

L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes.

Article 2 du traité de l'Union européenne (valeurs de l'Union)

Illustration de couverture : image générée par ChatGPT pour illustrer le thème de la réunion !



Propositions précédentes...

Sommaires

Sommaire court

Sommaires	3
La démarche	7
Le numérique.....	15
Les Nations Unies	23
L'Union européenne.....	26
Les Etats membres.....	36
Les régions	39
Les départements.....	55
La ville, les communes	58
Les Etats-Unis, la Chine et l'Union européenne	61
Les microprocesseurs	73
La 5G.....	79
Les données personnelles	88
Les réseaux sociaux.....	99
Le cloud.....	101
ERP.....	121
IA (Intelligence artificielle)	123
La sécurité	135
Le droit et la réglementation du numérique	137
La justice	141
L'environnement	146
La politique publique du numérique.....	147
Annexes.....	164

Sommaire long

Sommaires	3
Sommaire court	3
Sommaire long	3
La démarche	7
La question.....	7
La démarche.....	8
La subsidiarité.....	8
Le privé et le public	9
L'infrastructure numérique	10
Les infrastructures publiques.....	10
Les infrastructures privées.....	11
Le matériel et le logiciel	11
Un ministère du numérique.....	11
L'invitation à la réunion.....	13
Première invitation	13
Autre approche	13
L'ordre du jour	14
La présentation.....	14
Le document préparatoire	14
Le numérique.....	15
Les grandes dates du numérique	15
Qu'est-ce que le numérique ?.....	15
La numérisation transforme les activités humaines	16
Administration	16

Banque	16
Communication	17
Enseignement.....	17
Culture	17
Santé	17
Transport.....	18
Navigation	18
Voyages	18
Énergie.....	18
Emploi	18
Culture	19
La monnaie	19
Le commerce	20
Le numérique et la civilisation.....	20
Les Nations Unies	23
L'Union européenne.....	26
Les traités européens et le numérique	26
La stratégie de Lisbonne et le numérique	30
Le rapport Draghi et le numérique	33
Bilan de la stratégie de Lisbonne	35
Les programmes et les initiatives.....	35
Les Etats membres.....	36
La France.....	36
L'Allemagne	38
Les régions	39
L'Île-de-France	39
La Suisse	40
L'Irlande.....	41
Israël.....	42
La Bretagne	44
Internet en Bretagne.....	44
Les câbles sous-marins	45
L'importance stratégique de câbles sous-marins	46
Avantages d'une Connexion Élevée par Câbles Sous-Marins	46
Connexion directe.....	47
Les initiatives et les actions	49
Les Pays de la Loire	51
Les départements.....	55
Le Morbihan.....	55
La ville, les communes	58
La ville de Lorient.....	58
Les Etats-Unis, la Chine et l'Union européenne	61
Les Etats-Unis	61
Le numérique aux Etats-Unis	61
La comparaison USA-UE	64
La Chine.....	66
Le numérique en Chine.....	66
La comparaison Chine-USA.....	70
Les microprocesseurs	73
Les différents microprocesseurs.....	73
La position de l'Union européenne dans les microprocesseurs	74
Conception et production	76
Economie des microprocesseurs	77
Les microprocesseurs russes	77
La 5G.....	79

La 4G et la 5G.....	79
Délai de mise en place de la 5G.....	82
La 5G chinoise	83
Linux	85
Android	85
Le smartphone.....	85
La bureautique.....	86
Les alternatives à Microsoft office.....	86
Les données personnelles	88
Safe harbor, Privacy shield et Data Privacy Framework	88
Le Privacy Shield.....	89
Les données de santé aux USA	91
Le crédit social.....	92
Les données de santé.....	95
Le recours au Conseil d'Etat	96
Les réseaux sociaux.....	99
Tik Tok.....	99
Le cloud.....	101
L'Union européenne	102
La France.....	102
L'enjeu économique.....	102
La Bretagne	103
Dispositions réglementaires pour un cloud souverain.....	103
GAIA-X	104
Les évolutions à venir	105
Un cloud souverain régional	107
Les entreprises bien positionnées.....	109
Les entreprises bien positionnées en Bretagne.....	111
Le cloud et Gaia-X.....	113
Megalis et le cloud	114
Megalis et La fibre 44	116
Megalis et câbles sous-marins.....	117
Megalis et les opérateurs internationaux.....	118
Megalis et la Normandie	120
ERP.....	121
Les principaux acteurs	121
ERP et souveraineté numérique	121
IA (Intelligence artificielle)	123
Définition	123
L'Union européenne	123
La France.....	123
Stratégie nationale pour l'intelligence artificielle.....	123
Rapport Vilani	124
La Bretagne	125
Analyse SWOT de la filière IA	125
Observatoire de l'intelligence artificielle et de la datascience en Bretagne	125
Acteurs.....	125
Pays-de-la Loire	126
Les pionniers.....	127
Les évolutions prévisibles	127
Les futures ruptures	129
Conditions du positionnement favorables pour les prochaines ruptures.....	130
Politiques publiques américaines versus politiques publiques européennes pour l'IA.....	132
Une exception Mistral AI ?	133
La sécurité	135

Echelon.....	135
Microsoft Cowdstrike	135
Le droit et la réglementation du numérique	137
Le RGPD.....	137
Pas de RGPD aux USA.....	138
La justice	141
Le RGPD.....	141
Le Digital Service Act (DSA) and Markets.....	142
Le Digital Market Act (DMA).....	143
L'environnement	146
La politique publique du numérique.....	147
Comparaison UE-USA.....	147
Financements publics : subventions et autres	148
Réinventer la poudre ?	150
Le marché unique numérique.....	151
La boussole numérique	151
Une hybridation ?.....	152
Orienter le financement public vers l'infrastructure publique	154
Efficacité du financement public de la superstructure privée	155
« sandbox » Bretagne.....	158
Apprentissage innovant et très haut débit	160
Droit à l'expérimentation en Bretagne	162
Annexes.....	164
Le numérique en Bretagne	164
Des initiatives remarquables en Bretagne.....	165
B-Com	165
Treebal.....	165
Icodia	165
iot.bzh	166
pik.bzh	167
Anne Kerdi	167
BreizhIA	167
Des événements du numériques en Bretagne.....	168
Connect'in	168
Breiz dataday	168
Glossaires du numérique.....	168
Bibliographie et vidéographie.....	168
Livres.....	168
Sites Internet.....	168

La démarche

Les ordinateurs, plus on s'en sert moins, moins ça a de chance de mal marcher.

Proverbe shadok

Dans sa réflexion sur les institutions et les politiques publiques en Bretagne, le Cercle Pierre Landais – Association pour le développement local examine l'ensemble des politiques publiques souhaitables pour la Bretagne, ce qui amène le cercle à se poser une série de questions intitulées :

Quelle politique publique pour la Bretagne ?

Se poser ces questions pour une région française d'un Etat membre de l'Union européenne, c'est se poser la question pour toutes les régions et tous les Etats membres de l'Union européenne et s'intéressant aux réponses qu'apportent les autres régions et Etats membres.

Cette question est déclinée pour le numérique en :

Quel numérique pour la Bretagne ?

La question

Les Américains innovent, les Chinois copient et les Européens réglementent.

Proverbe international

La question posée sous-tend celle de la souveraineté numérique¹ qui situe le numérique au même niveau que les fonctions dites régaliennes : le droit et la justice, la diplomatie, la sécurité et la défense... Soit l'importance de la question.

La souveraineté numérique amène à se comparer aux Etats-Unis, les pionniers, et la Chine, les copieurs. Le tableau ci-dessous illustre une partie de la question :

	USA	UE	Chine
	GAFAM		BATX
Moteur de recherche	Google		Baidu
Achat en ligne	Amazon		Alibaba
Réseau social	Facebook	Treebal	Tencent TikTok
Téléphonie, électronique	Apple		Xiaomi
Système exploitation	Microsoft	Linux Android e- solution	?

Tableau 1 - Acteurs majeurs de l'Internet dans le monde

¹ Vie publique - Définition et enjeux de la souveraineté numérique (<https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique>).

Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) sont aussi suivis d'autres pionniers, les NATU (Netflix, Airbnb, Tesla, Uber) qui eux aussi acquièrent une dimension internationale.



Figure 1 – NATU

Certaines applications françaises acquièrent percent en France (Blablacar, Le bon coin, Doctolib...), mais ne s'étendent pas u peu à l'international.

Si la navigation satellitaire peut être rattachée au numérique, l'Union européenne est présente avec Galileo au côté du GPS américain et du chinois BeiDou. On peut considérer que Linux et le protocole TCP/IP adopté par Internet, sont des réussites européennes, qui ne lui confèrent pas pour autant une position de leader mondial.

Le constat principal, c'est que l'Union européenne est quasiment absente de la révolution numérique, elle n'en et pas un acteur majeur ou moteur. La Chine semble mieux se positionner que l'UE pour rattraper les Américains.

La démarche

La finalité de la question posée² est d'évaluer la politique publique du numérique en Bretagne : ce domaine sera d'abord examiné selon deux grilles de lecture :

1. La déclinaison des politiques publiques du numérique dans l'Union européenne déclinée selon les différents niveaux de subsidiarité,
2. La distinction public-privé pour le numérique.

La subsidiarité

Pour ce deuxième point, la subsidiarité se dissocie selon les niveaux : Union européenne, Etat membre France, régions Bretagne, départements, pays, communes et groupements de communes (en prenant l'exemple du Pays de Lorient et de). Sans oublier le niveau des Nations Unies, actif dans le numérique. Soit :

1. Nations Unies
2. Union européenne (à comparer aux USA ou à la Chine, et sur certains points la Russie)
3. France (et autre Etats membres : Allemagne, Italie...)

² Conformément à sa vocation (comprendre, analyser et améliorer les institutions et les politiques publiques en Bretagne). Comme pour toutes les questions posées lors des réunions du Cercle Pierre Landais – Association pour le développement local et régional : quelles politiques publiques pour la Bretagne ?, l'objectif est de définir une ou plusieurs politiques publiques du domaine en question. Ce domaine correspondant en général à un ministère dans un Etat moderne et démocratique avec séparation des pouvoirs.

4. Bretagne (ou autres régions européennes, ou Etats de taille comparable à la Bretagne : Irlande, Suisse...)
5. Départements ou pays (département du Morbihan ou Pays de Lorient)
6. Communes et groupements de communes (communauté d'agglomération de Lorient ou ville de Lorient par exemple)

La souveraineté numérique se décline selon les niveaux de subsidiarité : si un niveau supérieur assure cette souveraineté, les niveaux inférieurs bénéficieront de cette souveraineté. Dans la mesure où la Bretagne est une région d'un Etat membre de l'Union européenne, la question se transpose au niveau européen : l'Union européenne assure-t-elle sa souveraineté numérique, celle de ses Etats membres et de ses régions ? Si besoin, ces Etats membres et ces régions complètent-ils leur souveraineté numérique ?

La souveraineté subsidiaire sera intuitivement mieux assurée s'il y a cohérence dans les politiques publiques déclinées aux différents niveaux, ce qui n'est pas toujours évident.

