*)** décrit l'ensemble des composants logiciels, bibliothèques et dépendances utilisés dans une application.
- une **HBOM (*Hardware Bill of Materials*)** recense les composants matériels (équipements, microprogrammes, composants critiques).
- une **CBOM (*Cyber Bill of Materials*)** étend cette logique aux éléments de sécurité : algorithmes de chiffrement, certificats, protocoles, dépendances cryptographiques.
- une **IA BOM (*Artificial Intelligence Bill of Materials*)** vise à documenter les modèles utilisés, leurs versions, leurs jeux de données d'entraînement, leurs dépendances techniques et leurs mécanismes d'alignement.

En croisant ces informations, l'IA peut identifier des dépendances invisibles dans le code, l'infrastructure ou les chaînes de sécurité, et détecter des points de concentration critiques. Couplée à des capacités de simulation, elle permet d'évaluer les impacts potentiels d'une vulnérabilité, d'une défaillance de fournisseur ou d'une rupture de chaîne d'approvisionnement, renforçant ainsi la capacité d'anticipation stratégique.

En matière de sécurité opérationnelle, l'IA offre **des capacités avancées de détection d'incidents et de renforcement de la résilience**. Elle facilite le triage et l'enrichissement des alertes, la corrélation de volumes massifs de journaux, la détection de comportements anormaux et l'assistance à l'analyse en situation de crise. En réduisant le bruit et en mettant en évidence les signaux faibles, elle améliore la réactivité des équipes et contribue à limiter l'impact des incidents majeurs.

L'IA peut également renforcer les **capacités de remédiation**. En suggérant des actions de réponse, en contribuant à la définition et à la génération de *playbooks*, et en capitalisant sur les retours d'expérience, elle aide les organisations à structurer et accélérer leurs réponses tout en conservant un contrôle humain sur les décisions critiques.

Enfin, utilisée comme **outil pédagogique**, l'IA peut accélérer la montée en compétence. Elle aide à comprendre des systèmes complexes, à documenter des architectures, à explorer des scénarios et à transmettre le savoir. Dans cette perspective, l'IA devient un **amplificateur de compétences**, contribuant à réduire la dépendance humaine et organisationnelle plutôt qu'à l'aggraver.



## 5.3. Conditions pour une IA au service de l'autonomie numérique

Pour que l'intelligence artificielle contribue réellement à **réduire les dépendances numériques**, plutôt qu'à les renforcer, plusieurs principes structurants se dégagent des échanges menés avec les RSSI, les décideurs publics et les acteurs de l'écosystème. Ces principes ne relèvent pas uniquement de la technologie : ils engagent des choix **politiques, industriels, organisationnels et culturels.**

Le premier principe consiste à **préserver et développer des capacités locales d'infrastructure**. L'IA repose sur des ressources critiques – calcul, stockage, réseau – qui conditionnent l'autonomie réelle. Disposer de ***Clouds* souverains ou de confiance**, de datacenters locaux et de capacités de calcul mutualisées permet de réduire la dépendance aux *hyperscalers* extra-européens, de mieux maîtriser la localisation des données et de garantir la continuité des services en cas de crise géopolitique ou industrielle. Ces capacités ne visent pas l'autarcie, mais la possibilité de choix réels et réversibles.

Le second principe est le **soutien actif à l'open source**. Modèles ouverts, *frameworks*, bibliothèques et outils MLOps constituent un levier essentiel pour éviter que l'ensemble de la chaîne de valeur de l'IA ne soit capturée par quelques acteurs dominants. L'open source favorise la transparence, l'auditabilité, l'innovation distribuée et l'émergence d'écosystèmes locaux. Il permet également aux organisations de comprendre, adapter et améliorer les outils qu'elles utilisent, plutôt que de dépendre de boîtes noires propriétaires.

Dans le même esprit, il est crucial de **favoriser l'émergence de solutions et d'un marché de la donnée franco-européens**. La donnée est la matière première de l'IA. Sans capacités locales de collecte, de partage et de valorisation des données, l'autonomie reste illusoire. Développer des espaces de données sectoriels, interopérables et conformes aux cadres réglementaires européens permet de soutenir l'innovation tout en protégeant les intérêts économiques et sociétaux.

Un autre principe fondamental est la **clarification de la gouvernance**. Qui décide quels modèles sont utilisés ? Pour quelles finalités ? Avec quelles données ? Sous quelles contraintes réglementaires, éthiques et de sécurité ? Sans réponses claires à ces questions, l'IA risque de s'imposer par défaut, au gré des offres du marché, plutôt que par choix stratégique. Une gouvernance explicite est indispensable pour aligner les usages de l'IA avec les objectifs de l'organisation ou de la puissance publique.

La **documentation et l'auditabilité** constituent également des piliers clés. Il s'agit d'assurer la traçabilité des données d'entraînement, des versions de modèles, des paramètres et des décisions assistées par l'IA. Cette exigence est essentielle pour la conformité réglementaire, la gestion des risques, la confiance des utilisateurs et la capacité à rendre des comptes. Une IA non documentée est une source de dépendance et d'opacité supplémentaire.

Enfin, aucun de ces principes ne peut fonctionner sans un effort massif de **formation, de sensibilisation et d'éducation**. Il est important d'éviter que l'IA soit perçue comme une « boîte noire magique ». Développer une culture d'usage critique chez les décideurs, les juristes, les opérationnels et les utilisateurs finaux est une condition de l'autonomie. Comprendre comment une IA raisonne, quelles sont ses limites, ses biais et ses conditions d'apprentissage permet de mieux l'utiliser, de la questionner et, le cas échéant, de la corriger. Comme le rappelle l'adage : si l'éducation est coûteuse, l'ignorance l'est toujours davantage.

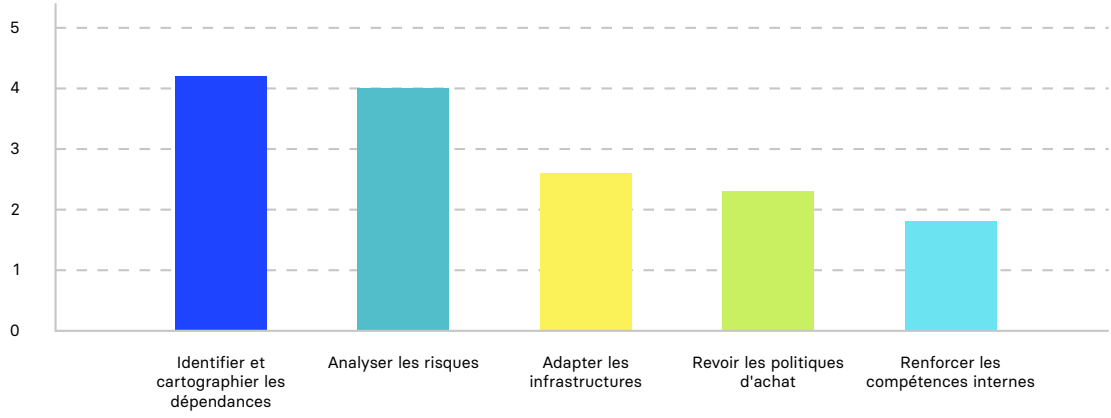
# 6. Pistes de solutions opérationnelles

La maîtrise des dépendances numériques constitue aujourd'hui un enjeu central pour les organisations. Longtemps perçue comme une problématique abstraite ou réservée aux infrastructures IT, elle s'impose désormais comme un facteur déterminant de résilience, de continuité d'activité et de liberté de décision. Pour les RSSI, le défi n'est plus seulement d'identifier ces dépendances, mais de les intégrer dans une démarche opérationnelle cohérente, soutenable et alignée avec la stratégie globale de l'entreprise.

Cette démarche ne vise ni l'autonomie totale, irréaliste dans un monde interconnecté, ni une remise en cause idéologique des technologies dominantes. Elle cherche au contraire à transformer une dépendance souvent subie en une dépendance **choisie, comprise et gouvernée**.



**Quelles sont les solutions opérationnelles qui permettraient de mieux maîtriser nos dépendances numériques ?**
**SONDAGE CESIN (150 RÉPONSES)**




**L'identification et la cartographie des dépendances ainsi que l'analyse des risques sont les deux pistes opérationnelles les plus citées par les membre du CESIN.**

*(1 moins important, 5 plus important)*

## 6.1. Nommer la dépendance numérique et l'ancrer dans la gouvernance

La première condition de toute action est la reconnaissance explicite du sujet. La dépendance numérique ne peut être traitée efficacement tant qu'elle reste diluée dans d'autres problématiques – cybersécurité, *Cloud*, conformité ou achats – sans être nommée comme telle. Or, **elle dépasse largement le périmètre de la DSI ou du RSSI**.

Elle **engage directement la stratégie de l'organisation**, en conditionnant ses trajectoires technologiques et économiques. Elle concerne le juridique, du fait des asymétries contractuelles et des lois extraterritoriales. Elle touche les fonctions achats, souvent en première ligne dans les choix structurants. Elle affecte la gestion des tiers, la conformité réglementaire, les métiers et, plus profondément encore, les compétences internes et la capacité de l'entreprise à comprendre et maîtriser ses propres systèmes.

Ancrer le sujet dans la gouvernance suppose donc de l'inscrire explicitement **à l'agenda des instances dirigeantes** : comité exécutif, comité des risques, conseil d'administration. Cette inscription ne peut reposer uniquement sur des arguments techniques. Elle passe par la mise en perspective de **scénarios de rupture crédibles** : indisponibilité prolongée d'un fournisseur critique, retrait ou modification unilatérale de licences, sanctions économiques ou décisions souveraines impactant l'accès à des services essentiels.

Ces scénarios relèvent souvent de ce que l'on qualifiait hier de **« cygnes noirs » : des événements à faible probabilité mais à impact systémique**. L'évolution du contexte géopolitique et réglementaire tend toutefois à réduire cette improbabilité perçue. Dès lors, le rôle du RSSI est d'aider la gouvernance à intégrer ces risques dans ses arbitrages, au même titre que les risques financiers ou industriels.

La dépendance numérique doit ainsi devenir un **objet de pilotage**, non un angle mort.

## 6.2. Rendre visibles les dépendances : une cartographie orientée métier

Une dépendance non identifiée ne peut être maîtrisée. La deuxième étape consiste donc à rendre visibles les chaînes de dépendance qui structurent le fonctionnement réel de l'organisation. Cette visibilité ne doit toutefois pas être confondue avec une recherche d'exhaustivité technique, souvent illusoire et coûteuse.

Les organisations disposent déjà de multiples inventaires : cartographies applicatives, référentiels d'infrastructures, listes de fournisseurs, analyses de processus critiques. L'enjeu n'est pas de créer un inventaire supplémentaire, mais de **faire dialoguer l'existant** et de l'enrichir avec une lecture spécifique des dépendances.

Les approches de type SBOM pour les logiciels, HBOM pour les matériels, ou leurs équivalents émergents pour les modèles d'IA et les jeux de données, apportent une granularité utile. Elles permettent de **mieux comprendre la composition des systèmes modernes** et **leurs interdépendances**. Toutefois, ces outils n'ont de valeur que s'ils sont reliés aux processus métiers et aux services réellement critiques pour l'organisation.

