

# Un numérique souverain, de confiance, *rêve ou réalité ? réalité ou utopie ?*

**Jeudi 19 septembre 2024**



Coordination scientifique :

**Judith NICOGOSSIAN**

(Association Française d'Anthropologie  
- école de Grenoble)

**Bernard MONNIER (MIM)**



GRENOBLE



Renseignements, programme... :



## Table des matières

<b>1/ Introduction.....</b>	<b>3</b>
<b>2/ Point d'étape sur la stratégie nationale pour le cloud computing .....</b>	<b>3</b>
<b>3/ Souveraineté et confiance numérique : Défis et perspectives .....</b>	<b>5</b>
<b>4/ Enjeux du numérique pour la Santé .....</b>	<b>7</b>
<b>5/ Les politiques de souveraineté numérique au défi des dépendances technologiques de l'Europe .....</b>	<b>9</b>
<b>6/ Verre à moitié vide ou à moitié plein : où situer l'offre souveraine aujourd'hui ? .....</b>	<b>11</b>
<b>7/ Intelligence Artificielle et Souveraineté Technologique .....</b>	<b>12</b>
<b>8/ Présentations de CV.....</b>	<b>13</b>
<b>9/ Technologies quantiques et souveraineté .....</b>	<b>14</b>
<b>10/ Table Ronde – Souveraineté numérique : Le cloud.....</b>	<b>15</b>
<b>11/ Vision de la souveraineté par les entrepreneurs .....</b>	<b>17</b>
<b>12/ La souveraineté numérique via le soutien au développement d'une offre nationale et européenne – l'exemple du cloud .....</b>	<b>18</b>
<b>13/ Préserver la souveraineté numérique de l'État en investissant dans des outils numériques mutualisés.....</b>	<b>19</b>



**Compte-rendu du séminaire :**

**Un numérique souverain, de confiance, rêve  
ou réalité ? réalité ou utopie ?**

**Le 19 septembre 2024**

**Amphithéâtre Becquerel  
École Polytechnique**

**Coordination scientifique :**

**Bernard Monnier (MIM) et  
Judith Nicogossian (Association Française d'Anthropologie – école de  
Grenoble)**

## 1/ Introduction

Bernard Monnier introduit la journée et notamment comment est née l'idée de ce séminaire. Une histoire qui est déjà en partie racontée dans l'interview à [retrouver en ligne ici](#). Il revient sur l'erreur qui est faite dans la fusion des concepts de confiance et souveraineté, notamment dans l'annonce du partenariat en Thalès et Google France. Comment pouvait-on affirmer que ce cloud était « souverain » en s'associant avec une société américaine ?

Il revient ensuite sur le contexte du cloud en 2024, avec une quantité de données produites qui explose, dépassant le zettaoctet. Et qui devraient à chaque fois doubler tous les deux ans. Selon lui, la souveraineté doit s'établir à plusieurs niveaux, au niveau de la production des données (capteurs), au niveau du stockage, au niveau applicatif (software et hardware) et au niveau du financement... Le but de la journée est de savoir où l'on se situe dans cette chaîne de souveraineté.

Il prend alors l'exemple de Xavier Niel, qui affirme avoir lancé son laboratoire d'IA, Kyutai, tout en étant au conseil d'administration de TikTok. Un membre du public intervient pour préciser que de toute manière Kyutai est basé en partie sur des fonds de Google... Doit-on dire que c'est souverain ?

Pour lui, la question n'est pas de savoir si cette dépendance ou ces associations sont bonnes ou mauvaises, mais dans ce contexte, il ne faut point parler de souveraineté, si c'est n'est pas le cas. Bernard Monnier entend, pour ce séminaire, revenir à la définition des choses.

## 2/ Point d'étape sur la stratégie nationale pour le cloud computing Vincent Coudrin, DINUM (Direction interministérielle du Numérique)

[Ressource ici](#)

[Vidéo ici](#)

La Dinum a la charge de la transformation numérique de l'État au service du citoyen. Vincent Coudron a travaillé sur la stratégie nationale pour le Cloud. Il précise que toute la réflexion a eu lieu au moment de la pandémie de Covid, alors que tout le monde était confiné. Elles ont croisé différents sujets : celui de la résilience de l'État et de la souveraineté des ministères (alimentaire, médicale, numérique), de la compétitivité, basé sur le rapport Villani, qui dit qu'on ne peut pas rester sur le bord de la route en matière d'IA, et a posé les bases du Health data Hub, (surtout sur le Cloud et la notion d'hyperscalabilité, qui permet de bâtir des applications avec une forte économie de moyens pour un grand nombre d'utilisateurs. Il revient ainsi sur l'exemple de WhatsApp, qui lors de son rachat par Facebook, reposait sur 60 personnes pour 460 millions d'utilisateurs), et enfin, au niveau hardware : la crise du Covid a pointé notre dépendance à Taiwan en matière de semi-conducteurs, et donc du contexte géopolitique.

Il décrit alors en quoi consiste la stratégies Cloud de l'État. Elle repose sur différents axes :

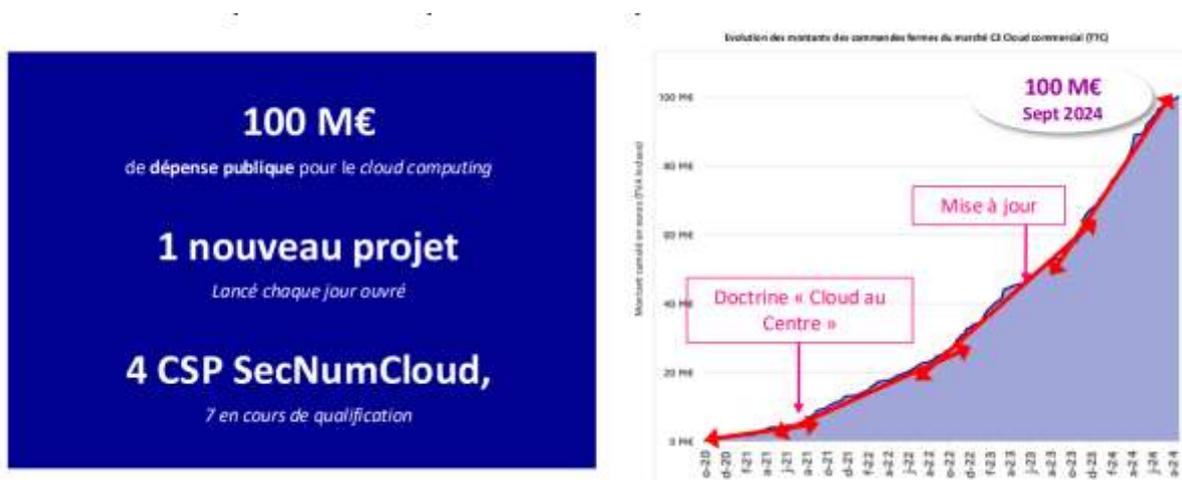
- Le cloud est nécessaire car l'État a un enjeu de transformation (penser usager, progresser sur l'IA et le Big Data, passage à l'échelle pour minimiser les coûts, et améliorer la sobriété numérique)
- un enjeu de souveraineté, qui intègre la confidentialité, l'indépendance vis-à-vis des services – personne ne peut vous couper le courant, votre droit doit primer sur celui des autres, vous devez avoir un leadership technologique et d'accès aux technologies les plus récentes. « Pour l'armée, l'enjeu c'est de gagner la guerre, pas de faire fabriquer vos munitions à Saint Etienne », ironise-t-il. Et la souveraineté intègre également la notion de réversibilité : pouvoir changer facilement et quand vous le souhaitez de technologie ou de services.
- et un enjeu d'accélération.

