Digital113

Cluster numérique Sud de France

DIGITAL 113, LE COLLECTIF POUR **PROPULSER LE NUMÉRIQUE D'OCCITANIE**

au-delà des frontières

CONJONCTURE, ENJEUX ET PERSPECTIVES POUR L'ÉCONOMIE NUMÉRIQUE EN 2026

WWW.DIGITAL113.FR

Conjoncture, enjeux et perspectives pour l'Économie Numérique en 2025

L'écosystème numérique, en Occitanie comme ailleurs, fait face à une convergence d'enjeux technologiques, réglementaires et économiques qui imposent une adaptation rapide des stratégies et des modèles opérationnels.

L'Occitanie s'affirme comme le 3ème pôle numérique français : avec plus de 131 000 emplois, 18 500 établissements et 8,1 milliards d'euros de richesse générée, la filière numérique régionale représente 7,7% de la richesse dégagée dans la région. C'est dans ce contexte que Digital 113, fort de ses 300 membres, publie sa note annuelle de conjoncture pour éclairer les décideurs du numérique d'Occitanie. *Source : INSEE/DREETS Occitanie.*

Après une année 2024 déjà marquée par le ralentissement, 2025 aura été une année de consolidation difficile. Dans un contexte macroéconomique instable (instabilité politique nationale, tensions géopolitiques et incertitudes économiques durables) le marché du numérique a enregistré une croissance limitée à +2%, avec des disparités profondes selon les métiers : forte progression pour les éditeurs de logiciels (+8,2%), mais décroissance pour les ESN (-1,8%) et le conseil en technologies (-2,5%). *Source : Numeum.*

Trois prises de conscience majeures ont structuré les réflexions des acteurs du numérique en 2025 : la fragilité de la compétitivité européenne face aux États-Unis, la transformation fulgurante engendrée par l'IA générative qui oblige les entreprises à passer de l'expérimentation à l'industrialisation, et une prise de conscience accrue des dépendances technologiques dans un contexte géopolitique tendu. La souveraineté numérique, longtemps reléguée au second plan, s'impose comme une priorité stratégique assumée, tant pour les entreprises que pour les décideurs publics.

Toutefois, une inflexion positive s'amorce en fin d'année, tirée par les premiers déploiements opérationnels de l'IA générative, la montée en puissance du SaaS (77% des nouveaux projets au S2 2025) et l'émergence de projets de souveraineté numérique. Numeum prévoit une accélération de la croissance à +4,3% pour 2026.

Parmi les principaux freins qui persistent :

- **Ralentissement des investissements :** réduction des aides publiques et des incitations fiscales (CIR, CII, subventions régionales), dans un contexte de fragilité économique.
- **Pression réglementaire croissante :** application progressive des normes européennes (IA Act, NIS2, DORA, Cyber Resilience Act) dans un cadre encore instable.
- **Concentration des investissements** sur le Cloud, l'IA et la cybersécurité, au détriment des projets de transformation plus larges.
- **Tensions géopolitiques comme accélérateur de souveraineté :** le contexte international pousse les organisations à reconsidérer leurs dépendances technologiques, ouvrant un momentum historique pour les acteurs européens du numérique.

Cette note est issue des travaux des Factory de Digital 113 et de données diverses issues de sources institutionnelles et sectorielles (Numeum, ANSSI, Gartner, Bpifrance, Deloitte, IBM, Flexera, KPMG…). Elle contribue à une vision prospective des défis et opportunités qui impacteront la compétitivité des entreprises du numérique d'Occitanie en 2026.

I. Enjeux technologiques majeurs

A. Gouvernance des données et intégration de l'IA

L'année 2025 a encore une fois été marquée par l'accélération des avancées technologiques dans le monde de l'IA et de la data. Les acteurs américains poursuivent une course effrénée, poussant les entreprises à comprendre, s'approprier et déployer ces nouvelles approches à un rythme soutenu. Si la majorité des organisations ont désormais compris l'importance stratégique de ces nouveaux usages, elles continuent de se heurter à la difficulté du passage à l'acte, aussi bien au niveau stratégique qu'opérationnel. Le passage de l'expérimentation à la mise en œuvre concrète, l'acculturation des équipes, et la capacité à définir une stratégie à moyen terme restent autant d'obstacles sur ce parcours de transformation.

Selon Numeum, près de 40% des acteurs du secteur constatent déjà un impact positif de l'IA générative sur leurs marges et leur chiffre d'affaires en 2025, signe d'un passage progressif de l'expérimentation à des usages opérationnels créateurs de valeur. Les gains de productivité liés à l'IA générative sont estimés en moyenne à 12,5% en 2025, avec une progression attendue à 17% en 2026.

Forts de ces enseignements, les entreprises projettent leur stratégie Data/IA 2026 autour de **6 enjeux majeurs :**

1/ Gouvernance DATA & IA : passer de l'intention à l'action opérationnelle

- Choisir une méthodologie adoptée :privilégier une approche itérative avec un choix technologique stable plutôt qu'attendre «l'outil parfait».
- Identifier et lever les freins, notamment humains, pour déployer les actions auprès des équipes.
- Prioriser les cas d'usage IA en fonction des enjeux métiers et de leur valeur opérationnelle.
- Garantir la disponibilité de données suffisamment fiables avant de lancer des projets d'IA. Un défi majeur pour les entreprises n'ayant pas encore pleinement assimilé leur première transformation numérique.

2/ Culture DATA & IA et transformation des métiers

- Comprendre comment l'IA transforme les métiers : évolution des pratiques, disparition de certains rôles et création de nouveaux.
- Accompagner les équipes pour intégrer et faire évoluer l'usage de l'IA dans leurs activités quotidiennes.
- Adopter des méthodes éprouvées pour faciliter l'adoption des outils d'IA générative auprès de l'ensemble des collaborateurs, et identifier les cas d'usage IAg prioritaires.
- Evaluer et développer la maturité data des équipes comme condition préalable à une adoption réussie de l'IA, sans ce socle, les entreprises risquent de déployer des outils sans cadre clair, au risque de décevoir les métiers et de fragiliser la conduite du changement.