La cartographie des dépendances doit donc partir des fonctions essentielles : quels services sont indispensables à la continuité d'activité ? Quels processus reposent sur des fournisseurs ou des plateformes difficiles à substituer ? Où se concentrent les points de fragilité ?

À cette lecture fonctionnelle s'ajoutent **des dimensions souvent sous-estimées** : la chaîne de sous-traitance, la localisation géographique et juridique des services, l'actionnariat des fournisseurs, l'exposition à des cadres légaux extraterritoriaux. L'objectif n'est pas de qualifier moralement ces dépendances, mais d'identifier les **zones de concentration critique**, là où une défaillance unique pourrait produire des effets en cascade.

## 6.3. Analyser et prioriser les risques liés aux dépendances

Identifier les dépendances n'est qu'une étape intermédiaire. La valeur de la démarche réside dans la capacité à les analyser et à les hiérarchiser. Toutes les dépendances ne posent pas le même niveau de risque, et toutes ne justifient pas le même niveau d'investissement.

Cette analyse s'inscrit naturellement dans les **cadres existants de gestion des risques**. Elle consiste à relier chaque dépendance aux impacts potentiels sur les processus métiers, aux enjeux de données (sensibilité, localisation, volumes), aux risques cyber associés et aux contraintes réglementaires applicables.

Ce travail permet de distinguer des **dépendances acceptables**, parce que maîtrisées, substituables ou à impact limité, et des **dépendances critiques**, caractérisées par une faible capacité de remplacement, un impact métier majeur et une exposition juridique ou géopolitique élevée.

L'enjeu n'est pas d'éliminer toute dépendance, mais de fournir aux instances de gouvernance une **vision hiérarchisée et arbitrable**. Une dépendance critique peut être acceptée, mais elle doit alors l'être en connaissance de cause, avec des mesures de mitigation explicites et un suivi dans le temps.

> ***« Identifier les dépendances ne suffit pas. Le vrai enjeu est de les hiérarchiser, de comprendre lesquelles sont acceptables et lesquelles deviennent critiques, afin de permettre des arbitrages éclairés au niveau de la gouvernance. »***
>
> — Eric VAUTIER
> Groupe ADP

## 6.4. Adapter les architectures pour préserver des marges de manœuvre dans le temps

Les choix d'architecture jouent un rôle déterminant dans la création, l'amplification ou la maîtrise des dépendances numériques. Ils sont souvent réalisés sous la contrainte de délais, de coûts ou de compétences disponibles, sans que les dépendances induites soient pleinement explicitées ni planifiées. Or, ces choix structurent le système d'information sur le long terme et conditionnent directement la capacité de l'organisation à évoluer, à résister aux ruptures et à conserver sa liberté d'arbitrage.

Intégrer la dépendance numérique dans l'architecture ne consiste pas à chercher à la supprimer, mais à la **rendre visible, pilotable et progressive**. Toute architecture crée des dépendances ; l'enjeu est de décider lesquelles sont acceptables, pour quelle durée, et selon quelles conditions elles pourront être remises en cause. Cette logique suppose de traiter la dépendance comme un paramètre d'architecture à part entière, au même titre que la performance, la sécurité ou les coûts, et de l'inscrire dans une trajectoire assumée.

Les **architectures fortement intégrées**, reposant sur des services propriétaires étroitement imbriqués, maximisent souvent l'efficacité et la rapidité de mise en œuvre à court terme. En contrepartie, elles réduisent fortement les capacités d'évolution et rendent toute sortie globale complexe, coûteuse, voire incompatible avec les exigences de continuité d'activité. À l'inverse, **des architectures modulaires, fondées sur des interfaces standardisées, des formats de données ouverts** et des couches d'abstraction clairement définies, permettent d'introduire des dépendances de manière graduelle et réversible.

La **conteneurisation** s'inscrit dans cette logique en offrant une portabilité accrue des charges applicatives et une meilleure séparation entre les applications et les infrastructures sous-jacentes. Lorsqu'elle est correctement mise en œuvre, elle facilite les scénarios de migration, de redéploiement ou de fonctionnement multi-environnements. Elle ne constitue toutefois pas une garantie automatique d'indépendance : son efficacité dépend fortement des services périphériques auxquels les conteneurs sont adossés (réseau, stockage, identité, observabilité), qui peuvent eux-mêmes devenir des points de dépendance critiques.

Le **recours aux architectures *serverless*** illustre une autre forme de dépendance, plus diffuse mais souvent plus profonde. En déléguant une part importante de la gestion opérationnelle au fournisseur, le *serverless* apporte des gains significatifs en agilité et en élasticité. En contrepartie, il renforce l'adhérence à des services spécifiques et complique les scénarios de sortie ou de portage vers d'autres environnements. L'enjeu n'est pas d'exclure ces approches, mais de les utiliser de manière ciblée, en connaissance de cause, et en les limitant aux périmètres où leur dépendance est jugée acceptable.

La gestion des chaînes d'intégration et de déploiement constitue également un levier clé. **Découpler les chaînes de CI (*Continuous Integration*) et de CD (*Continuous Deployment/Delivery*)** permet de réduire les dépendances croisées entre les outils, les environnements et les fournisseurs. Ce découplage renforce la capacité à changer une brique sans remettre en cause l'ensemble de la chaîne, et facilite l'adaptation progressive de l'architecture. À l'inverse, des pipelines fortement intégrés à un écosystème unique peuvent devenir des vecteurs de verrouillage aussi contraignants que les plateformes applicatives elles-mêmes.

La question des points de défaillance uniques reste centrale. La résilience ne découle ni automatiquement du *Cloud* ni du SaaS, mais de choix architecturaux explicites : séparation des fonctions critiques, redondance géographique ciblée, diversification raisonnée de fournisseurs pour certains services clés, et capacité à fonctionner en mode dégradé. Ces mécanismes doivent être pensés dès la conception et intégrés dans une planification d'architecture, plutôt que rajoutés a posteriori sous la contrainte d'un incident.

Enfin, l'objectif n'est pas de dupliquer intégralement les systèmes ni de construire des architectures idéales sur le papier, mais de définir un **chemin de sortie crédible**, même partiel. Ce chemin peut être progressif, coûteux et limité dans le temps, mais il doit exister, être documenté et régulièrement réévalué. En intégrant la dépendance numérique dans une **démarche de planification architecturale, les organisations transforment une contrainte implicite en un choix maîtrisé**, compatible avec l'innovation, la performance et la résilience de long terme.

## 6.5. Faire des achats et des contrats un levier de maîtrise

Les politiques d'achat constituent l'un des leviers les plus déterminants – et pourtant les plus sous-estimés – dans la maîtrise des dépendances numériques. Les choix contractuels engagent souvent l'organisation pour plusieurs années et façonnent durablement son niveau d'autonomie, bien au-delà des décisions purement techniques. Une dépendance excessive n'est d'ailleurs que rarement le fruit d'un choix technologique isolé : elle est presque toujours la conséquence d'une **décision d'achat insuffisamment éclairée par les risques de long terme**.

Traditionnellement, les achats numériques ont été guidés par des critères de coût, de rapidité de déploiement et de couverture fonctionnelle. Or, dans un contexte de concentration des marchés et de plateformisation croissante, ces critères, pris isolément, favorisent mécaniquement des situations de verrouillage. Revoir les politiques d'achat ne signifie donc pas complexifier systématiquement les processus, mais **élargir la grille de lecture** pour y intégrer explicitement la question de la dépendance.

Cela commence dès la phase d'appel d'offres. Introduire des critères liés à la dépendance numérique permet de déplacer le débat en amont, avant que les choix ne deviennent irréversibles. **Les exigences de réversibilité**, l'usage de **formats de données ouverts, l'interopérabilité avec des solutions tierces ou encore la transparence sur les sous-traitants** et les lieux d'hébergement ne doivent plus être considérées comme des options secondaires ou des « clauses de confort ». Elles constituent des éléments structurants de la résilience future de l'organisation. Leur absence, au contraire, doit être analysée comme un risque explicite, susceptible d'être arbitré au plus haut niveau.

La négociation contractuelle représente un second temps clé. Dans de nombreux cas, les organisations concentrent leurs efforts sur la localisation des données, tout en négligeant les conditions dans lesquelles elles sont traitées, analysées ou enrichies. Or, la dépendance la plus critique se situe souvent dans les phases de traitement des données, notamment dans les environnements *Cloud* et les services SaaS avancés. **Clarifier contractuellement où et comment les données sont utilisées, quelles juridictions** s'appliquent, et quelles obligations pèsent sur le fournisseur en cas de réquisition par une autorité étrangère est devenu indispensable, même si ces garanties ne sont jamais absolues.

Les **clauses relatives à la continuité de service et aux pénalités en cas d'interruption** prolongée jouent également un rôle structurant. Elles ne compensent jamais pleinement un arrêt d'activité, mais elles traduisent un rapport de force et incitent le fournisseur à intégrer la résilience dans ses propres arbitrages. De la même manière, la prévisibilité des modèles tarifaires, les plafonds d'augmentation et les mécanismes d'alerte en cas d'évolution majeure conditionnent la soutenabilité économique de la relation dans le temps. Une dépendance devient critique non seulement lorsqu'un service est indisponible, mais aussi lorsqu'il devient financièrement incontournable.

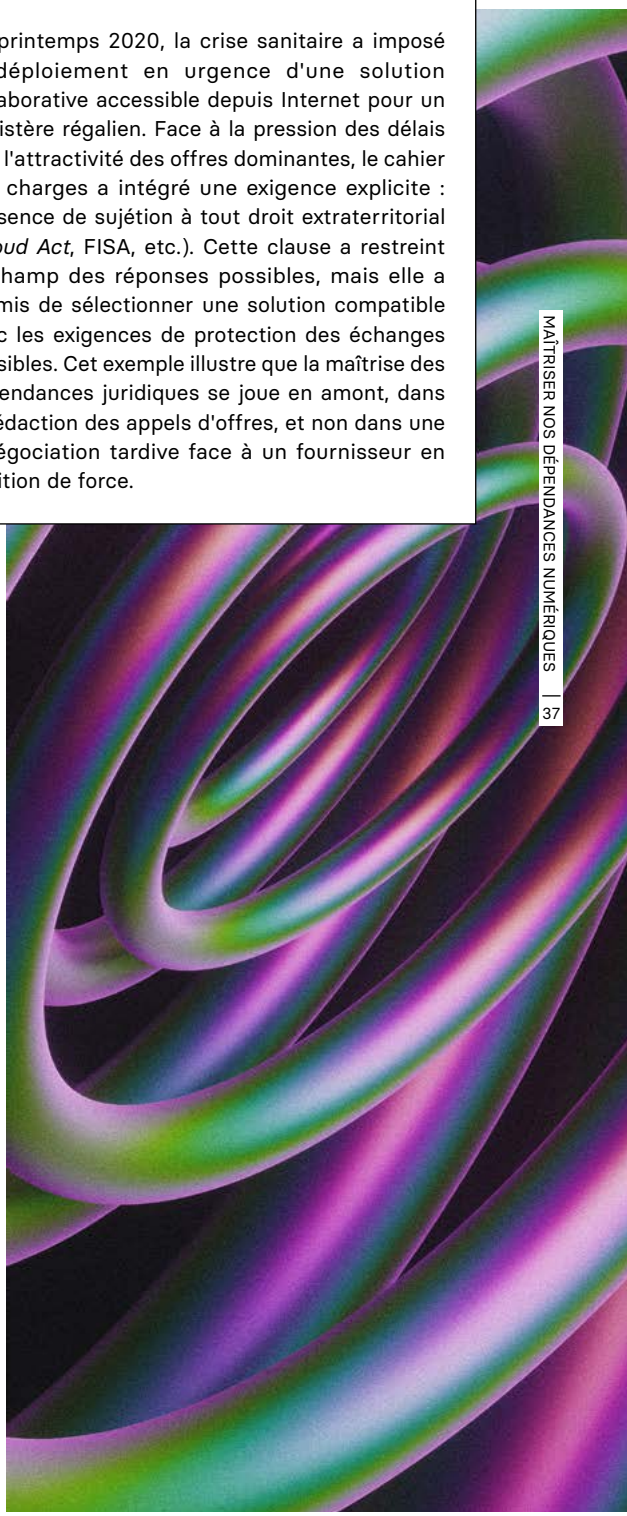
Lorsque cela est réaliste, la **diversification des fournisseurs constitue un levier complémentaire**. Le *double-sourcing*, par exemple pour des fonctions de supervision, de gestion des incidents ou certains équipements critiques, permet de limiter les effets de concentration et de renforcer la capacité de négociation. Il ne s'agit pas d'une règle universelle : toutes les fonctions ne se prêtent pas à une telle approche, et les coûts induits peuvent être significatifs. En revanche, pour certains services clés, **l'absence totale d'alternative doit être identifiée comme un risque stratégique assumé**, et non comme une situation subie.