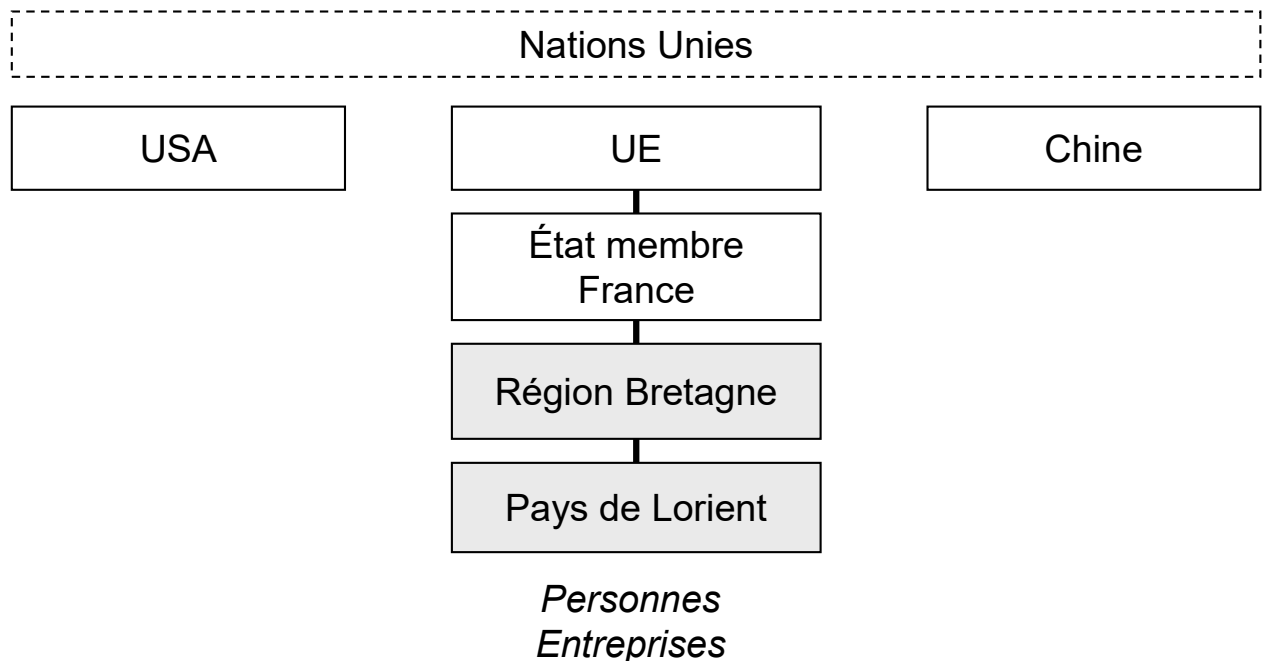


Figure 2 – Numérique et subsidiarité (simplifié sans le département et la communauté de communes).

L'efficacité de toutes politiques publiques (dans tous domaines) tient en particulier à une bonne articulation entre tous ces niveaux.

Le privé et le public

Dans la mesure où la finalité sera la politique publique du numérique, ce vaste sujet qui impacte toutes les activités humaines fera d'abord la distinction entre :

- Les acteurs privés :
 - les personnes : soient les personnes individuelles et les associations de personnes, plus simplement, les associations,
 - les entreprises, selon tous formats (unipersonnelles, selon toutes tailles...).
- L'acteur public qui gèrent une infrastructure publique par diverses entités administratives rattachées à un ministère du numérique au sein du numérique

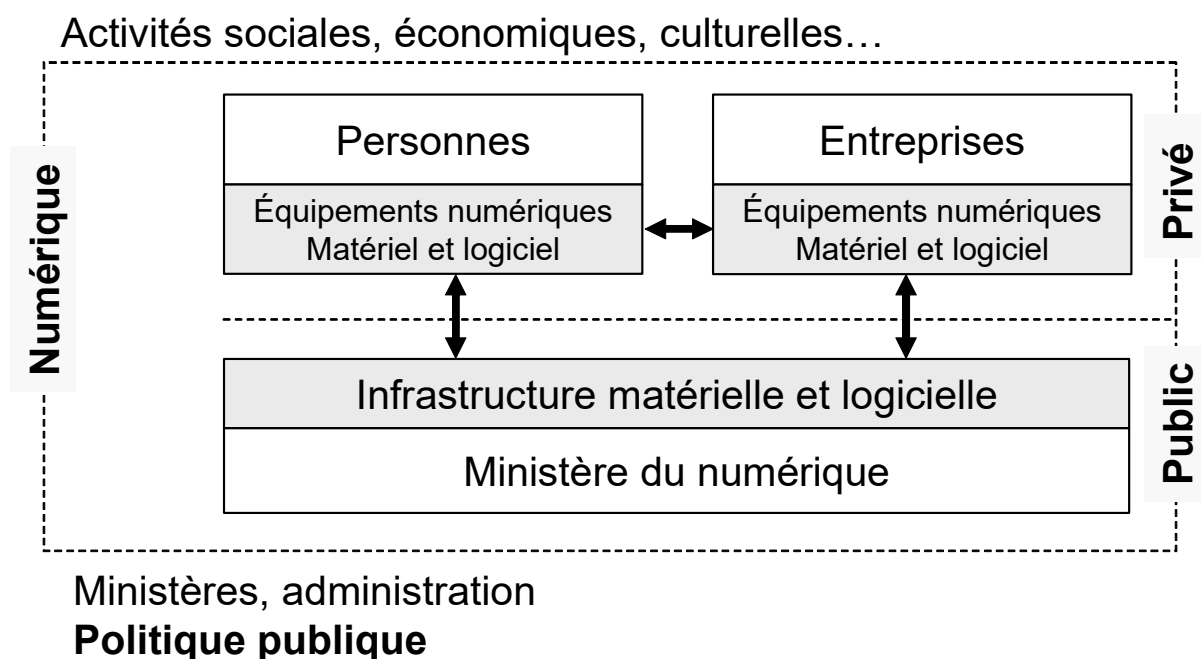


Figure 3 – Les principaux acteurs du numériques.

Les entreprises sont utilisatrices de services privés assurés par d'autres entreprises. Les personnes interagissent numériquement entre elles par divers supports numériques (messagerie, réseaux sociaux)

L'infrastructure et le service public sont nécessités par le fait que l'activité numérique globale doit être organisée par une autorité reconnue, en l'occurrence l'institution publique, et par la nécessité d'administrer des ressources monopolistiques (ne serait-ce que l'espace à réserver pour les réseaux du numérique). L'infrastructure publique associe ou non des entreprises privées, selon des approches différentes en termes de relations public-privé (voire de partenariats public-privé).

L'infrastructure numérique

Le numérique se caractérise par la production, la transformation et la transmission d'informations avec les distinctions entre :

- matériel et logiciel
- systèmes d'exploitation (operating system) et applications,
- Infrastructure publique et superstructure privée
- applications fixe et mobiles.

Les infrastructures publiques

- **Réseaux de transmission de données :** Inclure les réseaux filaires (fibre optique, cuivre) et sans fil (5G, LTE), avec un plan de couverture optimale et équitable. Penser aussi aux nouvelles technologies comme les réseaux satellitaires (Starlink, Galileo pour la navigation) et les réseaux LPWAN pour l'Internet des objets (IoT).
- **Centres de données :** Créer ou encourager l'établissement de centres de données régionaux ou locaux qui respectent les normes environnementales (efficacité énergétique, empreinte carbone) et garantissent la souveraineté des données.

- **Infrastructures de communication** : Développer des hubs régionaux pour les communications sécurisées (en lien avec les solutions européennes telles que GAIA-X), incluant des solutions pour les administrations publiques et les entreprises.

Les infrastructures privées

- **Réseaux privés** : Les entreprises déploient souvent leurs propres réseaux de communication, qui doivent être interopérables avec les infrastructures publiques. Cela inclut aussi la couverture des zones rurales ou isolées.
- **Infrastructures des particuliers** : Assurer l'accès des ménages à des infrastructures numériques performantes (haut débit) et sécurisées, avec des campagnes d'éducation à la cybersécurité pour protéger les équipements domestiques connectés.

Le matériel et le logiciel

Le matériel et les équipements

- **Composants** : Inclure une politique régionale visant à encourager la fabrication ou l'assemblage local de composants électroniques, en partenariat avec des acteurs industriels. Cela peut s'étendre à des solutions de souveraineté en microélectronique et en semi-conducteurs.
- **Équipements** : Promouvoir la production et l'adoption d'équipements de réseau (routeurs, antennes, serveurs), mais aussi des appareils utilisateurs (ordinateurs, smartphones) tout en soutenant les alternatives européennes aux géants américains ou asiatiques.
- **Installations** : Garantir la sécurité physique des infrastructures (protection contre les cyberattaques et les catastrophes naturelles), en collaboration avec les acteurs régionaux de la gestion de crise et les entreprises privées spécialisées en sécurité.

Le logiciel

Systèmes d'exploitation (Operating Systems) : Encourager l'utilisation de systèmes d'exploitation européens ou open-source (comme Linux) pour des raisons de sécurité et de souveraineté, en particulier dans les secteurs publics, l'éducation et les infrastructures critiques.

- Applications :

- **Applications d'entreprises** : Favoriser l'adoption de logiciels européens ou locaux pour les entreprises, dans les secteurs tels que la gestion des ressources, les plateformes de commerce, les outils de communication, etc.
- **Applications publiques** : Développer des solutions numériques régionales pour les services publics, en open-source, favorisant l'interopérabilité entre administrations.
- **Applications citoyennes** : Promouvoir des applications qui facilitent l'inclusion numérique, l'accès aux services régionaux, et la participation citoyenne.

Un ministère du numérique

La numérique est une activité récente dont on considère qu'elle fait suite à deux ruptures technologiques :

- L'apparition de l'ordinateur (après la seconde Guerre mondiale), avec les gros ordinateurs, les mini-ordinateurs puis les micro-ordinateurs, ou encore l'ordinateur individuel à la fin des années 1970
- L'interconnexion des ordinateurs avec en particulier Arpanet en 1969 puis l'émergence d'Internet

Ces ruptures ont impacté les télécommunications radioélectriques et satellitaires qui sont très largement numérisées.

Ces évolutions ont suscité dans tous les Etats, la mise en place d'une administration de cette nouvelle activité humaine à part entière.

A titre d'illustration les ministres ou secrétaire d'état du gouvernement français de puis l'apparition de la fonction ³:

- François Fillon, **Ministre des Technologies de l'information et de la Poste**, de plein exercice du 18 mai 1995 au 6 novembre 1995
- Pas de titulaire entre le 6 novembre 1995 et le 17 juin 2002
- Claudie Haighneré, **Ministre déléguée à la Recherche et aux Nouvelles technologies**, sous la tutelle du Ministre de la Jeunesse, de l'Éducation nationale et de la Recherche du 17 juin 2002 au 30 mars 2004
- Pas de titulaire entre le 30 mars 2004 et le 18 mars 2008
- Sous la Présidence de Nicolas Sarkozy :
- Éric Besson, **Secrétaire d'État chargé de la prospective, de l'évaluation des politiques publiques et du développement de l'économie numérique** du 18 mars 2008 au 15 janvier 2009
- Nathalie Kosciusko-Morizet, **Secrétaire d'État chargée de la Prospective et du Développement de l'économie numérique** du 15 janvier 2009 au 13 novembre 2010
- Éric Besson, **Ministre chargé de l'Industrie, de l'Énergie et de l'Économie numérique** sous la tutelle du Ministre de l'Économie, des Finances et de l'Industrie du 29 juin 2011 au 10 mai 2012
- Sous la présidence de François Hollande :
- Fleur Pellerin, **Ministre déléguée chargée des Petites et Moyennes entreprises, de l'Innovation et de l'Économie numérique** sous la tutelle du ministre du Redressement productif du 16 mai 2012 au 31 mars 2014
- Axelle Lemaire, **Secrétaire d'État chargée du Numérique puis Secrétaire d'État chargée du Numérique et de l'Innovation** sous la tutelle du Ministre de l'Économie, du Redressement productif et du Numérique du 9 avril 2014 au 6 décembre 2016
- Christophe Sirugue, **Secrétaire d'État chargé de l'Industrie, du Numérique et de l'Innovation** du 27 février 2017 au 15 mai 2017
- Sous la présidence d'Emmanuel Macron :
- Mounir Mahjoubi, **Secrétaire d'État chargé du Numérique** du 17 mai 2017 au 21 juin 2017
- Cédric O, **Secrétaire d'État chargé de la Transition numérique et des Communications électroniques** sous la tutelle du Ministre de l'Économie, des Finances et de la Relance,
- Bruno Le Maire, **Ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique** du 20 mai 2022 au 4 juillet 2022
- Jean-Noël Barrot, **Ministre délégué chargé de la Transition numérique et des Télécommunications**, du 4 juillet 2022 au 20 juillet 2023 puis **Ministre délégué chargé du Numérique** du 20 juillet 2023 au 11 janvier 2024
- Marina Ferrari, **Secrétaire d'État chargée du Numérique** du 8 février 2024 au 21 septembre 2024,

3

D'après :

https://fr.wikipedia.org/wiki/Liste_des_ministres_fran%C3%A7ais_du_Num%C3%A9rique

- Clara Chappaz, **Secrétaire d'État chargée de l'Intelligence artificielle et du Numérique** sous la tutelle du Ministre de l'Enseignement supérieur et de la Recherche depuis le 21 septembre 2024 jusqu'à aujourd'hui.