3/ Maturité, qualité des données et souveraineté numérique

- Garantir la qualité des données tout en choisissant des outils selon des critères de sécurité et d'hébergement, et pas seulement de fonctionnalités.
- Trouver le bon équilibre entre performance et fiabilité, pour renforcer la confiance dans les systèmes IA.
- Évaluer les compromis que la souveraineté numérique implique sur les usages, les performances ou les outils.

4/ Économie de l'IA : pilotage des coûts et création de valeur

- Arbitrer entre l'utilisation d'un outil existant à 80% et le développement d'une solution sur mesure selon les contextes et enjeux.
- Intégrer les coûts cachés : acculturation, maintenance, sécurité, conformité, évolution des modèles.
- Mettre en place des indicateurs pour piloter la valeur créée dans le temps.

5/ Réglementation, éthique et responsabilité

- Garantir la transparence des usages IA vis-à-vis des collaborateurs, clients et partenaires.
- Définir la place de la responsabilité humaine dans les décisions appuyées par l'IA générative.
- Transformer les contraintes réglementaires (IA Act, RGPD, Data Act) en facteur de confiance et de différenciation.

6/ Propriété intellectuelle et IA

- Protéger les actifs immatériels de l'entreprise et intégrer la PI dans la gouvernance Data & IA.
- Définir les droits sur les contenus générés par l'IA et apporter la preuve de l'intervention humaine.

B. Cybersécurité et résilience opérationnelle

En 2025, le nombre de cyberattaques traitées par l'ANSSI reste stable avec 1 366 incidents recensés, contre 1 361 en 2024, un niveau qui demeure élevé comparé aux 1 112 incidents de 2023. L'ANSSI note une recrudescence significative des exfiltrations de données et l'émergence d'un brouillard technologique et organisationnel entre acteurs étatiques et cybercriminels, qui brouille les pistes et complique la détection.

Par ailleurs, le coût moyen d'une violation de données en France atteint 3,59 millions d'euros en 2025 selon IBM, soit une légère baisse de 7% par rapport à l'année précédente, portée par une meilleure détection grâce à l'IA. *Source : ANSSI, IBM Cost of a Data Breach 2025.*

70% des entreprises concernées par NIS2 ou DORA ne sont pas encore conformes. Si DORA est pleinement applicable depuis janvier 2025, la situation est plus nuancée pour NIS2, dont la transposition en droit français n'est toujours pas achevée, l'ANSSI ayant par ailleurs indiqué qu'aucune sanction ne serait appliquée avant trois ans. Des sanctions pouvant atteindre 10M€ ou 2% du CA restent néanmoins à terme une réalité pour les acteurs concernés.

On note cependant une hausse de 35% de la mise en place d'équipes SOC (Security Operations Center) dans les ESN et grands groupes.

Les enjeux pour les entreprises sont :

- **Intégration de l'IA en cybersécurité :** Automatisation de la détection d'anomalies et du monitoring de menaces via le Machine Learning et l'IA adaptative.
- **Conformité aux nouvelles normes européennes et sécurisation des produits :**
  La publication successive (entre 2022 et 2024) du Règlement DORA, de la Directive NIS2 et du Règlement Cyber Resilience Act (CRA) constituait un signal fort de la nécessité de renforcer le niveau de cybersécurité (+ généralisation des pratiques DevSecOps) pour le secteur financier, les fabricants de produits numériques et 18 secteurs critiques.
  L'année 2025 nous laisse cependant avec un goût d'inachevé : Si DORA est applicable depuis janvier 2025 et que CRA entre progressivement en application à compter de 2026, la transposition française de NIS2 progresse laborieusement depuis près de 2 ans tandis que pointe déjà l'Omnibus Numérique (un projet visant à simplifier le package RGPD/AI Act/NIS2 par des mesures "d' harmonisation " et de "simplification").
  Cette phase d'incertitude réglementaire laisse craindre que l'attentisme prévale pour de nombreux acteurs alors qu'elle pourrait (et devrait) être mise à profit par ces derniers pour une meilleure préparation dans un contexte cyber de plus en plus menaçant avec des attaques sophistiquées et industrialisées en hausse constante.
  Espérons que 2026 soit placée sous le signe de l'action constructive, tant pour notre écosystème que pour nos législateurs.
- **Sécurité des infrastructures Cloud, hybridation des environnements et réduction du risque client :** renforcement des architectures multi-cloud et des stratégies Zero Trust.

C. Informatique quantique et scalabilité des infrastructures

Le marché mondial des technologies quantiques pourrait peser 65 milliards de dollars d'ici 2030, avec une croissance annuelle moyenne de 30%. *Source : Deloitte.*
En France, une stratégie nationale dotée d'un budget de 1,8 milliard d'euros vise à positionner le pays parmi les leaders mondiaux, avec des acteurs émergents comme Pasqal, Quandela ou Alice & Bob. *Source : Bpifrance.*

Les TPME et ETI n'ont pas encore pris la mesure de la disruption de ces technologies. Les enjeux sont donc :

- **Maturité des plateformes :** avancées des frameworks quantiques (Qiskit, Cirq, Braket) qui rendent les technologies quantiques progressivement plus accessibles, avec des perspectives d'applications industrielles à moyen terme.
- **Quantique et chiffrement, une transition à anticiper :** le Q-Day, moment où un ordinateur quantique sera capable de casser les algorithmes de chiffrement traditionnels (RSA, ECC) est désormais une prévision réaliste placée au début des années 2030. L'ANSSI recommande aux organisations d'engager dès maintenant leur migration vers des algorithmes résistants au quantique, et appelle à une vigilance particulière face à la stratégie dite «Harvest Now, Decrypt Later», des acteurs malveillants collectant dès aujourd'hui des données chiffrées en vue de les déchiffrer après le Q-Day. *Source : ANSSI.*
- **Prospective :** impact transformateur attendu sur la santé (développement de nouveaux médicaments), la finance (optimisation des portefeuilles) et l'énergie (gestion des identités numériques et sécurité des échanges).