Dans ce contexte, le RSSI n'a pas vocation à devenir juriste ou acheteur. Son rôle est avant tout celui d'un **acteur d'interface et d'influence**, capable de traduire les enjeux techniques et opérationnels en risques compréhensibles par les fonctions achats, juridiques et financières. En travaillant étroitement avec ces équipes, il contribue à faire entrer la dépendance numérique dans la matrice de décision de l'entreprise, au même titre que les risques financiers, réglementaires ou réputationnels.

Repenser les politiques d'achat et les contrats ne permet pas d'éliminer toute dépendance. En revanche, cela permet de **transformer une dépendance implicite et non maîtrisée en une dépendance consciente, négociée et pilotée**, condition indispensable à toute stratégie de résilience numérique durable.

**EXEMPLE**

Au printemps 2020, la crise sanitaire a imposé le déploiement en urgence d'une solution collaborative accessible depuis Internet pour un ministère régalien. Face à la pression des délais et à l'attractivité des offres dominantes, le cahier des charges a intégré une exigence explicite : l'absence de sujétion à tout droit extraterritorial (*Cloud Act*, FISA, etc.). Cette clause a restreint le champ des réponses possibles, mais elle a permis de sélectionner une solution compatible avec les exigences de protection des échanges sensibles. Cet exemple illustre que la maîtrise des dépendances juridiques se joue en amont, dans la rédaction des appels d'offres, et non dans une renégociation tardive face à un fournisseur en position de force.



# 6.6. Investir dans les compétences et la culture : transformer la dépendance subie en dépendance maîtrisée

La maîtrise des dépendances numériques repose moins sur les technologies déployées que sur la **capacité des organisations à les comprendre**, les piloter et les remettre en question. Sans compétences internes suffisantes, la dépendance devient inévitable : elle ne résulte plus d'un choix éclairé, mais d'une contrainte subie.

La transformation numérique s'est souvent accompagnée d'une **externalisation** massive des infrastructures, des plateformes et des services. Si cette évolution a permis des gains de rapidité et d'agilité, elle a également contribué à une **érosion progressive des savoir-faire internes**. Or, externaliser un service ne doit jamais signifier externaliser la compréhension de son fonctionnement. Une organisation qui ne maîtrise plus les principes fondamentaux de ses systèmes d'information perd sa capacité d'arbitrage et se retrouve dépendante, non seulement techniquement, mais aussi cognitivement.

**Maintenir un socle de compétences techniques fondamentales** – systèmes, réseaux, sécurité – constitue donc une exigence stratégique. Ces compétences ne relèvent pas d'un modèle dépassé : elles sont indispensables pour gouverner des environnements complexes, notamment dans le *Cloud* et le SaaS, et pour évaluer de manière critique les promesses de sécurité, de résilience ou de réversibilité formulées par les fournisseurs. Ces compétences doivent être structurées, pérennisées et intégrées au cœur de la politique RH.

La montée en puissance du *Cloud*, de l'intelligence artificielle et des services managés impose par ailleurs une acculturation plus large. **Les choix technologiques engagent désormais des dimensions contractuelles, réglementaires et géopolitiques étroitement imbriquées**. Sans compétences permettant de comprendre ces interactions, les décisions privilégient mécaniquement le court terme, au détriment de la liberté d'action à long terme.

Au-delà des compétences individuelles, la maîtrise des dépendances numériques repose sur une **culture collective de vigilance**. Questionner les solutions « magiques », distinguer la commodité immédiate de l'autonomie durable et intégrer systématiquement la question du scénario de rupture – que se passe-t-il si ce fournisseur fait défaut ? – doivent devenir des réflexes partagés, au-delà des seules équipes techniques.

Investir dans les compétences et la culture constitue ainsi l'un des leviers les plus structurants pour transformer une dépendance subie en une dépendance consciente, maîtrisée et gouvernée.

# 6.7. *Cloud* et SaaS : réhabiliter la réversibilité comme discipline opérationnelle

Le recours massif aux solutions *Cloud* et SaaS a profondément transformé les architectures numériques des organisations. Ces modèles ont apporté des gains significatifs en agilité, en rapidité de déploiement et en mutualisation des ressources. Toutefois, ils ont également contribué à déplacer, voire à masquer, certaines formes de dépendance. Dans ce contexte, la **notion de réversibilité**, longtemps perçue comme théorique ou secondaire, retrouve aujourd'hui toute sa **pertinence opérationnelle**.

La réversibilité ne peut plus être envisagée comme une simple clause contractuelle destinée à rassurer. Elle constitue une **capacité réelle, qui se construit dès la conception des architectures et se valide dans la durée**. Être réversible ne signifie pas nécessairement pouvoir migrer instantanément l'ensemble des systèmes, mais disposer d'un chemin de sortie crédible, même partiel, permettant de maintenir une activité minimale ou de reconstruire ailleurs en cas de rupture majeure.

L'introduction de mécanismes de type **« *kill switch* »** s'inscrit dans cette logique. Dans les environnements *Cloud* et SaaS, **le *kill switch* est le plus souvent du côté du fournisseur**, qui dispose de la capacité d'interrompre ou de restreindre un service de manière unilatérale. L'enjeu, pour l'organisation, n'est donc pas de provoquer elle-même une rupture, mais de **construire une capacité de sortie et de reprise** face à une coupure imposée. La réversibilité repose ainsi sur des mécanismes permettant d'isoler un environnement, de limiter une propagation ou de fonctionner en mode dégradé, afin de préserver une continuité minimale et de redémarrer ailleurs dans un cadre maîtrisé.

La réversibilité ne devient effective que si elle est **régulièrement testée**. Organiser des exercices de sortie, de bascule ou de fonctionnement en mode dégradé permet de révéler les dépendances réelles, souvent plus profondes que celles identifiées sur le papier. Ces exercices mettent en lumière les écarts entre les hypothèses contractuelles et les capacités techniques effectives, et constituent un puissant levier de sensibilisation pour les équipes et la gouvernance.

Ainsi, dans des environnements *Cloud* et SaaS devenus structurants, la réversibilité ne doit plus être perçue comme une contrainte, mais comme une discipline de résilience. En redonnant à cette notion ses lettres de noblesse, les organisations transforment une dépendance subie en un choix maîtrisé, compatible avec l'innovation comme avec la continuité d'activité.

VUE MICRO : À l'échelle de l'organisation, la maîtrise des dépendances numériques devient une **composante essentielle de la mission du RSSI**. Elle prolonge naturellement la gestion du risque cyber vers des enjeux plus larges de résilience, de continuité d'activité et de liberté de décision. En éclairant les choix technologiques, contractuels et humains, le RSSI contribue à transformer des dépendances souvent subies en arbitrages assumés. Son rôle n'est pas de freiner l'innovation, **mais d'en garantir la soutenabilité**, en s'assurant que l'organisation conserve, à tout moment, la capacité de comprendre, de choisir et, le cas échéant, de se désengager.

VUE MACRO : À l'échelle macro, les dépendances numériques résultent de l'agrégation de milliers de décisions individuelles prises par les organisations. Ces choix façonnent la **résilience économique, la capacité d'action des États** et, in fine, la souveraineté numérique. La maîtrise des dépendances ne relève donc pas uniquement de la sécurité ou de la compétitivité, mais d'un enjeu stratégique collectif. En renforçant la capacité des acteurs publics et privés à piloter leurs dépendances, les États se dotent d'un levier essentiel pour préserver l'autonomie, la continuité des services essentiels et la stabilité de l'écosystème numérique.

> ***Être indépendant c'est maîtriser sa continuité de fonctionnement. C'est ne pas avoir à craindre un quelconque « kill switch » caché au tréfonds d'un composant essentiel. À l'heure où les relations internationales se tendent, combien de pays de l'UE se demandent si leurs avions de combat F-35 vont pouvoir décoller pour défendre un territoire européen convoité ?***
>
> — Thierry LELÉGARD
> SiPearl - Security Architecture

# 7. Pistes de solutions au plan stratégique et étatique

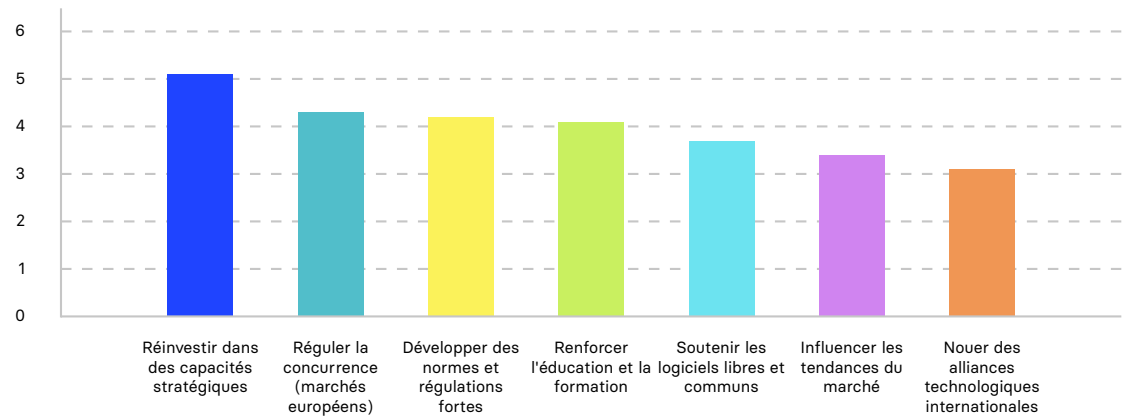
La maîtrise des dépendances numériques ne peut reposer uniquement sur les choix et les efforts des organisations, aussi matures soient-elles. Les rapports de force numériques sont globaux, structurés par des effets d'échelle, des concentrations industrielles et des dynamiques géopolitiques qui dépassent largement le périmètre d'action d'une entreprise ou d'une administration isolée. À ce titre, la réduction des dépendances les plus critiques suppose des politiques publiques volontaristes, cohérentes et inscrites dans le temps, au niveau national comme européen.

