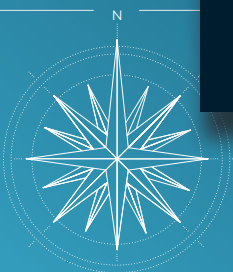
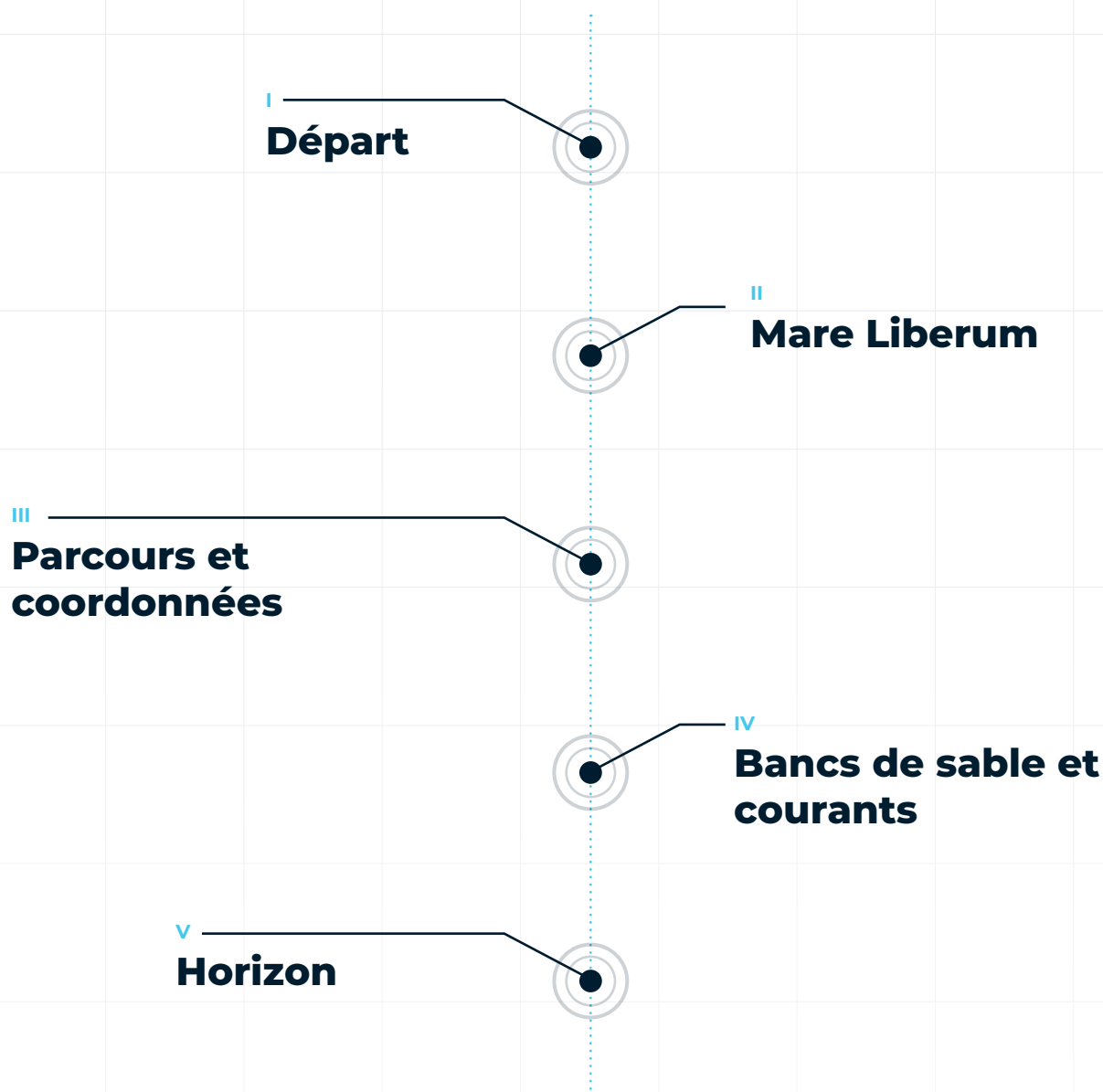




ÉTAT DE LA SOUVERAINETÉ NUMÉRIQUE EN 2026

Des eaux inexplorées





Sommaire

I Départ	3	IV Bancs de sable et courants	17
À propos de cette étude	4	Les nouvelles routes commerciales de l'Europe :	
Avant-propos : Prendre les commandes	5	Là où la souveraineté est la plus nécessaire	18
Résumé : Les principaux résultats en un coup d'œil	7	Les obstacles à la migration :	
II Mare Liberum	9	Pourquoi il reste difficile de changer de cap	20
Mare Liberum : de la mer libre au réseau libre	10	Le CLOUD Act, un signe avant-coureur :	
III Cours et coordonnées	11	entre attente et action	22
L'Allemagne : comparaison annuelle 2025/2026 :		V Horizon	25
De l'engagement en faveur de l'activité physique	12	Regard vers l'horizon : Dans quelle mesure l'indépendance	
Trois régions, une mission : Allemagne,		numérique d'ici 2035 est-elle réaliste ?	26
France et les pays nordiques	14	Conclusion : L'Europe n'a pas besoin de posséder l'océan numérique.	
		Mais il doit pouvoir naviguer à nouveau de manière autonome.	28



Un nouveau départ



À propos de cette étude

En Europe, la souveraineté numérique n'est plus depuis longtemps un sujet politique marginal. Elle est au cœur des débats stratégiques – au sein des ministères, des conseils d'administration et des centres de données. Cependant, il semble subsister un fossé considérable entre cette aspiration à l'indépendance et la réalité.

L'édition de l'année dernière du rapport « State of Digital Sovereignty » a donc été publiée avec une mission claire : étayer par des données fiables un débat qui, jusqu'alors, reposait principalement sur des déclarations politiques et des documents stratégiques. Le résultat était sans équivoque : la volonté de souveraineté était forte, mais sa mise en œuvre prenait du retard. La théorie n'avait pas encore été mise en pratique. Et il existait un fossé flagrant entre la perception subjective et la réalité.

En l'espace d'une seule année, le contexte des débats sur la souveraineté a sensiblement évolué. Les tensions géopolitiques ont modifié les stratégies informatiques, le CLOUD Act occupe une place plus importante dans l'agenda et les articles de presse faisant état de diplomates qui feraient activement pression contre les lois sur la souveraineté le montrent clairement : L'indépendance numérique est passée d'une question de mise en œuvre technique à une question de capacité d'action politique.

Il semblerait que l'Europe se dirige, en 2026, vers des eaux en partie inconnues. Le rapport de cette année intitulé « State of Digital Sovereignty : » : « Uncharted Waters » ne se contente donc pas d'examiner les changements intervenus depuis l'année dernière, mais s'intéresse également à la direction prise par les principaux acteurs européens.

Ce rapport élargit son champ d'analyse au-delà de l'Allemagne et interroge également des responsables informatiques en France et dans les pays nordiques que sont le Danemark, la Suède, la Norvège et la Finlande. L'Allemagne, la France et les pays nordiques : Trois régions qui marquent l'Europe de leur empreinte – et qui, chacune à leur manière, conçoivent, privilégient et mettent en œuvre la souveraineté numérique.

« Uncharted Waters » ne se veut pas un état des lieux des lacunes, mais une carte pour le départ – avec des coordonnées qui montrent jusqu'où l'Europe est déjà parvenue, où se trouvent les écueils et quelles routes mènent vers l'avenir.

Avant-propos : Prendre les commandes



48° 08'24,2" N
11° 31' 19,8" E

L'Europe se tient sur le pont d'un navire qui a longtemps navigué à l'aide de cartes étrangères. Les itinéraires étaient familiers, les ports sûrs et les instruments fiables. Mais soudain, l'horizon change. Les voies commerciales qui semblaient encore sûres hier traversent aujourd'hui des zones de turbulences politiques. La technologie, qui promettait autrefois avant tout de l'efficacité, détermine désormais la liberté d'action.

La « souveraineté numérique » donne souvent l'impression d'une attitude défensive ou d'un retrait par rapport à la voie commune.

C'est tout le contraire. La souveraineté ne signifie pas s'isoler du reste du monde. Cela signifie pouvoir tracer sa propre voie. Celui qui agit en toute autonomie peut choisir ses partenariats, mieux évaluer les risques, définir des normes et limiter les dépendances. Celui qui n'en est pas capable finira par se rendre compte qu'il n'est pas capitaine, mais simplement passager – même s'il paie le fret.

« La souveraineté ne signifie pas s'isoler du reste du monde. Cela signifie pouvoir tracer sa propre voie. »

Myra Security tire son nom de Nicolas de Myre, un saint qui est encore aujourd'hui considéré comme le saint patron des marins et des commerçants et qui est donc profondément ancré dans les villes hanséatiques allemandes. Cette ligne historique s'inscrit avec une précision étonnante dans notre présent. Autrefois, les marchands et les capitaines devaient savoir à quels vents ils pouvaient se fier, quelles routes étaient sûres et quels ports offraient une protection. Aujourd'hui, les entreprises et les autorités doivent savoir à quelles infrastructures elles peuvent confier leurs données, leurs processus et leurs modèles économiques – et à quelles autres elles ne le peuvent pas.

Dans le débat sur la souveraineté également, le « réseau » présente de fortes similitudes avec l'histoire maritime. Dans son ouvrage **Mare Liberum**, publié en 1609, le juriste néerlandais Hugo Grotius a écrit que la mer ne pouvait appartenir à personne et devait être accessible à toutes les nations. Il remettait ainsi en cause un ordre politique fondé sur la puissance, selon lequel l'Espagne et le Portugal revendiquaient des routes commerciales,

des mers et des voies d'accès, comme si les océans pouvaient être clôturés à la manière de terres agricoles. Grotius, l'un des pères fondateurs de la conception de la souveraineté, s'y est opposé. Il a formulé une idée qui allait plus tard marquer le commerce mondial : Les espaces libres ont besoin de règles équitables. Sinon, ils deviennent des instruments de pouvoir.

Aujourd'hui, les principales voies de circulation économiques ne passent plus par les océans, mais par les centres de données, les plateformes cloud, les piles logicielles et les services de sécurité. Celui qui contrôle cette infrastructure ne contrôle pas tout, mais suffisamment pour exercer une pression sur les marchés, les administrations et les entreprises. C'est précisément pour cette raison que le débat et la question de la souveraineté reprennent de l'importance.