Vincent Coudron fait ici une remarque d'importance : en 2021, la stratégie consistait, dans les deux premiers enjeux, de transformation et de souveraineté, à conserver la dialectique, et à prioriser l'un puis l'autre, dans un certain équilibre, ce qui est moins possible à l'heure actuelle, selon lui, où les arbitrages peuvent être plus douloureux.

Il détaille ensuite les éléments concrets sur laquelle reposent la stratégie nationale pour le Cloud :

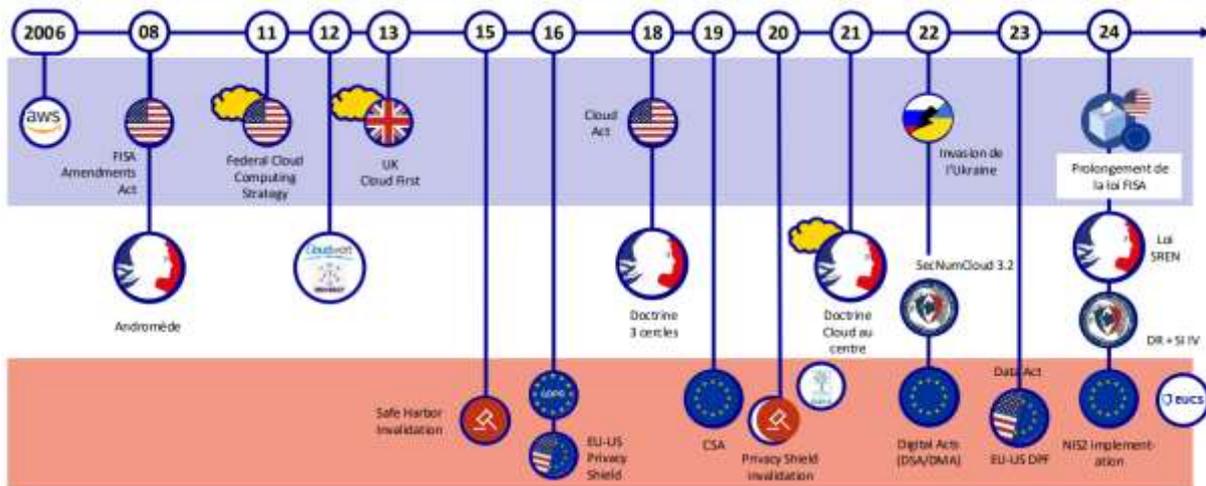
- le label SecNumCloud, pour le Cloud de confiance
- la doctrine Cloud au Centre qui oriente la commande publique
- une politique industrielle adaptée

Il argumente alors sur le fait que ces éléments se sont vérifiés matériellement dans les investissements de l'État :



Les investissements pour le cloud computing ont atteint les 100 millions d'euros de dépense publique depuis le lancement de la stratégie jusqu'à avril 2024.

Il revient alors sur tout le contexte géopolitique de la stratégie numérique depuis 2026 et en détaille les grandes dates dans une « super slides » de résumé :



Il pointe notamment que la guerre en Ukraine, en février 2022 a eu un grand impact dans le sens où elle a permis de redéfinir la notion d'ennemi. « En Europe, les USA ne sont plus considérés comme les méchants », précise-t-il. Et ce, toujours dans l'équilibrage de souveraineté entre leadership (accessibilité aux technologies) et confidentialité des données.

Il insiste alors sur le fait que ce contexte favorise les discussions et l'émergence de nouveaux standards (Euritas, Gaia-X...) ou la collaboration entre différents pays.

Enfin en conclusion, il revient sur différents points clés déterminants. Il insiste sur le fait que souveraineté et confidentialité ne sont en aucun cas synonyme, ou encore qu'il existe une dialectique entre la compétitivité et la protection, qui est inéluctable pour « sortir par le haut du débat ». Selon lui, la commande publique suffira pas, et l'État a besoin du soutien du privé et de l'accès au marché européen. La bataille des standards peut alors aider à cristalliser le marché.

En revanche, il termine sur le sujet de l'IA, qui va s'imposer à nous et poser de nouvelles questions de souveraineté dépassant largement la seule question de la politique du Cloud.

### 3/ Souveraineté et confiance numérique : Défis et perspectives

François Esnol-Feugas, ACN

[Ressource](#)

[Vidéo](#)

François Esnol-Feugas a créé différentes start-ups dans les technologies et la cybersécurité, dont Oxybox en 2014, qui protège les données des clients, et est membre du bureau de l'Alliance pour la Confiance Numérique (ACN). C'est une organisation professionnelle qui regroupe plus de 110 membres, différents acteurs français du numérique, pour porter les débats au niveau national, servir d'interlocuteur avec les pouvoirs publics et rédiger des livres blancs. Il insiste sur le fait que la cybersécurité est essentielle dans le débat de la souveraineté. C'est un domaine évidemment stratégique quand on veut construire la souveraineté, donner de la confiance : on va avoir besoin de technologies capables d'accompagner cette confiance. Vous ne pouvez pas construire de Cloud si vous n'intégrez pas des produits de cybersécurité

au sein de ce cloud, vous ne pouvez pas construire de voitures connectées, si vous n'intégrez pas de produits de cybersécurité dans ces voitures », détaille-t-il.

En 2024, l'ACN a dressé un observatoire afin de faire l'état des lieux de la filière de la confiance du numérique en France. François Esnol-Feugas dresse alors le bilan économique du secteur de la confiance numérique en France, car « le financement c'est le nerf de la guerre », admet-il. Dont voici les principaux chiffres. Notons que c'est la filière économique qui croît le plus vite (8%) de toutes les filières économiques françaises (à égalité avec l'industrie chimique, à 8%).



En matière de financement, si des plans publics comme France 2030 sont essentiels, François Esnol-Feugas souligne l'importance des investissements privés, car ils sont indispensables pour augmenter les capacités d'innovation dans le secteur. (Et l'innovation est aussi le nerf de la guerre).

À ce titre, il revient sur les levées de fonds dans le secteur de la confiance numérique, pour lequel il faut noter que sur les dernières opérations, les montants sont essentiellement captés par Ledger et Chapvision, deux mastodontes du secteur.

Montant des levées de fonds des startups françaises de la Confiance Numérique



□ Le nombre et le montant des levées de fonds des startups de la filière continue d'être élevée **depuis 5 ans**

□ La France est le **2<sup>ème</sup> pays d'Europe** en nombre de levées de fonds et **3<sup>ème</sup>** pour les montants levés

Il décrit alors les mécanismes de marché de la confiance numérique et en quoi l'État peut jouer un rôle déterminant, en étant exemplaire. « Si les mairies ont protégé leurs données, les TPE PME protégeront leurs données », affirme-t-il, mettant en avant le rayonnement de l'État. Idem pour le financement, il met en avant les différences de perspectives entre l'Europe (surtout la France) et les Etats-Unis. « Aux US, les investisseurs acceptent davantage la prise de risque, en partant du principe

que la société finira par créer un monopole, ce qu'on refuse dès le départ en France. Là-bas, on accepte de financer une activité déficitaire pendant 20 ans si les perspectives sont bonnes. Les commandes de l'État jouent aussi un rôle. On accepte de faire confiance à une entreprise qui n'a jamais fait ses preuves », explique-t-il. Il donne comme exemple SpaceX, qui avait déjà des commandes de l'État avant d'avoir envoyé une seule fusée dans l'espace. Or en numérique, ne pas acheter une solution qui n'est pas encore sortie pose des problèmes de financements. Ainsi aux US, le numérique pèse pour 10% du PIB quand en France, on est à 5,5%. Aussi, pour soutenir la filière, il faut à la fois soutenir l'offre par des mécanismes de financements, et soutenir la demande et l'orientation de la demande.