D. Cloud Computing, FinOps et Numérique Responsable

Cloud Computing

En France, le cloud affiche une croissance soutenue d'environ 20% par an, confirmant son rôle de socle incontournable de la transformation numérique. Cette dynamique est portée par l'essor du SaaS, 77% des nouveaux projets réalisés en SaaS au S2 2025 *(Source : Numeum)*, et par la montée en puissance de nouveaux workloads IA, plus intensifs en calcul et en données. Les enjeux pour les entreprises sont :

- **Souveraineté et choix d'architecture :** arbitrage entre hyperscalers américains et acteurs européens, dans un contexte où la souveraineté des données pèse de plus en plus dans les décisions.
- **Préparation des infrastructures à l'IA :** les workloads IA imposent de repenser le capacity planning et d'anticiper les besoins en GPU et capacités de calcul.

FinOps

Avec l'explosion des dépenses cloud, la maîtrise financière devient un enjeu stratégique. Selon Flexera 2025, 84% des responsables IT rencontrent des difficultés à optimiser les coûts de leur infrastructure cloud. Le FinOps s'impose comme une réponse culturelle autant que technique, à l'intersection de la performance technologique et de la discipline budgétaire. Les enjeux sont :

- **Gouvernance financière du cloud :** contrôle des coûts, évitement du surdimensionnement et responsabilisation de toutes les équipes sur l'impact financier de leurs choix techniques.
- **FinOps à l'ère de l'IA :** les workloads IA génèrent des coûts nouveaux et difficiles à prévoir, rendant indispensable une gestion proactive dans des configurations multi-cloud complexes.

E. Numérique Responsable

En 2026, le numérique responsable (NR) évolue dans un contexte fortement marqué par les enjeux de souveraineté et par l'essor rapide de l'IA, qui captent l'essentiel de l'attention stratégique des entreprises. Ce recul se traduit dans les faits : seulement 72% des TPE-PME françaises (-5 points) déploient au moins une mesure concrète de NR. *Source : Baromètre France Num 2025.* Pourtant, l'enjeu environnemental reste réel : en France, 4,4% des émissions de gaz à effet de serre sont liées au numérique, contre 2,5% en 2020, une progression amplifiée par l'essor de l'IA générative. *Source : ADEME 2025.*

Le cadre réglementaire reste peu lisible — refonte du label NR, abondance de travaux théoriques au détriment de l'action — même si la commande publique marque un tournant avec des critères RSE et carbone de plus en plus structurants dans les appels d'offres.

Les enjeux pour les entreprises sont :

- **Lisibilité du cadre NR :** s'approprier les référentiels existants sans attendre la stabilisation du label, et structurer une démarche progressive et mesurable.
- **Réponse aux appels d'offres publics :** formaliser une stratégie RSE et carbone pour répondre aux critères croissants de la commande publique.
- **Pilotage de l'empreinte numérique :** mesurer et réduire l'impact environnemental des infrastructures IT, amplifié par les nouveaux usages IA.
- **Éviter la fracture à deux vitesses :** les PME non soumises aux obligations ESG ont tout intérêt à anticiper des exigences qui se généralisent progressivement.

F. Innovation technologique et financement

Le plan France 2030 (54 Mds€ sur 2022-2027) consacre une part importante au numérique. Environ 35% de ce budget (≈ 8 Mds€) y était initialement dédié, même si les récentes réformes budgétaires ont étalé ces financements sur trois ans (5 Mds€/an sur 2025-2027). Le plan a déjà mobilisé près de 21 Mds€ en deux ans, illustrant son ampleur.

Au niveau européen, la France confirme son rôle de 2ème pays bénéficiaire d'Horizon Europe (11,4% des financements captés), tout en accusant un retard sur ses voisins dans les appels à projets de la filière numérique (9% des financements des projets collaboratifs du pilier II, contre 11,3% pour l'Espagne et 16,3% pour l'Allemagne). L'Occitanie confirme quant à elle la solidité de son écosystème d'innovation : 27% des dossiers Horizon Europe déposés par des acteurs régionaux ont été retenus, représentant 8,1% du montant total obtenu par la France. *Source : Occitanie Europe.*

Pour soutenir et développer l'innovation, les enjeux se confirment :

- **Optimisation de l'accès aux financements européens et nationaux :** Simplification de la structuration des dossiers pour les dispositifs Horizon Europe, BPI France et FEDER.
- **Arbitrage entre dette technique et innovation :** Stratégies de rationalisation des roadmaps produit, entre modernisation des bases technologiques et développement de nouvelles fonctionnalités.

Dans un contexte de tensions commerciales croissantes entre l'Europe et les États-Unis, les enjeux financiers pour les entreprises sont :

- **Transformer l'excellence technologique en succès commercial :** France 2030 et la réussite sur Horizon Europe doivent servir de levier pour conquérir des parts de marché à l'international, notamment pour les acteurs occitans dont le taux de sélection européen est reconnu.
- **Articuler financements publics et croissance privée :** mobiliser les dispositifs publics (Horizon Europe, BPI, FEDER) pour sécuriser les phases de R&D, tout en concentrant les ressources privées sur une croissance commerciale durable.
- **Transformer la solidité technique en avantage compétitif :** une infrastructure agile permet de livrer plus rapidement et de capter les opportunités de marché avant la concurrence.