L'enjeu n'est pas de viser une autonomie totale, irréaliste dans un monde interconnecté, mais de **reconstruire des capacités de choix**, de préserver des marges de manœuvre stratégiques et de limiter les dépendances jugées incompatibles avec la continuité des services essentiels, la protection des données ou l'exercice de la souveraineté démocratique.

***« Dans les environnements de Défense, j'ai appris que la souveraineté n'est pas l'absence de dépendance, mais la capacité à en connaître chaque maillon, à en mesurer l'impact et à disposer d'un chemin de repli crédible. Ce qui vaut pour le régalien vaut désormais pour toute organisation. »***

— Franck ROUXEL
Expert cybersécurité

**Quelles sont les leviers stratégiques qui permettraient de mieux maîtriser nos dépendances numériques ?**
**SONDAGE CESIN (150 RÉPONSES)**




**Le levier le plus important identifié est le réinvestissement dans les capacités stratégiques.**

*(1 moins important, 7 plus important)*

# 7.1. Clarifier l'ambition de souveraineté numérique

La souveraineté numérique est aujourd'hui **omniprésente dans les discours publics**, mais sa définition reste souvent floue, voire contradictoire. Utilisée comme un mot-valise, elle risque de devenir un slogan plus qu'un cadre d'action. Clarifier cette ambition constitue donc un préalable indispensable à toute politique efficace de maîtrise des dépendances numériques.

Plutôt qu'une souveraineté absolue, difficilement atteignable et potentiellement contre-productive, il apparaît plus pertinent de définir la souveraineté numérique autour de **capacités clés**. Il s'agit d'abord de la capacité à **concevoir, exploiter et faire évoluer des infrastructures critiques** : réseaux de télécommunications, capacités de calcul, services *Cloud*, systèmes d'identité numérique, plateformes de santé, de justice ou d'administration. Ces infrastructures constituent l'ossature numérique de la société ; leur indisponibilité ou leur contrôle externe peut avoir des conséquences systémiques.

La souveraineté numérique implique également la capacité à **protéger les données des citoyens**, des entreprises et des administrations **contre des ingérences étrangères**, qu'elles soient économiques, politiques ou judiciaires. Cette protection ne repose pas uniquement sur la localisation physique des données, mais sur la maîtrise des conditions juridiques, techniques et organisationnelles de leur traitement.

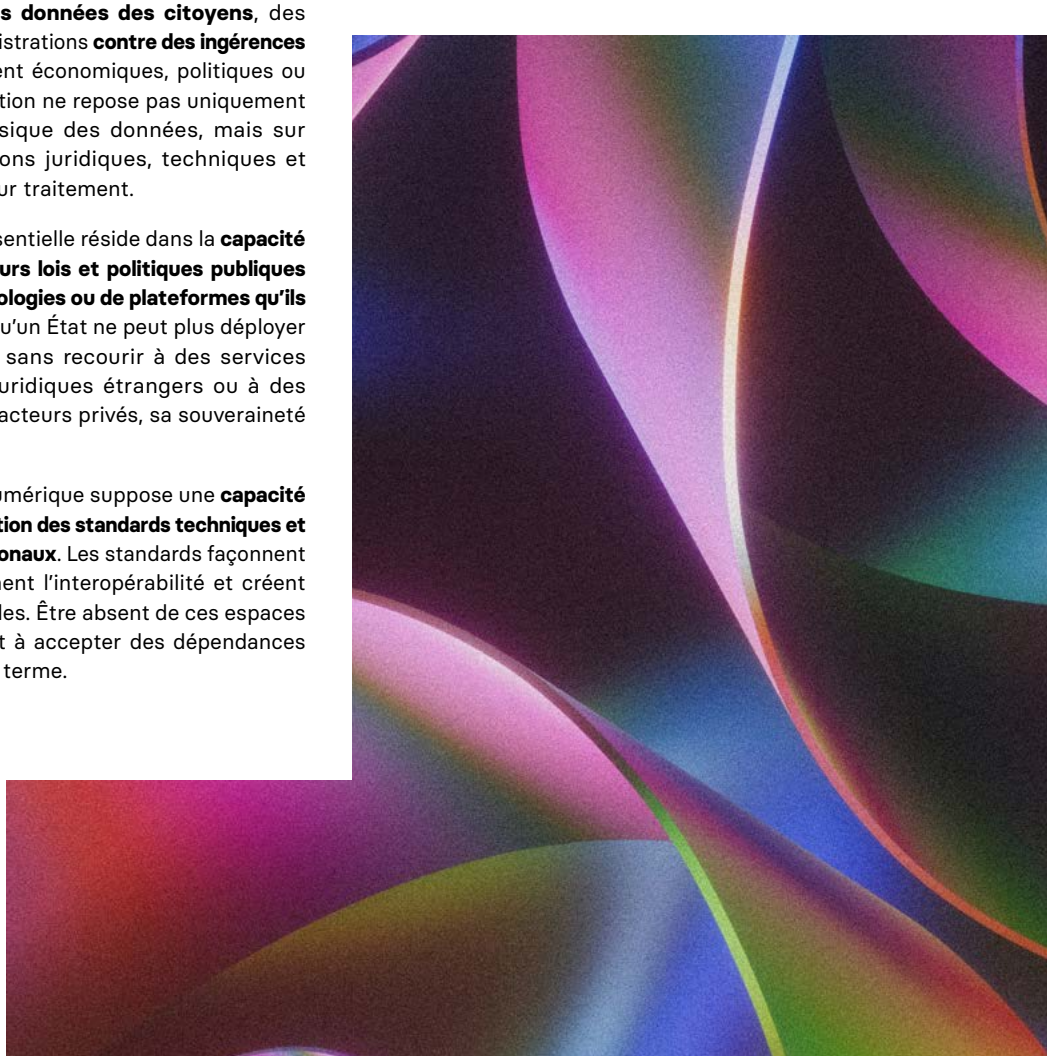
Une autre dimension essentielle réside dans la **capacité des États à appliquer leurs lois et politiques publiques sans dépendre de technologies ou de plateformes qu'ils ne maîtrisent pas**. Lorsqu'un État ne peut plus déployer une politique publique sans recourir à des services soumis à des cadres juridiques étrangers ou à des décisions unilatérales d'acteurs privés, sa souveraineté est de facto affaiblie.

Enfin, la souveraineté numérique suppose une **capacité d'influence dans la définition des standards techniques et réglementaires internationaux**. Les standards façonnent les marchés, conditionnent l'interopérabilité et créent des dépendances durables. Être absent de ces espaces de normalisation revient à accepter des dépendances structurelles sur le long terme.

Cette clarification est essentielle pour éviter deux écueils majeurs : d'une part, les effets de communication ou de « *sovereignty washing* », où des initiatives sont labellisées souveraines sans répondre à des critères précis ; d'autre part, les injonctions contradictoires adressées aux organisations, sommées d'être à la fois innovantes, compétitives, conformes et souveraines, sans cadre clair pour arbitrer.

Il est également important de reconnaître que la souveraineté numérique ne se décline pas de manière uniforme. Chaque organisation, publique ou privée, doit pouvoir s'approprier cette notion, définir son propre niveau de dépendance acceptable et identifier les indépendances indispensables à son fonctionnement. Dans cette perspective, l'Indice de Résilience Numérique (IRN) fournit un cadre commun permettant d'objectiver ces arbitrages, de mesurer les dépendances réelles et d'inscrire la souveraineté numérique dans une logique opérationnelle et pilotable, à l'échelle nationale comme européenne.





**L'INDICE DE RÉSILIENCE NUMÉRIQUE (IRN)**

**Mesurons le niveau de dépendance technologique de nos organisations, et reprenons notre destin numérique en main.**

Face à la concentration croissante des chaînes de valeur numériques (*Cloud*, données, logiciels, IA, infrastructures critiques), la question centrale n'est plus celle d'une souveraineté abstraite, mais celle de la capacité réelle des organisations à continuer d'opérer en situation de contrainte, de rupture ou de dépendance critique. C'est à cette problématique concrète que répond l'Indice de Résilience Numérique (IRN).

L'IRN est un standard ouvert de mesure conçu pour évaluer, de manière systémique et comparable, le niveau de résilience numérique d'une organisation, entreprise, acteur public ou opérateur d'infrastructure critique. Il vise à objectiver les dépendances technologiques, juridiques, économiques et opérationnelles qui structurent aujourd'hui les systèmes d'information et les chaînes de valeur numériques.

Contrairement aux approches centrées exclusivement sur la cybersécurité ou la conformité réglementaire, l'IRN adopte une lecture transversale de la résilience, intégrant à la fois :

- les dépendances aux fournisseurs et aux technologies critiques (*Cloud*, logiciels, IA, données, infrastructures).
- les capacités de maîtrise, de réversibilité et de continuité d'activité.
- les enjeux de gouvernance, de conformité réglementaire (DORA, NIS2, *Data Act, AI Act*) et de responsabilité.
- l'inscription de l'organisation dans des écosystèmes de confiance interopérables, notamment au sein des *data spaces* européens.

L'indice repose sur une méthodologie structurée autour de piliers et de critères publics, élaborée de manière collaborative avec des acteurs publics, industriels, académiques et institutionnels. Cette méthodologie permet de produire :

- un score global de résilience numérique.
- une analyse fine par grands domaines de dépendance.
- des trajectoires de progrès opérationnelles, adaptées au contexte sectoriel et à la maturité de chaque organisation.

La gouvernance de l'IRN est assurée par l'association *Digital Resilience Initiative*, structure indépendante de type « association de place », présidée par Olivier Sichel, directeur général de la Caisse des Dépôts et président de Digital New Deal. Elle garantit l'ouverture, la neutralité, la robustesse méthodologique et l'évolution du standard dans la durée.

L'initiative a été lancée conjointement par David Djaïz, Yann Lechelle et Arno Pons (Digital New Deal), avec l'ambition de doter les acteurs économiques et publics d'un outil concret pour piloter la résilience numérique comme un enjeu de continuité stratégique, au même titre que l'énergie, les chaînes d'approvisionnement ou la finance.

En faisant de la mesure un préalable à l'action, l'Indice de Résilience Numérique constitue un socle commun de langage, de comparaison et de pilotage, destiné à transformer la puissance normative européenne en capacités opérationnelles durables.

# 7.2. Réinvestir dans les capacités stratégiques

La maîtrise des dépendances numériques suppose un **réinvestissement ciblé dans certaines capacités stratégiques**, identifiées comme critiques pour la résilience collective. Il ne s'agit ni de tout internaliser ni de reconstruire intégralement des filières complètes, mais d'identifier les maillons où une dépendance totale serait inacceptable.