Il revient alors sur les enjeux à venir de l'écosystème de la confiance numérique, qui malgré ses bons chiffres et ses perspectives, reste limitée. Il souligne la prise de conscience des enjeux de confiance numérique, surtout dans un cadre de menaces accrues, et insiste sur le dynamisme des petits acteurs.

Pour son avenir, l'ACN entend favoriser encore la construction d'un écosystème dynamique, et renforcer les synergies et collaboration entre grands groupes et start-up, PME et ETI du secteur. Il détaille également les passerelles avec les autres pays européens. À ce titre, l'ACN a signé un partenariat avec Teletrust, son homologue allemand. Cette question européenne est fondamentale car aujourd'hui, elle se pense en termes de pays, et non en termes de continent. Ainsi, les Finlandais, qui ne développent pas de solutions, ont le choix de travailler avec des solutions allemandes, françaises, qui ne répondent pas, par culture, ou taille de marché trop faible. Alors ils se rapatrient sur les solutions américaines, qui en termes de souveraineté, sont pour eux identiques.

« Il y a énormément de trous dans la raquette dans la manière dont l'Europe gère les acteurs européens et le marché européen. Ce dernier est grand mais malheureusement n'est pas tout à fait uniforme, en termes d'accès au marché, de règles, en termes de langue ni en termes de sensibilité marketing, ni en termes de relais pour pouvoir aller adresser les différents marchés individuels », détaille-t-il.

Il termine en ouvrant sur la question de l'intelligence artificielle, qui est sujet sur lequel l'ACN planche depuis un an, mais qui n'en est encore qu'à ses balbutiements.

## 4/ Enjeux du numérique pour la Santé

**Antoine Tesnière, Paris Santé Campus**

Pas de présentation.

### [Vidéo ici](#)

Antoine Tesnière commence par préciser l'enjeu spécifique des données de santé qui recèlent un caractère intime, et donc nécessitent un regard spécifique. Il précise que le domaine de la médecine est davantage régulé que les autres domaines, comme les transports ou la musique. La transformation numérique de la santé est donc plus longue et moins souple que d'autres secteurs.

Il vante ensuite les bienfaits de l'innovation sur la médecine, et notamment sur le fait que les délais de recherche sont plus courts, en prenant comme exemple les maladies infectieuses, en se focalisant sur les épidémies. Il aura fallu 40 ans pour arriver à stabiliser l'épidémie de Sida, (et 20 ans pour identifier convenablement le virus), mais pour Ebola « il n'aura fallu que quelques mois pour identifier le virus et trouver un vaccin, puis pour le covid, seuls quelques mois pour mettre en place un vaccin et le diffuser à l'échelle mondiale », détaille-t-il. Selon lui, si les échelles de temps se raccourcissent c'est

parce que la connaissance augmente, et si la connaissance augmente, c'est parce que la connaissance est mieux diffusée, mieux partagée, ce qui permet de mieux l'accumuler et de mieux l'exploiter. Et il attribue ces avancées au numérique.

Évoquant l'intelligence artificielle, il pointe le fait que l'IA générative n'est que la pointe émergée de l'iceberg, car cela fait longtemps que dans le corps médical, des travaux et des outils utilisent ces approches depuis plusieurs années. Il donne comme exemple les pompes à insuline, qui nécessitent une mesure en se piquant le doigt, par le passé, et qui dorénavant, utilisent des algorithmes personnalisés via des capteurs sur la peau que le patient porte en permanence.

Il arrive alors sur la stratégie de l'État en matière de données de santé, qui suit l'état de la population, via le codage des actes de soins qui sont exécutés par les médecins et enregistrés dans de grandes bases de données. Antoine Tesnière souligne que c'est assez rare en Europe d'avoir un pays qui ait mis en place une telle politique de santé basée sur la donnée. Toute cette stratégie demande d'être cadrée en termes de régulation, de mettre en place des certifications pour encadrer les acteurs, mais aussi pour que différents hôpitaux puissent échanger des données selon les mêmes protocoles.

Il en vient alors à la stratégie européenne de gestion des données, puisque ce mode opératoire est désormais appliqué au niveau supranational. Les bases de données de santé se posent donc à différents niveaux : national, inter-établissements de santé, et à cela s'ajoute un troisième niveau qui sont les données de santé quotidiennes propre à chaque utilisateur et collectées par des systèmes types montres connectées, ou par des établissements qui ne sont point des établissements de santé.

Ces données de la « vie réelle », à la différence des données nationales contrôlées par l'assurance maladie, ou des données des hôpitaux, cadrés par des protocoles stricts, ne sont pas structurées, sont plus ouvertes, et posent d'autres questions juridiques de partage et de protection.

De manière générale, il insiste sur le fait que la France a souvent été pionnière dans la protection et la régulation des données de santé, qui revêtent un caractère spécifique, et restent contrôlées par le patient. A l'inverse, aux Etats-Unis, par exemple, les données de santé sont considérées comme des données de marché. Ainsi la collecte et la mesure des données de santé en France est en concurrence avec des acteurs privés, et des capitalisations boursières gigantesques. Autre différence en Asie, la donnée de santé est un bien commun contrôlé par l'État. Sa collecte et son échange ne relève donc pas d'une question de propriété.

Mais cela n'empêche nullement l'Europe d'innover en matière de données. Antoine Tesnière donne alors plusieurs exemples d'innovation (pendant la crise covid sur les données infectieuses mise à jour de manière quotidienne sur tout le territoire – même les outre-mers).

Il soulève alors la question du rapport au temps dans l'accès à ces données pour les acteurs privés, qui doivent faire une demande projet avant d'accéder aux données brutes. Il faut alors 12 à 18 mois pour obtenir l'autorisation, pour des raisons réglementaires, et environ six mois de traitement ensuite, quand dans d'autres régions du monde ce délai est beaucoup plus court. Améliorer ce laps de temps peut alors donner un avantage extrêmement compétitif pour certaines organisations.

Il arrive alors à la question européenne de la coordination des politiques multi-pays dans la gestion des données de santé. Un point qui a accéléré avec la crise Covid, et leur mode de financement.

Il pointe tout de même que l'on peut être découragé face aux avancées scientifiques de certains acteurs américains (Google, Facebook ou Apple) notamment du fait du traitement de données massives qui ont donné lieu à des publications scientifiques extrêmement pertinentes. Le recours à l'intelligence artificielle est en cela très percutant. Il insiste alors sur la nécessité de créer des synergies

entre certaines start-up et les services de l'État pour tenter d'améliorer cette compétitivité européenne.