II. Enjeux sectoriels spécifiques

Le monde économique fait actuellement face aux enjeux du développement du numérique et des technologies. Après une année 2025 marquée par un ralentissement global (+2%), deux secteurs majeurs – l'industrie et la banque – particulièrement atones ont pesé sur l'ensemble de la filière numérique, représentant à eux seuls près de 45% du marché IT en France. La reprise attendue en 2026 repose précisément sur leur redémarrage.
Source : Numeum.

- **Industrie & Manufacturing :** perspectives 2026 : +4,5%. Après une année 2025 difficile, le secteur repart grâce aux investissements dans la robotisation, l'IoT industriel et les jumeaux numériques pour optimiser la production et la gestion des chaînes d'approvisionnement. *Source : Numeum.*
- **Banque & Assurance :** Perspectives 2026 : +2,9%. Retour à la croissance après une année atone, porté par les investissements dans l'IA pour l'analyse des fraudes et l'optimisation des risques, ainsi que par le développement de solutions fintech et blockchain. *Source : Numeum.*
- **Santé & e-Santé :** croissance soutenue confirmée. Explosion de la télémédecine et des plateformes de suivi patient. Usage accru de l'IA pour l'analyse des données médicales et les diagnostics assistés.
- **Secteur Public & Smart Cities :** 2025 aura été l'année de la prise de conscience : le contexte géopolitique a mis en lumière la vulnérabilité des infrastructures et logiciels publics face aux géants américains et chinois. Si cette prise de conscience est réelle, elle se heurte encore à un décalage grandissant entre les attentes en matière de souveraineté (SecNumCloud, ISO27001) et la réalité des budgets disponibles ou de la maturité de la demande. L'enjeu pour 2026 est de traduire cette conscience politique en décisions d'investissement concrètes, notamment sur la modernisation des infrastructures IT et l'expansion des projets de villes intelligentes.
- **Commerce & Retail :** croissance confirmée, portée par le développement du commerce omnicanal et du paiement sans contact. Usage intensif du Big Data et de l'IA pour la personnalisation des offres. Source : Numeum.
- **Agri/Agro :** le secteur présente un visage contrasté. Les petits producteurs et exploitants continuent leur appropriation progressive du numérique et de l'IA, avec des solutions dites «prosumer» leur permettant de répondre aux enjeux d'optimisation des rendements et de résilience face aux aléas climatiques. À l'inverse, les grands acteurs retombent dans les travers de la consolidation et de l'ERPisation à outrance, au détriment de leur performance digitale. Pourtant, le numérique reste une valeur ajoutée considérable pour ceux qui parviennent à le mettre en œuvre efficacement.
- **Mobilités :** parvenir à la neutralité carbone, à la compétitivité, à la souveraineté technologique, à la résilience et à la sécurité. Développer la performance industrielle (IA, cyber, jumeaux numériques), les véhicules intelligents (passage à la 5G, réglementation et sécurité) et digitaliser les systèmes d'énergie (smart charging, vehicle to grid…). *Source : UE, Cluster Totem, SRI.*
- **Bâtiments :** les enjeux de la transition numérique dans le secteur du bâtiment sont de renforcer la sécurité des travailleurs (sûreté des chantiers, géolocalisation, réalité virtuelle), regagner la confiance du public (relation client, coordination et suivi de chantier, plateformes B2C), s'aligner sur les problématiques environnementales (efficacité énergétique des bâtiments) et faciliter le quotidien des entrepreneurs (maquette numérique, outils collaboratifs, dématérialisation et automatisation de la gestion administrative). *Source : SRI.*

- **Eau :** enjeux importants sur la gestion de la ressource, les conflits d'usage et la prédiction. Obligation d'une meilleure utilisation de la donnée par les acteurs publics pour faire face à des collectifs engagés, très enclins à utiliser l'open data et les IA génératives pour justifier leurs positions. *Source : SRI, acteurs publics.*
- **Énergies :** accompagner la transition énergétique des territoires et de l'économie, l'industrialisation des gaz verts, le stockage de l'énergie électrique, le développement des énergies renouvelables et de leur monitoring, l'efficacité énergétique des filières. *Source : SRI.*

A. Focus : Numérique en santé et données médicales

Le secteur de la santé connaît une transformation profonde portée par le numérique et l'IA. Le Ségur du numérique en santé (2 milliards d'euros investis) franchit une nouvelle étape en 2025-2026 : plus de 23 millions d'utilisateurs actifs sur Mon Espace Santé, 513 millions de documents partagés sur l'année, et une hausse de 56% des consultations de dossiers numériques par les professionnels de santé. *Source : Agence du Numérique en Santé, novembre 2025.*

Sur le volet souveraineté, la Plateforme des données de santé (Health Data Hub) abandonne définitivement les solutions extra-européennes pour un hébergement souverain qualifié SecNumCloud, avec pour objectif d'héberger une copie complète du Système National des Données de Santé (SNDS) d'ici fin 2026. *Source : Ministère délégué chargé de la Fonction publique, février 2026.*

Par ailleurs, France 2030 investit 95 millions d'euros pour soutenir l'excellence de la filière imagerie et 50 millions d'euros sur les nouveaux usages numériques en santé. *Source : Direction générale des Entreprises.*

Le numérique en santé fait l'objet d'un cadre européen et français qu'il faut appréhender et qui, s'il pose des contraintes, apporte également des opportunités :

- **Comprendre le cadre légal, technique et fonctionnel** pour obtenir et utiliser des données de santé, dans un environnement réglementaire en construction (RGPD, règlement EHDS entré en vigueur en 2025).
- **Réutilisation secondaire des données de santé :** enrichissement du catalogue SNDS et simplification des accès, avec plus de 200 projets de recherche soutenus par le Health Data Hub en 2025.
- **Interopérabilité et structuration des entrepôts de données de santé**, condition indispensable à l'exploitation de la donnée à grande échelle et aux échanges européens.
- **Usage de l'IA pour le traitement et l'analyse de données médicales :** segmentation d'images, analyse prédictive, assistance diagnostique et essais cliniques, portés notamment par les projets PARTAGES (LLM appliqués à la santé) et SHAIPED (consortium européen IA médicale).
- **Besoins et contraintes des établissements de santé** pour l'acquisition de solutions numériques, dans un contexte de budgets contraints et de cybersécurité renforcée.
- **Modalités d'accès au marché** des outils numériques dédiés à la santé, avec les appels à projets du Health Data Hub et le dispositif «Pionniers de l'IA» de France 2030 (10 millions d'euros pour 23 premiers lauréats en février 2026).