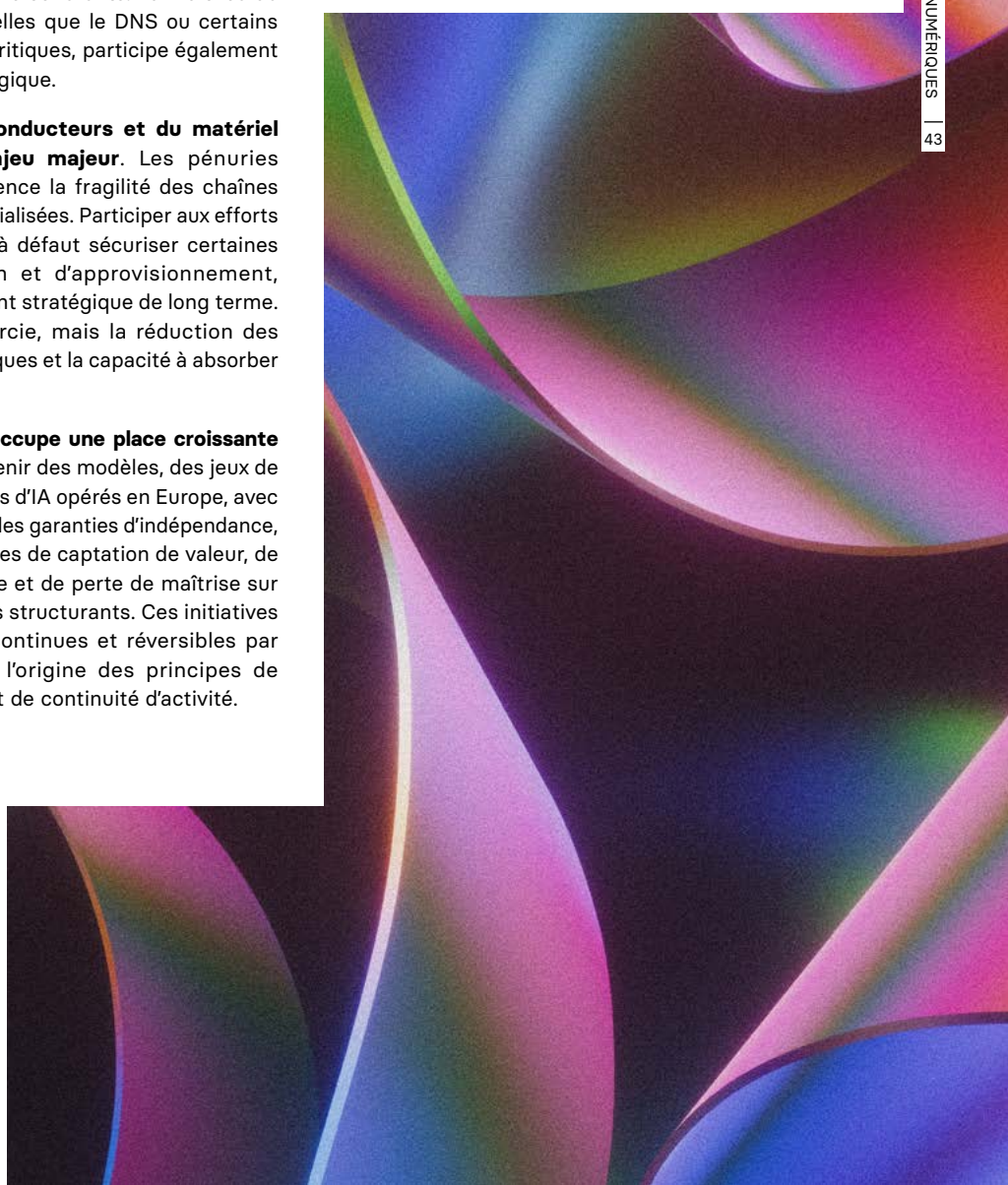
**Les infrastructures de *Cloud* et de calcul constituent un premier domaine clé**. Soutenir des offres de *Clouds* de confiance, de *Clouds* souverains ou de *Clouds* sectoriels permet de proposer des alternatives crédibles aux acteurs dominants, notamment pour les usages sensibles ou critiques. Ces initiatives gagnent à s'inscrire dans des modèles de fédération et d'interopérabilité, évitant la reproduction de silos nationaux et favorisant des écosystèmes européens cohérents. La maîtrise de briques fondamentales, telles que le DNS ou certains services d'infrastructure critiques, participe également de cette autonomie stratégique.

**Le domaine des semi-conducteurs et du matériel représente un autre enjeu majeur**. Les pénuries récentes ont mis en évidence la fragilité des chaînes d'approvisionnement mondialisées. Participer aux efforts de réindustrialisation, ou à défaut sécuriser certaines capacités de production et d'approvisionnement, constitue un investissement stratégique de long terme. L'objectif n'est pas l'autarcie, mais la réduction des dépendances les plus critiques et la capacité à absorber des chocs externes.

**L'intelligence artificielle occupe une place croissante dans cette réflexion**. Soutenir des modèles, des jeux de données et des plateformes d'IA opérés en Europe, avec une gouvernance claire et des garanties d'indépendance, permet de limiter les risques de captation de valeur, de dépendance technologique et de perte de maîtrise sur des usages de plus en plus structurants. Ces initiatives doivent être pensées « continues et réversibles par design », intégrant dès l'origine des principes de portabilité, d'auditabilité et de continuité d'activité.

Dans l'ensemble de ces domaines, la logique n'est pas de substituer systématiquement des solutions locales à des solutions globales, mais de **rééquilibrer les rapports de force** en créant des **alternatives crédibles**, soutenables et compatibles avec les exigences opérationnelles des acteurs publics et privés.

Toutefois, ces investissements ne prennent pleinement sens que s'ils s'inscrivent dans des modèles de partage et de gouvernance évitant la reconstitution de nouvelles dépendances, en particulier autour des données et de l'intelligence artificielle. C'est dans cette logique que s'inscrit l'approche des *data spaces* portée par Digital New Deal.



**LES *DATA SPACES* SELON DIGITAL NEW DEAL**

**Une infrastructure de partage de données et de gouvernance, socle des intelligences artificielles de confiance**

Pour Digital New Deal, un *data space* est, en résumé, à la fois une infrastructure de partage de données et un cadre de gouvernance. Il ne s'agit pas uniquement de technologies, mais d'un modèle organisationnel permettant à des acteurs publics et privés de coopérer autour de données tout en évitant leur centralisation et l'enfermement de la valeur.

À ce titre, les *data spaces* constituent aujourd'hui la meilleure alternative opérationnelle aux modèles intégrés des *hyperscalers*, dont les offres combinant *Cloud*, données et IA tendent à créer des silos technologiques et économiques. Là où ces modèles reposent sur la centralisation des données et la captation de la valeur, les *data spaces* proposent une gouvernance décentralisée, fondée sur des règles partagées, des standards ouverts et la maîtrise des usages par les producteurs de données.

Un *data space* repose sur trois principes structurants :

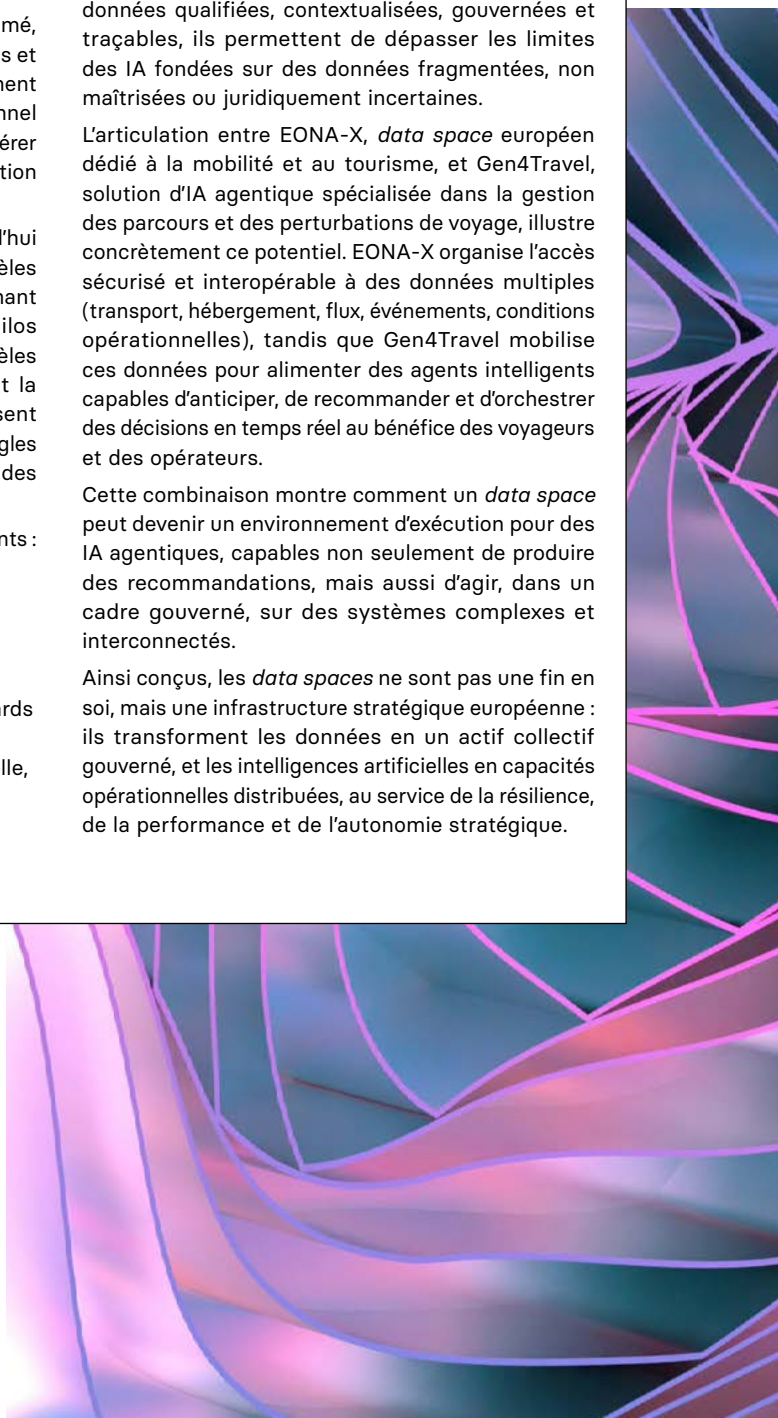
- la souveraineté d'usage, chaque acteur conservant le contrôle des conditions d'accès, d'exploitation et de réversibilité de ses données.
- l'interopérabilité, fondée sur des standards ouverts et des référentiels communs.
- la confiance juridique et organisationnelle, intégrant conformité réglementaire, traçabilité et responsabilité.

Dans cette approche, les *data spaces* constituent le socle indispensable au déploiement d'intelligences artificielles de confiance, en particulier des IA génératives et agentiques. En fournissant des données qualifiées, contextualisées, gouvernées et traçables, ils permettent de dépasser les limites des IA fondées sur des données fragmentées, non maîtrisées ou juridiquement incertaines.

L'articulation entre EONA-X, *data space* européen dédié à la mobilité et au tourisme, et Gen4Travel, solution d'IA agentique spécialisée dans la gestion des parcours et des perturbations de voyage, illustre concrètement ce potentiel. EONA-X organise l'accès sécurisé et interopérable à des données multiples (transport, hébergement, flux, événements, conditions opérationnelles), tandis que Gen4Travel mobilise ces données pour alimenter des agents intelligents capables d'anticiper, de recommander et d'orchestrer des décisions en temps réel au bénéfice des voyageurs et des opérateurs.