Les résultats de cette étude montrent que : L'Europe souhaite opérer un changement de cap et est déjà en train de le mettre en œuvre. Les responsables informatiques en Allemagne, en France et dans les pays nordiques considèrent la souveraineté numérique comme un enjeu stratégique. Ce qui, en 2025, ressemblait encore plutôt à une déclaration d'intention se transforme en 2026 en une véritable dynamique.

Il va sans dire que l'Europe n'a pas la voie toute tracée. L'Europe n'a toutefois pas besoin de posséder l'océan numérique. Il doit pouvoir naviguer à nouveau de manière autonome.

De nombreuses entreprises et institutions ont mis en place, au fil des années, des environnements logiciels qui se sont développés à l'image d'une flotte de véhicules, comme décrit ici : planche après planche, pont après pont, avec des routines bien ancrées et des équipages qui manient les mêmes instruments depuis des décennies. Personne ne peut rééquiper de telles flottes du jour au lendemain. Il existe toutefois un large consensus sur le fait qu'elles doivent s'adapter à cette nouvelle donne. Cette étude constitue une feuille de route pour suivre précisément cette voie.



Katharina M. Schwarz

Responsable de la
communication internationale
Myra Security GmbH



**L'Europe n'a
pas besoin de
posséder l'océan
numérique.
Mais elle doit pouvoir
naviguer à nouveau de
manière autonome.**

Résumé analytique

La souveraineté numérique a fait son entrée dans les entreprises européennes : ELLE N'EST plus, un simple slogan politique, mais un principe d'action stratégique. Les résultats de cette étude, menée auprès de responsables informatiques en Allemagne, en France et dans les pays nordiques, dressent un tableau clair : La volonté d'autonomie numérique ne cesse de croître et se traduit de plus en plus par des décisions concrètes.

La volonté de souveraineté gagne en maturité – et en ampleur

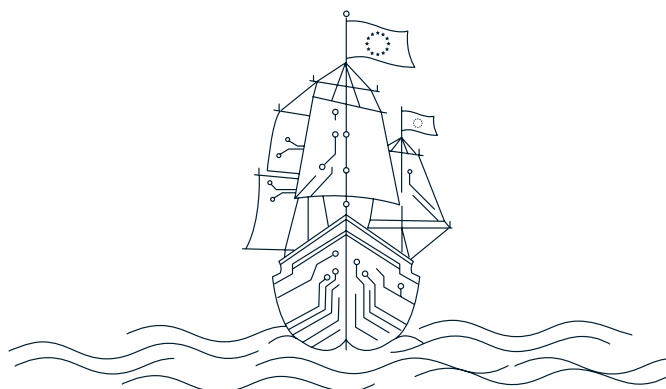
En Allemagne, 87,5 % des décideurs informatiques se prononcent en faveur d'une utilisation privilégiée des produits numériques européens pour les infrastructures critiques, contre 84,4 % l'année précédente. Le soutien augmente, mais sa répartition est différente : La part des « Oui, sans aucun doute » passe de 66,1 % à 47,2 %, tandis que celle des « Plutôt oui » passe de 18,3 % à 40,3 %. Cette conviction demeure, mais elle devient plus sobre, plus mûre, plus réfléchie. Il convient de noter à cet égard la disparition quasi totale des positions de rejet catégorique : Seuls 0,3 % des personnes interrogées affirment que les produits européens du secteur des infrastructures critiques ne doivent en aucun cas être privilégiés, contre 5,5 % l'année dernière. Dans la comparaison entre pays, la France arrive en tête avec un taux d'approbation combiné de 93,6 %, suivie des pays nordiques avec 88,9 %, puis de l'Allemagne avec 87,5 %.

Du souhait à l'action : un revirement en chiffres

En l'espace d'un an, la souveraineté numérique passe d'une question d'état d'esprit à une question de mise en œuvre. En 2026, près de deux fois plus d'entreprises en Allemagne seront activement engagées dans la mise en place de solutions logicielles européennes : 39,7 % contre 20,4 % l'année précédente. La proportion de personnes prévoyant de changer de fournisseur au cours des six prochains mois passe de 3,9 % à 20,4 %, soit une hausse de plus de 400 %. Dans le même temps, la proportion de décideurs qui ne souhaitent pas adopter de logiciels européens s'effondre presque totalement, passant de 47,7 % à 4,6 %. Le nombre d'indécis passe de 17,4 % à 3,9 %. Un revirement complet. Une comparaison européenne montre également que : Dans ces trois régions, seule une infime minorité de personnes rejette systématiquement les logiciels européens : 4,6 % en Allemagne, 3,3 % dans les pays nordiques et 2,4 % en France.

Trois régions, trois personnalités

Si l'on compare la situation à l'échelle européenne, on constate des mentalités différentes. La France arrive en tête avec 93,6 %, grâce à sa conviction profonde de privilégier les logiciels européens dans le secteur public ainsi que dans le secteur des infrastructures critiques. Dans le même temps, la France est toutefois le pays qui recourt le plus souvent aux logiciels américains en réaction à des événements géopolitiques. 24,8 % des décideurs informatiques français le déclarent, contre 19,8 % en Allemagne et 16,9 % dans les pays nordiques. Les décisions politiques prises après la période d'enquête, notamment la migration vers Linux annoncée par l'administration publique française, laissent toutefois entrevoir un début de changement de cap. Les pays nordiques se distinguent par leur cohérence et leur constance : Quel que soit l'horizon de planification considéré, ces chiffres restent constamment élevés, et seuls 3,3 % des personnes interrogées rejettent catégoriquement un changement de mode de transport. C'est l'Allemagne présente le tableau le plus équilibré : une forte volonté d'agir, une évaluation pragmatique des risques et le taux de migration le plus élevé à la suite de l'adoption du CLOUD Act.



La géopolitique, un catalyseur – mais pas un catalyseur sans ambiguïté

Les événements récents ont modifié les stratégies informatiques dans ces trois régions. Près de la moitié des personnes interrogées déclarent avoir davantage mis l'accent sur leur propre souveraineté : 51,5 % en Allemagne, 50,0 % en France et 48,9 % dans les pays nordiques. En ce qui concerne l'utilisation accrue des logiciels européens, les pays nordiques arrivent en tête avec 50,8 %, suivis de l'Allemagne avec 47,8 % et de la France avec 40,3 %. Le fait que, parallèlement, une part significative des entreprises de toutes les régions utilise à nouveau davantage de logiciels américains montre que : L'incertitude géopolitique joue un rôle de catalyseur, mais elle n'oriente pas tout le monde dans la même direction.

Il existe certes des obstacles, mais la majorité y voit des opportunités

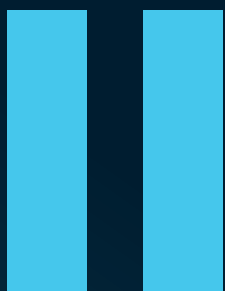
Dans toutes les régions, les responsables informatiques citent comme principaux obstacles au changement les coûts élevés de migration, le manque d'informations sur les alternatives européennes et les doutes d'ordre technique. Mais la perspective décisive est l'inverse : Si un peu plus des deux tiers des décideurs allemands du secteur informatique ne considèrent pas les coûts élevés de la migration comme un obstacle majeur, le tableau d'ensemble reflète moins les freins que les potentiels existants. C'est la France qui affiche le résultat le plus optimiste : 7,1 % des personnes interrogées ne voient aucun obstacle, contre 5,9 % dans les pays nordiques et 5,7 % en Allemagne. Le principal défi ne consiste donc pas à surmonter les résistances, mais à donner une orientation.

L'Europe croit en son essor numérique – le Nord montre la voie

La cybersécurité, l'intelligence artificielle et les services cloud s'imposent, toutes régions confondues, comme les domaines technologiques les plus critiques en matière de souveraineté. Le CLOUD Act n'est plus, depuis longtemps, un simple détail juridique : Dans aucune de ces trois régions, la proportion de personnes interrogées qui ne le connaissent pas ne dépasse 4,0 %. Et les perspectives d'avenir s'annoncent étonnamment optimistes, avec toutefois des disparités régionales marquées : 49,5 % des décideurs informatiques des pays nordiques estiment qu'une indépendance numérique quasi totale de l'Europe est réaliste d'ici dix ans, contre 39,6 % en Allemagne et 33,7 % en France. La nature de cette confiance est particulièrement révélatrice : Alors que dans les pays nordiques, 68,4 % des entreprises européennes affirment être en mesure de développer des produits numériques compétitifs à l'international dans la plupart des domaines, ce chiffre s'élève à 50,6 % en France et à seulement 45,8 % en Allemagne. Le Nord ne se contente pas de croire que l'Europe peut y parvenir : il est convaincu que l'Europe en est déjà capable.

49,5 %

des décideurs nordiques du secteur informatique estiment qu'une large autonomie numérique de l'Europe est réaliste d'ici les dix prochaines années



Mare Liberum

Mare Liberum – de la mer libre au réseau libre

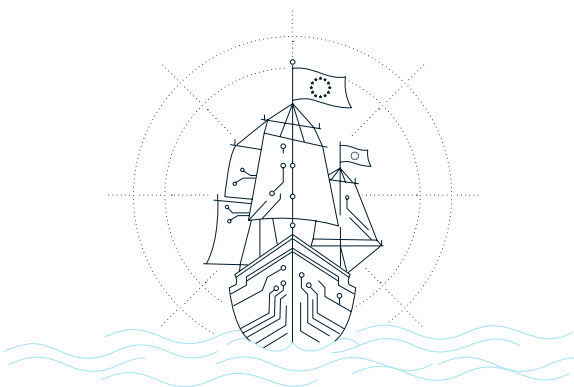
Hugo Grotius, le Santa Catarina et une idée qui a changé le monde

En 1603, des navires de la Compagnie néerlandaise des Indes orientales ont capturé le navire marchand portugais Santa Catarina dans le détroit de Malacca, au large des côtes de Singapour. Ce n'était pas un braquage comme les autres. Il s'agissait d'un acte politique – au cœur d'une lutte de pouvoir autour des routes commerciales, des épices et du contrôle des océans.