B. Éditeurs de logiciels

Avec une croissance de +8,2% en 2025 et des perspectives à +8,4% en 2026, les éditeurs de logiciels confirment leur rôle de moteur du marché numérique français. Cette dynamique repose sur la migration accélérée vers le SaaS, la demande soutenue en IA et cybersécurité, et des engagements contractuels plus longs.
Source : Numeum.

Pour autant, les défis restent nombreux, notamment autour de l'intégration de l'IA qui pose de nouveaux enjeux technologiques et économiques.

Les enjeux pour les entreprises sont :

- **Intégration de l'IA pour un progiciel augmenté :** choisir les bonnes technologies, maîtriser les coûts, garantir l'éthique et la conformité (RGPD, IA Act), ajouter de la valeur au produit par l'IA et proposer des agents IA adaptés aux métiers.
- **Cybersécurité des solutions :** trouver l'équilibre entre sécurité et expérience utilisateur, sensibiliser les clients, intégrer des solutions adaptées aux budgets contraints des PME-ETI et s'adapter à l'évolution des cyberattaques, notamment celles générées par l'IA.
- **Qualité de service (QoS) pour des clients plus exigeants :** gérer la scalabilité, anticiper les attentes clients, mesurer et améliorer en continu la satisfaction, réduire le churn.

- **Innovation et roadmap :** arbitrer entre court et long terme, optimiser les ressources (humaines, techniques, financières), rester agile face aux évolutions du marché et valoriser le remboursement de la dette technique.
- **Croissance dans un contexte de morosité économique :** maintenir l'équilibre entre rentabilité et innovation, sécuriser la trésorerie, renforcer la valeur perçue des solutions pour fidéliser les clients, augmenter le revenu récurrent et s'adapter au contexte géopolitique actuel.
- **SaaS et IA as a Service (AIaaS) :** montée en puissance des modèles d'abonnement modulaire, avec un mix entre licence fixe et consommation variable. Les usages évoluent profondément : là où les utilisateurs effectuaient des recherches sur Google pour trouver un service ou une application, ils interrogent désormais des LLM comme ChatGPT. Au-delà de l'enjeu SEO, les éditeurs SaaS devront s'intégrer dans les marketplaces d'agents LLM, notamment via le protocole MCP, pour rester visibles et accessibles dans ces nouveaux parcours utilisateurs.
- **Dépendance aux géants américains et souveraineté numérique :** la forte dépendance aux services et outils non-européens expose les éditeurs à des risques croissants de perte de contrôle des données et de souveraineté numérique, dans un contexte géopolitique qui donne une dimension nouvelle à ces enjeux. Au-delà de la conformité réglementaire, les éditeurs doivent désormais anticiper un mode dégradé «hors fournisseurs US» dans leurs plans de prévention reprise et de continuité d'activité (PRA/PCA), ainsi que pour leurs outils de travail quotidiens. Peu de solutions européennes matures et compétitives existent aujourd'hui pour les remplacer — ce déficit constitue à la fois un risque et une opportunité pour les acteurs européens.

C. Directions des Systèmes d'Information

L'évolution des budgets IT en 2025 est de +4,5% en moyenne en France, mais avec un déplacement des investissements vers le Cloud, la cybersécurité et l'IA. *Source : Gartner*
72% des DSI considèrent l'IA comme un axe prioritaire, mais seulement 35% ont déjà mis en place des solutions opérationnelles. *Source : IDC*
60% des entreprises françaises ont migré une partie de leur infrastructure vers le Cloud hybride, mais 40% déclarent encore des difficultés à optimiser leurs coûts. *Source : Numeum*
75% des DSI déclarent des difficultés à recruter en général et particulièrement des experts en cybersécurité et en IA. Augmentation des salaires IT de +8% en moyenne pour les postes les plus recherchés. *Source : Apec*

En 2026, **les principaux enjeux** adressés par les Décideurs IT sont :

- **Intégration de l'IA :** optimisation et automatisation notamment pour ce qui concerne la chaîne de traitement des données
- **Gouvernance :** méthodes et outils de priorisation ainsi que de suivi des projets
- **Souveraineté numérique :** cadre applicable, acteurs, trajectoires (plénière de juin)
- **Cybersécurité et IA :** détection et prévention des menaces par le machine learning
- **Innovation :** identification de nouvelles solutions au travers des startups locales

Avec la montée en puissance de l'IA, les DSI font face à un enjeu majeur de repositionnement : faut-il internaliser les compétences et développer des fonctionnalités en s'appuyant sur l'IA, au risque de se substituer aux éditeurs ? Ou conforter le rôle traditionnel du DSI, structurer les besoins, garantir les usages et la sécurité, et identifier les partenaires robustes ? Ce débat, loin d'être tranché, est au cœur des réflexions du Factory Décideurs IT en 2026.