Cette combinaison montre comment un *data space* peut devenir un environnement d'exécution pour des IA agentiques, capables non seulement de produire des recommandations, mais aussi d'agir, dans un cadre gouverné, sur des systèmes complexes et interconnectés.

Ainsi conçus, les *data spaces* ne sont pas une fin en soi, mais une infrastructure stratégique européenne : ils transforment les données en un actif collectif gouverné, et les intelligences artificielles en capacités opérationnelles distribuées, au service de la résilience, de la performance et de l'autonomie stratégique.



# 7.3. Réguler, mais de manière opérable – une dépendance maîtrisée

L'Europe s'est dotée ces dernières années d'un ensemble dense de cadres réglementaires (RGPD, DSA, DMA, NIS2, DORA, *AI Act,* CRA ...) visant à encadrer les usages numériques, protéger les données et **limiter certaines formes de dépendance**. Ces réglementations peuvent contribuer à réduire les abus de position dominante, **à imposer des obligations de transparence et de responsabilité**, et à renforcer la sécurité des services essentiels.

Toutefois, les retours de terrain soulignent la nécessité de rendre cette régulation plus lisible et plus opérable. Une complexité excessive ou une instabilité réglementaire peuvent paradoxalement **renforcer les acteurs déjà dominants, seuls capables d'absorber les coûts de conformité** et d'adapter rapidement leurs organisations. **Les acteurs plus petits**, pourtant essentiels à la diversité de l'écosystème, **se retrouvent alors pénalisés**.

L'enjeu consiste donc à compatibiliser plusieurs objectifs parfois perçus comme antagonistes : souveraineté, innovation, compétitivité et protection des droits. Une régulation efficace doit fixer des principes clairs, stables et proportionnés, tout en laissant des marges d'expérimentation et d'adaptation. Elle doit également s'accompagner de mécanismes de soutien et d'accompagnement, afin que les **exigences réglementaires ne deviennent pas elles-mêmes un facteur de dépendance.**

Les réglementations européennes NIS2, DORA et le *Cyber Resilience Act* (CRA) constituent des avancées importantes pour renforcer la cybersécurité et la résilience opérationnelle du tissu économique européen. Elles imposent des exigences accrues en matière de gestion des risques, de sécurité des chaînes d'approvisionnement, de gouvernance des tiers et de capacités de réponse aux incidents.

Toutefois, ces cadres traitent principalement de **l'événement redouté « incident cyber »** – compromission, indisponibilité, perte d'intégrité ou de confidentialité – et n'adressent que de manière indirecte **l'événement redouté « dépendance numérique »**, entendu comme l'incapacité structurelle à maintenir ou rétablir une fonction critique en raison d'une dépendance technologique, juridique, organisationnelle ou géopolitique.

NIS2 s'inscrit ainsi dans une logique de protection des services essentiels, DORA dans une approche continue de résilience opérationnelle du secteur financier, et le CRA dans une sécurisation des produits numériques tout au long de leur cycle de vie. Ces approches, bien que légitimes, visent prioritairement l'élévation du niveau de sécurité face à des menaces cyber, y compris opportunistes, plutôt que la réduction explicite des dépendances structurelles.

D'autres textes européens contribuent plus directement à cette problématique. Le ***European Chips Act*** traite la dépendance industrielle en soutenant le développement de capacités européennes en matière de semi-conducteurs, afin de sécuriser des chaînes d'approvisionnement stratégiques. Le ***EU Data Act*** agit quant à lui sur les dépendances opérationnelles et contractuelles, en facilitant la portabilité des données et le changement de fournisseur *Cloud*, afin de limiter les situations de verrouillage.

La Directive REC *(Critical Entities Resilience)*, quant à elle, apparaît plus directement alignée avec la problématique de la dépendance numérique. Elle introduit explicitement la prise en compte, dans l'analyse des risques, des **dépendances et interdépendances entre secteurs et entités critiques**, y compris vis-à-vis des États membres voisins et des pays tiers. Appliquée aux entités relevant de NIS2, elle ouvre la voie à une approche plus systémique de la résilience. L'enjeu devient alors l'articulation cohérente de ces cadres afin de traiter, au-delà de l'incident cyber, les vulnérabilités structurelles liées aux dépendances numériques.

# 7.4. Orienter le marché pour réduire les dépendances numériques critiques

Dans la logique défendue par le CESIN, orienter le marché vers des solutions et services numériques ne dépendant pas de contextes extra-européens ne relève ni d'un protectionnisme idéologique ni d'une recherche illusoire d'indépendance totale. Il s'agit d'une démarche pragmatique visant à **réduire des dépendances jugées incompatibles avec la continuité de l'action publique, la responsabilité démocratique et la capacité de décision des États.**

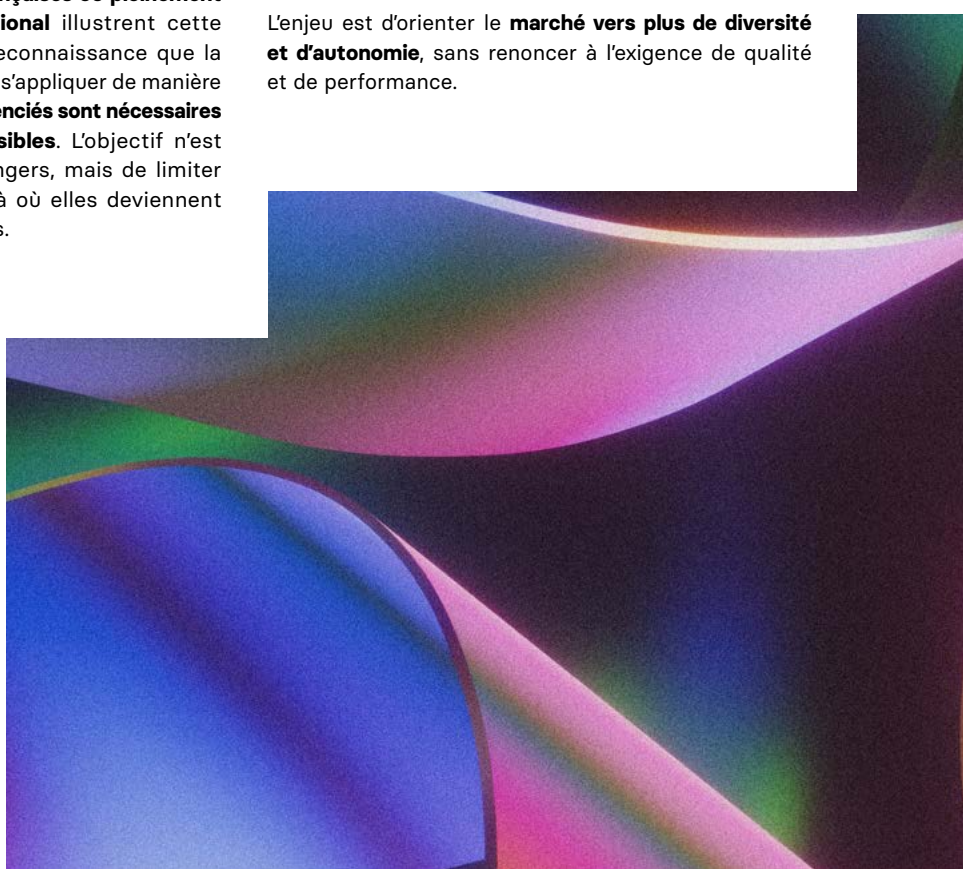
Certaines fonctions numériques sont devenues des **socles critiques** du fonctionnement des administrations et des services essentiels : communication et collaboration, visioconférence, identité numérique, hébergement et traitement des données, cybersécurité, *Cloud* ou intelligence artificielle appliquée aux missions régaliennes. Lorsqu'elles reposent sur des solutions soumises à des cadres juridiques, réglementaires ou politiques extra-européens, les risques dépassent la seule dimension technologique : extraterritorialité du droit, décisions unilatérales de fournisseurs dominants, concentration excessive des usages et impossibilité de reprise en main en situation de crise.

Les orientations récentes imposant, pour certaines administrations et certains usages, le recours à des **solutions de visioconférence françaises ou pleinement maîtrisées dans un cadre national** illustrent cette évolution. Elles traduisent la reconnaissance que la neutralité technologique ne peut s'appliquer de manière uniforme, et que **des choix différenciés sont nécessaires sur les fonctions les plus sensibles**. L'objectif n'est pas d'exclure des acteurs étrangers, mais de limiter des dépendances excessives là où elles deviennent structurellement problématiques.

Dans ce contexte, la **commande publique constitue un levier central**. Par le volume des achats et par l'exemplarité qu'elle incarne, elle permet de traduire ces orientations stratégiques en dynamiques de marché concrètes. On observe une tendance croissante à intégrer des critères de souveraineté, de réversibilité et d'ouverture des standards dans les appels d'offres. Cette évolution envoie progressivement un signal aux fournisseurs, tout en maintenant les exigences de qualité, de sécurité et de performance. De même, l'idée d'allouer une part des marchés à des acteurs européens ou locaux, ou d'expérimenter des solutions ouvertes, des *Clouds* de confiance ou des modèles d'IA maîtrisés, s'installe dans le débat public et institutionnel. Ces orientations, encore inégalement mises en œuvre, visent à structurer à terme un écosystème plus diversifié et plus résilient.

**Allouer une part des marchés à des acteurs européens ou locaux**, dans une logique inspirée de mécanismes de type *European Business Act* ou *Small Business Act*, peut également contribuer à structurer un tissu industriel plus diversifié. **L'expérimentation par les administrations de solutions ouvertes**, de *Cloud*s de confiance ou de **modèles d'IA maîtrisés** permet également de réduire l'aversion au risque et de démontrer la faisabilité de trajectoires alternatives.

L'enjeu est d'orienter le **marché vers plus de diversité et d'autonomie**, sans renoncer à l'exigence de qualité et de performance.



# 7.5. Soutenir les communs numériques et l'open source

**Une part importante de l'infrastructure numérique mondiale repose sur des logiciels libres**, des standards ouverts et des communs numériques. Systèmes d'exploitation, serveurs web, bibliothèques cryptographiques, *middlewares*, outils de développement ou *frameworks* d'intelligence artificielle constituent les briques de base de la quasi-totalité des services numériques modernes, y compris ceux opérés par les plus grandes plateformes mondiales. **Pourtant, ces composants essentiels demeurent sous estimés dans les politiques industrielles.**

Cet état de fait s'accompagne de fragilités structurelles. De nombreux projets open source critiques **sont souvent sous-financés**, leur maintenance reposant sur un nombre très limité de contributeurs, parfois bénévoles. Cette situation crée un paradoxe : des infrastructures utilisées à l'échelle planétaire reposent sur des ressources humaines et financières extrêmement contraintes. Les incidents récents liés à la *supply chain* logicielle ont démontré que la compromission ou l'abandon d'un composant open source pouvait avoir des conséquences systémiques, bien au-delà de son périmètre apparent.

Trois incidents ont rappelé que des **briques *open source* discrètes ou non connues** peuvent devenir des dépendances critiques à l'échelle mondiale.

En **2014, Heartbleed (OpenSSL)** a montré que le chiffrement du web reposait sur une bibliothèque essentielle, **sous-financée et sous-maintendue**. Avec le recul, cet épisode illustre aussi qu'une mobilisation collective (financement, audits, gouvernance) peut renforcer durablement un commun critique.