L'Espagne et le Portugal s'étaient partagé le monde. Le traité de Tordesillas (1494) a tracé une ligne à travers l'Atlantique : à l'ouest de celle-ci, l'Espagne ; à l'est, le Portugal. Les mers, selon cette revendication, appartenaient à ces couronnes. Les Pays-Bas voyaient les choses différemment – et ont chargé un jeune juriste de formuler cette objection : Hugo Grotius.

Son ouvrage intitulé **Mare Liberum** – « La mer libre » – a été publié en 1609. Grotius a fait valoir que : La mer n'appartient à personne. De par sa nature, elle est accessible à toutes les nations. Quiconque la revendique revendique l'irrevendable.

Pour les uns, il s'agissait d'une théorie déconnectée de la réalité, pour les autres, d'une arme juridique dans une lutte de pouvoir économique. En tout état de cause, il s'agit là du point de départ d'une réflexion qui continue aujourd'hui encore de façonner le droit international : Les espaces communs nécessitent des règles justes – sinon, ils risquent de devenir des instruments de pouvoir.



Chaque génération a ses propres mers

La conception de Grotius selon laquelle la mer est un espace libre s'est imposée. Elle est devenue le fondement du commerce mondial moderne et, dans sa conséquence la plus profonde, de la notion même de souveraineté.

Aujourd'hui, les principales routes commerciales de l'économie mondiale ne traversent plus les océans. Ils vous guident à travers les centres de données, les plateformes cloud, les piles logicielles et les services de sécurité. Les navires transportant des épices s'appellent aujourd'hui « flux de données ». Les ports maritimes s'appellent aujourd'hui « hyperscalers ». Les nouveaux obstacles sont les API, les contrats de licence et les normes de chiffrement.

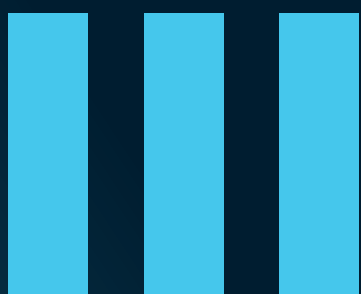
Une fois encore, quelques acteurs revendiquent le contrôle de ces espaces communs – non pas par des décrets royaux, mais par le biais d'architectures de plateformes, d'effets de verrouillage, d'interventions juridiques extraterritoriales et de leur simple puissance de marché.

Comme les entreprises européennes n'ont pas trouvé d'alternatives réalistes pendant longtemps, cela a donné lieu non seulement à un problème d'approvisionnement, mais aussi à un problème de pouvoir.

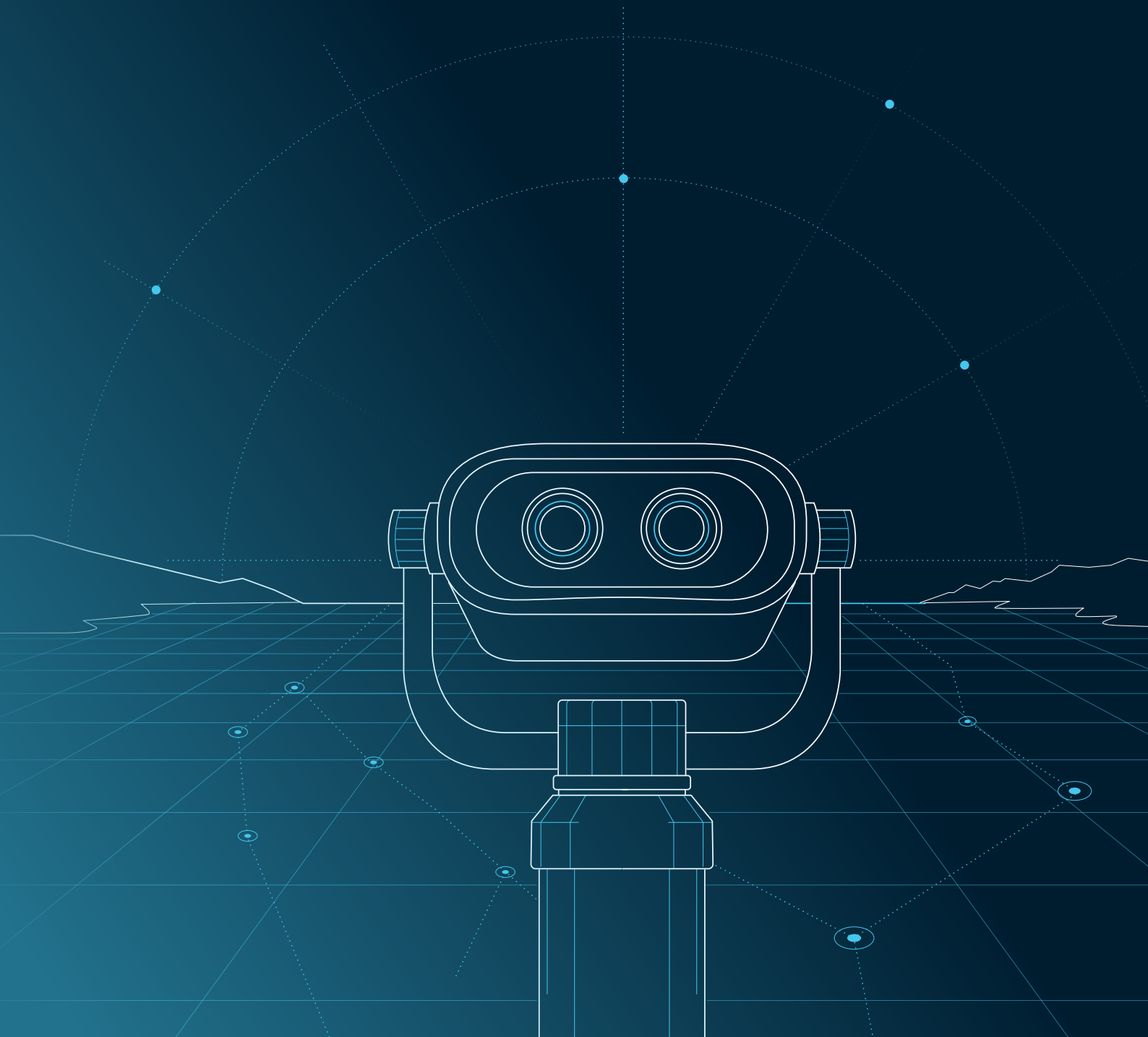
Un nouveau « Mare Liberum » pour le monde numérique

À cette époque, le « Mare Clausum » – la mer fermée – s'opposait au « Mare Liberum ». L'Europe ne souhaite ni l'isolement, ni un « conflit » avec les technologies américaines ou asiatiques. Il vise à empêcher que des infrastructures numériques critiques ne se retrouvent de fait prisonnières de zones relevant d'une juridiction étrangère. En ce sens, la revendication de l'Europe en matière de souveraineté numérique revient à ce que Grotius réclamait à l'époque : des espaces ouverts, des règles équitables et une véritable liberté de choix.

Des océans numériques plus ouverts pour une nouvelle génération de commerçants.



Parcours et coordonnées



L'Allemagne : comparaison annuelle 2025/2026 – de l'engagement à la mise en œuvre

Un signal devient une stratégie

En 2025, l'Allemagne a clairement montré que la souveraineté numérique n'était plus un sujet marginal.

84,4 % des décideurs informatiques se sont prononcés en faveur d'une utilisation prioritaire de produits numériques européens par les États et les exploitants d'infrastructures critiques. Un message clair de la part Le marché réclame des alternatives. L'année 2026 nous dira si ce signal s'est transformé en stratégie. Les données semblent indiquer que oui.

Question 1 – Fournisseurs européens pour les infrastructures critiques : une volonté inébranlable, une position plus nuancée

Cette conviction fondamentale reste inébranlable. En 2026, 87,5 % des décideurs allemands du secteur informatique estiment que les opérateurs des infrastructures critiques devraient privilégier les produits numériques européens, ce qui représente une légère hausse par rapport à 2025.

La nature de ce consentement évolue toutefois clairement. La part des personnes répondant « plutôt oui » passe de 18,3 % à 40,3 %, soit plus du double. La proportion d'indécis augmente modérément, passant de 7,3 % à 9,3 %. Ce qui, à première vue, semble être un affaiblissement s'avère, à y regarder de plus près, être un signe de maturité : L'enthousiasme sans réserve de l'année dernière cède la place à un consensus sobre, mais solide.

Cela apparaît particulièrement clairement à l'autre extrémité de l'échelle : la réponse « Non, en aucun cas » a pratiquement disparu, passant de 5,5 % en 2025 à 0,3 % en 2026. Un an après la première enquête, les responsables informatiques en Allemagne se prononcent donc encore plus fermement en faveur de la souveraineté numérique dans les infrastructures critiques.

Question 2 – Adoption des logiciels européens : le marché connaît un essor pro-européen

Ce changement est encore plus marqué lorsqu'il s'agit de savoir si les entreprises prévoient d'adopter des solutions logicielles européennes. En 2025, 20,4 % des décideurs allemands du secteur informatique étaient activement engagés dans ce processus de mise en œuvre. En 2026, ce chiffre s'élèvera déjà à 39,7 %, soit près du double.

À l'autre extrémité du spectre, la tendance est tout aussi claire. La part des entreprises qui rejettent catégoriquement tout changement a chuté de 47,7 % à 4,6 %, soit une baisse de plus de 90 %. La part des « Je ne sais pas » a baissé de 17,4 % à 3,9 %.

Alors qu'en 2025, de nombreux décideurs informatiques n'avaient pour certains même pas encore envisagé les alternatives européennes, un an plus tard, ils surfent clairement sur une vague technologique pro-européenne.



ALLEMAGNE

Votre entreprise prévoit-elle de mettre en place une ou plusieurs solutions logicielles européennes à l'avenir ?

Période	2025	2026	Changement
Déjà en cours de mise en œuvre	20,4 %	39,7 %	+94,6 %
Dans un délai de 6 mois	3,9 %	20,4 %	+423,1 %
Entre 7 et 12 mois	5,3 %	16,8 %	+217,0 %
Entre 13 et 24 mois	3,1 %	14,8 %	+377,4 %
Non	47,7 %	4,6 %	-90,4 %
Je ne sais pas	17,4 %	3,9 %	-77,6 %

Qu'est-ce qui a déclenché ce changement ?