D. Entreprises de Services Numérique (ESN)

Après une année 2025 difficile, le marché des ESN recule de -1,8% pour atteindre 34,3 milliards d'euros, avec une reprise attendue à +1,4% en 2026, soit 35 milliards d'euros. *Source : Numeum.*

Les enjeux pour les entreprises sont :

- **Repositionnement sur la valeur ajoutée :** la demande se déporte des grands programmes vers des projets plus courts et ciblés, centrés sur l'IA, la cybersécurité et la modernisation des systèmes.
- **Pression sur les marges :** Face à la hausse des salaires et des coûts d'exploitation, les ESN doivent industrialiser leurs processus. Si 81% identifient l'IA générative comme première opportunité de marché, son impact sur les marges reste encore hétérogène. *Source : KPMG/Numeum.*
- **Gestion des talents :** 59% des ESN privilégient la formation interne au recrutement, avec une compétition accrue sur les profils expérimentés en IA et cybersécurité. *Source : Numeum.*

- **RSE comme critère différenciant :** 67% des grandes entreprises déclarent que l'impact carbone pèse dans la sélection des prestataires, faisant de l'engagement RSE un avantage concurrentiel dans les appels d'offres. *Source : KPMG/Numeum.*

E. Réseaux, hébergement, infogérance

Pour ces acteurs, les enjeux sont multiples face à des marchés variés (publics, industriels, individuels…) et des situations conjoncturelles (fin du déploiement du FTTH, impacts environnementaux du numérique, réglementations diverses etc…) ainsi que la montée en puissance de certaines technologies :

- **Environnementaux :** Réduction du coût des data centers, optimisation des PUE, incitation à la mutualisation dans les data center (plutôt que multiplication du matériel et des petits hébergements), durabilité, ou encore limitation de la consommation d'énergie,
- **Technologiques :** adapter les infrastructures à la montée en puissance de l'IA, développement de la connectivité (5G et ses cas d'usage, IoT, continuité); POP (point d'entrée opérateurs) et réduction de la latence; architectures hybrides combinant contrôle local et scalabilité du cloud pour optimiser les performances et la conformité, agilité dans le stockage de données, transport et optimisation des flux de données (compression, charge répartie…), comprendre les impacts possibles du quantique sur les infrastructures;
- **Réglementaires :** protection des données, sécurité de fonctionnement, enjeux de labellisation/certification, réglementation européenne (AI Act, NIS 2, DORA..), identification des exigences réglementaires selon le type de client (santé, banque…)
- **Attentes client :** conception de nouvelles offres (cybersécurité, hébergement sécurisé), numérique de confiance, rapidité de réponse aux incidents, souveraineté et résilience — un enjeu de plus en plus sensible offrant aux hébergeurs nationaux une opportunité de reprendre des parts de marché —, label de confiance.

Menaces : disponibilité du hardware (processeurs, carte mère, barrettes mémoire…), conjoncture internationale et dépendance aux solutions hors Union Européenne.

III. Enjeux transverses de développement

A. Ressources humaines

Les entreprises du numérique font face à des enjeux critiques et parfois contradictoires concernant leurs ressources humaines.

Les enjeux pour les entreprises sont :

- **Métiers du numérique bouleversés en lien avec l'IA et la data :**
  > Transformation : nouvelles habitudes, nouveaux outils, nouvelles façons de travailler
  > Disparition : de certains métiers ou réduction des effectifs sur des missions historiques
  > Création : émergence de nouveaux profils (ingénieur IA, prompt engineer, AI product manager…)
- **Mixité, diversité et inclusion :** s'assurer de s'entourer de tous les profils, toutes les compétences, toutes les visions pour innover, se challenger et éviter les biais.
- **Evolution du métier RH :**
  > Accompagnement renforcé lié aux changements profonds actuels (sociétaux, technologiques, etc…) : participer à la définition d'un nouveau cadre, soutenir les Managers, rassurer les collaborateurs, etc…
  > Gestion de crise "permanente" dans un contexte de transformation accélérée.
  > Formation / Sensibilisation aux risques : cyber malveillance, respect de la réglementation (IA Act, RGPD…), avec une attente croissante vis-à-vis des RH pour définir les politiques associées.
  > Participation à la mesure de la productivité, notamment dans l'évaluation de l'impact de l'IA sur les équipes.
- **Evolution des salaires :**
  Après des années de forte croissance des rémunérations IT, la tendance s'inverse nettement. Les salaires se stabilisent voire reculent sur les profils généralistes, avec un salarié sur deux n'ayant bénéficié d'aucune revalorisation en 2025. Source : Baromètre Seyos / LHH. Dans le Sud de la France, le nombre de candidats disponibles augmente, rendant le marché plus concurrentiel et les entreprises plus sélectives dans leurs recrutements. Source : Fed IT. Seuls les profils experts en IA, cybersécurité et data continuent de tirer leur épingle du jeu avec des rémunérations en progression. Une tendance à confirmer en 2026.

B. Commerce et stratégie Sales & Market

La structuration des équipes commerciales reste souvent un point faible des PME et ETI numériques. En 2026, l'IA s'impose comme un accélérateur majeur de la performance commerciale, avec des entreprises utilisant un CRM enrichi à l'IA enregistrant une hausse de productivité commerciale de 35%. Source : Gartner 2025.

Les enjeux pour les entreprises sont :

- **Automatisation des cycles de vente :** scoring prédictif des leads, personnalisation des offres, automatisation des relances — les stratégies commerciales assistées par IA deviennent un standard.
- **Évolution des modèles d'affaires :** adoption de modèles transactionnels flexibles (consommation à l'usage, abonnements modulaires, freemium optimisé), portés par la généralisation du SaaS et de l'AIaaS.
- **Hybridation des compétences commerciales :** le commercial de 2026 doit maîtriser à la fois les outils IA, la lecture des données et la relation client stratégique. 72% des dirigeants de PME-ETI peinent encore à trouver des usages IA concrets dans leurs processus commerciaux. *Source : Bpifrance Le Lab.*
- **Écosystème de confiance :** la capacité à s'appuyer sur un réseau de partenaires fiables pour faciliter la collaboration et accélérer les cycles de vente reste un enjeu majeur pour les acteurs de l'écosystème numérique régional.

C. Internationalisation

22% du chiffre d'affaires des entreprises du numérique françaises provient de l'export. Source : Numeum.