On observe donc un évolution qui part d'un ministre des postes, puis un ministre des postes et des télécommunications, un ministre des télécommunications et du numérique et maintenant un ministre du numérique et de l'intelligence artificielle...

Nous retiendrons un ministère du numérique couvrant les communications désormais numérisées et l'intelligence artificielle, une nouvelle extension du numérique.

L'invitation à la réunion

Première invitation

(voir mail)

Autre approche

(pas utilisée)

La prochaine réunion aura donc pour thème :

Quel numérique pour la Bretagne ?

Soit Internet, les réseaux et les télécommunications, le matériel et le logiciels, les applications fixes et mobiles... La question du numérique sous-tend la question de la « souveraineté numérique », soit la capacité d'un Etat à contrôler et à gérer ses données administratives, celles de ses entreprises et de ses citoyens, ses infrastructures numériques, et les technologies de l'information. Plus encore qu'en d'autres domaines, cette question porte donc d'abord sur les relations entre les Etats-Unis, la Chine et l'Union européenne : les Américains innove, les Chinois copient et les Européens réglementent... cet adage semble plus pertinent encore pour le numérique. Nouveau cas avec l'intelligence artificielle.

L'Union européenne prend diverses initiatives en matière de numérique : ces mesures assurent-elle sa souveraineté numérique, celle de ses Etats membres et de leur régions ? Ou l'idéologie de la concurrence et l'aversion à l'intervention étatique expliquent-elles la quasi-absence de l'UE vis-à-vis des GAFAM et leurs équivalents chinois ? Y-a-t-il (à l'instar des relations économiques) une « naïveté » européenne qui annihile l'esprit même de la souveraineté ou de l'indépendance, en l'occurrence numérique, vis-à-vis des Etats-Unis (Privacy Shield, données de santé ...) ou de la Chine (5G...) ? La propension à la réglementation explique-t-elle la faible créativité et la difficulté à rattraper un retard ?

La stratégie de l'Union européenne sera-t-elle mise en défaut après les élections américaines en cas de victoire du candidat républicain Donald Trump ? Ce candidat a déclaré que le PDG d'Apple, Tim Cook, l'a appelé pour discuter des milliards de dollars d'amende infligés à Apple dans l'UE (déclaration lors de son intervention sur le podcast PBD) et il a déclaré qu'il ne laisserait pas l'UE « profiter » des entreprises américaines comme Apple s'il était réélu. L'Union européenne aurait ensuite prévenu le PDG de Twitter/X qu'elle pourrait calculer les amendes contre la plateforme de médias sociaux en incluant les revenus des autres entreprises d'Elon Musk, notamment Space Exploration Technologies Corp. et Neuralink Corp.

La stratégie défensive et punitive de l'Union européenne résistera-t-elle dans un conflit larvé ou ouvert avec les Etats-Unis ou une telle situation sera-t-elle propice à la prise d'initiatives comme par exemple un service de messagerie comme Treebal écologiquement responsable ?

Les déclinaisons des mesures et des programmes européens au niveau des Etats membres et des régions sont-elles cohérentes dans ce domaine récent et évolutif ? La souveraineté

numérique doit-elle en définitive être assurée localement par les entreprises et les personnes individuelles ? dans une démarche fondée sur la résilience et la synergie citoyennes ?

L'ordre du jour

Voir présentation

La présentation

Voir document en ligne.

Le document préparatoire

La méthode appliquée pour la constitution de ce document relève de la démarche générale du cercle : discussion et construction. La discussion amène à poser la question sur le sujet traité, d'où certaines questions à choix multiples dans le document qui seront intégrées au site <https://united-citizens.eu> en cours de refonte

Le présent document utilise largement l'intelligence artificielle générative qui se révèle un outil très puissant pour élaborer et tester un sujet aussi complexe que le numérique. Ce qui permet un exposé synthétique et clair de la situation actuelle et fait gagner un temps considérable comparativement à une recherche sur internet.

Le présent document utilise donc largement les l'intelligence artificielle générative (ChatGPT et Perplexity en particulier, mais aussi Google Bard, Mistral AI, Perplexity...). Ce qui permet de dégrossir le sujet selon les grands thèmes des réunions :

- Enquête, documentation, instruction...
- Analyse, évaluation... (questions)
- Esquisses ou propositions de politiques publiques ou de projet

Une des finalités du document préparatoire est d'identifier des questions à mettre en ligne sur le site united-citizens.eu en cours de refonte. L'IA propose des réponses à ces questions qui sont généralement correctes et même « bien-pensante ». Ces questions sont reprises lors de la réunion et des réponses plus critiques pourront être émises.

L'inconvénient – ou l'avantage - de cette approche est de générer un document volumineux. Pour s'y repérer, examiner la structure globale du sommaire court et la structure plus globale dans le sommaire long où un article correspond généralement à une question.

Le numérique

Les grandes dates du numérique

Année	Événement	Description
1940s	Ordinateur Central	Développement des premiers ordinateurs centraux, comme l'ENIAC (1945), utilisés pour des calculs complexes.
1960s	Mainframe et temps partagé	Les ordinateurs centraux sont utilisés dans les entreprises et les institutions pour le traitement des données
1970s	Ordinateur Personnel	Émergence des premiers ordinateurs personnels (PC), comme l'Altair 8800 (1975) et le Apple II (1977).
1980s	Réseaux Locaux (LAN)	Développement de réseaux locaux permettant la communication entre ordinateurs dans les entreprises.
1990s	Internet	Commercialisation de l'Internet avec le World Wide Web (1991), transformation des communications et de l'accès à l'information.
1995	E-commerce	Lancement de plateformes de commerce en ligne comme Amazon (1994) et eBay (1995).
2000s	Réseaux Sociaux	Émergence des réseaux sociaux comme Facebook (2004), Twitter (2006), et YouTube (2005), modifiant les interactions sociales.
2010s	Cloud Computing	Adoption massive du cloud computing, permettant le stockage et le traitement des données à distance (ex. AWS lancé en 2006).
2010s	Big Data	Croissance des technologies et des outils pour le traitement de grandes quantités de données.
2016	Intelligence Artificielle	Progrès significatifs en IA avec des avancées en apprentissage profond et en traitement du langage naturel (ex. AlphaGo de DeepMind).
2020s	IA Générative et automatisation	Émergence de modèles génératifs avancés (ex. GPT-3) et automatisation des tâches grâce à l'IA et à l'apprentissage automatique.
2023	Réglementation sur les technologies numériques	Adoption de régulations comme le DSA et le DMA par l'UE pour encadrer les plateformes numériques et la protection des données.

Qu'est-ce que le numérique ?

Qu'est-ce que le numérique ? je donne ma compréhension de façon spontanée. Le numérique tient à la numérisation, digitalisation en anglais, qui fait qu'un traitement matériel d'un objet ou d'une information est réalisé par un logiciel. Ce logiciel traite une donnée formée par une succession d'octets (on pourrait dire de binary digits, bits). Le numérique remplace le traitement matériel des activités humaines par l'exécution du logiciel. Deuxième autre idée forte: le numérique entraîne une dématérialisation du traitement, mais cette dématérialisation n'est qu'intermédiaire entre l'objet ou l'information en entrée et elle ne dispense pas d'un support matériel pour exécuter le logiciel, typiquement un ordinateur et ses périphériques et désormais aujourd'hui, des canaux de communication entre différents processeurs répartis pour traiter un logiciel réparti.

Votre définition du numérique est claire et pertinente, notamment en soulignant deux points essentiels : la numérisation des activités humaines par le biais de logiciels, et le fait que la dématérialisation ne peut se faire sans un support matériel.

Voici quelques idées complémentaires à votre réflexion :

1. **Numérisation** : Vous avez bien pointé que le numérique repose sur le traitement d'informations via des suites de bits (0 et 1). Cette numérisation concerne à la fois les données, comme les images, les textes, ou les sons, et les objets physiques à travers des technologies comme l'Internet des objets (IoT) ou l'impression 3D.

2. **Dématérialisation** : La dématérialisation rend possible la gestion, le traitement, et le partage d'informations sans avoir besoin de manipuler directement des objets physiques. Cela est particulièrement visible dans des domaines comme le travail à distance, les services financiers en ligne, ou encore les archives numériques. Toutefois, comme vous l'avez noté, cette dématérialisation n'élimine pas le besoin d'infrastructures matérielles (ordinateurs, serveurs, réseaux, etc.).

3. **Virtualisation des processus** : Le numérique permet de virtualiser non seulement les données, mais aussi les processus (comme la gestion de production, les interactions sociales via les réseaux, ou encore les services publics en ligne), ce qui réduit les délais, les coûts, et les obstacles géographiques.

4. **Communication et traitement distribués** : Les logiciels modernes, répartis sur plusieurs processeurs ou serveurs à travers le monde, permettent une capacité de traitement et une résilience accrue. Les canaux de communication (réseaux, Internet) que vous mentionnez permettent cette répartition des ressources et des informations de manière quasi instantanée.

En somme, le numérique est un ensemble qui englobe à la fois la dématérialisation des processus et des informations tout en s'appuyant sur une infrastructure physique nécessaire pour faire fonctionner ces transformations. Vous avez bien saisi que le cœur du numérique repose sur la capacité des logiciels à traiter des informations codées, avec des supports matériels qui sous-tendent cette exécution.

La numérisation transforme les activités humaines

Administration

Avantages : La digitalisation des démarches administratives a permis de réduire considérablement les erreurs humaines grâce à des systèmes automatisés. Les formulaires en ligne et les plateformes numériques facilitent le traitement des demandes, accélèrent les procédures, et offrent une manière plus éco-responsable de gérer les documents, réduisant la consommation de papier. Cela améliore également l'accessibilité et la transparence des services administratifs.

Inconvénients : Toutefois, le passage au numérique comporte des défis, notamment en matière de sécurité des données. Les informations personnelles peuvent être vulnérables aux cyberattaques, et la gestion des données sensibles devient cruciale. De plus, des problèmes techniques tels que les bugs ou les pannes peuvent entraver l'accès aux services en ligne, et certains citoyens peuvent éprouver des difficultés à s'adapter à ces nouveaux outils numériques.