En **2021, Log4j / Log4Shell** a révélé l'ampleur des **dépendances**: une bibliothèque de journalisation, intégrée partout (souvent sans visibilité), est devenue une vulnérabilité majeure touchant des milliers d'organisations, y compris via des logiciels tiers.

En **2025**, la tentative d'injection de ***backdoor* dans liblzma/xz** a confirmé le risque : une bibliothèque perçue comme secondaire s'est révélée suffisamment stratégique pour menacer des environnements serveurs critiques avant d'être détectée.

Dans ce contexte, le soutien aux communs numériques ne relève pas d'une posture idéologique, mais d'un **choix stratégique de résilience**. Financer durablement certains communs critiques – en particulier dans les domaines de la cryptographie, des systèmes d'exploitation, des serveurs, des *middlewares* ou des *frameworks* d'IA – permet de réduire des dépendances silencieuses mais profondes. Il s'agit moins de créer de nouveaux projets que de renforcer ceux qui sont déjà au cœur de l'écosystème numérique mondial.

Les **politiques publiques** disposent de plusieurs leviers pour agir. Le financement direct et pérenne de projets identifiés comme critiques constitue une première étape, à condition qu'il s'inscrive dans une **logique de long terme** et non dans des appels à projets ponctuels. Encourager les **administrations et les entreprises publiques à contribuer activement**, par du code, des audits de sécurité ou un soutien financier, permet également de renforcer ces communs tout en développant des compétences internes. Enfin, promouvoir des **modèles de gouvernance ouverts, inclusifs et transparents** garantit que ces communs restent des espaces partagés, résistants aux captations d'intérêts particuliers.

Soutenir les communs numériques, c'est ainsi investir dans une infrastructure collective qui **réduit la dépendance à des solutions propriétaires fermées**, tout en renforçant la sécurité, l'interopérabilité et la souveraineté de long terme.

# 7.6. Développer les compétences, la culture numérique et la sensibilisation à la dépendance numérique

La maîtrise des dépendances numériques ne peut être atteinte sans un effort structuré et durable de formation et de sensibilisation. Les dépendances ne résultent pas uniquement de choix techniques complexes, mais très souvent de décisions prises par des acteurs insuffisamment outillés pour en percevoir les implications à moyen et long terme. Former ne consiste donc pas seulement à transmettre des compétences techniques, mais à développer une **capacité collective de lecture critique** des choix numériques.

**Chez les ingénieurs et les professionnels du numérique**, la formation doit dépasser la maîtrise des outils et des plateformes. Elle doit intégrer une compréhension des architectures globales, des mécanismes de dépendance induits par certaines technologies (*Cloud*, SaaS, IA, services managés), ainsi que des enjeux juridiques et géopolitiques qui conditionnent l'usage de ces technologies. Par exemple, un architecte capable d'évaluer l'impact d'une architecture *serverless* sur la réversibilité ou d'anticiper les effets d'un verrouillage contractuel contribue directement à la réduction des dépendances structurelles.

**La sensibilisation des dirigeants** constitue un levier tout aussi déterminant. La dépendance numérique est fréquemment le produit d'arbitrages stratégiques orientés par des critères de coût, de rapidité ou de performance apparente, sans évaluation explicite des risques de dépendance. Développer une culture du risque numérique chez les décideurs permet d'introduire des questions structurantes dans les processus de décision : que se passe-t-il si un fournisseur devient indisponible, change ses conditions économiques ou se trouve soumis à une contrainte juridique externe ? Des dispositifs de sensibilisation, tels que des ateliers de scénarios de rupture ou des exercices de crise intégrant des dépendances numériques, ont démontré leur efficacité pour rendre ces risques tangibles.

**Les citoyens constituent enfin un maillon essentiel de cette chaîne de sensibilisation**. L'éducation au numérique, à l'information et aux algorithmes permet de mieux comprendre les logiques de plateforme, les mécanismes de recommandation ou la captation des données. Par exemple, comprendre pourquoi un service gratuit peut créer une dépendance durable ou comment des algorithmes influencent les usages et les comportements contribue à renforcer l'autonomie individuelle et, par extension, la résilience collective.

Sans cette montée en compétence et cette sensibilisation à tous les niveaux, **la tentation restera forte de privilégier le chemin de moindre résistance** : celui des solutions clés en main proposées par quelques acteurs dominants. À court terme, ces solutions répondent à des besoins réels ; à long terme, elles peuvent enfermer les organisations et les sociétés dans des dépendances croissantes, difficiles à remettre en cause. Développer une culture partagée de la dépendance numérique constitue ainsi un investissement essentiel pour préserver la capacité de choix, d'innovation et de souveraineté.

# 7.7. Nouer des alliances et coopérations internationales

Aucun État européen ne dispose, seul, des capacités industrielles, financières et technologiques nécessaires pour rééquilibrer les rapports de force numériques mondiaux. La **coopération internationale**, en particulier entre démocraties partageant des valeurs et des cadres juridiques proches, apparaît donc comme un enjeu central.

Ces coopérations peuvent prendre plusieurs formes. La **définition de standards partagés** permet de favoriser l'interopérabilité, de limiter les effets de verrouillage et de peser collectivement dans les instances internationales de normalisation. Le **développement d'infrastructures interopérables**, qu'il s'agisse de *Cloud*, de données ou de services numériques publics, permet de mutualiser les investissements tout en réduisant les dépendances à des acteurs extérieurs. Les **programmes conjoints de recherche et développement** renforcent quant à eux la capacité d'innovation et la maîtrise de technologies émergentes.

La réciprocité constitue un principe clé de ces alliances. **Coopérer en matière de données, de régulation ou de protection des droits** suppose des engagements équilibrés et transparents, afin d'éviter des asymétries durables. L'objectif n'est pas de créer de nouveaux blocs fermés, mais de bâtir des écosystèmes ouverts, capables de coopérer sans perdre leur capacité de décision.

Ces alliances doivent toutefois être conçues avec lucidité. La coopération internationale n'exonère pas d'une vigilance constante sur les rapports de force, les dépendances créées et les trajectoires technologiques induites. Une dépendance peut en remplacer une autre si elle n'est pas explicitement analysée et gouvernée.

# CONCLUSION
# Vers une autonomie numérique choisie, mesurée et gouvernée

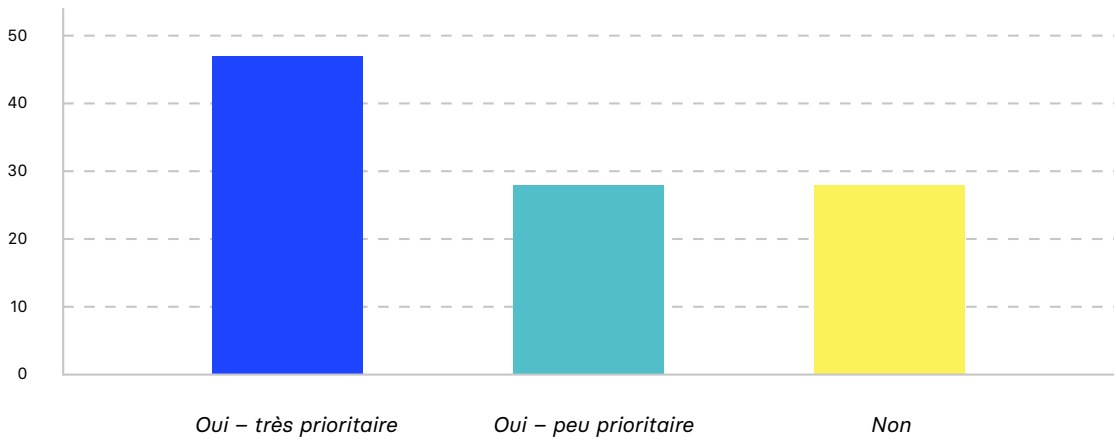
Ce livre blanc s'est construit autour d'un constat désormais partagé par les RSSI, les décideurs publics et les acteurs du numérique : la dépendance numérique n'est ni un accident, ni une anomalie, ni un échec individuel. Elle est le produit logique d'un modèle de transformation numérique fondé sur la recherche d'efficacité, de rapidité et de mutualisation, dans un environnement globalisé et fortement concentré. La question n'est donc pas de savoir s'il faudrait sortir de toute dépendance, mais de déterminer lesquelles sont acceptables, lesquelles deviennent critiques, et à quelles conditions elles peuvent être maîtrisées dans le temps.

L'enjeu fondamental réside dans la capacité à conserver des marges de manœuvre réelles : comprendre ses dépendances, les rendre visibles, les relier aux fonctions critiques, et disposer de chemins de repli crédibles lorsque les équilibres économiques, juridiques ou géopolitiques se dégradent. Dans un monde numérique profondément interconnecté, l'autonomie ne se décrète pas ; elle se construit comme une capacité dynamique, faite de choix explicites, d'arbitrages assumés et de gouvernance continue.

***« Dans un contexte où le numérique est devenu un levier de puissance géopolitique, la dépendance technologique constitue un risque stratégique pour les organisations. La prise de conscience de ces enjeux est une formidable opportunité pour renforcer la résilience, restaurer des marges de manœuvre et développer des écosystèmes français et européens capables de soutenir une innovation durable et maîtrisée. »***

— Orion RAGOZIN
Membre du CESIN

**La maîtrise des dépendances numériques fait-elle partie de vos missions ?**
**SONDAGE CESIN (150 RÉPONSES)**




**La réduction des dépendances numériques est identifiée comme faisant partie de la mission du RSSI.**

À l'échelle des organisations, et en particulier du point de vue des RSSI, la dépendance numérique ne peut plus être traitée comme un sujet périphérique ou uniquement technique. Elle touche directement à la continuité d'activité, à la soutenabilité économique des modèles IT, à la conformité réglementaire dans la durée et, plus largement, à la liberté de décision de l'entreprise ou de l'administration. Le RSSI voit ainsi son rôle évoluer : au-delà de la prévention et de la réponse aux incidents cyber, il devient un acteur central de la lucidité stratégique, capable de relier des choix technologiques apparemment rationnels à leurs conséquences structurelles de long terme.

Cette montée en responsabilité suppose un décloisonnement profond des fonctions. La maîtrise des dépendances numériques ne relève ni du RSSI seul, ni de la DSI, ni des achats ou du juridique pris isolément. Elle exige une approche transversale, intégrée à la gouvernance des risques, où les décisions technologiques sont mises en regard des enjeux contractuels, réglementaires, financiers et géopolitiques. Dans ce contexte, accepter qu'une dépendance soit un **choix stratégique explicite**, documenté et piloté, constitue un signe de maturité bien plus fort que l'illusion d'un contrôle total.

***« Le RSSI ne se limite pas seulement à protéger des systèmes. Il aide l'organisation à comprendre ses dépendances, à en mesurer les risques et à garder des marges de manœuvre. En reliant technique, métiers et gouvernance, il fait de la dépendance numérique un sujet de décision »***

— Eric SINGER
Membre du CESIN

C'est précisément pour sortir d'une approche abstraite ou idéologique de la souveraineté numérique que des outils de mesure deviennent indispensables. L'Indice de Résilience Numérique (IRN) s'inscrit dans cette logique. En objectivant les dépendances technologiques, juridiques, économiques et opérationnelles, il permet aux organisations comme aux pouvoirs publics de qualifier leur niveau réel de résilience, d'identifier les concentrations critiques et de piloter des trajectoires de progrès. Mesurer devient alors un acte de gouvernance : non pour comparer ou sanctionner, mais pour éclairer les arbitrages et sortir du pilotage à l'intuition.