Dans un environnement international marqué par la fragmentation des échanges et la montée des rivalités commerciales, l'export s'impose plus que jamais comme un levier stratégique de croissance. Les entreprises ayant déjà une expérience à l'international ont d'ailleurs mieux résisté en 2025 que les non-exportatrices, confirmant que l'internationalisation est un facteur de résilience. Pour 2026, les intentions d'exportation des PME-ETI tiennent bon malgré une forte montée des craintes géopolitiques et commerciales. *Source : Baromètre Export Bpifrance Le Lab 2026.*

- **Menaces : asymétrie réglementaire et dépendance aux acteurs non-européens**
  Les membres de l'UE imposent des normes strictes à ses entreprises mais accueillent dans le même temps des entreprises étrangères non conformes aux réglementations européennes. Ainsi, de grands groupes américains peuvent vendre librement sur le sol européen tout en étant soumis à des législations extraterritoriales qui autorisent leur État à accéder aux données utilisateurs. Des abus de position dominante d'entreprises étrangères sont régulièrement observés sur le marché européen, qu'il s'agisse de refus de se conformer aux obligations réglementaires locales ou d'autres comportements anticoncurrentiels. Certains de ces abus ont pu être sanctionnés par les autorités nationales de régulation, mais ces procédures restent longues et les effets dissuasifs limités. L'enjeu pour les entreprises européennes est de réussir à faire face à cette stratégie qui tend à étouffer toute concurrence, en s'appuyant notamment sur la gratuité de certains services comme levier d'éviction.

- **Opportunités : un momentum historique pour les acteurs européens**
  Le marché du numérique mondial a répondu de manière forte au contexte géopolitique, à savoir la position ultra dominatrice des Etats-Unis et l'instabilité géopolitique mondiale, par une ferme volonté d'acquisition de solutions souveraines et même de remplacement de solutions non-européennes déjà en place. Ce phénomène est largement constaté depuis 2025 par des leaders mondiaux basés en France et reconnus par les cabinets américains Gartner, IDC, Forrester, Frost & Sullivan … qui voient leur chiffre d'affaires à l'international fortement augmenter. Ce contexte international représente un véritable momentum pour les entreprises françaises et européennes du numérique. Seul le marché américain reste fermement dans sa logique "America first" tandis que le reste du monde s'ouvre à l'Europe et à ses solutions réglementées.

IV. Sécurité économique : un enjeu stratégique pour la souveraineté numérique

(Partie rédigée en collaboration avec les services de l'État en région, représentants territoriaux du Service de l'Information Stratégique et de la Sécurité Économiques (SISSE), en charge de la mise en œuvre de la politique publique de sécurité économique.)

Dans un contexte d'intensification des tensions géopolitiques, de compétition technologique mondiale accrue et d'extraterritorialité croissante des normes juridiques, la sécurité économique s'impose désormais comme un enjeu structurant pour les entreprises du numérique.

L'Occitanie se distingue par une concentration exceptionnelle d'actifs stratégiques : filières aéronautique et spatiale de rang mondial, écosystèmes santé et biotechnologies, énergie, industrie avancée, ainsi qu'un tissu dense de startups deeptech et d'acteurs du numérique.

Cette richesse technologique place la région parmi les territoires français les plus ciblés par les tentatives d'ingérence économique étrangère, qu'elles soient informationnelles, capitalistiques, juridiques ou technologiques.

Dans cette dynamique, le numérique occupe une position centrale et ambivalente :

- Il constitue un levier majeur de compétitivité, d'innovation et de rayonnement international.
- Il représente également un vecteur d'exposition stratégique, en raison de l'interconnexion permanente des systèmes, de la circulation mondiale des données, des infrastructures cloud globalisées, des partenariats technologiques transnationaux et des modèles SaaS accessibles sans frontière.

Autrement dit, le numérique n'est pas seulement un secteur à protéger : il est aussi le canal par lequel s'opèrent les tentatives de captation, d'influence ou de déstabilisation.

A. Principales menaces relevant de la sécurité économique

Les risques dépassent le seul champ de la cybersécurité et concernent l'ensemble du patrimoine stratégique de l'entreprise.

Parmi les menaces identifiées :

- Captation technologique : appropriation de savoir-faire, d'algorithmes, de codes sources, de données ou de résultats de R&D.
- Prédation capitalistique : prises de participation opportunistes dans des entreprises fragilisées ou stratégiques.
- Déstabilisation juridique ou normative : procédures étrangères visant à obtenir des informations sensibles.
- Pressions extraterritoriales : demandes d'autorités étrangères de communication de données stratégiques.
- Ingérences informationnelles et atteintes réputationnelles.
- Atteintes au patrimoine scientifique, économique et technique, au sens des intérêts stratégiques nationaux.

Dans une économie fondée sur la donnée, l'IA et la propriété intellectuelle, la protection des actifs immatériels devient un facteur clé de souveraineté et de résilience.

B. Un dispositif territorial structuré en Occitanie

La politique publique de sécurité économique repose sur un dispositif coordonné en région, associant les services de l'État, les acteurs institutionnels et l'écosystème économique.

Les Délégués à l'information stratégique et à la sécurité économiques (DISSE), représentants territoriaux du Service de l'Information Stratégique et de la Sécurité Économiques (SISSE), assurent notamment :

- La veille stratégique et la détection des risques liés aux investissements étrangers en France (IEF).
- L'identification et la cartographie des entités économiques stratégiques.
- L'animation de la politique publique d'intelligence économique territoriale auprès des préfets de région.
- L'accompagnement des entreprises confrontées à des situations sensibles.

En Occitanie, un réseau des Référents Sécurité Économique, animé par les DISSE, associe plusieurs acteurs clés de l'écosystème. Digital 113 y participe activement, contribuant à la diffusion d'une culture de protection du patrimoine stratégique au sein de la filière numérique régionale.

Ce dispositif agit en complémentarité avec les acteurs de la cybersécurité (ANSSI, forces de sécurité, plateformes nationales), dans une logique globale de protection du tissu économique régional.