Cette hausse brutale intervient à un moment où le contexte géopolitique a radicalement changé. En février 2026, un article publié par l'agence de presse Reuters a révélé que le Département d'État américain avait donné pour consigne à ses diplomates du monde entier de lutter activement contre les initiatives en matière de souveraineté numérique.

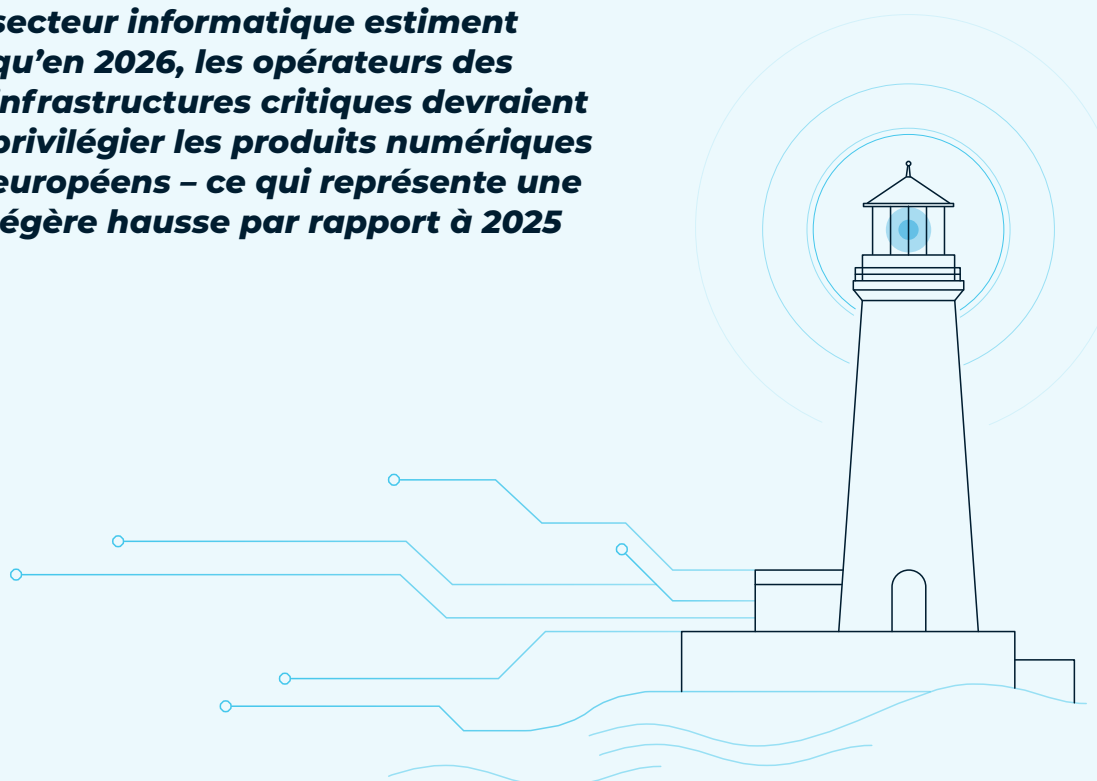
La Cour pénale internationale (CPI), située à La Haye, ayant émis en mai 2024 des mandats d'arrêt à l'encontre du Premier ministre israélien Benjamin Netanyahu et de l'ancien ministre de la Défense Yoav Gallant pour des crimes de guerre présumés commis dans la bande de Gaza, le gouvernement américain a également imposé, à l'été 2025, des sanctions à l'encontre de plusieurs juges de la CPI. En conséquence, leur accès à un certain nombre de plateformes et de services de paiement américains a été bloqué. La Cour pénale internationale a alors remplacé ses logiciels bureautiques Microsoft

par une solution allemande. En juin 2025, Anton Carniaux, directeur juridique de Microsoft France, a confirmé devant le Sénat français que l'entreprise serait tenue de communiquer des données en cas de demande des autorités américaines formulée conformément à la loi, quel que soit le lieu de stockage de ces données. Il n'a pas pu donner de garantie quant à la protection des données des utilisateurs en Europe. Le CLOUD Act, qui oblige les prestataires américains à transmettre aux autorités américaines, sous certaines conditions, des données stockées même au sein de l'UE, est soudainement devenu un sujet d'actualité.

La souveraineté numérique ne se limite pas à la géographie. La conclusion principale est la suivante : La souveraineté des données ne dépend pas de l'emplacement du serveur, mais de la structure du fournisseur, de la juridiction et du contrôle opérationnel.

87,5 %

des décideurs allemands du secteur informatique estiment qu'en 2026, les opérateurs des infrastructures critiques devraient privilégier les produits numériques européens – ce qui représente une légère hausse par rapport à 2025



Trois régions, une mission.

Comparaison entre l'Allemagne, la France et les pays nordiques

Une même destination, trois itinéraires différents

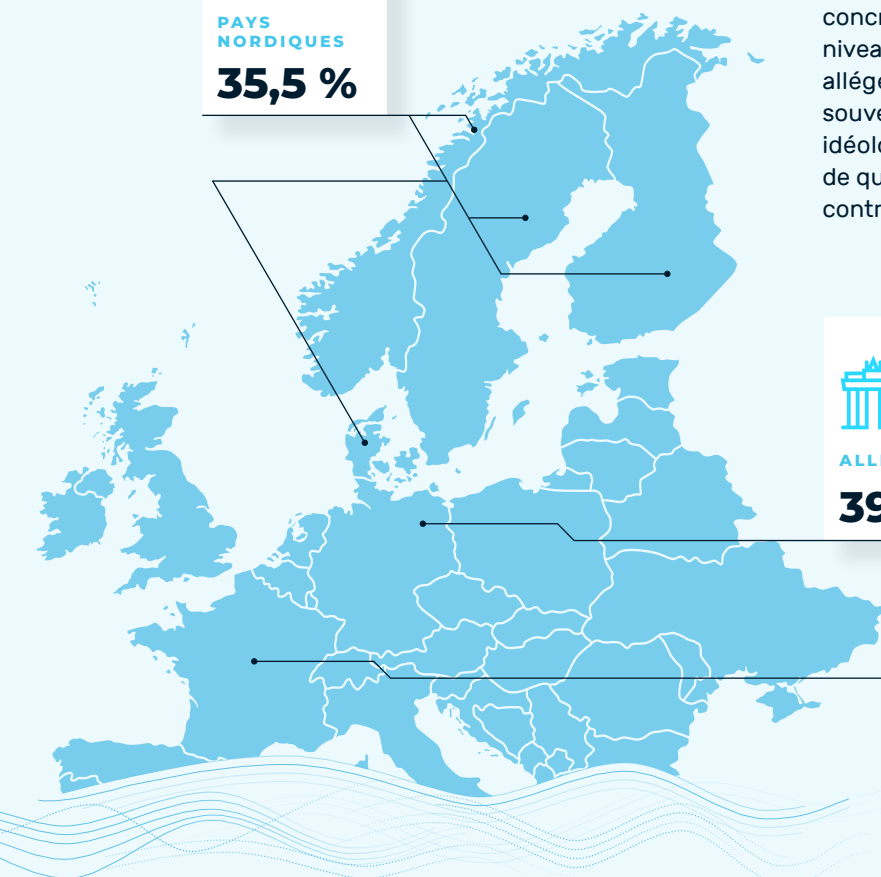
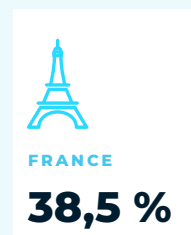
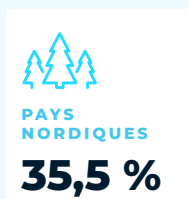
En 2026, une tendance que l'Europe a souvent tendance à négliger se dessine : La souveraineté numérique n'est pas un navire affrété en commun. Chaque région navigue à l'aide d'instruments différents, en empruntant des routes différentes, mais la destination à l'horizon est la même.

L'Allemagne tire ses origines de l'industrie. Le pays envisage la souveraineté numérique sous l'angle des chaînes d'approvisionnement, des infrastructures critiques et, surtout, des petites et moyennes entreprises. La question fondamentale : Comment trouver un équilibre face à des dépendances qui se sont développées au fil du temps, sans compromettre la stabilité opérationnelle ?

La France s'appuie sur son autonomie stratégique. L'État joue traditionnellement un rôle important dans le domaine des technologies clés et dispose d'une capacité d'action centralisée. En France, la « souveraineté numérique » ne ressemble pas à un nouveau mot à la mode, mais plutôt à la transposition numérique d'une raison d'État bien connue.

Les pays nordiques s'appuient sur une expérience concrète du numérique. Caractérisés par un haut niveau de maturité numérique, des administrations allégées et une solide culture de la sécurité, la souveraineté y apparaît moins comme une question idéologique que comme une question d'architecture de qualité : Ce qui fonctionne, c'est sûr et facile à contrôler.

Les responsables informatiques qui sont actuellement en train de passer à des technologies européennes



Qui procède au changement et quand ? Comparaison à trois volets des plans de mise en œuvre

	Allemagne	France	Pays nordiques
Déjà en cours de mise en œuvre	39,7 %	38,5 %	35,5 %
Dans un délai de 6 mois	20,4 %	17,9 %	19,9 %
Dans un délai de 7 à 12 mois	16,8 %	18,0 %	18,2 %
Dans un délai de 13 à 24 mois	14,8 %	13,3 %	16,9 %
Dans plus de 25 mois	5,9 %	4,0 %	7,5 %
Non	4,6 %	2,4 %	3,3 %
Je ne sais pas	3,9 %	10,1 %	5,9 %

L'Allemagne arrive en tête en ce qui concerne la proportion d'entreprises qui se tournent déjà activement vers des alternatives européennes. Les pays nordiques affichent systématiquement les valeurs les plus élevées ou les deuxièmes plus élevées sur presque tous les horizons de

planification, ce qui témoigne d'une propension constante au changement : pratiquement aucune entreprise ne s'y oppose. La France affiche certes la plus faible proportion de personnes clairement opposées (2,4 %), mais également la plus forte proportion d'indécis (10,1 %).