Banque

Avantages : La digitalisation des services bancaires a considérablement facilité l'accès aux services financiers. Les banques en ligne permettent aux utilisateurs de gérer leurs comptes 24 heures sur 24 et 7 jours sur 7, offrant ainsi une grande flexibilité. Les transactions sont plus rapides et les processus de gestion sont simplifiés, réduisant le besoin de se rendre physiquement dans une agence. De plus, les services en ligne souvent permettent une meilleure gestion de l'argent grâce à des outils de suivi et de prévision des dépenses.

Inconvénients : Cependant, la digitalisation présente des risques notables. La cybersécurité devient un enjeu majeur avec la possibilité de fraudes et de piratages, mettant en danger les informations financières des utilisateurs. De plus, la dépendance à une connexion Internet est essentielle, et les problèmes de connexion peuvent entraver l'accès aux services bancaires. Les utilisateurs moins à l'aise avec les technologies peuvent aussi se sentir exclus ou confrontés à des difficultés pour naviguer dans les plateformes en ligne.

Communication

Avantages : La digitalisation de la communication a transformé la manière dont les individus interagissent, rendant les échanges plus rapides et moins coûteux. Les emails et les messageries instantanées permettent de communiquer avec des personnes partout dans le monde en temps réel, facilitant ainsi la collaboration internationale et la gestion des relations personnelles et professionnelles.

Inconvénients : En revanche, la surabondance de messages et la dépendance aux outils numériques peuvent entraîner des distractions et une surcharge d'informations. De plus, la communication en ligne peut parfois manquer de la profondeur émotionnelle des interactions en face à face, et les risques de sécurité, tels que le phishing et les violations de données, restent préoccupants.

Enseignement

Avantages : Les cours en ligne et les ebooks ont démocratisé l'accès à l'éducation, offrant aux apprenants une flexibilité et une accessibilité accrues. Les ressources éducatives sont désormais disponibles à tout moment et peuvent être adaptées aux besoins individuels. Cela réduit également les coûts associés aux manuels et permet un apprentissage plus personnalisé.

Inconvénients : Cependant, l'enseignement en ligne peut présenter des défis, tels que le manque d'interaction personnelle et de soutien direct, ce qui peut affecter la qualité de l'apprentissage pour certains étudiants. La nécessité d'équipements technologiques et d'une connexion Internet fiable peut également exclure certains individus, créant des disparités dans l'accès à l'éducation.

Culture

Divertissement

Avantages : Le streaming vidéo et les jeux en ligne ont révolutionné le divertissement en offrant un accès instantané à une vaste gamme de contenus. Les utilisateurs peuvent choisir parmi des millions de films, séries et jeux, avec des options de personnalisation et de recommandation basées sur leurs préférences. Cette flexibilité et cette variété enrichissent l'expérience de divertissement et offrent des possibilités d'engagement et de socialisation.

Inconvénients : Néanmoins, ces technologies peuvent entraîner des risques d'addiction et une consommation excessive de données. Les utilisateurs peuvent également rencontrer des problèmes de confidentialité liés à la collecte de données personnelles pour les recommandations et la publicité ciblée. La surcharge de contenu et la nécessité de gérer des abonnements multiples peuvent également compliquer l'expérience de divertissement.

Santé

Avantages : Les dossiers médicaux électroniques permettent un accès rapide et centralisé aux informations médicales, améliorant ainsi la coordination des soins et la qualité des traitements. Les professionnels de santé peuvent partager facilement les informations entre eux, ce qui facilite le diagnostic et la gestion des soins. De plus, les patients peuvent accéder à leurs dossiers et suivre leur santé plus efficacement.

Inconvénients : Toutefois, la digitalisation des informations de santé présente des défis, notamment le risque de fuites de données sensibles et les préoccupations concernant la cybersécurité. Les systèmes de dossiers médicaux électroniques peuvent être vulnérables aux attaques et aux violations

de données, ce qui nécessite des mesures strictes pour protéger les informations personnelles des patients.

Transport

Avantages : Les billets électroniques et les réservations en ligne ont simplifié le processus de planification et de réservation de voyages. Les voyageurs peuvent acheter leurs billets, gérer leurs itinéraires et suivre leurs réservations de manière plus pratique. La digitalisation a également permis des innovations telles que les alertes en temps réel pour les retards et les changements d'itinéraire.

Inconvénients : En revanche, la dépendance aux technologies peut entraîner des complications en cas de problèmes techniques ou de pannes de système. Les voyageurs peuvent rencontrer des difficultés pour résoudre des problèmes rapidement sans assistance physique. De plus, les questions de sécurité concernant les informations personnelles et de paiement restent préoccupantes.

Navigation

Avantages : La digitalisation a révolutionné la navigation avec l'introduction des GPS sur smartphones. Les utilisateurs bénéficient d'une précision en temps réel, de mises à jour automatiques des cartes, et d'itinéraires optimisés en fonction du trafic actuel. Cela rend les déplacements beaucoup plus efficaces et permet une planification de voyage plus facile, tout en offrant des fonctionnalités supplémentaires comme les alertes sur les conditions routières.

Inconvénients : En revanche, la dépendance aux technologies GPS peut poser des problèmes. Les appareils peuvent rencontrer des difficultés en cas de perte de signal ou d'erreurs de localisation, affectant ainsi la fiabilité des directions. De plus, la collecte de données de localisation pose des questions de confidentialité, et les utilisateurs doivent être conscients des risques associés à la vie privée et à la sécurité des informations personnelles.

Voyages

Avantages : Les réservations en ligne et les billets électroniques ont simplifié la planification des voyages en offrant une commodité accrue et une capacité de comparaison des options. Les voyageurs peuvent gérer leurs réservations facilement et accéder à des informations en temps réel, ce qui améliore l'expérience de voyage et réduit les erreurs de réservation.

Inconvénients : Toutefois, la digitalisation peut entraîner des problèmes techniques et des risques de fraude en ligne. Les utilisateurs peuvent rencontrer des difficultés avec les systèmes de réservation en cas de problèmes techniques, et la sécurité des transactions en ligne peut être une préoccupation constante.

Énergie

Avantages : Les compteurs intelligents et les relevés numériques permettent un suivi plus précis et en temps réel de la consommation d'énergie. Ces technologies offrent des alertes pour les anomalies et permettent une gestion plus efficace des ressources énergétiques. Cela peut conduire à des économies d'énergie et à une meilleure planification des besoins énergétiques.

Inconvénients : Cependant, les compteurs intelligents peuvent soulever des préoccupations en matière de confidentialité des données, car ils collectent des informations détaillées sur la consommation des utilisateurs. Les coûts d'installation et de maintenance de ces technologies peuvent également être élevés, et il peut y avoir des défis techniques liés à leur intégration avec les infrastructures existantes.

Emploi

Ressources humaines

Avantages : La digitalisation des processus de recrutement, tels que les CV numériques et les entretiens vidéo, a accéléré la recherche et la sélection des candidats. Les recruteurs peuvent accéder

à un plus grand nombre de candidats et effectuer des évaluations plus efficaces grâce aux outils en ligne. Cela rend le processus de recrutement plus transparent et accessible.

Inconvénients : Cependant, le manque de contact personnel lors des entretiens vidéo peut affecter la qualité des évaluations et des interactions. Les biais technologiques peuvent également influencer les décisions de recrutement, et les candidats peuvent se sentir désavantagés s'ils n'ont pas accès à une technologie adéquate.

Culture

Avantages : Les applications de cuisine et les recettes en ligne offrent un accès instantané à une grande variété de recettes et de conseils culinaires. Cela permet aux utilisateurs de découvrir de nouvelles recettes, de personnaliser leurs plats, et d'améliorer leurs compétences culinaires avec des guides interactifs et des vidéos.

Inconvénients : Cependant, la dépendance aux outils numériques peut limiter l'utilisation des méthodes traditionnelles de cuisine et poser des problèmes si l'accès à Internet est interrompu. Les utilisateurs doivent également être conscients des risques potentiels liés à la confidentialité des données lorsqu'ils utilisent des applications de cuisine.

La monnaie

La monnaie électronique

La monnaie électronique remplace la monnaie papier ...

1. Accessibilité et Inclusion :

- **points favorables:** La disparition de la monnaie papier pourrait simplifier les transactions en rendant les paiements plus rapides et pratiques via les méthodes électroniques. Cela pourrait également réduire les coûts liés à la production et à la gestion de la monnaie physique.
- **points défavorables:** Les personnes sans accès facile aux services bancaires numériques ou aux technologies nécessaires pourraient être exclues. Cela inclut les personnes âgées, celles vivant dans des zones rurales éloignées, et les personnes à faibles revenus.

2. Sécurité et Fraude :

- **points favorables:** Les transactions électroniques peuvent réduire certains risques associés à la monnaie papier, comme le vol et la contrefaçon. Elles peuvent également offrir des mécanismes de sécurité avancés pour protéger les fonds.
- **points défavorables:** Les systèmes de paiement électroniques peuvent être vulnérables aux cyberattaques, aux fraudes numériques et aux erreurs techniques. Cela nécessite des mesures de sécurité renforcées pour protéger les données personnelles et financières.

3. Efficacité et Coûts :

- **points favorables:** L'élimination de la monnaie papier peut réduire les coûts de production, de gestion et de transport. Les transactions électroniques peuvent également offrir des processus plus rapides et plus efficaces.
- **points défavorables:** Les coûts de mise en place et de maintenance des systèmes électroniques peuvent être élevés, notamment pour les infrastructures nécessaires à leur fonctionnement.

4. Impact Environnemental :

- **points favorables:** La disparition de la monnaie papier peut réduire la consommation de ressources naturelles et l'empreinte écologique associée à la production de monnaie physique.
- **points défavorables:** Les systèmes électroniques nécessitent une consommation d'énergie et une gestion des déchets électroniques, ce qui peut également avoir un impact environnemental.

5. Pratiques Culturelles et Habitudes :

- **points favorables:** La numérisation peut moderniser les pratiques commerciales et financières, facilitant les transactions dans une économie de plus en plus numérique.
- **points défavorables:** Certaines cultures et traditions valorisent l'utilisation de la monnaie papier. Sa disparition pourrait affecter les pratiques culturelles et les habitudes de consommation.

Question : la monnaie électronique doit-elle remplacer totalement la monnaie papier ?

Réponse : oui – non – NSP

Le commerce

Achats

Avantages : Le commerce en ligne a apporté une commodité sans précédent, permettant aux consommateurs de faire leurs achats à tout moment et de n'importe où. Les plateformes en ligne offrent une vaste gamme de produits et permettent de comparer facilement les prix. Cela a également entraîné une réduction des coûts liés aux magasins physiques et amélioré l'efficacité des achats grâce à des recommandations personnalisées et des avis clients.

Inconvénients : Cependant, les achats en ligne présentent des inconvénients tels que le risque accru de fraude en ligne et les problèmes liés à la confidentialité des informations de paiement. Les consommateurs peuvent aussi rencontrer des difficultés pour évaluer la qualité des produits avant l'achat, ce qui peut entraîner des retours ou des déceptions. De plus, les achats en ligne peuvent encourager une consommation excessive et une dépendance aux technologies.

Le commerce en ligne permet à chaque entreprise de commerce de vendre directement à des clients. Mais encore faut-il être visible et des grands sites comme Amazon, Alibaba... trônent sur ce marché et associe des entreprises qui deviennent très dépendantes de ces grands acteurs et doivent accepter leurs conditions.