Il conclue alors en pointant la nécessité de sensibiliser tous les acteurs aux enjeux du numériques, notamment dans certaines organisations qui pourraient avoir une défiance envers ce domaine, malgré les progrès phénoménaux qui ont été réalisés et qui ouvrent la voie à davantage d'avancées considérables.

## 5/ Les politiques de souveraineté numérique au défi des dépendances technologiques de l'Europe

**Henri d'Agrain Cigref**

### [Vidéo ici](#)

Henri d'Agrain est un ancien officier de marine. En fin de carrière, il a notamment travaillé au sein de l'État-major en tant que directeur des systèmes d'information et de l'autorité de cybersécurité de la Marine Nationale. Il a quitté la Marine en 2013 pour devenir personne qualifiée auprès des parlementaires de la Commission supérieure du numérique et délégué générale du Cigref depuis 2016.

Le Cigref « réussir le numérique » est un réseau de grandes entreprises et administrations publiques françaises. Il les accompagne en tant que Think Tank et développe des stratégies d'influence au sein des pouvoirs publics et des milieux académiques.

Il point tout d'abord que les adhérents du Cigref n'utilisent pas le terme de souveraineté, car il est « utilisé à tort et à travers », sans être bien défini, et « notamment par des acteurs qui ont intérêt à entretenir une certaine confusion » à son égard, estime-t-il.

Google Cloud, par exemple, définit la souveraineté numérique comme « la façon dont les organisations gardent le contrôle et leur autonomie à mesure qu'elle développent leur stratégie de transformation numérique et de migration vers le Cloud ». Elle s'inscrit donc dans le cadre de l'utilisation d'un outil spécifique. Idem, AWS est en train d'investir massivement dans un projet de Cloud souverain avec 15 milliards de dollars en Allemagne « on comprend bien certaines positions allemandes sur le sujet », tacle-t-il. Idem, VMWare a organisé une conférence à Bruxelles pour expliquer en quoi cette entreprise était « le champion du numérique pour la souveraineté de l'Europe ».

À l'inverse, pour le Cigref, la notion de souveraineté doit être réservée à l'État. Il en donne alors la définition reconnue par les adhérents : « **la notion de souveraineté est un attribut exclusif des états, et dans sa définition la plus orthodoxe : la souveraineté et le pouvoir suprême reconnu à l'état qui implique l'exclusivité de sa compétence sur le territoire national et son indépendance dans l'ordre international où il n'est limité que par ses propres engagements.** »

Tous les autres usages répondent à des objectifs commerciaux.

Selon lui, on retrouve deux usages du terme de souveraineté en économie : une par des acteurs non-européens afin de valoriser ses solutions et avoir accès au marché européen, une autre pour faire valoir sa vision plus protectionniste et interdire l'accès au marché européen. Ce terme a une faible connotation juridique mais un très fort impact émotionnel et politique.

Or jamais une entreprise ne définit ses besoins en termes de souveraineté.

Henri d'Agrain décrit ensuite le marché européen partagé entre trois acteurs américains : AWS, Microsoft et Google. Les providers européens ont vu leurs parts de marché passer de 20% en 2017 à 10% en 2024, sachant que ces mêmes providers européens ont vécu des croissances à deux chiffres.

Il discute ensuite du rapport de Mario Draghi, publié cet été, qui estime que la bataille du Cloud est perdue, et qu'il faut se concentrer sur les couches supérieures, et donc notamment les applications. Cela est discutable car le Cloud n'est pas un domaine du numérique comme un autre, il en est la base et ce qui permet le monde numérique. « Tout se résume à des hardwares et de l'énergie », explique-t-il citant l'entrepreneur Philippe Dewost.

Il fait alors le parallèle entre la stratégie française sur le Cloud et la stratégie de désindustrialisation de la France « l'usine sans usine », qui nous a mis en situation totale de dépendance vis-à-vis de la Chine.

Revenant sur le rapport de Draghi, il établit le comparatif entre les gains de l'industrie américaine et européenne: si on retire l'industrie numérique, les gains sont identiques entre les zones géographiques. On peut donc parler de « tuyaux » directement établi entre la croissance américaine et la croissance européenne, la première aspire toute la deuxième.

Selon Henri d'Agrain, il faut s'interroger profondément sur cette situation, et c'est un des thèmes les moins bien traité dans le rapport du Commissaire européen.

Il liste alors les différents risques que cette situation crée.

Le premier est géostratégique. Si des divergences géostratégiques étaient amenées à exister entre l'Europe et les Etats-Unis, « de la même manière que la Russie a agité la menace du robinet énergétique avec l'Europe, que se passerait-il si les Etats-Unis agitaient le robinet numérique sur l'Europe ? » ?

Le deuxième est économique, par la captation de croissance par les USA de la valeur européenne. Les gains de productivité apportés par le numérique seront absorbés, à l'échelle, par un autre territoire. Et ce d'autant plus que sur un même marché, tous les acteurs bénéficient des mêmes gains apportés par le numérique. Au global, il n'y a donc aucune différentiation entre les acteurs, mais un gain de productivité général absorbé par des acteurs d'un autre territoire. Il explicite alors deux abus de position de dominante « caractérisé » selon ses dires : Microsoft qui augmente de 50% ses tarifs pour le « pack » Office 360, et VMWare, qui depuis son rachat par un géant américain (Broadcom) a multiplié par cinq ses tarifs. « Au total, ce sont 8 milliards qui sont ponctionnés sur l'économie européenne sans aucun gain de productivité pour les entreprises françaises ».

Enfin, le troisième risque est juridique. Puisque les frontières en termes de numérique ne sont pas celles du monde physique. Il cite alors la section 7 du Foreign Intelligence Surveillance Act, qui fait passer la frontière américaine dans tous les GPU américains où qu'ils soient sur la planète. Cette législation, prolongée régulièrement, l'a été de nouveau en avril 2024. Elle autorise les renseignements américains à faire de la récolte massive de données, sans mandat judiciaire, sur toutes les données des personnes non américaines, simplement parce qu'elles sont stockées sur un serveur américain. Et la Chine possède également la même loi. Ainsi quand on stocke des données sur des serveurs d'une entreprise de droits étrangers, aucune législation ne permet de se prémunir de la récolte de ces données par les services de surveillance de ces états étrangers.

Henri d'Agrain invite ainsi à une réflexion collective lorsqu'il s'agit de données concernant des domaines sensibles et stratégiques.

Il donne ensuite des leviers d'actions :

- un législatif et réglementaire (renforcement des normes européennes pour contrôler ces géants et protéger les actifs immatériels européens)
- un économique, par une augmentation de la politique de l'offre. Si l'UE et la France soutient la politique de l'offre, le Cigref invite les États membres à renforcer également la politique de l'offre, par la commande publique, par exemple. Ou des mécanismes fiscaux qui incitent les entreprises à utiliser les services certifiés (SecNumCloud ou le schéma européen de certification des services Cloud).

Il souligne par ailleurs que la pratique de renseignement économique n'est pas un tabou dans le monde Anglo saxon et que la section 7 du FISA permet évidemment cette pratique, afin d'accélérer la concurrence des entreprises américaines.

En conclusion, il présente les travaux du Cigref en la matière : un référentiel sur le Cloud de confiance, qui a été traduit en cahier des charges techniques, pour qu'il soit plus concret. Il termine en alertant sur le fait que si ses sujets ne font pas partie des priorités, la vassalisation technologique européenne sera totale, et il n'y aura pas de retour en arrière.