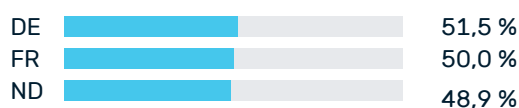
La géopolitique, un facteur déterminant ? Comment les événements politiques modifient les stratégies informatiques

Les bouleversements de l'ordre mondial se répercutent depuis longtemps déjà dans les salles de serveurs. Dans ces trois régions, environ la moitié des décideurs informatiques interrogés par considèrent que l'accent mis sur la souveraineté nationale résulte directement des événements géopolitiques :

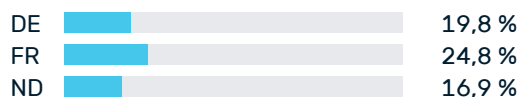
En Allemagne, un décideur informatique sur cinq, et en France un sur quatre, déclare recourir davantage aux logiciels américains en raison d'événements géopolitiques

En Allemagne, un décideur informatique sur cinq, et en France, un sur quatre, déclare utiliser davantage de logiciels américains en raison des événements géopolitiques. Ces chiffres montrent que les vents contraires n'entraînent pas toujours

Une attention accrue portée à la souveraineté nationale



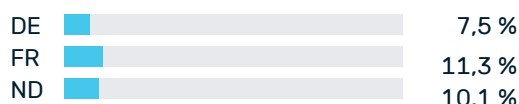
Recours accru aux logiciels américains



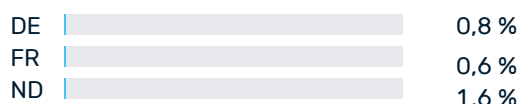
Un recours accru aux logiciels européens



Aucun changement



Je ne sais pas / sans réponse



une correction des cours. Pour les entreprises fortement dépendantes des marchés américains, un ancrage plus étroit dans les infrastructures américaines peut également constituer une stratégie de protection.



Le cas particulier de la France : le décalage entre les principes et la pratique

C'est en France (93,6 %) que le souhait de voir l'Europe prendre en charge la souveraineté en matière d'infrastructures critiques est le plus marqué. Et pourtant, la France est la région où les événements géopolitiques ont le plus souvent conduit à un développement des logiciels américains – et celle où la plupart des décideurs informatiques indiquent que rien n'a changé dans leur stratégie informatique.

Cela s'explique en partie par la période couverte par l'enquête. L'enquête s'est déroulée de fin février à début mars 2026, à un moment où les grandes orientations politiques en France n'avaient pas encore été définies. Ce n'est qu'ensuite qu'a été annoncée la décision de remplacer progressivement Windows par Linux au sein de l'administration publique française. Ce changement de cap n'apparaît pas encore dans les données.

IV

Hauts-fonds et courants

Les nouvelles routes commerciales de l'Europe – Là où la souveraineté est la plus nécessaire

L'architecture de la souveraineté

La souveraineté numérique peut sembler abstraite, mais elle se concrétise dans des domaines technologiques très précis. Quelle infrastructure cloud prend en charge les processus métier critiques ? Quelle architecture de sécurité protège les hôpitaux, les fournisseurs d'énergie ou les administrations ? Et sur quels systèmes d'IA reposeront à l'avenir les décisions, l'automatisation et la création de valeur ?

Les données de l'enquête montrent clairement que : Les décideurs européens du secteur informatique considèrent que, lorsqu'il s'agit de déterminer quels domaines technologiques sont, selon eux, les plus importants pour la souveraineté numérique, plusieurs secteurs technologiques sont étroitement liés. C'est précisément là que naissent les nouveaux courants et les nouvelles interdépendances de l'économie numérique – et c'est là aussi qu'ils perçoivent la nécessité de cibler clairement les efforts en matière de souveraineté. En effet, si l'on ne parvient pas à gagner en indépendance dans ce domaine, c'est là que se trouvent les écueils qui rendent les entreprises et les États vulnérables.

Cybersécurité : le point de repère commun

La cybersécurité est le domaine dans lequel les trois régions sont le plus en accord. Pays nordiques : 68,4 %, Allemagne : 57,6 %, France : 57,1 %.

Cela n'a rien de surprenant. La souveraineté se joue sur la vulnérabilité. La cybersécurité est un havre de sécurité au cœur de la tempête numérique : elle détermine la capacité d'une entreprise à détecter les attaques, à maintenir la disponibilité de ses services, à protéger ses données et à surmonter les crises. Sans sécurité, la souveraineté n'est qu'un concept théorique dépourvu de réalité opérationnelle.

Intelligence artificielle : le domaine d'avenir

L'IA constitue le deuxième grand domaine faisant l'objet d'un consensus.

La France arrive en tête avec 52,4 %, suivie de l'Allemagne avec 50,1 %, tandis que les pays nordiques se situent juste derrière avec 48,6 %.

Services cloud : la salle des machines de l'économie moderne

47,2 % des décideurs informatiques nordiques, 46,0 % des décideurs allemands et 38,1 % des décideurs français considèrent que les services cloud sont essentiels pour la souveraineté.

Applications, données, modèles d'IA, processus clients : tout passe de plus en plus par l'infrastructure cloud.

Quiconque ne dispose pas ici de liberté de choix perd une marge de manœuvre stratégique : non pas en théorie, mais au quotidien, dans la pratique.

Semi-conducteurs et puces : Le regard industriel de l'Allemagne

en tant que pays traditionnellement axé sur le matériel informatique, les responsables informatiques allemands considèrent le secteur des semi-conducteurs et des puces comme nettement plus crucial pour la souveraineté que leurs homologues européens. Plus d'une personne sur quatre (26,8 %) estime qu'il est nécessaire d'agir dans ce domaine en Allemagne, ce qui place ce pays nettement devant les pays nordiques (18,6 %) et la France (18,1 %).

Les pays nordiques : Le pragmatisme en profondeur

Les responsables informatiques nordiques affichent les pourcentages les plus élevés dans les domaines suivants : cloud (47,2 %), cybersécurité (68,4 %), téléphonie mobile et communication (27,7 %), ainsi que logiciels bureautiques et d'entreprise (23,1 %). Des chiffres, qui témoignent d'une approche pragmatique : où les données sont-elles générées chaque jour, comment sont-elles transférées de A vers B, et qui les protège ?

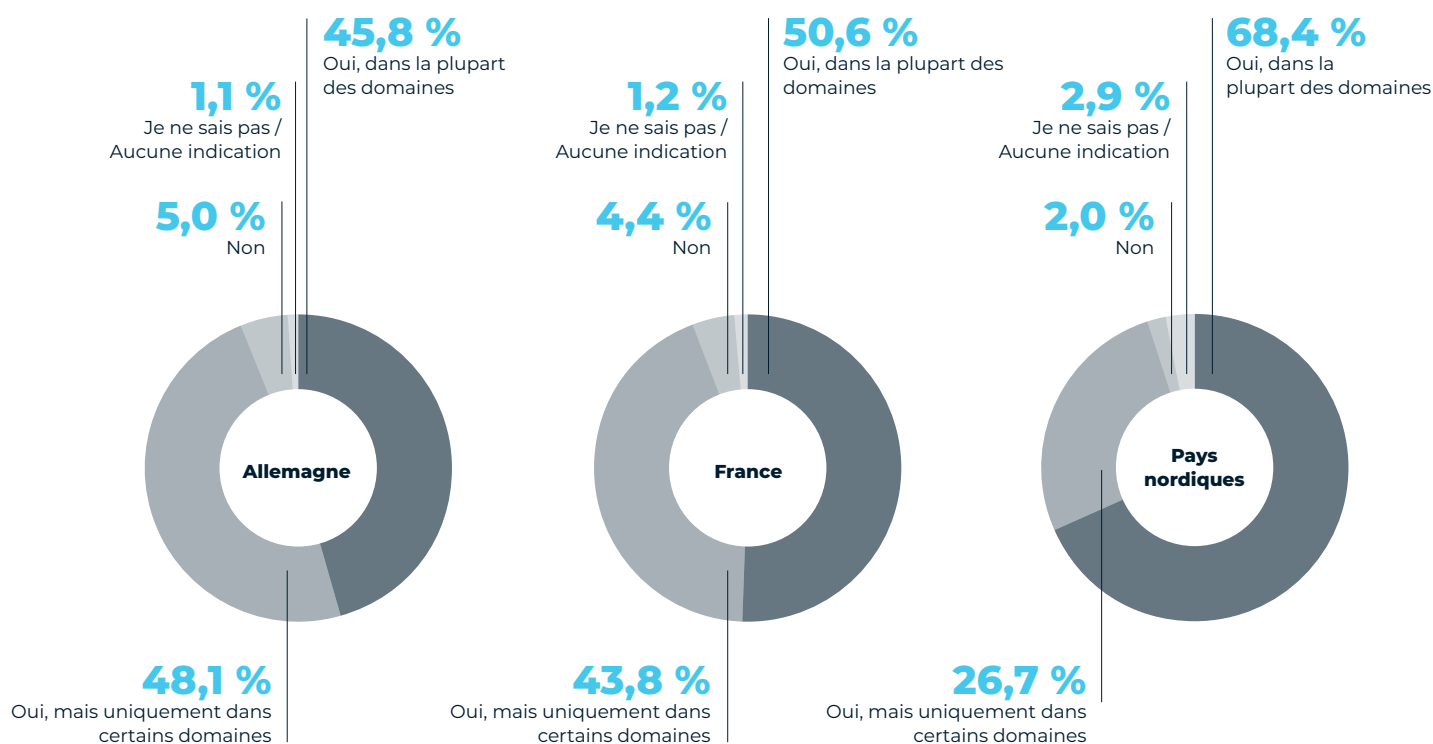
L'Europe a-t-elle confiance en elle-même ? Confiance dans la compétitivité européenne

Les responsables informatiques européens se prononcent clairement en faveur des technologies européennes. Mais derrière cette décision stratégique se cache une question plus fondamentale, qui est rarement posée ouvertement : L'Europe est-elle vraiment à la hauteur ? Quiconque souhaite remplacer les fournisseurs américains par des alternatives européennes doit être convaincu que ces alternatives existent non seulement, mais qu'elles sont également suffisamment viables pour garantir à long terme ses propres circuits commerciaux numériques. Sinon, la volonté de changement manque de fondement opérationnel.