Le numérique et la civilisation

Le numérique, souvent utilisé de manière interchangeable avec le terme digital, entraîne en effet une profonde transformation de la civilisation contemporaine. Si les termes peuvent être similaires, leur portée va au-delà du simple changement technologique : ils touchent à l'organisation sociale, aux modèles économiques, aux rapports humains et à la culture. Voici quelques façons dont le numérique modifie la civilisation :

1. Révolution des modes de production et de consommation

Le numérique a radicalement changé la manière dont les biens et services sont produits, distribués et consommés. Avec l'automatisation, les robots industriels, l'intelligence artificielle (IA) et l'Internet des objets (IoT), des secteurs comme l'industrie manufacturière, l'agriculture et les services ont vu leurs processus transformés. Par exemple :

- Automatisation et IA remplacent ou assistent les tâches humaines, ce qui redéfinit les emplois et les compétences requises.
- E-commerce et plateformes en ligne modifient les habitudes de consommation, dématérialisant l'acte d'achat (ex. : Amazon, Uber).

Économie des plateformes (Uber, Airbnb) réorganise la manière dont les ressources sont échangées.

2. Transformation des relations humaines

Les outils numériques modifient en profondeur les interactions sociales :

Réseaux sociaux : Le développement des plateformes numériques (Facebook, Twitter, Instagram) a transformé la manière dont les gens interagissent et partagent des informations, créant une culture mondiale interconnectée. Cela change les relations sociales en introduisant des formes d'interaction médiées par des interfaces.

Communication instantanée : Le numérique permet une communication quasi immédiate, réduisant les distances géographiques et transformant les dynamiques familiales, professionnelles et amicales.

3. Nouvelles formes de travail et d'organisation sociale

La digitalisation du travail est en train de modifier profondément la manière dont les sociétés fonctionnent :

- **Télétravail** : La numérisation des infrastructures permet le travail à distance, une tendance accélérée par la pandémie de COVID-19. Cela reconfigure les espaces urbains et les dynamiques professionnelles.
- **Nomadisme numérique** : Grâce à l'accessibilité des technologies numériques, certains individus peuvent travailler de n'importe où, ce qui transforme la relation au lieu de travail et à l'emploi.
- **Économie de l'attention** : L'économie numérique repose sur la capacité à capter l'attention des utilisateurs via des interfaces engageantes. Cela crée de nouvelles dynamiques commerciales et économiques basées sur l'engagement des utilisateurs (publicité, médias sociaux).

4. Changement des modes d'apprentissage et d'éducation

L'impact du numérique est particulièrement visible dans l'éducation :

- **Éducation en ligne** : Les plateformes numériques ont transformé l'accès au savoir (MOOCs, plateformes comme Coursera, Khan Academy). Cela démocratise l'éducation, permettant l'accès à des formations pour des populations éloignées des systèmes éducatifs traditionnels.
- **Éducation personnalisée** : L'intelligence artificielle permet de développer des outils d'apprentissage adaptatifs, qui répondent aux besoins spécifiques des étudiants.

5. Impact sur les politiques et les démocraties

Le numérique bouleverse aussi la manière dont les sociétés s'organisent politiquement :

- **Participation citoyenne** : Les plateformes numériques permettent de nouvelles formes de participation démocratique, comme les pétitions en ligne, les forums de débat, ou encore les initiatives de démocratie participative.
- **Fake news et manipulation de l'information** : Le numérique a également transformé la circulation des informations, rendant plus facile la diffusion de fausses informations ou la manipulation médiatique à grande échelle, ce qui peut fragiliser les démocraties.

6. Redéfinition de la vie privée et des libertés individuelles

Le numérique modifie les concepts de vie privée et de sécurité :

- **Données personnelles** : Avec la numérisation croissante des activités humaines, la collecte de données personnelles devient omniprésente (ex. : via les smartphones, objets connectés, réseaux sociaux), ce qui pose des questions sur la protection de la vie privée et la souveraineté des individus.
- **Cybersécurité** : La numérisation des infrastructures critiques (énergie, finance, santé) rend les États et les entreprises plus vulnérables aux cyberattaques, soulevant des enjeux de sécurité nationale et mondiale.

7. Changement culturel et philosophique

Le numérique transforme les fondements mêmes de la culture :

- **Dématérialisation de la culture** : Les œuvres culturelles (livres, films, musiques) sont désormais accessibles en ligne, modifiant les modalités de production et de consommation culturelle. Cela rend la culture plus accessible, mais entraîne aussi des tensions sur les droits d'auteurs et la viabilité économique des créateurs.
- **Identité numérique** : Avec l'essor des réseaux sociaux, l'identité d'une personne ne se limite plus à son environnement physique, mais inclut aussi sa présence numérique, redéfinissant la perception de soi et des autres.

Conclusion : le numérique comme vecteur de transformation civilisationnelle

Oui, le numérique modifie profondément la civilisation. Il ne s'agit pas seulement d'un changement technique, mais d'une transformation globale qui affecte tous les aspects de la vie humaine, des relations sociales à l'économie, en passant par la culture, la politique et l'identité. Le numérique accélère le processus de mondialisation tout en posant des défis majeurs en termes de souveraineté, de vie privée, de sécurité et d'équité sociale. Il redéfinit les rapports entre l'humain et la technologie, entraînant des réflexions philosophiques sur la nature du travail, de la communication, et de la réalité elle-même.

Les Nations Unies

C'est peut-être le Pacte numérique mondial⁴ selon sa Révision 3⁵ qui exprime au mieux une vision du numérique au service des droits humains et d'un développement durable.

<https://www.intgovforum.org/fr/aboutabout-us>

ChatGPT : Comment sont organisées les Nations Unies pour le numérique : quelles sont les orientations, les programmes ... ?

Les **Nations Unies (ONU)** jouent un rôle central dans la coordination des politiques mondiales en matière de numérique, en particulier en ce qui concerne la **gouvernance d'Internet**, la **protection des droits de l'homme en ligne**, et la **promotion de l'inclusion numérique**. Bien que l'ONU ne soit pas un acteur direct dans le développement technologique, elle s'efforce d'encadrer et d'orienter les efforts internationaux pour garantir que la révolution numérique soit inclusive, équitable et respectueuse des droits humains. Voici comment les Nations Unies sont organisées autour des enjeux numériques, ainsi que les programmes et initiatives clés.

1. Organisation principale : l'UIT (Union internationale des télécommunications)

L'**Union internationale des télécommunications (UIT)** est l'une des plus anciennes agences spécialisées des Nations Unies, créée en 1865 pour coordonner les standards mondiaux en matière de télécommunication. Aujourd'hui, l'UIT joue un rôle crucial dans la gestion des infrastructures numériques et la régulation des technologies de l'information et de la communication (TIC). Les rôles de l'UIT :

- **Gouvernance des télécommunications et de l'Internet** : L'UIT établit des normes internationales pour les télécommunications et les TIC, facilitant ainsi l'interconnexion mondiale et le bon fonctionnement des réseaux télécoms.
- **Harmonisation des fréquences** : Elle coordonne l'utilisation du spectre des fréquences radio et des orbites satellitaires, essentiels pour la diffusion de signaux de télécommunication, de téléphonie mobile, et de technologies de communication sans fil.
- **Cybersécurité** : L'UIT aide les pays membres à renforcer leurs capacités de cybersécurité par la coopération internationale, la formation, et le partage de bonnes pratiques pour faire face aux menaces cybernétiques mondiales.
- **Inclusion numérique** : Elle œuvre pour réduire la fracture numérique en facilitant l'accès à Internet et aux TIC pour les populations des pays en développement.

Les programmes clés de l'UIT :

- **Connect 2030 Agenda** : Un programme qui vise à promouvoir un accès universel aux TIC d'ici 2030, en ligne avec les Objectifs de développement durable (ODD). Ce programme se concentre sur la connectivité Internet, la cybersécurité, l'utilisation des données pour le développement durable, et l'innovation numérique.
- **World Summit on the Information Society (WSIS)** : Un sommet mondial sur la société de l'information, lancé en 2003, qui vise à promouvoir le dialogue entre les gouvernements, les entreprises et la société civile pour discuter des enjeux de la gouvernance d'Internet et de la société numérique.

⁴ ONU – Pacte numérique mondiale (<https://www.un.org/techenvoy/fr/global-digital-compact>).

⁵ ONU - Révision n° 3 du Pacte numérique mondial (https://www.un.org/techenvoy/sites/www.un.org/techenvoy/files/general/GDC_Rev_3_silence_procedure.pdf).

- **Global Cybersecurity Agenda (GCA)** : L'UIT promeut des initiatives de cybersécurité au niveau mondial pour renforcer la coopération internationale face aux cybermenaces croissantes.

2. Commission des Nations Unies sur la science et la technique au service du développement (CSTD)

La **Commission des Nations Unies sur la science et la technique au service du développement (CSTD)**, sous l'égide de la Conférence des Nations Unies sur le commerce et le développement (CNUCED), se concentre sur les aspects politiques et économiques des technologies numériques.

Orientations principales de la CSTD :

- **Égalité numérique** : Favoriser l'accès équitable aux technologies numériques pour tous les pays et groupes sociaux. Cela comprend la promotion de politiques qui aident les pays en développement à tirer parti de l'économie numérique.
- **Intégration des TIC dans les politiques de développement** : Conseiller les gouvernements sur la manière d'intégrer les technologies numériques dans leurs stratégies de développement économique et social, en lien avec les Objectifs de développement durable (ODD).
- **Recherche et développement** : Encourager les pays membres à investir dans la recherche et l'innovation technologique pour favoriser le développement durable.

3. Forum sur la gouvernance de l'Internet (IGF)

Le **Forum sur la gouvernance de l'Internet (IGF)**, initié par le **Sommet mondial sur la société de l'information (WSIS)** et encadré par les Nations Unies, est une plateforme multilatérale pour débattre des questions relatives à la gouvernance de l'Internet.

Rôle et objectifs de l'IGF :

- **Gouvernance d'Internet** : L'IGF réunit des représentants des gouvernements, des entreprises, de la société civile et des chercheurs pour débattre des questions liées à la gouvernance de l'Internet, telles que la protection des données, la neutralité du net, la cybersécurité, et la liberté d'expression en ligne.
- **Promotion d'un Internet ouvert et accessible** : L'IGF encourage un modèle de gouvernance multipartite pour garantir que l'Internet reste un outil libre et accessible à tous, tout en respectant les droits fondamentaux.

4. Initiatives en matière de droits numériques et d'inclusion

Les Nations Unies ont intégré les enjeux des droits numériques dans plusieurs de leurs initiatives, reconnaissant que les **droits humains** doivent être protégés également dans le domaine numérique. Les dispositions clés :

- **Protection des droits de l'homme en ligne** : Le **Conseil des droits de l'homme** des Nations Unies a reconnu que les **droits humains en ligne** doivent être protégés de la même manière que les droits hors ligne. Cela inclut la protection de la liberté d'expression, de la vie privée, et de la protection contre la surveillance abusive.
- **Inclusion numérique** : L'ONU travaille à réduire la fracture numérique entre pays développés et en développement, et entre différentes catégories sociales, en s'assurant que l'accès aux TIC et à Internet est universel et inclusif.
- **Coalition pour l'égalité numérique** : Initiative mondiale pour promouvoir l'accès équitable au numérique, en particulier dans les pays en développement, en lien avec les Objectifs de développement durable (ODD).