Et malheureusement, à lire le rapport Draghi, le travail à faire sur le sujet reste total.

## 6/ Verre à moitié vide ou à moitié plein : où situer l'offre souveraine aujourd'hui ?

**Alain Garnier, Jamespot**

[Ressource ici](#)

[Vidéo ici](#)

Alain Garnier est fondateur de Jamespot, une société éditrice de logiciel collaboratif, d'environ cinquante employés et qui est utilisée par 400 000 personnes. Il est impliqué dans le monde numérique depuis des années, notamment en tant que président de l'association Efel Power, qui défend les logiciels français, et en tant que membre de Numeum Cap Digital.

Selon lui, on peut avoir deux visions du numérique à l'heure actuelle, une totalement désespérée (le verre à moitié vide) ou pleine d'espoir (le verre à moitié plein). Mais avant toute chose, « rien n'est écrit », et on pourra y arriver. Il tance alors le « défaitisme français » qu'il trouve d'une « rare puissance ». À force de se dire que tout est perdu, tout sera perdu.

Alain Garnier commence alors par un constat « négatif » : 76 % des achats numériques en B2B en France sont de provenance américaine. Il va jusqu'à parler de « domination totale ». On pourrait parler d'urgence. « Le problème c'est que cela fait quinze ans qu'on parle d'urgence, qu'elle s'aggrave et qu'on ne la traite pas », ajoute-t-il.

Il parle alors de Schizophrénie des dirigeants, dont 93% pensent que c'est un problème, et pourtant, font tout l'inverse de ce qu'ils pensent.

Il présente alors plusieurs chiffres : la France pèse 0,4% du numérique mondial, alors qu'elle devrait en représenter 3%.

Mais malgré ce paysage négatif, le numérique produit pas mal de croissance. Le numérique c'est 6% de croissance, le logiciel, 12%, et 25% pour le Cloud. Mais malgré cela, nous perdons des parts de marché.

Il zoome alors sur le secteur particulier des logiciels de collaboration. Des entreprises qui servent déjà de nombreux utilisateurs. Et il affirme que de nombreuses personnes estiment que l'on n'a pas les offres « au niveau », mais c'est faux. « Le souci c'est que l'on n'arrête pas de leur chercher des poux. Teams était-il réussi dès le départ ? Non. », affirme-t-il. Il estime donc que les dirigeants sont souvent plus cléments avec les solutions américaines, dans les faits. Et que le « tapis rouge » a été déroulé pour Microsoft, avec sa solution Teams.

Il parle alors du manque de détermination face à des solutions qui arrivent, pour tenter d'être à niveau. Tout est question d'investissement, mais pas que financiers. C'est aussi un investissement humain, et des histoires de choix. Il relate alors l'exemple de l'appel à projet public, qui a été un fiasco total.

Il évoque alors le sujet de l'IA en estimant que la réglementation n'est pas du tout assez stricte, notamment en matière de droit d'auteur. « Comment peut-on garantir que l'IA n'est pas un pilleur de données et en particulier de copyright ? Car l'IA pille de manière massive, aujourd'hui, comme Google l'a fait, on l'a laissé faire et nos journaux se sont écroulés. Veut-on que tout ce qui produit de l'intelligence s'écroule ? Ou veut-on faire payer OpenAI sur le fait que quand il des données copyrightées, il doit payer tout comme quand vous achetez un livre ? »

Il arrive alors aux grandes entreprises qui font affaires avec les grands groupes américains, comme Carrefour et rappelle, comme Henri d'Agrain, que « prendre une solution sur étagère d'un géant américain ne fait gagner strictement aucune part de marché, car tout le monde fait comme vous. »

Il revient alors sur les stratégies de Cloud de retailers, comme Lidl. Et insiste sur le fait qu'à partir du moment où l'on affirme « je n'ai pas pu faire autrement », l'on fait face à son incapacité historique, estimant que c'est une posture « infantile ».

Enfin, il revient sur l'aspect légal du problème, et notamment les lois extraterritoriales américaines qui sont une des sources du problème. Il s'interroge sur la manière avec laquelle nous utilisons le droit en Europe, pour contrer les avancées des géants de l'Oncle Sam.

## 7/ Intelligence Artificielle et Souveraineté Technologique

**Stéphane Delaye, Eviden**

[Ressource ici](#)

[Vidéo ici](#)

Stéphane Delaye est Chief Technology Officer chez Eviden. Il est spécialisé dans les systèmes critiques, sans que cela ne représente toute l'activité d'un industriel. Après une rapide présentation d'Eviden, il présente sa vision de l'intégration de la technologie d'intelligence artificielle. Selon lui, le but n'est pas de mettre de l'IA dans les systèmes, mais de rendre les systèmes intelligents. À partir du moment, où l'objectif change, cela permet d'inclure de l'humain dans la boucle.

Idem, il revient sur la notion de souveraineté, qui signifie pour lui obtenir une liberté d'action. Pour le cas particulier des systèmes critiques (armées, défense, renseignement...) une IA doit aussi être robuste, pour viser l'excellence, éthique, en supprimant les biais, et auditable.

Pour ChatGPT par exemple, ce n'est pas un problème d'algorithme de confiance, ou de compréhension du système, en tant que théoricien, mais de confiance dans les données. C'est un modèle probabiliste. « Si dans ces données, davantage de personnes disent que la terre est plate, il finira par dire que la terre est plate », affirme-t-il. Ce n'est donc pas un souci de technologie, mais de données.

Il décrit ensuite l'approche d'Eviden, pour les systèmes critiques. Selon lui, même si le domaine avance très vite, des intangibles ne bougent pas.

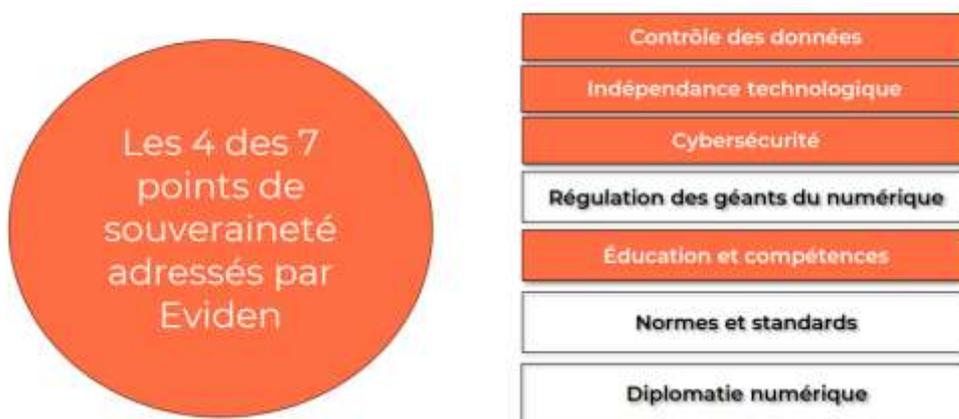
Pour maîtriser ainsi l'écosystème, il n'entraîne les IA que sur des données connues, donc les données des clients, maîtrisées. Il affirme que c'est très simple de placer un bug dans un système d'IA et d'entraînement.

Il revient ensuite sur une « histoire technologique de l'IA », en recontextualisant notamment la place de la France dans cette histoire.