Les réponses des responsables informatiques interrogés dressent un tableau nuancé. Dans les trois régions, une grande majorité estime que les entreprises européennes sont capables de développer des produits numériques compétitifs. Une analyse approfondie de l'étendue de cette confiance – qu'elle se limite à certains segments ou qu'elle s'étende à de larges pans de l'économie

numérique – révèle un fossé nord-sud manifeste. Si l'on additionne les réponses positives, les trois régions affichent toutes un taux compris entre 94 et 95 % environ – ce qui témoigne d'une forte confiance de base. La différence essentielle réside dans l'intensité de cette confiance : Plus des deux tiers des décideurs nordiques (68,4 %) estiment que l'Europe peut atteindre la souveraineté numérique « dans la plupart des domaines ». Ils font ainsi preuve d'une confiance profonde et affirmée dans la technologie européenne. Les responsables informatiques allemands et français partagent cet optimisme de fond, mais sont davantage enclins à adopter une position plus prudente, du type « Oui, mais uniquement dans certains domaines ».

Mais : Les bases d'un essor technologique européen crédible existent déjà au sein de l'ensemble des décideurs. Ce qui manque, ce n'est pas la conviction, mais des projets phares et des exemples de référence capables de transformer la confiance générale en décisions concrètes.



Les atouts complémentaires de l'Europe

Ces trois profils de priorités distincts se complètent parfaitement : L'Allemagne apporte son expertise en matière de matériel informatique et sa richesse industrielle. La France fait preuve d'ambition en matière d'IA et d'une volonté stratégique de prendre les devants. Les pays nordiques apportent leur expertise du cloud, leur culture de la cybersécurité et leur capacité à mettre en œuvre des solutions de manière pragmatique.

L'Europe, qui a pourtant vu le jour en tant que communauté, n'a pas besoin de ce levier de souveraineté individuel. Il lui suffit de réunir ces atouts complémentaires si elle souhaite se doter d'une architecture européenne.

Les obstacles à la migration : Pourquoi ce changement de cap reste difficile, mais est tout à fait réalisable

De nombreuses entreprises et institutions ont mis en place, au fil des années, des environnements logiciels qui se sont développés à l'image d'une flotte : Planche après planche, pont après pont, avec des routines bien ancrées et des équipages qui manient les mêmes

instruments depuis des décennies. Personne ne peut rééquiper de telles flottes du jour au lendemain. Il existe toutefois un large consensus sur le fait qu'elles doivent s'adapter face à ces nouveaux enjeux.

Les obstacles à une migration vers : comparaison entre trois solutions informatiques européennes

Manque d'informations sur les alternatives européennes

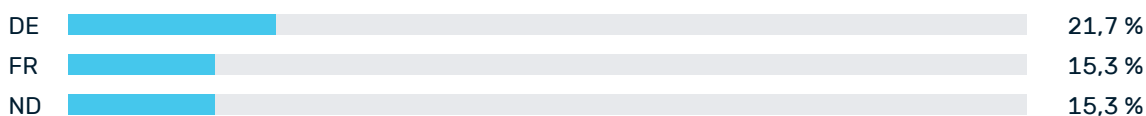
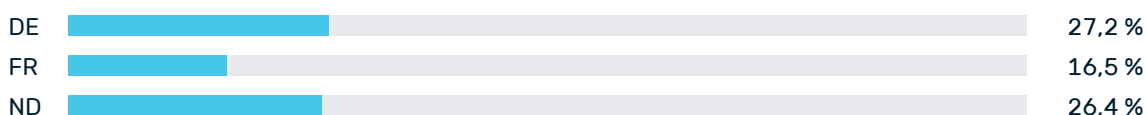
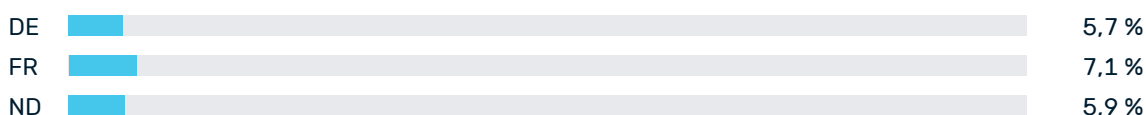
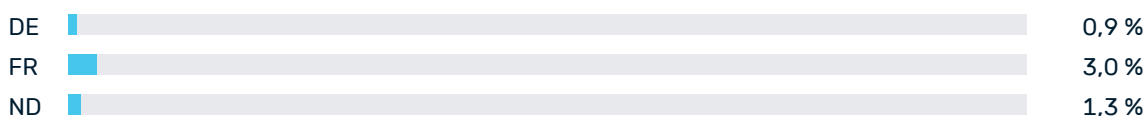
DE		33,5 %
FR		33,1 %
ND		42,0 %

Performances techniques insuffisantes

DE		31,0 %
FR		27,2 %
ND		24,4 %

Coûts de migration élevés

DE		34,6 %
FR		34,7 %
ND		39,7 %

Absence de sentiment d'urgence**Résistance interne / Politique****Impossibilité d'intégration****D'autres obstacles****Aucun obstacle n'est à signaler****Je ne sais pas****Les coûts liés à la migration : bien réels, mais pas déterminants dans la plupart des cas**

Dans toutes les régions, les coûts élevés liés à la migration figurent parmi les obstacles les plus fréquemment cités au passage à des solutions informatiques européennes. Et pourtant : Environ deux tiers des responsables informatiques allemands ne la considèrent pas comme un obstacle majeur. En France également, la proportion de personnes qui ne considèrent pas les coûts liés à la migration comme un frein s'élève à environ 65 % ; dans les pays nordiques, elle est d'environ 60 %. Ces coûts sont bien réels, mais ils ne constituent pas, pour la majorité, une raison de ne pas changer de cap.

Ce qui n'est pas visible n'est pas acheté – et ce qui n'est pas acheté se développe plus lentement

Lacunes en matière d'information – La visibilité est un facteur stratégique

Le manque de connaissance des alternatives européennes freine 42,0 % des responsables informatiques dans les pays nordiques, 33,5 % en Allemagne et 33,1 % en France. À l'inverse, signifie : Dans ces trois régions, la majorité des décideurs informatiques ne sont pas freinés par un manque d'informations. Une bonne alternative ne sert toutefois pas à grand-chose si elle ne figure pas sur la liste restreinte. Sinon, cela entraîne un problème de marché caractérisé par un mécanisme qui s'autoalimente : Ce qui n'est pas visible n'est pas acheté – et ce qui n'est pas acheté se développe plus lentement. Les places de marché, les cadres de certification et une communication ciblée ne sont pas des éléments secondaires dans la mise en place d'une nouvelle infrastructure souveraine.

Une nette majorité croit aux capacités techniques de l'Europe

Seuls 24,4 % des décideurs informatiques nordiques citent des performances techniques insuffisantes comme obstacle au changement ; les trois quarts d'entre eux n'ont aucune réserve d'ordre technique. Cela correspond à la grande confiance dont font

preuve les pays nordiques quant à leur capacité à atteindre, dans une large mesure, la souveraineté numérique au cours des 10 prochaines années. En Allemagne, près d'un de la population (31,0 %) doute des capacités techniques du pays. À l'inverse, cela signifie également que 69,0 % ne le font pas.

Les responsables informatiques considèrent-ils l'utilisation de logiciels européens comme un risque pour leur entreprise ?

	Allemagne	France	Pays nordiques
Oui, risque élevé	14,8 %	15,9 %	16,6 %
Oui, risque faible	58,8 %	55,1 %	62,2 %
Aucun risque	23,4 %	24,6 %	16,6 %
Oui, combiné	73,6 %	71,0 %	78,8 %

Le fait que les pays nordiques perçoivent le risque migratoire combiné le plus élevé (78,8 %) n'est pas en contradiction avec leur détermination : c'en est le revers. Quiconque connaît les défis liés aux transformations informatiques complexes et décide néanmoins de changer de cap ne le fait pas par naïveté, mais par choix mûrement réfléchi. Ce sont les décideurs français du secteur informatique qui affichent le plus grand optimisme au niveau européen : Une personne sur quatre (24,6 %) ne voit aucun risque à adopter des solutions européennes.

Quiconque connaît les transitions informatiques complexes et décide néanmoins de changer de cap ne le fait pas par naïveté, mais par un choix mûrement réfléchi.

Le CLOUD Act, un signe avant-coureur – entre attente et action

Une loi qui rend les frontières visibles

La loi intitulée « Clarifying Lawful Overseas Use of Data Act » – ou CLOUD Act en abrégé – a été adoptée aux États-Unis en 2018. Il oblige les entreprises technologiques américaines à accorder aux autorités américaines, sur demande, l'accès aux données stockées, quel que soit l'endroit où ces données sont physiquement stockées dans le monde. Un serveur situé à Francfort et exploité par un fournisseur

américain est donc potentiellement soumis à la juridiction des États-Unis. Il en résulte pour les entreprises européennes une relation de dépendance structurelle : Le RGPD a pour objectif de protéger les données à caractère personnel conformément au droit européen ; parallèlement, le CLOUD Act instaure un droit d'accès parallèle et extraterritorial susceptible de contourner de fait cette protection. Les entreprises doivent donc se conformer aux normes européennes en matière de protection des données, tout en restant exposées à des accès externes qu'elles ne peuvent ni contrôler ni exclure de manière sûre.

Comment l'Europe réagit-elle ? Comparaison de mesures concrètes

Quelles mesures votre entreprise compte-t-elle prendre face au CLOUD Act, qui oblige les prestataires américains à transmettre aux autorités américaines les données stockées même au sein de l'Union européenne ?

Mesure	Allemagne	France	Pays nordiques
Ne voient pas la nécessité d'agir	5,0 %	6,1 %	3,6 %
Changement de fournisseur	16,4 %	18,5 %	13,3 %
Changement de fournisseur prévu	32,4 %	21,0 %	28,7 %
Renforce le chiffrement	34,6 %	27,0 %	30,9 %
Suivre l'évolution de la situation	47,6 %	39,1 %	51,8 %
Aucune mesure particulière	3,9 %	7,3 %	3,6 %
Le CLOUD Act n'était pas connu	1,7 %	4,0 %	2,6 %
Je ne sais pas / Sans réponse	2,7 %	4,8 %	3,6 %

En ce qui concerne la loi CLOUD Act, l'Allemagne et les pays nordiques font preuve de la plus grande volonté d'agir : 32,4 % des décideurs informatiques allemands prévoient de changer de fournisseur, tandis que 16,4 % l'ont déjà fait. En France, si 18,5 % ont déjà changé de fournisseur – le taux le plus élevé des trois régions –, rares sont les responsables informatiques qui envisagent d'autres mesures. Seuls 3,6 % des décideurs informatiques des pays nordiques estiment

qu'il n'y a pas lieu d'agir, contre 5,0 % en Allemagne et 6,1 % en France. Le fait que le CLOUD Act ne soit inconnu que d'une infime minorité des personnes interrogées – ce chiffre ne dépasse 4,0 % dans aucune des trois régions – montre avant tout une chose : Ce sujet a définitivement fait son entrée parmi les priorités des décideurs européens du secteur informatique.