5. Objectifs de développement durable (ODD) et numérique

Le numérique joue un rôle crucial dans la réalisation des **Objectifs de développement durable (ODD)** adoptés en 2015. L'ONU reconnaît que la transformation numérique est un levier essentiel pour atteindre ces objectifs, notamment pour :

- **ODD 9 : Innovation et infrastructures** : Encourager le développement d'infrastructures TIC de qualité, accessibles et durables pour stimuler l'innovation et les processus industriels.
- **ODD 4 : Éducation de qualité** : Favoriser l'accès à des solutions numériques pour l'éducation, en particulier dans les régions les moins connectées, grâce à des plateformes d'apprentissage en ligne et à la numérisation de l'enseignement.
- **ODD 8 : Travail décent et croissance économique** : Le numérique permet de créer de nouvelles opportunités économiques, notamment via l'économie des plateformes, l'automatisation et l'IA, mais soulève aussi des défis en matière de travail équitable et de droits sociaux.

6. ONU et partenariats numériques

L'ONU travaille en étroite collaboration avec des organisations internationales, des entreprises privées, et des ONG pour promouvoir l'innovation numérique et garantir que le numérique soit inclusif et sécurisé pour tous :

- **Partenariats public-privé** : L'ONU collabore avec des entreprises technologiques (comme Google, Microsoft, etc.) et des acteurs locaux pour mettre en œuvre des projets de transformation numérique, notamment dans les pays en développement.
- **Tech for Good** : Initiatives visant à utiliser les technologies numériques pour répondre à des défis mondiaux, comme le changement climatique, les inégalités, et la santé publique.

Conclusion : Les Nations Unies sont structurées autour de plusieurs agences et programmes qui se concentrent sur la **gouvernance du numérique**, la **réduction de la fracture numérique**, la **protection des droits de l'homme en ligne**, et la **cybersécurité**. L'UIT, la CSTD et l'IGF sont parmi les principales entités au sein de l'ONU qui pilotent ces efforts, tandis que des initiatives comme le **Programme Connect 2030** et l'**Agenda 2030 pour les ODD** reconnaissent l'importance du numérique pour atteindre un développement durable, équitable et inclusif.

L'Union européenne

Les traités européens et le numérique

Qu'est-ce que les traités de l'Union européenne (TUE et TFUE) prévoient en matière de numérique ?

Les **traités de l'Union européenne (UE)**, en particulier le **Traité sur l'Union européenne (TUE)** et le **Traité sur le fonctionnement de l'Union européenne (TFUE)**, fournissent le cadre juridique fondamental pour les politiques numériques de l'UE, bien que le terme "numérique" ou "technologies numériques" ne soit pas explicitement mentionné dans les textes de ces traités adoptés dans les années 1990. Cependant, de nombreuses dispositions permettent de **développer, réguler et promouvoir le numérique** au sein de l'UE, et des interprétations ont évolué au fil du temps pour englober les avancées dans ce domaine.

Voici les principaux articles des traités qui influencent les politiques numériques de l'UE :

1. Le Traité sur l'Union européenne (TUE)

Le **TUE** fixe les principes généraux et les objectifs de l'Union européenne, notamment ceux qui s'appliquent aux technologies numériques dans le cadre plus large de la promotion de la croissance économique, de la compétitivité et des droits fondamentaux.

a. Article 3 TUE

L'article 3 du TUE précise les objectifs de l'Union européenne, notamment la promotion d'un **développement économique équilibré et durable**, la mise en place d'une économie **sociale de marché hautement compétitive** et l'amélioration du **bien-être des citoyens**.

Cet article soutient le développement des infrastructures numériques et des **technologies numériques** comme éléments essentiels pour atteindre une économie compétitive et innovante. L'**accès à l'Internet haut débit**, le développement des **technologies de l'information et de la communication (TIC)**, et la **cybersécurité** sont considérés comme des leviers fondamentaux pour la réalisation de ces objectifs.

b. Article 6 TUE

Cet article incorpore la **Charte des droits fondamentaux de l'UE** dans le cadre juridique de l'Union. La Charte contient des dispositions directement liées au numérique, comme la **protection des données personnelles** (article 8 de la Charte), la **liberté d'expression** (article 11), et le **droit au respect de la vie privée** (article 7).

Ces articles forment le fondement juridique pour des initiatives comme le Règlement général sur la protection des données (RGPD) et d'autres mesures liées aux droits numériques des citoyens européens.

2. Le Traité sur le fonctionnement de l'Union européenne (TFUE)

Le **TFUE** va plus loin en définissant des compétences spécifiques qui permettent à l'UE d'adopter des législations et des initiatives liées au numérique. Il couvre divers aspects qui affectent directement le développement du numérique dans les États membres.

a. Article 4 TFUE – Compétences partagées

L'article 4 définit les **compétences partagées** entre l'Union et les États membres dans des domaines clés, notamment :

- **Marché intérieur** : La régulation des marchés numériques et le marché unique numérique.
- **Politique sociale** : Inclut l'inclusion numérique et la lutte contre la fracture numérique.

Politique économique et monétaire : La transformation numérique comme levier pour la croissance économique.

Transport, énergie et réseau transeuropéen : Les infrastructures numériques font partie intégrante des réseaux transeuropéens de communication.

b. Articles 114 et 115 TFUE – Harmonisation du marché intérieur

Ces articles habilitent l'UE à adopter des législations destinées à l'**harmonisation des règles** au sein du marché intérieur. En matière numérique, cela a permis la mise en œuvre de nombreuses régulations visant à créer un **marché unique numérique**, comme la suppression des **frais d'itinérance mobile** en 2017, ou la régulation des **services numériques** (Digital Services Act, Digital Markets Act).

c. Article 170 TFUE – Réseaux transeuropéens

L'article 170 du TFUE prévoit le développement de **réseaux transeuropéens** dans les domaines des transports, de l'énergie et des télécommunications. Le texte encourage la mise en place de **réseaux de communication numériques** et d'infrastructures numériques comme le **déploiement de la fibre optique** et de la **5G** dans l'ensemble de l'Union européenne.

C'est dans ce cadre que des projets tels que le **déploiement de la 5G** à l'échelle européenne ou la coordination du **très haut débit** entre les États membres sont soutenus.

d. Articles 173 et 179 TFUE – Industrie et innovation

L'article 173 TFUE (ex-article 157 TCE) concerne la **politique industrielle** et promeut la compétitivité de l'industrie européenne, y compris les technologies numériques. Il fait référence à la nécessité d'encourager l'innovation technologique dans l'UE, un domaine clé pour le numérique.

L'UE a utilisé cet article pour soutenir des initiatives telles que les **clusters technologiques** et des programmes comme **Horizon Europe** pour le financement de la **recherche et innovation** en matière de numérique, notamment dans des secteurs comme l'intelligence artificielle, la **blockchain**, et le **cloud computing**.

e. Article 191 TFUE – Environnement

L'article 191 traite de la politique environnementale de l'UE et souligne la nécessité d'intégrer la durabilité dans toutes les politiques. En matière numérique, cela se traduit par des initiatives pour réduire l'empreinte carbone des technologies numériques, promouvoir des centres de données plus écologiques et encourager le **recyclage des appareils électroniques** dans une économie circulaire.

f. Article 16 TFUE – Protection des données

L'article 16 du TFUE garantit le droit à la **protection des données personnelles**. Cet article a été le fondement juridique pour l'adoption du **Règlement général sur la protection des données (RGPD)**, un texte pionnier en matière de protection de la vie privée et de régulation des données dans le monde numérique.

Le **RGPD** est l'une des pierres angulaires de la politique numérique de l'UE, assurant une protection stricte des données personnelles des citoyens européens et imposant des règles claires aux entreprises numériques, qu'elles soient basées dans ou en dehors de l'Union.

g. Articles 165 et 166 TFUE – Éducation et formation professionnelle

Ces articles prévoient la coordination des politiques éducatives et de formation au sein de l'UE, ce qui inclut le développement des **compétences numériques**. Ces dispositions permettent à l'UE de soutenir des programmes visant à renforcer les compétences numériques des citoyens et des travailleurs européens, notamment dans le cadre de la **transition numérique** des secteurs industriels et de l'économie.

3. Objectifs numériques dans le cadre de la stratégie de l'Union européenne

Au-delà des traités eux-mêmes, l'UE a adopté plusieurs stratégies numériques basées sur ces dispositions légales pour répondre aux défis de la **transformation numérique**.

a. Stratégie pour un marché unique numérique

L'UE a lancé la stratégie pour un **marché unique numérique** en 2015 pour harmoniser le cadre réglementaire à travers l'Union et lever les barrières qui empêchent la libre circulation des biens, des services et des capitaux dans l'environnement numérique. Cette stratégie repose sur les bases juridiques des articles du TFUE relatifs au marché intérieur et à l'innovation.

b. Stratégie européenne pour les données

Cette stratégie repose sur les dispositions concernant le marché intérieur et les données pour créer un **marché unique des données**, où les données peuvent circuler librement, tout en garantissant le respect des normes de **protection des données** (RGPD) et la souveraineté numérique de l'UE.

c. Cybersécurité

L'UE a renforcé sa législation sur la **cybersécurité** en adoptant la **Directive NIS** (réseaux et systèmes d'information), qui s'appuie sur les compétences partagées de l'UE et des États membres dans le domaine de la sécurité intérieure et du marché intérieur.

Conclusion : Les **traités de l'UE** (TUE et TFUE) fournissent les **bases juridiques** pour les politiques numériques de l'Union européenne, même s'ils ne traitent pas explicitement du numérique dans leurs formulations initiales. Les articles sur le **marché intérieur**, l'**innovation**, la **protection des données** et les **réseaux de télécommunications** permettent à l'UE de mettre en place des législations et des initiatives qui façonnent l'avenir numérique du continent. Ces dispositions sont renforcées par des stratégies comme le **marché unique numérique** ou la **stratégie européenne pour les données**, qui visent à assurer un développement numérique inclusif, durable, et respectueux des droits des citoyens européens.

L'UE et le numérique

ChatGPT : Comment est organisée l'Union pour le numérique : quelles sont les directions de la commission, les programmes ... ?

L'Union européenne (UE) a mis en place une stratégie numérique ambitieuse pour renforcer sa **souveraineté numérique**, protéger les droits de ses citoyens, et promouvoir l'innovation technologique. Cette stratégie est gérée principalement par la **Commission européenne**, qui élabore des politiques, des programmes et des initiatives pour répondre aux défis du numérique et assurer le leadership technologique de l'Europe.

1. Direction générale des réseaux de communication, du contenu et des technologies (DG CONNECT)

La **DG CONNECT** est l'entité clé de la Commission européenne chargée de la mise en œuvre des politiques numériques de l'UE. Elle est responsable de la régulation du marché unique numérique, de la protection des données, de l'innovation technologique et de la cybersécurité. Les principaux objectifs de la DG CONNECT :

- **Promouvoir l'innovation numérique** : Soutenir les technologies émergentes telles que l'intelligence artificielle (IA), la blockchain, et l'Internet des objets (IoT).
- **Réguler le marché unique numérique** : Assurer que les entreprises et les consommateurs puissent bénéficier d'un accès équitable et sécurisé aux services numériques dans l'ensemble de l'UE.
- **Développement des infrastructures numériques** : Soutenir le déploiement de la 5G, la fibre optique et les réseaux de communication sécurisés.

- **Cybersécurité** : Renforcer les capacités de cybersécurité à travers des initiatives législatives et des programmes de financement.

Les actions de la DG CONNECT sont supervisées par la **commissaire européenne en charge du numérique**, qui en 2024 est Margrethe Vestager, avec Thierry Breton en charge du marché intérieur et des aspects numériques associés.