Pour l'expérience, il a demandé à ChatGPT de définir la souveraineté numérique, qui l'a défini en sept points. Les éléments rouges sont ceux traités par Eviden. À ce niveau, Bernard Monnier intervient,

### Les points à l'étude dans le groupe

Quels enjeux pour Eviden



car selon lui, la plupart des points évoqués ne traitent pas de la souveraineté, mais de la confiance, et ChatGPT fait donc une confusion entre les deux notions.

Puis Stéphane Delaye présente les services de conseil en souveraineté numérique d'Eviden pour une transition vers le cloud contrôlée, et présente un outil de scoring qui permet d'évaluer un « score de souveraineté », utilisé par Eviden. Il affirme que selon lui, il n'existe pas dans le monde de modèle d'IA qui soit totalement souverain.

## 8/ Présentations de CV

Se présentent ensuite trois jeunes en quête d'emplois ou d'alternances : Sylvain, doctorant, Carell, étudiante et Victor, étudiant.

[Vidéo Ici](#)

## 9/ Technologies quantiques et souveraineté

**Philippe Duluc, Eviden**

[Ressources ici](#)

[Vidéo ici](#)

Philippe Duluc a travaillé pour la Défense et pour le premier Ministre, pendant une vingtaine d'année, puis a rejoint Orange, et le groupe Atos. Il parlera notamment de deux révolutions technologiques : la cryptographie asymétrique et l'informatique quantique. Dans chaque cas, il commence par un bref rappel historique, puis détaille comment la révolution quantique remet en question la première.

Pour l'informatique quantique, deux innovations majeures sont à distinguer : la cryptographie quantique (dans les années 80) et le calcul quantique avec l'algorithme de Peter Shor. Il précise que les algorithmes de factorisation sont exponentiels. C'est le cœur des algorithmes RSA, de cryptographie, puisqu'il s'agit de mettre en place des opérations faciles à faire dans un sens (multiplier) et très complexe à faire dans l'autre sens (factoriser). Mais l'algorithme de Shor est venu changer toute l'approche, puisque son temps de calcul n'est plus exponentiel, mais polynomial. Donc en ajoutant des bits à factoriser, on ne multiplie plus l'opération par un temps exponentiel mais par un temps linéaire. Une révolution.

Ainsi, le risque qui plane au-dessus de l'informatique quantique est très important. Si on parvient à utiliser convenablement la technologie, toute la sécurité d'internet tombe à l'eau. La cryptographie étant assurée par un temps de calcul trop long pour l'échelle humaine. Mais cette probabilité reste faible. On sait qu'une telle machine n'existe pas encore à ce jour, et que la probabilité de la trouver reste pour le moment assez faible.

Les services secrets américains ont investi beaucoup d'argent pour travailler sur la cryptographie quantique...

Philippe Duluc détaille alors différents cas d'usage essentiellement dans les domaines du renseignement et du militaire, et dresse le bilan des avancées. Trois domaines sont présentés : la cryptographie quantique, les capteurs quantiques et le calcul quantique.

**La cryptographie quantique** : assez avancée. Eviden par exemple, réalise de la cryptographie post-quantique.

**Les capteurs quantiques** : certains existent comme le gravimètre à atomes froids, d'autres sont encore en développement comme les systèmes de navigation inertiels, qui permettent de se passer de GPS, mais d'autres sont encore au stade de l'exploration comme la détection de sous-marin, ou les avions furtifs.

**Le calcul quantique** : Les émulateurs quantiques sont assez avancés (Qaptiva d'Eviden). Pour les autres cas d'usage comme les processeurs quantiques, ceux qui sortent actuellement n'atteignent pas l'accélération exponentielle, du fait de leur taille (10 et 50 qubits seulement). Ce qui interdit encore des cas d'usage en simulation de physique nucléaire, ou de matériaux critiques, idem pour les simulations électromagnétiques.

Pour revenir sur la souveraineté, Philippe Duluc revient sur les modes de contrôle à l'exportation, et notamment un récent arrêté de du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies.

Enfin, il revient sur l'autre mamelle de la souveraineté : la souveraineté financière. Il rappelle qu'en 2021, sur les 2,2 milliards d'investissements dans le quantique, 1,7 milliard ont eu lieu aux Etats-Unis,

et seuls 50 millions en France (qui était pourtant une bonne année). Il note toutefois que sur les 1,7 milliard américain, 1,5 ont été captés par trois entreprises : Rigetti, PsiQuantum et IonQ. Il conclut alors sur la nécessité d'un plan national d'investissement dans ces technologies pour pallier le manque du secteur.

## 10/ Table Ronde – Souveraineté numérique : Le cloud

### [Vidéo ici](#)

La table ronde est modérée par Judith Nicogossian, de l'Association Française d'Anthropologie. Elle introduit le sujet en dressant le parallèle entre la technologie et la religion, une dimension d'analyse introduite par Yuval Noah Harari. Selon elle, la souveraineté numérique s'observe sous trois angles : une dimension juridico-économique, une dimension technologique et une dimension mythologique.

La table ronde réunit Nicolas Hernandez de chez Aleph, Julien Levrard de chez OVH Cloud, et Takwa Nasri de chez Dassault Systèmes.

Julien Levrard commence en répondant à la question sur la définition du Cloud Computing. Pour lui, ce marché procède de la standardisation de l'externalisation des serveurs des entreprises. Au départ, chacune stockait ses données, mais on s'est aperçus que cela coûtait moins cher et offrait davantage de possibilité que de confier cette tâche à des sous-traitants externes. De nouvelles promesses sont nées pour les clients : n'avoir virtuellement aucune ressource en termes de dimensionnement, de nouvelles opportunités dans la capacité à croître ou pour développer de nouveaux usages ; les entreprises peuvent aussi s'affranchir des contraintes matérielles et ne plus être liés aux problématiques de hardware. Takwa Nasri, chez Outscale (une marque de Dassault Systèmes) présente elle sa vision des différentes difficultés à résoudre sur la question de la souveraineté. Selon elle, la dépendance aux acteurs internationaux pose des questions de sécurité, de confidentialité et aussi d'autonomie. Il faut donc y répondre par des mesures techniques et organisationnelles.

Arrive alors Caroline Henry, avocate spécialisée dans le numérique pour le cabinet Phase 4 avocat et est vice-présidente du HealthCare Data Institute un Think Tank dédié à la réflexion sur les données de santé. Selon elle, la question de la souveraineté ne se pose pas assez dans le domaine du droit des données, et notamment des données de santé. Elle cite alors le rapport du Conseil d'État sur la souveraineté, qui a eu le mérite d'établir les définitions des concepts. On voit alors émerger les notions de souveraineté interne (i.e. comment l'État s'organise pour exercer le pouvoir via les institutions) et la souveraineté externe, (i.e. les caractéristiques de l'agencement avec les autres États). La souveraineté s'exerce sur un territoire, ou sur une population. S'établit alors un Pacte : non-ingérence et respect du pouvoir des autres États. La question de la souveraineté dans le domaine juridique est ainsi double : comment faire des choix en tant que peuple français, sans être dépendant des technologies étrangères ? Et comment se prémunir du risque d'ingérence de puissances étrangères ? Takwa Nasri insiste, lorsque l'on parle de sécurité, sur la dimension organisationnelle des mesures, et elle estime que le prisme technique est malheureusement souvent le premier qui vient à l'esprit. Elle prévient alors : attention à ne pas négliger l'autre, afin de maîtriser toute la chaîne de valeur.