La lettre du PDG : Mise en garde contre le « sovereignty washing »

Cette évolution se manifeste également dans le secteur européen du cloud. En avril 2026, 25 PDG d'entreprises européennes spécialisées dans le cloud et le numérique ont mis en garde la Commission européenne contre une définition trop vague de la souveraineté numérique. Votre lettre ouverte concernant le projet de loi « Cloud and AI Development Act » s'oppose à une pratique que le secteur qualifie désormais de « sovereignty washing ».

Il s'agit d'offres qui promettent un contrôle européen, mais qui perpétuent des dépendances vis-à-vis des instances centrales.

Les prestataires mettent en avant leurs centres de données situés dans l'UE, leurs filiales locales ou des noms de produits à consonance souveraine. Parallèlement, les structures du groupe, les droits d'administration, la gestion technique ou les chemins d'accès juridiques hors d'Europe sont maintenus.

Ce que signifie réellement la souveraineté des données – trois niveaux de contrôle

Le débat sur la souveraineté numérique a profondément modifié la perception de la souveraineté en matière de données. De nos jours, le simple fait que les serveurs soient situés à Francfort ou à Stockholm ne suffit pratiquement plus à prouver que le traitement des données est souverain. Les questions relatives au contrôle effectif, aux dépendances et à la capacité d'action occupent de plus en plus le devant de la scène : Qui gère les systèmes et les clés ? Quels sont les juridictions compétentes en cas d'urgence ? Et dans quelle mesure une organisation conserve-t-elle son indépendance vis-à-vis des fournisseurs et des plateformes ?

Dans ce contexte, plusieurs pays européens mettent en place des initiatives politiques et organisationnelles visant à renforcer la mise en œuvre concrète de la souveraineté numérique. En Allemagne, le Centre pour la souveraineté numérique de l'administration publique (ZenDiS) élabore des critères et des méthodes d'évaluation pour une informatique souveraine au sein de l'administration. La liberté de choix, la capacité d'action et l'influence sur les prestataires constituent notamment les objectifs stratégiques centraux de la souveraineté numérique. En France, la Direction interministérielle du numérique (DINUM) adopte, avec « La Suite Numérique », une approche similaire visant à mettre à disposition des outils administratifs open source coordonnés par l'État. Depuis 2024, ces deux établissements collaborent également au niveau institutionnel.

Cette étude aborde donc la souveraineté des données selon trois niveaux de contrôle :

Contrôle technique : Qui gère les clés de chiffrement ? Qui a accès aux journaux, aux sauvegardes, aux identités et aux interfaces d'administration ? Le contrôle technique signifie qu'aucun acteur externe ne peut accéder aux données à l'insu de l'exploitant et sans son consentement.

Contrôle juridique : Quelle est la législation applicable au prestataire, à sa société mère et à l'accès aux données en cas de crise ? Il ne doit pas exister de compétences parallèles relevant d'ordres juridiques étrangers – par exemple en vertu de lois extraterritoriales – si l'on souhaite parvenir à une véritable souveraineté en matière de données.

Contrôle opérationnel : En cas de crise, une entreprise peut-elle agir : changer de stratégie, s'isoler, poursuivre ses activités ? Le contrôle opérationnel signifie que les systèmes sont conçus de manière à ce que les scénarios de transition et de sortie puissent être testés et mis en œuvre de manière réaliste, sans compromettre le bon fonctionnement de l'entreprise.

Le simple fait que les serveurs soient situés à Francfort ou à Stockholm ne suffit pratiquement plus aujourd'hui à prouver que le traitement des données est souverain

La dépêche américaine – Quand la dépendance prend un visage politique

En février 2026, un article de l'agence de presse Reuters a révélé que le Département d'État américain avait donné pour instruction à ses diplomates du monde entier de s'opposer activement aux lois relatives à la localisation des données et à la souveraineté numérique. Ce qui n'était au départ qu'une dépendance technique est ainsi devenu un programme géopolitique ouvertement affiché.

Pour les décideurs européens du secteur informatique, cela se traduit par une évolution de la

perception des risques : Les dépendances vis-à-vis des infrastructures américaines ne relèvent donc plus uniquement de décisions d'approvisionnement neutres, mais constituent également des points d'entrée potentiels pour des pressions extérieures.

Le CLOUD Act en tant que tel fait l'effet d'un éclair dans le ciel nocturne. Un danger potentiel qui peut frapper à tout moment et révéler des choses qui devraient en réalité rester cachées.

V Horizon



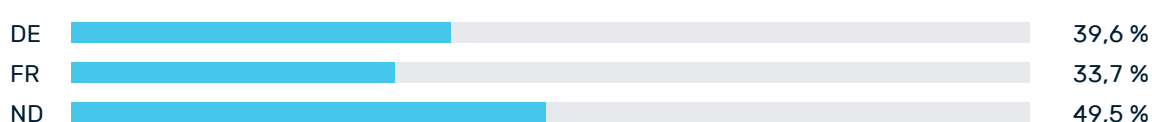
Regard vers l'horizon – Dans quelle mesure l'indépendance numérique d'ici 2035 est-elle réaliste ?

L'évaluation dans le cadre d'une comparaison à trois

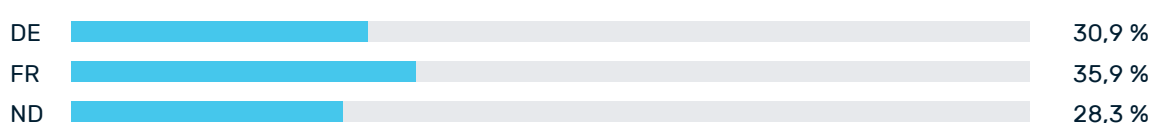
Une indépendance numérique totale



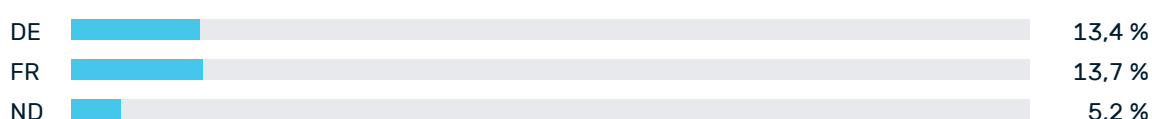
Une grande autonomie numérique



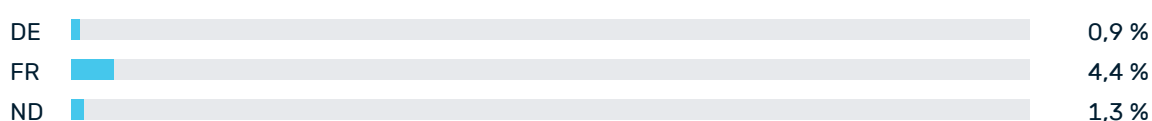
L'indépendance dans des domaines clés



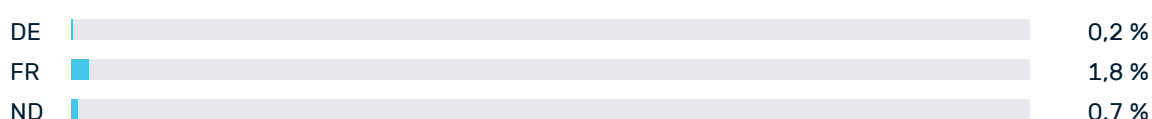
Réduction minimale des dépendances



Aucun changement



Je ne sais pas / Sans réponse



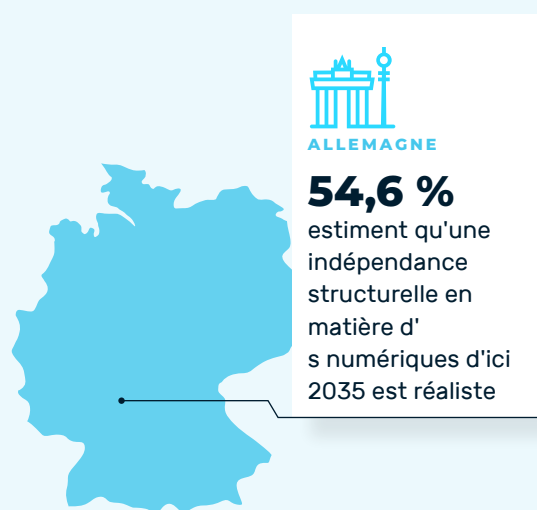
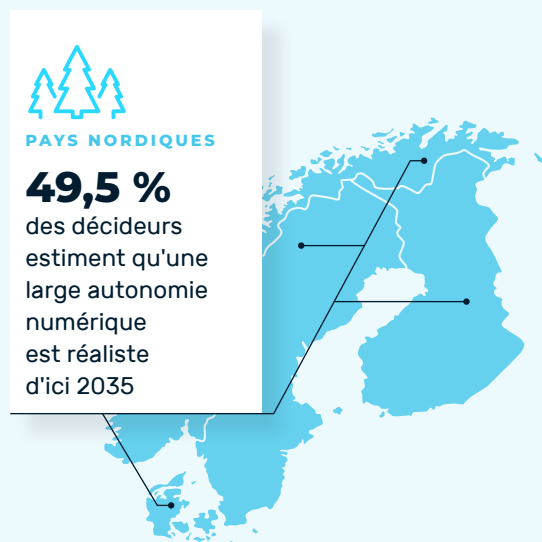
Une amélioration quelconque (combinée)



Pays nordiques : Un optimisme fondé sur des faits concrets

49,5 % des décideurs informatiques nordiques estiment qu'une indépendance numérique quasi totale d'ici 2035 est réaliste – c'est le seul chiffre qui s'approche de la barre des 50 %. 15,0 % supplémentaires estiment même que l'Europe est capable d'atteindre une indépendance totale. Au total, 64,5 % des décideurs informatiques des pays nordiques estiment que l'Europe pourra atteindre la souveraineté structurelle d'ici dix ans.