2. Les principaux programmes et initiatives numériques de l'Union européenne

a. Programme pour une Europe numérique (Digital Europe Programme)

Le programme **Digital Europe** (2021-2027) est le principal mécanisme de financement des projets numériques à travers l'UE. Il dispose d'un budget d'environ 7,5 milliards d'euros et se concentre sur cinq grands domaines :

- **Supercalculateurs** : Investir dans des infrastructures de calcul haute performance pour renforcer la compétitivité européenne dans les domaines de la recherche, de la science et de l'industrie.
- **Intelligence artificielle (IA)** : Développer et utiliser l'IA de manière éthique et responsable, tout en soutenant l'adoption de ces technologies dans tous les secteurs.
- **Cybersécurité** : Renforcer la résilience des infrastructures numériques, sécuriser les réseaux européens et améliorer la coopération en matière de cybersécurité.
- **Compétences numériques avancées** : Former les Européens aux compétences numériques, en particulier dans des domaines comme l'IA, les big data, la cybersécurité et la robotique.
- **Utilisation généralisée des technologies numériques** : Soutenir l'adoption des technologies numériques dans les secteurs public et privé, y compris les PME et les administrations.

b. Programme Horizon Europe

Horizon Europe (2021-2027), doté d'un budget de 95,5 milliards d'euros, est le principal programme de financement de la recherche et de l'innovation de l'UE. Bien qu'il couvre un large éventail de sujets, la **numérisation** et les technologies de rupture y occupent une place centrale. Le programme soutient la recherche en IA, en blockchain, en technologies quantiques, ainsi que dans les domaines des technologies vertes et numériques.

c. Plan d'action pour le marché unique numérique

L'UE a mis en place un **plan d'action pour le marché unique numérique** visant à créer un espace unique où les biens et services numériques peuvent circuler librement. Les objectifs clés incluent :

- **Suppression des obstacles réglementaires** : Harmoniser les législations nationales pour créer un marché unique où les entreprises peuvent opérer sans entraves.
- **Neutralité du net** : Assurer un accès égal à l'infrastructure Internet et empêcher les fournisseurs de réseaux de discriminer certains services en ligne.
- **Réduction des frais d'itinérance** : L'UE a mis fin aux frais d'itinérance pour les appels, les SMS et l'utilisation de données dans ses États membres en 2017.

d. Stratégie européenne pour la cybersécurité

Cette stratégie, révisée en 2020, vise à protéger les citoyens, les entreprises et les institutions contre les cybermenaces. Elle comprend :

- **NIS2 Directive (Network and Information Systems Security Directive)** : Harmonise les exigences de cybersécurité pour les États membres de l'UE et améliore leur capacité à réagir aux incidents cybernétiques.
- **EU Cybersecurity Act** : Renforce les pouvoirs de l'Agence européenne pour la cybersécurité (ENISA) et met en place des certifications de cybersécurité pour les produits et services numériques.

e. Stratégie pour l'intelligence artificielle

La Commission européenne a lancé une stratégie ambitieuse pour l'IA afin de faire de l'Europe un leader dans le domaine de l'IA éthique et responsable. Elle s'articule autour de trois axes :

- **Investissement dans la recherche et l'innovation en IA.**
- **Mise en place de règles éthiques et légales pour l'utilisation de l'IA**, en particulier pour garantir la transparence, l'équité et le respect des droits fondamentaux.
- **Déploiement de l'IA dans le secteur public et privé**, en soutenant l'adoption de l'IA dans des domaines comme la santé, l'industrie, et la sécurité.

f. Initiative GAIA-X

GAIA-X est un projet paneuropéen visant à créer une infrastructure de cloud computing souveraine en Europe. L'objectif est de développer un cloud européen sécurisé et conforme aux normes de l'UE (protection des données, transparence, interopérabilité), qui permettrait aux entreprises européennes de stocker et de traiter leurs données en toute confiance. Ce projet a été initié par la France et l'Allemagne, mais il s'étend à plusieurs autres États membres et partenaires industriels.

3. Législation et cadres réglementaires numériques

L'Union européenne adopte une approche rigoureuse pour réglementer l'environnement numérique, à travers plusieurs législations clés :

- **RGPD (Règlement général sur la protection des données)** : Ce règlement de 2018 est la pierre angulaire de la protection des données personnelles dans l'UE. Il impose des obligations strictes aux entreprises quant à la manière dont elles collectent, traitent et stockent les données des citoyens européens.
- **Digital Services Act (DSA) et Digital Markets Act (DMA)** : Adoptées en 2022, ces lois visent à réguler les grandes plateformes numériques (Google, Amazon, Facebook) en imposant des règles de transparence, de modération de contenu, et en limitant les pratiques anticoncurrentielles.

4. Compétences numériques et inclusion

La **Commission européenne** et les États membres investissent massivement dans les compétences numériques pour répondre à la demande croissante en experts numériques. Le plan **Digital Skills and Jobs** est une initiative qui vise à former et à renforcer les compétences numériques dans toute l'Europe :

- **Digital Skills and Jobs Coalition** : Cette initiative réunit des États membres, des entreprises, des organisations éducatives et des associations pour améliorer les compétences numériques des citoyens européens.

Conclusion : L'Union européenne organise sa politique numérique autour de plusieurs directions stratégiques majeures, gérées par des entités comme la DG CONNECT et soutenues par des programmes de financement ambitieux tels que Digital Europe et Horizon Europe. L'objectif global est de garantir la souveraineté numérique de l'Europe, de protéger les droits des citoyens, d'encourager l'innovation et de créer un marché unique numérique compétitif et inclusif.

La stratégie de Lisbonne et le numérique

Que représentait le numérique dans la "stratégie de Lisbonne de l'Union européenne" ?

La stratégie de Lisbonne, adoptée par l'Union européenne lors du Conseil européen de Lisbonne en mars 2000, avait pour objectif principal de faire de l'UE "l'économie de la connaissance la plus compétitive et la plus dynamique du monde d'ici 2010". Le numérique a joué un rôle crucial dans

cette stratégie, car il a été identifié comme un levier essentiel pour renforcer la compétitivité économique de l'Europe, favoriser l'innovation et accélérer la transition vers une économie basée sur la connaissance.

Voici comment le numérique était intégré dans la stratégie de Lisbonne :

1. Le numérique comme moteur de la "société de la connaissance"

L'un des piliers de la stratégie de Lisbonne était de construire une économie de la connaissance, avec une forte attention portée à l'utilisation des technologies de l'information et de la communication (TIC) pour stimuler l'innovation, l'éducation et la productivité.

a. Technologies de l'information et de la communication (TIC)

Les TIC étaient vues comme des facteurs clés pour moderniser les secteurs de l'économie européenne. La stratégie soulignait que l'adoption généralisée des technologies numériques dans les entreprises et les administrations publiques permettrait d'améliorer l'efficacité, d'innover dans les processus de production et de fournir de nouveaux services à forte valeur ajoutée.

- **Digitalisation des services publics** : La stratégie de Lisbonne encourageait les États membres à développer l'e-gouvernement (administration électronique) pour améliorer l'accès aux services publics par le numérique et pour moderniser l'administration en utilisant les TIC.
- **Secteurs d'avenir** : Des industries comme les télécommunications, les logiciels, et les services Internet étaient identifiées comme des moteurs de la nouvelle économie.

b. Soutien à l'innovation et à la recherche numérique

Le soutien à la recherche et au développement des technologies numériques était l'un des objectifs clés de la stratégie. La stratégie de Lisbonne recommandait une augmentation significative des investissements en R&D, avec une cible fixée à 3 % du PIB de l'UE consacré à la recherche d'ici 2010.

- **Innovation dans le numérique** : L'accent était mis sur la promotion des technologies de pointe comme l'intelligence artificielle, les télécommunications de nouvelle génération (telles que le haut débit), et les services numériques.
- **Partenariats public-privé** : La stratégie encourageait la collaboration entre les gouvernements, les universités et les entreprises pour stimuler l'innovation technologique, notamment dans le secteur numérique.

2. eEurope : L'initiative numérique de la stratégie de Lisbonne

L'initiative eEurope faisait partie intégrante de la stratégie de Lisbonne et avait pour objectif de développer une société de l'information en Europe, en démocratisant l'accès à Internet et en intégrant les technologies numériques dans tous les aspects de la société.

a. eEurope 2002

Lancé en 1999, avant même l'adoption de la stratégie de Lisbonne, le programme eEurope 2002 visait à permettre à tous les citoyens européens d'accéder à l'Internet à haut débit et à utiliser les TIC pour améliorer leur vie quotidienne. Il s'agissait de :

- **Connecter les écoles et les administrations** : Les établissements d'enseignement et les administrations publiques devaient être dotés d'une connexion Internet rapide et d'outils numériques pour moderniser les processus.
- **Promouvoir l'e-commerce et l'e-gouvernement** : L'initiative encourageait le développement du commerce électronique et des services publics en ligne.
- **Réduire la fracture numérique** : L'initiative visait à garantir que toutes les régions d'Europe, y compris les zones rurales, aient accès aux technologies numériques, afin de ne pas creuser l'écart entre les différentes régions ou catégories sociales.

b. eEurope 2005

Suite au succès initial d'eEurope 2002, le programme eEurope 2005 a été lancé pour approfondir les efforts numériques dans plusieurs domaines, notamment en garantissant :

- **Un accès Internet à haut débit généralisé** : Le programme visait à garantir que tous les citoyens européens aient un accès facile à Internet à haut débit, en incitant les États membres à développer les infrastructures nécessaires.
- **Développement de services numériques avancés** : En particulier dans les secteurs de la santé (e-santé), de l'éducation (e-learning) et de l'administration (e-gouvernement).

3. Encouragement de la compétitivité via le numérique

Le développement numérique était considéré comme un levier essentiel pour renforcer la compétitivité de l'UE sur la scène internationale.

a. Accélération de l'adoption des TIC dans les entreprises

La stratégie de Lisbonne encourageait fortement l'adoption des TIC par les entreprises, notamment les petites et moyennes entreprises (PME), afin d'améliorer leur compétitivité. Cela incluait :

- **Commerce électronique** : Les entreprises européennes devaient adopter les technologies numériques pour vendre leurs produits et services en ligne, élargissant ainsi leur marché et améliorant leur efficacité.
- **Réseaux numériques** : Les entreprises étaient encouragées à utiliser les TIC pour optimiser leurs chaînes de production et mieux collaborer avec leurs fournisseurs et partenaires grâce à des réseaux numériques.

b. Réforme du cadre réglementaire pour le numérique

La stratégie de Lisbonne prévoyait de moderniser le cadre réglementaire de l'UE afin de lever les barrières au commerce numérique. Cela comprenait des actions pour :

- **Harmoniser la régulation des télécommunications** : L'UE a travaillé à la mise en place d'un marché unique des télécommunications, facilitant le déploiement de l'Internet haut débit à l'échelle européenne.
- **Propriété intellectuelle et contenu numérique** : La stratégie cherchait à protéger la propriété intellectuelle dans l'environnement numérique et à faciliter l'échange de contenus numériques au sein de l'UE.