Nicolas Hernandez présente à son tour son entreprise, Aleph Networks, qui développe des technologies de moteur de recherche sur le Dark Web. C'est dans ce cadre que cette dernière a dû développer une offre de Cloud. Comme l'entreprise a commencé en travaillant pour le Ministère des

Armées, elle dû « prendre le problème à l'envers ». Ce sont d'abord les contraintes techniques et organisationnelles qui ont imposé un cadre de souveraineté. Pour Nicolas Hernandez, dans le domaine du Dark Web, le Cloud c'est simplement l'ordinateur d'une autre personne. Mais selon lui, il y a différents paliers, au niveau des infrastructures, parfois difficiles à saisir. Cette opacité sur la lisibilité technique de ce qu'est le Cloud, cette complexité à se représenter concrètement ce en quoi il retourne, continue d'alimenter le mythe, et dessert une bonne compréhension du secteur, et la cause de la souveraineté.

Pour Aleph Networks, il est possible aujourd'hui d'être souverain : tout simplement car ils le sont. Pas de Google, pas de sous-traitants externes étrangers « et ce depuis dix ans et sur de grosse volumétrie de donnée ». Ainsi, les entreprises en ont « et la capacité et la compétence ». La souveraineté n'est qu'une question de moyens et de priorité. C'est ce qui le rend « optimiste » sur la question.

Julien Levrard refuse une vision duale de la question de la souveraineté. La souveraineté « n'est pas un interrupteur que l'on allume, avec une offre souveraine cher et complexe et une offre non souveraine facile et pas cher. La souveraineté c'est une famille de risques, c'est une notion étatique qui, pour une entreprise, ne veut pas dire grand-chose. »

Les intervenants détaillent alors les différents niveaux de souveraineté et les contraintes concrètes qu'elle pose dans les organisations, en passant par les besoins clients, qui ne sont pas les mêmes. « Certains clients se moquent de la souveraineté, ils sont internationaux et ont besoin de services qui fonctionnent 24h/24h et 7jours/7jours », estime Julien Levrard. Et les entreprises doivent avant tout répondre aux attentes du marché. Chez OVH, environ 20% des clients ont des demandes de souveraineté formulées. Le débat ne concerne donc pas tous les clients.

Arrive alors Servane Augier, de l'entreprise Numspot, dont le rôle est de faciliter, pour les entreprises, la gestion du risque, afin de basculer dans le Cloud leurs données sensibles, et ainsi externaliser la gestion des données critiques sans crainte. Elle revient sur la certification SecNumCloud, qui intègre 400 points techniques précis, et insiste sur le fait que la difficulté de ce label est avant tout technique avant d'être juridique. Mais pour elle, c'est davantage de confiance dont il est question ici que de souveraineté. D'ailleurs, de nombreux clients de toutes les tailles finissent par en faire la demande dans les contrats et les appels d'offres. Et « comme la confiance ne se décrète pas », le label SecNumCloud révèle toute son efficacité.

Julien Levrard tient à préciser que la question de la souveraineté peut paraître simple lorsqu'on doit bâtir un data center dès le départ en France, mais dès lors que le projet consiste à adapter une structure existante, c'est beaucoup plus difficile. Car il faut revoir toute l'organisation sans la mettre en danger. Nicolas Hernandez ajoute alors un autre concept important, celui de la transparence, qui commence également à être demandé. Les opérateurs doivent alors lister, pour chaque flux de données, d'où il part, où il va et par où il passe. Et il estime que dans 95% des cas, lorsque les entreprises refusent de donner des détails et invoquent des questions de propriétés intellectuelles, elles fuient. En réalité, c'est pour des raisons d'imperfections des systèmes.

La table ronde se poursuit, évoquant tous ces thèmes, en allant sur la question des valeurs européennes, des projets d'intelligence artificielle, et des choix à faire dans l'équilibre entre respect des valeurs et innovations technologiques. Car la souveraineté induit des contraintes techniques qui peuvent être handicapantes.

Les intervenants seront dans l'ensemble très positifs sur les capacités européennes et françaises à intégrer le Cloud de manière souveraine, tempérant le fameux « retard français », ou la « dette technologique » face à des grands acteurs étrangers.

## 11/ Vision de la souveraineté par les entrepreneurs

- **AI-VIDENCE - David Cortes, AI-Vidence**

### Vidéo ici

David Cortes a monté une start-up, AI-Vidence, spécialisée dans l'explicabilité des intelligences artificielles, et il donne sa vision de la dépendance ou non à des systèmes édités par des opérateurs étrangers.

Pour la suite logicielle, les équipes parviennent à utiliser des systèmes Open Sources, afin d'éviter Microsoft, notamment, et cela fonctionne très bien, selon le fondateur. Pour la partie cloud - car la jeune pousse héberge des données – il est possible de stocker les données par des opérateurs français, sur le sol français (OVH, ScaleWay) et un accès aux infrastructures des calculateurs français. Ce n'est qu'une question de volonté.

David Cortes fait ensuite un éclairage de la question via une carte des câbles sous-marins d'échanges de données, qui donnent une lumière d'où transitent les données, notamment en regardant ceux déployés par Google...

Il fait ensuite un autre éclairage sur la question du financement des start-ups, en revenant sur le fait que l'amorçage est souvent assez faisable (pour 100 ou 300 keuros). Mais dès que la levée atteint le million en série A ou B, les investisseurs n'y vont que si un Capital Venture américain y va. Pour les séries C. seules les CV américains permettent de lever des sommes allant de 10 à 100 millions d'euros.

- **PROBABL : Yann Lechelle, fondateur de :Probabl**

Entrepreneurs de la tech, Yann Lechelle a monté six entreprises, dans le domaine du numérique : réseaux sociaux, application, mobile... Il commence par raconter son histoire, et notamment sous l'angle financier, explicitant la réalité pour les investisseurs et les conditions de marché, notamment lorsqu'Apple, dans le cadre des applications, décide de manière unilatérale, de changer les règles du jeu, et peut décider de la vie ou de la mort d'entreprises.

Il revient sur l'exemple d'une start-up qu'il a monté sur le vocal, où personne en France ne voulait faire de série B, et qui a été rachetée 40 millions de dollars par Sonos aux Etats-Unis, un fabricant d'enceinte. Cette exemple illustre selon lui la difficulté en France à faire grandir des jeunes pousses qui finissent sous giron américain. Il insiste alors que le fait que la souveraineté numérique française est « ras les paquerettes », car elle n'est pas financièrement indépendante. La faute aux achats endogènes trop peu nombreux. Si France Digitale tente d'établir un fichier des fournisseurs français des entreprises du numérique, le pourcentage frise les 1 pour mille. Un grand problème selon lui, car de grands acteurs ne jouent pas le jeu.

Mais il reste positif, en estimant que si les entrepreneurs ne se soucient pas de souveraineté, c'est une bonne chose, car ils se concentrent sur le fait de réussir. En revanche, le régalien comment à prendre conscience des enjeux, du fait des crises récentes (Covid, guerre en Ukraine, Trump...) notamment en ce qui concerne le Cloud.