À l'échelle macro, la dépendance numérique pose une question politique au sens plein du terme : celle de la capacité collective à décider, à agir et à garantir la continuité des fonctions essentielles dans un environnement numérique dominé par des acteurs globaux. Les États et l'Union européenne ne peuvent se limiter à une régulation a posteriori de marchés déjà structurés par des effets d'échelle massifs. Ils doivent clarifier leur ambition de souveraineté numérique comme une **capacité d'action durable**, reposant sur des infrastructures critiques maîtrisées, des compétences, des communs numériques solides et une capacité d'influence sur les standards.

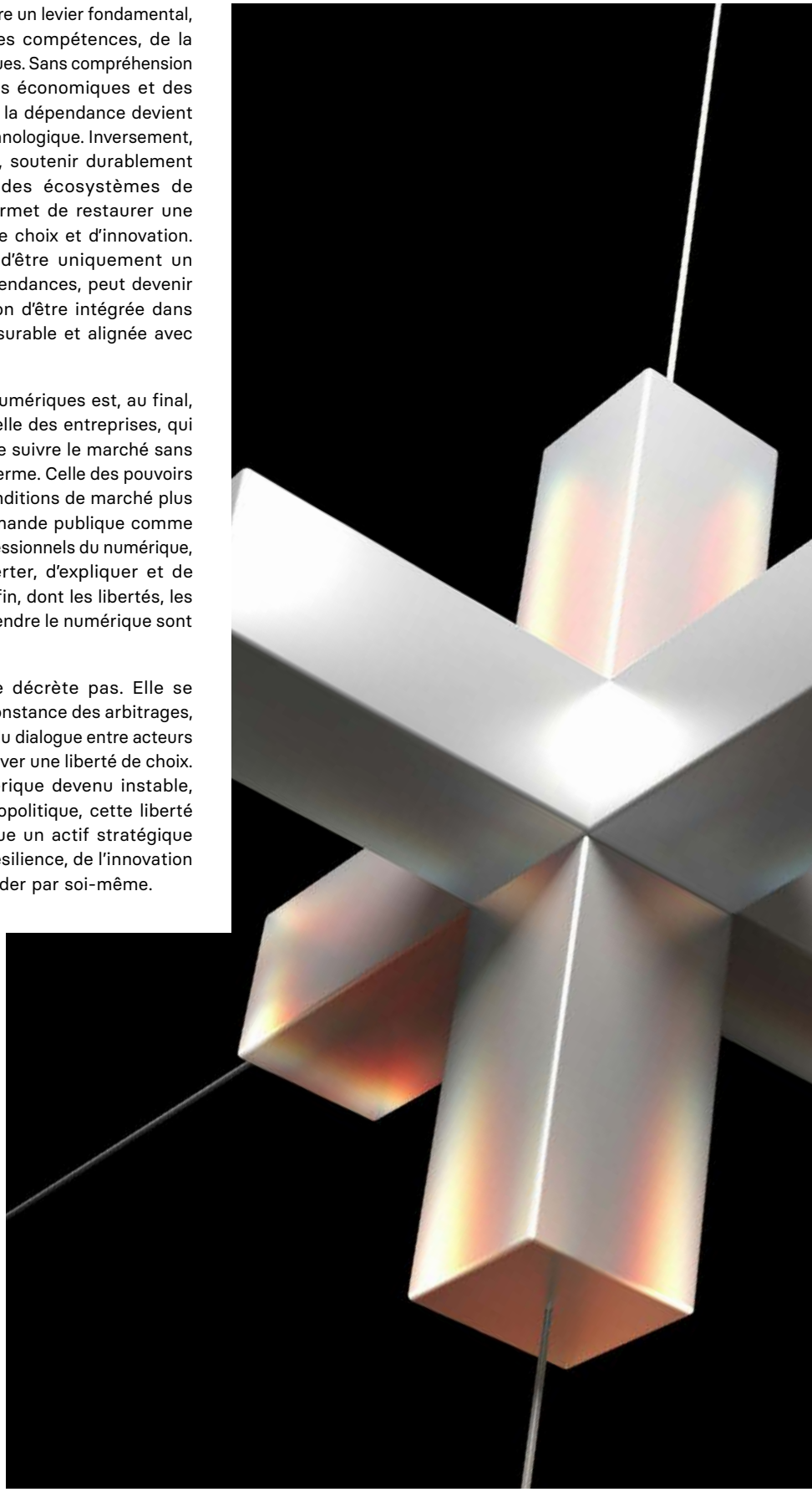
Dans cette perspective, l'approche des *data spaces,* telle que portée par Digital New Deal, ouvre une voie structurante. En organisant le partage des données autour de règles de gouvernance explicites, de standards ouverts et d'une souveraineté d'usage, les *data spaces* constituent une alternative crédible aux modèles de plateformisation intégrée. Ils permettent de coopérer sans centraliser, d'innover sans capturer la valeur, et de développer des intelligences artificielles de confiance sans créer de nouvelles dépendances systémiques. Ils incarnent une vision européenne de l'interdépendance : choisie, réversible et gouvernée.

Les cadres réglementaires européens – NIS2, DORA, CRA, *AI Act* – contribuent à renforcer la sécurité et la résilience face aux incidents cyber, mais montrent leurs limites lorsqu'ils abordent la dépendance uniquement sous l'angle de l'événement technique. La directive sur la résilience des entités critiques marque une évolution importante en intégrant explicitement la notion de dépendances et d'interdépendances. L'enjeu, désormais, est d'articuler ces cadres de manière cohérente afin de traiter non seulement les incidents, mais aussi les vulnérabilités structurelles de long terme.

Enfin, ce livre blanc met en lumière un levier fondamental, souvent sous-estimé : celui des compétences, de la culture et des communs numériques. Sans compréhension des architectures, des modèles économiques et des cadres juridiques sous-jacents, la dépendance devient cognitive avant même d'être technologique. Inversement, investir dans les compétences, soutenir durablement l'open source et structurer des écosystèmes de données et d'IA gouvernés permet de restaurer une capacité collective d'analyse, de choix et d'innovation. L'intelligence artificielle, loin d'être uniquement un facteur d'amplification des dépendances, peut devenir un outil de maîtrise, à condition d'être intégrée dans une gouvernance explicite, mesurable et alignée avec les valeurs démocratiques.

La maîtrise des dépendances numériques est, au final, une responsabilité partagée. Celle des entreprises, qui ne peuvent plus se contenter de suivre le marché sans en mesurer les risques de long terme. Celle des pouvoirs publics, appelés à créer des conditions de marché plus équilibrées et à utiliser la commande publique comme levier stratégique. Celle des professionnels du numérique, qui ont la responsabilité d'alerter, d'expliquer et de proposer. Celle des citoyens enfin, dont les libertés, les données et la capacité à comprendre le numérique sont directement en jeu.

L'autonomie numérique ne se décrète pas. Elle se construit dans la durée, par la constance des arbitrages, la capacité à mesurer, la qualité du dialogue entre acteurs et la volonté collective de préserver une liberté de choix. Dans un environnement numérique devenu instable, concentré et profondément géopolitique, cette liberté n'est pas un luxe : elle constitue un actif stratégique essentiel, au fondement de la résilience, de l'innovation durable et de la capacité à décider par soi-même.



# Résumé en 5 points

**Le CESIN contribue au débat sur la souveraineté technologique en rappelant les 5 piliers de progrès incontournables :**

1. **Autonomie choisie, ni indépendance totale ni résignation.** L'objectif est une autonomie numérique lucide, négociée et réversible – entre l'illusion d'indépendance totale et la dépendance subie comme prix de l'innovation.

2. **Évolution du rôle du RSSI.** Le RSSI doit élargir son champ au-delà de la cybersécurité : continuité d'activité, risques juridiques, géopolitiques. De part son savoir technologique, son implication dans le projet d'entreprise (y compris du service public non marchand), son lien avec les métiers et les écosystèmes de partenaires, sa connaissance des acteurs, sa vue sur la réalité des opérations, il contribue à la définition interne des dépendances et au plan d'autonomie choisie.

3. **Responsabilités des pouvoirs publics.** Clarifier l'ambition de souveraineté en politiques concrètes, rendre la réglementation opérable, utiliser la commande publique comme levier stratégique, et soutenir les communs numériques et l'open source.

4. **Responsabilité partagée et trajectoire continue.** L'autonomie numérique est une responsabilité collective (entreprises, États, professionnels, citoyens) et une trajectoire à piloter en permanence – pas un état stable à atteindre.

5. **L'autonomie choisie n'est pas un combat et ne contribue à aucun projet politique.** Elle résulte d'un équilibre complexe entre l'existant, la dette technologique des entreprises, la capacité d'innovation et de pérennité des solutions alternatives à l'existant, les politiques publiques industrielles, l'exemplarité des donneurs d'ordre publics, la mise en place des contrôles transparents sur toutes les géographies, la réversibilité et la discussion contractuelle.

***« La souveraineté numérique, ce n'est ni l'indépendance totale ni la résignation : c'est une autonomie choisie, collective et pilotée dans la durée. »***

— Eric DOMAGE
PAC Analyst

# Maîtriser nos dépendances numériques

IN CYBER FORUM EUROPE

*en partenariat avec*

CESIN

**MARS 2026**

Le numérique est devenu l'infrastructure invisible de nos organisations, de nos économies et de nos démocraties.

*Cloud*, plateformes, IA, composants critiques : nos choix technologiques façonnent désormais notre liberté d'action.

Ce livre blanc repose sur une conviction simple : la question n'est pas d'éliminer toute dépendance, mais de la rendre visible, arbitrable et gouvernée.

Il invite à adopter 6 postures clés :

**1. Reconnaître la dépendance comme un risque systémique**

La dépendance numérique n'est pas un simple enjeu technique. Elle affecte la continuité d'activité, la protection des données, la résilience économique et la souveraineté décisionnelle.

**2. Passer d'une dépendance subie à une dépendance gouvernée**

L'objectif n'est ni l'autarcie ni le rejet du *Cloud* ou de l'IA, mais la lucidité : rendre visibles les dépendances, les hiérarchiser et intégrer la réversibilité dans les architectures et les contrats.

**3. Élargir le rôle du RSSI et des fonctions risques**

Le RSSI devient un acteur stratégique, capable de relier choix technologiques, résilience opérationnelle et enjeux géopolitiques.

**4. Articuler régulation et stratégie industrielle**

La cybersécurité ne suffit pas. La maîtrise des dépendances suppose des politiques publiques cohérentes, des capacités industrielles critiques et une régulation opérable.

**5. Soutenir les communs numériques et les compétences**

*Open source,* standards ouverts, formation et culture numérique sont des leviers structurants de résilience collective.

**6. Coopérer sans recréer de nouvelles dépendances**

Les alliances entre démocraties sont nécessaires, mais doivent préserver la capacité de choix et éviter de nouvelles asymétries.