Cet optimisme ne vient pas de nulle part. Les pays nordiques ont connu la transformation numérique plus tôt et de manière plus approfondie que la plupart des autres régions européennes. Quiconque a déjà constaté à quelle vitesse une société peut transformer son infrastructure numérique est plus enclin à croire qu'elle y parviendra à nouveau.

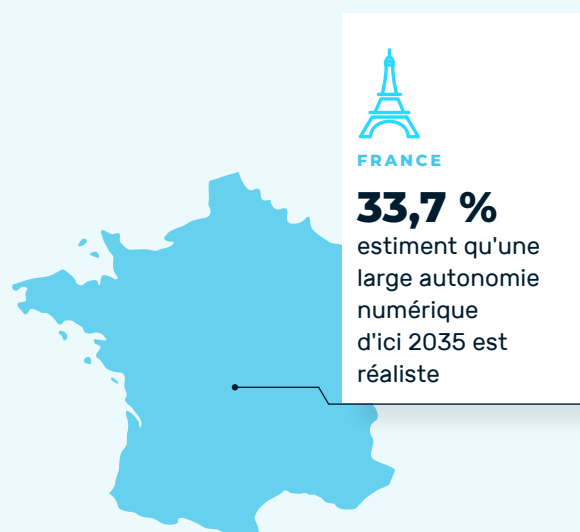


Allemagne : Un optimisme mitigé

54,6 % des décideurs allemands du secteur informatique estiment que l'Europe pourra renforcer sa souveraineté structurelle d'ici 2035. Près d'une personne sur quatre (39,6 %) estime qu'une indépendance numérique quasi totale est réaliste : un optimisme sectoriel qui témoigne de la tendance bien connue des Allemands à décomposer les grandes transformations en sous-projets gérables.

France : Du réalisme plein de potentiel

Dans l'ensemble, c'est la France qui se montre la plus pessimiste : Seuls 33,7 % considèrent qu'une large autonomie est réaliste, et 6,2 % ne croient absolument pas à un quelconque changement – ce qui représente le pourcentage le plus élevé de toutes les régions. Mais en y regardant de plus près, on constate que : En matière d'indépendance dans des domaines clés, la France arrive même en tête avec 35,9 %. La France raisonne en termes de priorités, et non en termes absolus.



Conclusion : L'Europe n'a pas besoin de posséder l'océan numérique. Mais elle doit pouvoir naviguer à nouveau de manière autonome.

Une Europe qui a pris conscience

Cette étude montre une Europe en pleine mutation. Pas dans un sprint, mais dans un changement de cap radical.

Les responsables informatiques en Allemagne, en France et dans les pays nordiques ont intégré la souveraineté numérique comme un enjeu stratégique. Ils adaptent les stratégies informatiques. Vous prévoyez des migrations. Vous investissez dans des logiciels européens. Vous percevez des risques – mais, ils ne s'en servent pas comme prétexte.

L'Allemagne envoie un signal fort : La proportion d'entreprises qui ont déjà adopté des logiciels européens a presque doublé en l'espace d'un an. La proportion de ceux qui refusent catégoriquement de changer a chuté de 47,7 % à 4,6 %. Il ne s'agit pas de légers changements, mais d'une transformation structurelle en temps réel.

La proportion d'entreprises qui ont déjà adopté des logiciels européens a presque doublé en l'espace d'un an

Les enseignements à tirer de ces trois régions

L'Allemagne adopte une approche rigoureuse et prudente. Ce pays dispose d'un secteur industriel solide et d'une expertise en matière d'infrastructures essentielles. Les obstacles sont bien réels : coûts de migration élevés, environnements informatiques complexes, nécessité de parvenir à un consensus en interne. Mais la proue a pivoté.

La France aborde la souveraineté d'un point de vue stratégique et bénéficie d'un élan politique favorable. Les données révèlent une forte volonté de souveraineté, mais aussi une mise en œuvre opérationnelle hésitante. Les récentes décisions politiques de la France ne laissent toutefois aucun doute sur le fait qu'elle a trouvé sa nouvelle orientation.

Les pays nordiques sont les pionniers pragmatiques de l'Europe. Un haut niveau de maturité numérique, une grande ouverture au changement, associés à une forte confiance dans la compétitivité européenne. Les pays nordiques montrent la voie à suivre – lorsque le pragmatisme et la culture numérique se rencontrent.

Ensemble, ces trois atouts peuvent constituer un parcours européen : L'Allemagne fournit des fondations industrielles.

La France fait preuve d'une volonté politique et affiche ses ambitions en matière d'IA. Les pays nordiques apportent leur maturité numérique et leur expérience en matière de mise en œuvre.

Que faudrait-il qu'il se passe ? Cinq axes d'action



48° 08'24,2" N
11° 31' 19,8" E



La question de Grotius : (La liberté de la mer) revisitée

Hugo Grotius n'a pas écrit **Mare Liberum** parce qu'il aimait les conflits. Il a écrit cela parce qu'il s'est rendu compte que, sans règles équitables, les espaces communs deviennent des instruments de pouvoir.

L'Europe est aujourd'hui confrontée à la même question fondamentale.

Il vise à créer l'équivalent numérique de ce que Grotius réclamait à l'époque : des espaces ouverts, des règles équitables, une véritable liberté de choix.

L'océan numérique ne doit pas appartenir à une

poignée de personnes. Il doit rester ouvert, sécurisé et pouvoir être utilisé de manière équitable.

L'Europe n'a pas besoin de posséder cette mer.

Mais il doit pouvoir naviguer à nouveau de manière autonome. L'essentiel est désormais non seulement de tirer parti du soutien des décideurs européens du secteur informatique et de prendre les rênes, mais surtout de continuer à les tenir fermement.

Nicolas de Myre – saint patron des marins et des commerçants, et pilier de la souveraineté numérique

Myra était une ville portuaire située sur la côte sud de l'Asie Mineure, dans l'actuelle Turquie. Saint Nicolas, évêque au IV^e siècle, est devenu le saint patron des marins et des marchands.

Quiconque expédiait des marchandises par des itinéraires peu sûrs ou pratiquait le commerce sur de longues distances cherchait, en son nom, à trouver des repères et à gagner la confiance.

Autrefois, les cartes, les phares et les ports déterminaient le succès d'un voyage commercial.

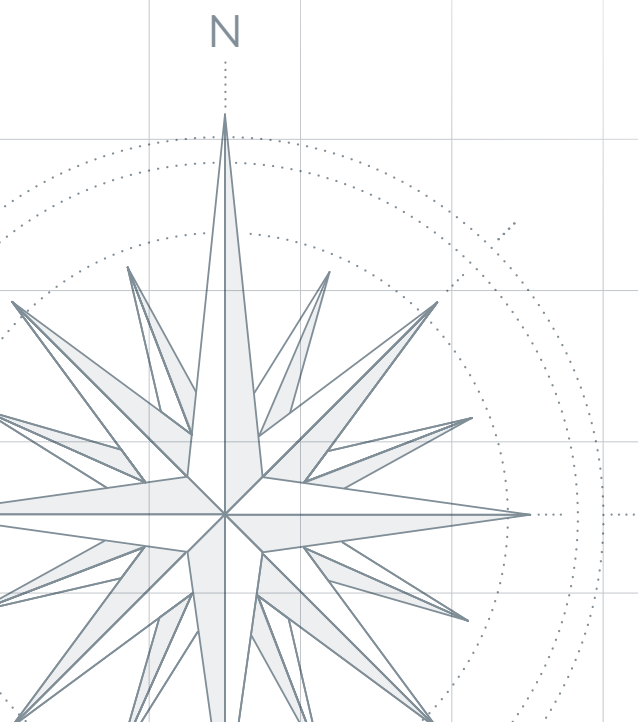
Aujourd'hui, ce sont l'architecture de sécurité, la souveraineté des données et le choix de l'infrastructure appropriée qui font la différence.

Pour Myra Security, la mission reste la même :

Une protection sur les chemins dangereux. La fiabilité là où cela compte vraiment.

Nicolas de Myre protégeait ceux qui partaient.

Myra Security protège les internautes qui naviguent sur le net.



Myra State of Digital Sovereignty 2026

(version numérique de l'étude + documents complémentaires)

En scannant le code QR, vous accéderez à la version numérique de l'étude ainsi qu'à des documents complémentaires et à des informations supplémentaires.



Remarque méthodologique :

Ces résultats s'appuient sur une enquête Civey réalisée pour le compte de Myra Security auprès de 1 818 décideurs informatiques en Allemagne (1 007), en France (504) et dans les pays nordiques : le Danemark (76), la Norvège (76), la Suède (78) et la Finlande (77). Ce sondage s'est déroulé du 25 février au 5 mars 2026. L'enquête a été réalisée en ligne ; pour les questions permettant plusieurs réponses, il était possible de sélectionner plusieurs domaines. La marge d'erreur statistique est d'environ ± 5 %. La souveraineté numérique est définie ici comme la capacité à recourir à des solutions logicielles européennes plutôt que de dépendre de fournisseurs non européens.

Remarque concernant la langue et l'égalité entre les sexes :

Pour faciliter la lecture, le masculin générique est utilisé dans ce rapport. Sauf indication contraire explicite, toutes les désignations de personnes s'appliquent de la même manière à tous les genres.

Made in Germany



Myra protège ce qui compte vraiment. Dans le monde numérique.

Vous souhaitez en savoir plus sur la manière dont nos solutions peuvent vous aider à augmenter votre chiffre d'affaires, à réduire vos coûts et à protéger vos applications contre les attaques malveillantes ? Notre équipe d'experts se fera un plaisir de vous conseiller de manière personnalisée et d'élaborer une solution sur mesure pour votre organisation. Nous vous invitons à prendre rendez-vous dès aujourd'hui pour un entretien de conseil sans engagement.

**Les cyberattaques coûtent cher,
mais un entretien sans engagement ne vous coûtera rien.**

Myra Security GmbH

☎ +49 89 414141 - 345

🌐 www.myrasecurity.com

@ info@myrasecurity.com