En tant qu'ancien DG de Scaleway, il évoque ensuite l'état d'esprit des acteurs en présence, sur le marché, avec les gafam, très fort en lobbying, et sur le fait que l'Europe s'interdit de faire du protectionnisme, quand tous les autres pays le font. Mais selon lui, la brèche se situe au niveau du multcloud, en imposant aux acheteurs de multisourcer les prestataires, et d'en choisir un local, comme cela se fait sur d'autres marchés, ce qui permettra de créer un appel d'air, en finançant les plus petits opérateurs.

Il présente ensuite son nouveau projet Scikit Learn, une bibliothèque libre de droit en Python destinée au machine learning, développée par l'Inria, et qui a désormais changé de nom pour devenir : Probabl. Le projet comptabilise 5 milliards de téléchargements, en moyenne 68 millions par mois, dans tous les pays du monde. La structure a changé très récemment, et Probabl inaugure un nouveau statut, celui d'entreprises à mission de souveraineté industrielle et numérique. Le but est d'allier la souplesse d'une start-up tout en gardant l'état actionnaire, avec une répartition équitable entre les finances privées et les finances publiques.

## 12/ La souveraineté numérique via le soutien au développement d'une offre nationale et européenne – l'exemple du cloud

**Adrien Laroche, Direction Générale des Entreprises**

[Vidéo ici](#)

[Ressource ici](#)

Adrien Laroche est le coordinateur de la stratégie Cloud France 2030, ce plan d'investissement de 54 milliards d'euros, pour préparer la France de 2030. Après avoir posé la problématique autour de la faible part de marché des acteurs français et européen dans le Cloud, il décrit les trois piliers du plan national : le cloud de confiance, la doctrine « Cloud au centre », établie par une circulaire du cabinet du premier ministre, consistant à choisir le Cloud comme mode de stockage par défaut des données de l'État. Pour les données sensibles, le stockage se fait soit au sein des cloud de l'État (Pi et Nubo) soit dans des serveurs qualifiés SecNumCloud.

Adrien Laroche note que peu de domaine au sein de l'État arrive à combiner soutien à l'offre, processus de protection et soutien par l'achat public, qui selon lui, amène de très bons résultats.

Le troisième pilier de la stratégie consiste en une accélération du développement de service Cloud « innovants et compétitifs ».

Il revient alors sur la stratégie pro-concurrentielle mise en place par l'État, entre le Digital Market Act, la régulation de l'intermédiation des données et le tout récent Data Act, qui vise encadrer l'interopérabilité autour des données, mais surtout la suppression des frais de migration des données. Il revient alors sur le travail mené par l'Autorité de la concurrence, ou encore quelques détails portés par la loi SREN, de régulation de l'espace numérique. Il détaille enfin les efforts de structuration de l'écosystème Cloud en France, mais aussi à l'échelon européen, puisque les deux sont liés, en revenant notamment sur Gaia-X, ou encore le comité stratégique de filière numérique présidé par Michel Paulin.

Il passe alors en revue, toute la stratégie développée par l'Etat, pour soutenir l'écosystème. Une stratégie qui se décline en matrice car portant sur trois échelons : l'infrastructure, la couche logicielle et la couche applicative, et à différents niveaux : la recherche, le soutien à l'offre, et l'innovation.

Le tout est résumé ci-dessous :

## Vue d'ensemble de la stratégie cloud France 2030



Adrien Laroche détaille alors les grands principes de soutiens à l'offre, et notamment la sélection des projets, pour que chaque entreprise réponde bien à un besoin précis en matière de Cloud de confiance, et que si elles se voient financées, c'est pour une question précise. Il ajoute alors le principe de démonstrateur, qui revient à contrôler l'investissement dans le projet, afin que les entreprises ne fassent pas ce qu'elles veulent de l'argent qu'on leur donne.

Enfin, il n'omet pas le volet formation, déjà primordial au sein de l'État, mais qui reste un élément important de la stratégie pour une bonne sélection des fournisseurs et des projets, et une compréhension des enjeux, aussi bien techniques que politico-économiques sous-jacents.

## 13/ Préserver la souveraineté numérique de l'État en investissant dans des outils numériques mutualisés

**Stéphanie Schaer, Directrice interministérielle du numérique**

[Vidéo ici](#)

[Ressource ici](#)

Stéphanie Schaer est directrice interministérielle du numérique depuis 2 ans. Depuis son arrivée, une nouvelle stratégie numérique de l'État a été mise en place. Cette dernière se veut extrêmement simplifiée, « elle tient sur une feuille recto-verso, pour que chaque agent puisse se l'approprier », précise-t-elle. Le but est d'améliorer l'efficacité de l'action publique et de changer la manière dont les grands projets numériques sont conduits.

La stratégie se base également sur la formation, sur la simplification de la circulation des données, et la souveraineté numérique.

La complexité du problème du numérique en France, c'est de faire travailler ensemble, de manière désilotée, des administrations qui n'ont pas fait les mêmes choix techniques dans leur histoire. Au total, ce sont 2,5 millions d'agents qui doivent travailler sur ces systèmes.

Pour ce qui est de la souveraineté, l'État a tenté de bien définir les choses, et deux éléments de bases reviennent de manière récurrente : l'unité au droit extraterritorial (le fait qu'un autre état ne peut pas avoir accès à des données sécurisées de l'État) et surtout l'indépendance technologique, ou plutôt la limitation de la dépendance technologique. Pour lutter contre cela, il faut diversifier ses fournisseurs et ses technologies.

Sur la formation, Stéphanie Schaer admet que la baisse d'effectif dans la fonction publique a eu un effet sur les compétences de l'État qui a dû externaliser, mais depuis 2 ans, les services numériques ont réinternalisé des activités afin de conserver et monter en compétence sur les sujets. Au total, sur l'année 2024, ce sont 345 postes qui ont été réinternalisés.

Au niveau des projets, la directrice interministérielle estime que la bonne échelle est celle de l'Europe, et que dès que quelque chose est fait au niveau français, il faut le partager au niveau européen. Pour ce faire, les projets en open source, sont une bonne façon de faire, pour permettre à chaque administration d'avoir accès à des outils qui sont mutualisés avec les autres. Elle précise ainsi que le réseau interministériel sécurisé qui permet à 14 000 agents de travailler de manière totalement sécurisée, et cela a permis de limiter les impacts en cas d'attaque Dos.

Elle revient alors, à travers d'exemple concrets sur les limites (routeurs) et les projets porteurs de la stratégie (le LLM Albert).

Elle insiste alors sur les besoins d'interconnexion entre les outils, et revient donc sur l'exemple de France Connect, qui d'un point de vue utilisateur, mais aussi et surtout pour les agents, facilite l'interopérabilité entre les systèmes. Au total, 1800 services y sont connectés (sans que cela ne se voit du côté des utilisateurs). Elle détaille alors la politique de connexion pour les agents dans différents ministères. Une mise en œuvre extrêmement simplifiée et s'interroge sur une mise en œuvre européenne d'une telle interopérabilité.

Tout cela ne constitue évidemment qu'une première étape et beaucoup de choses restent à construire. Elle revient sur la signature en février 2024, avec son homologue allemand, d'un accord pour travailler ensemble sur ces sujets. Ici, la notion de « Commun » et donc d'Open Source est très importante. In fine, certains services pourront être payants, pour les collectivités ou des entreprises, ce qui permettrait également de financer ces communs.

Elle conclut en affirmant que le sujet de la souveraineté numérique, dans les états membres européens, est clairement en train de prendre de l'intérêt, que la prise de conscience est réelle et générale.