C. Numérique et sécurité économique : un enjeu systémique

Pour les éditeurs de logiciels, ESN, hébergeurs, opérateurs cloud et acteurs de l'IA, la sécurité économique implique :

- L'identification des données et actifs stratégiques critiques.
- La structuration d'une politique interne de protection du patrimoine immatériel.
- L'anticipation des risques liés aux levées de fonds, partenariats internationaux et marchés étrangers.
- La maîtrise des obligations liées à la loi n°68-678 du 26 juillet 1968 dite « loi de blocage », imposant la saisine préalable du SISSE en cas de demande étrangère d'informations sensibles.

Dans un environnement d'internationalisation accélérée et de modèles économiques exposés mondialement, la sécurité économique doit être intégrée dès la conception des stratégies de développement.

D. Outils d'accompagnement et diagnostics

Afin d'accompagner les entreprises dans cette démarche, la Direction Générale des Entreprises met à disposition des outils gratuits de diagnostic.

Le dispositif **Diagseco**, accessible en ligne, permet d'évaluer le niveau de maturité d'une entreprise en matière de sécurité économique et d'identifier ses vulnérabilités prioritaires :
Ces outils constituent une première étape structurante avant la mise en œuvre d'une politique formalisée de protection des actifs stratégiques.

L'année 2026 marque un tournant pour les entreprises du numérique : après une année 2025 de consolidation difficile, les signaux de reprise sont réels pour celles qui sauront se positionner rapidement autour de cinq impératifs stratégiques.

- **Industrialiser l'IA :** passer définitivement de l'expérimentation à la création de valeur opérationnelle, en s'appuyant sur des données de qualité et une gouvernance solide.
- **Renforcer la résilience :** face à une pression cyber croissante et un cadre réglementaire en évolution, la robustesse des infrastructures et des modèles d'affaires n'est plus optionnelle.
- **Saisir le momentum souveraineté :** le contexte géopolitique crée une fenêtre d'opportunité historique pour les acteurs européens. Les entreprises françaises et occitanes ont les atouts pour en tirer parti.
- **Investir dans les talents :** former, fidéliser et diversifier les équipes reste un enjeu fondamental pour conduire la transformation.
- **Protéger son patrimoine stratégique :** dans un contexte d'ingérences économiques croissantes et de tensions géopolitiques, intégrer la sécurité économique dès la conception des stratégies de développement n'est plus optionnel — c'est un facteur clé de souveraineté et de résilience.

Dans ce contexte, Digital 113 et ses membres ont un rôle central à jouer pour fédérer l'écosystème numérique d'Occitanie et porter collectivement l'ambition d'un numérique souverain, responsable et compétitif, au-delà des frontières.

Plus de 40 personnes ont contribué à cette note: administrateurs, pilotes des Factory, et permanents de Digital 113 :

- Françoise NAUTON-INGLIS - SPIRIIT
- Christophe SAINT-PIERRE - MDP DATA PROTECTION
- Arnaud LADRIÈRE - WISP SOLUTIONS
- Simon BRETIN - FLUTILLIANT
- Gaël PHILIPPE - DATASULTING
- Magali GERMOND - LUMIAIRE CONSEIL
- Jean-Louis FRAYSSE - BOTDESIGN
- Amélie LECLERCQ - DIGITAL 113
- Claire MONTEILLET - DIGITAL 113
- Mathilde ALARCON - DIGITAL 113
- Eric STURM - DIGITAL 113
- Angélique RANDOLET - DIGITAL 113
- Virginie ROUTABOUL - DIGITAL 113
- Maud CHAUVET - DIGITAL 113
- Fanny COLAVITTI - DIGITAL 113
- Anaïs EVANDRE - DIGITAL 113
- Julien KALTNECKER - DIGITAL 113
- Martin VERGEZ - DIGITAL 113
- Cédric BATHELET - SI CLOUD
- Audrey GIRMENS - INFORSUD
- Elise SAMOUILLAN - VAL SOFTWARE
- Bruno TÉZENAS DU MONTCEL - NETIA
- Adrien GIULIANI - DEVENSYS CYBERSECURITY
- Anne-Claire DUBREUIL - SICOVAL
- Ronnie GARCIA - OVEA
- Nicolas BERTRAND - IOCEAN
- Nathalie PRUVOST - LISIO
- Jean-Louis SOUMET - ZENIT CONSEILS
- Frédéric LERICHE - DEVENSYS CYBERSECURITY
- Cyril YVER - CAP HORNIER
- Grégoire DE JABRUN - TALLEM
- Gilles LAVIGNE - FRANCE TRAVAIL
- Anne CARON - CDC HABITAT
- Claire BASTY - DISSE Occitanie SERVICE ÉCONOMIQUE DE L'ETAT EN RÉGION
- Pierre TARRADAS - LAZARSOFT
- Stéphane SAAD - OPTIMUM EXECUTIVE
- Caroline DE RUBIANA - CYBER'OCC
- Frédéric MUH - BEA SOLUTIONS
- Nicolas SUSSER - SI CLOUD
- Athéna CALMETTES - FORMIND
- Olivier ARZALIER - CGI
- Jean-François ESCALA - CONSULT'IL
- Hubert GREGOIRE - EXFABRICA
- Fabrice VINCENT - UBIKA
- Anne CORDEL - ARCADE

Digital113

WWW.DIGITAL113.FR | CONTACT@DIGITAL113.FR

Digital 113 est le groupement professionnel qui fédère plus de 300 entreprises du numérique dans la région Occitanie.
Ce Cluster a pour mission d'accélérer le développement économique de ses membres, d'augmenter les synergies avec les leaders économiques et technologiques et d'accroître la coopération entre startups, grands comptes et partenaires. Elle anime l'écosystème numérique régional, développe le maillage territorial et représente la filière auprès des institutionnels locaux, régionaux et nationaux.