4. Développement des compétences numériques

L'un des piliers de la stratégie de Lisbonne était de renforcer les compétences des citoyens européens pour qu'ils puissent participer pleinement à la nouvelle économie numérique.

a. Amélioration de l'éducation numérique

La stratégie encourageait les États membres à réformer leurs systèmes éducatifs pour intégrer les compétences numériques dans les programmes scolaires. Cela comprenait :

- **Formation aux TIC** : Promouvoir l'enseignement des TIC dès le plus jeune âge et tout au long de la vie pour permettre aux travailleurs de s'adapter aux exigences du marché du travail numérique.
- **Éducation continue** : Encourager la formation continue des citoyens européens pour qu'ils puissent bénéficier des nouvelles technologies tout au long de leur carrière.

b. Réduire la fracture numérique par l'éducation

La stratégie de Lisbonne mettait l'accent sur l'importance de réduire la fracture numérique entre les différentes catégories sociales et régions de l'UE, en assurant que tous les citoyens puissent avoir accès aux outils et compétences nécessaires pour profiter des opportunités offertes par le numérique.

5. Évaluation et réajustement : Stratégie Europe 2020

En 2010, la stratégie de Lisbonne n'ayant pas pleinement atteint ses objectifs, elle a été révisée et remplacée par la stratégie Europe 2020, qui a intégré le numérique comme un axe encore plus central pour la croissance. Europe 2020 a fixé des objectifs spécifiques liés au développement des infrastructures numériques, à l'innovation technologique, et à la transformation numérique de l'économie, renforçant l'accent mis sur les TIC dans la stratégie de Lisbonne.

Conclusion

Le numérique était au cœur de la stratégie de Lisbonne de l'Union européenne, bien qu'il ait été envisagé principalement à travers le prisme des technologies de l'information et de la communication (TIC). Il était considéré comme un outil essentiel pour moderniser l'économie européenne, améliorer la compétitivité des entreprises, créer de nouveaux services publics numériques, et stimuler la recherche et l'innovation. Cette stratégie a posé les bases des initiatives numériques actuelles de l'UE, en plaçant les TIC comme moteurs de la transformation économique et sociale européenne.

Le rapport Draghi et le numérique

Que représente le numérique dans le récent rapport Draghi ?

Le **rapport Draghi**, rédigé en 2023 sous la direction de **Mario Draghi**, ancien président de la Banque centrale européenne et Premier ministre italien, présente des recommandations pour renforcer la compétitivité et la résilience de l'économie européenne dans un monde en transformation rapide. Le **numérique** joue un rôle central dans ce rapport, qui souligne son importance pour la **croissance économique**, la **compétitivité** de l'UE, et la **souveraineté technologique** face aux défis mondiaux. Voici les principaux aspects du numérique dans le rapport Draghi :

1. Le numérique comme levier de compétitivité économique

Le rapport Draghi insiste sur le fait que le numérique est un **levier essentiel** pour améliorer la **compétitivité** des entreprises européennes et maintenir l'UE dans la course mondiale face aux grandes puissances technologiques, notamment les États-Unis et la Chine. Il appelle à une accélération de la **transition numérique** dans les secteurs stratégiques, soulignant que le numérique est au cœur de **l'économie de demain**.

a. Transformation numérique des entreprises

Modernisation des PME : Le rapport met en avant l'importance d'aider les petites et moyennes entreprises (PME) à adopter les technologies numériques (intelligence artificielle, automatisation, big data, etc.) afin d'améliorer leur productivité et de rester compétitives sur le marché mondial.

Accélérer l'adoption de l'IA et des nouvelles technologies : Le rapport recommande des mesures pour encourager **l'adoption rapide de l'intelligence artificielle (IA)**, de la **blockchain**, et de **l'Internet des objets (IoT)** dans les industries européennes.

b. Innovation numérique

Le rapport Draghi souligne que l'UE doit renforcer son soutien à **l'innovation numérique**, notamment en augmentant les **investissements en recherche et développement (R&D)** dans les technologies émergentes. Il propose une augmentation du budget pour des programmes comme **Horizon Europe**, afin de favoriser le développement de technologies de pointe et de renforcer les écosystèmes d'innovation en Europe.

Startups et entreprises technologiques : Draghi insiste sur la nécessité de soutenir les **startups technologiques européennes**, à travers des incitations fiscales et des financements plus accessibles, afin de créer un écosystème dynamique d'innovation.

2. Souveraineté numérique européenne

Le rapport place un fort accent sur la **souveraineté numérique** de l'Europe, considérée comme cruciale pour garantir l'indépendance de l'UE vis-à-vis des grandes entreprises technologiques non européennes (comme les **GAFAM** américaines ou les géants technologiques chinois). L'UE doit renforcer ses infrastructures et technologies propres pour assurer la sécurité et la résilience de son économie numérique.

a. Développement d'une infrastructure numérique souveraine

- **Cloud souverain** : Draghi insiste sur la nécessité de construire une **infrastructure de cloud souverain**, à l'image de l'initiative **GAIA-X**, qui permettrait de réduire la dépendance de l'Europe aux fournisseurs américains comme Amazon Web Services, Microsoft Azure ou Google Cloud.
- **Semi-conducteurs** : Le rapport met également l'accent sur le renforcement de la production européenne de semi-conducteurs, qui sont essentiels pour la souveraineté numérique. Draghi soutient l'initiative de l'UE visant à produire 20 % des semi-conducteurs mondiaux d'ici 2030, dans le cadre du Chips Act.

b. Protection des données et cybersécurité

- **Cybersécurité** : La **cybersécurité** est un autre aspect clé de la souveraineté numérique. Le rapport recommande des investissements massifs dans la cybersécurité pour protéger les infrastructures critiques et les données des entreprises et des citoyens européens contre les cyberattaques.
- **Régulation des données** : Draghi encourage une meilleure régulation des données personnelles et des données industrielles, en continuant à appliquer et à renforcer des réglementations comme le **Règlement général sur la protection des données (RGPD)** et en développant un cadre pour le partage et l'exploitation sécurisée des données industrielles.

3. Infrastructure numérique et connectivité

Le rapport Draghi insiste sur l'importance de développer des infrastructures numériques robustes et inclusives, essentielles pour que l'économie numérique prospère à l'échelle européenne.

a. Accès à la 5G et à la fibre optique

Le rapport souligne la nécessité d'accélérer le **déploiement de la 5G** et des **réseaux de fibre optique** à travers l'Europe. Une connectivité rapide et fiable est un élément fondamental pour permettre le développement d'innovations comme l'Internet des objets, les véhicules connectés et l'industrie 4.0.

b. Réduire la fracture numérique

Draghi met également l'accent sur la **réduction de la fracture numérique** en Europe, en garantissant que toutes les régions, y compris les zones rurales, puissent accéder à Internet à haut débit. Le rapport recommande des investissements supplémentaires pour étendre la couverture de la fibre optique et de la 5G dans les zones mal desservies.

4. Compétences numériques

Le rapport Draghi souligne l'importance de développer les **compétences numériques** des citoyens européens, afin de répondre à la demande croissante de talents qualifiés dans le domaine technologique.

a. Formation et éducation numériques

- **Education numérique** : Draghi propose de renforcer l'enseignement des **compétences numériques** dès le plus jeune âge, en intégrant des programmes de codage, de robotique, et d'intelligence artificielle dans les systèmes éducatifs européens.
- **Formation continue** : Le rapport recommande également des programmes de reconversion pour les travailleurs touchés par l'automatisation, en les formant aux compétences numériques pour les préparer aux emplois de demain.

b. Attirer les talents technologiques

Le rapport suggère que l'UE doit adopter des mesures pour attirer et retenir les **talents technologiques** en Europe, notamment en facilitant l'accès aux visas pour les travailleurs hautement qualifiés dans le secteur numérique.

5. Intégration du numérique dans la transition verte

Le rapport Draghi intègre également le numérique dans les objectifs plus larges de la **transition écologique**. Le numérique est perçu comme un **outil crucial** pour atteindre les objectifs climatiques et environnementaux de l'UE.

a. Numérique vert

Le rapport recommande de promouvoir les technologies numériques qui permettent de **réduire l'empreinte carbone** des secteurs économiques. Cela inclut l'utilisation de l'**intelligence artificielle** et de l'**Internet des objets** pour optimiser l'efficacité énergétique dans les industries, ainsi que des **centres de données verts** pour réduire la consommation d'énergie liée aux infrastructures numériques.

Conclusion : Dans le **rapport Draghi**, le numérique est présenté comme un **pilier stratégique** de la compétitivité future de l'Europe, tant pour sa croissance économique que pour sa souveraineté technologique. Les recommandations du rapport visent à accélérer la **transformation numérique** des secteurs industriels, à renforcer les **infrastructures numériques souveraines**, à garantir la **cybersécurité** et à former les **compétences numériques** nécessaires pour que l'UE reste un acteur mondial de premier plan dans le domaine des technologies numériques. Le rapport reconnaît également l'importance du numérique pour soutenir les **objectifs écologiques**, soulignant le rôle des technologies numériques dans la transition vers une économie plus verte.

Commentaires : pas d'évaluation, d'explication et le même discours

Bilan de la stratégie de Lisbonne

Est-ce que le rapport Draghi représente, en particulier pour le numérique, un bilan de la stratégie de Lisbonne ? et ce bilan est-il chiffré, au moins partiellement ?

[réponse à intégrer]

Les programmes et les initiatives

L'Union européenne a investi le numérique par différentes initiatives (qui sont accessibles par divers sites. En particulier :

- Le Digital Europe programme : <https://digital-strategy.ec.europa.eu/en/faqs/questions-and-answers-digital-europe-programme>
- Les Work programme : <https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital>
- European Digital Innovation Hubs : <https://digital-strategy.ec.europa.eu/en/activities/edihs>
- European Chips Act : <https://digital-strategy.ec.europa.eu/en/policies/european-chips-act>

Les Etats membres

La France

ChatGPT : Comment est organisée la France pour le numérique : quelles sont les directions de la commission, les programmes ... ?

La **France** a structuré sa stratégie numérique autour de plusieurs institutions, directions et programmes pour répondre aux enjeux de la **souveraineté numérique**, de la **transition numérique** des entreprises et de l'administration, ainsi que de l'**inclusion numérique** pour tous les citoyens. Le numérique est un secteur stratégique pour le gouvernement, car il touche à la fois aux infrastructures, à l'innovation, à la sécurité et à la régulation des services numériques. Voici une vue d'ensemble des directions clés et des programmes associés à la politique publique numérique en France.

1. Direction générale des entreprises (DGE)

La **Direction générale des entreprises (DGE)**, rattachée au **ministère de l'Économie, des Finances et de la Relance**, est l'un des principaux acteurs de la politique numérique en France. Elle est responsable de la mise en œuvre des politiques publiques en matière d'innovation, de compétitivité et de développement numérique des entreprises.

Rôles et objectifs :

- **Soutien à l'innovation numérique** : Encourager les entreprises, notamment les PME et startups, à adopter des technologies numériques innovantes telles que l'intelligence artificielle (IA), le big data, la blockchain, et l'Internet des objets (IoT).
- **Transformation numérique des PME** : Promouvoir la transition numérique des petites et moyennes entreprises à travers des programmes spécifiques comme France Num.
- **Cyber-sécurité** : Assurer la promotion de bonnes pratiques en matière de cybersécurité dans les entreprises et soutenir les initiatives pour renforcer la résilience des infrastructures.

2. Agence nationale de la sécurité des systèmes d'information (ANSSI)

L'**ANSSI** est l'organisme public chargé de la cybersécurité en France, sous l'autorité du **Secrétariat général de la défense et de la sécurité nationale (SGDSN)**.

Rôles et missions :

- **Protection des infrastructures critiques** : Assurer la sécurité des systèmes d'information des administrations publiques et des entreprises stratégiques (énergie, transport, finance).
- **Conseil et assistance** : Fournir des conseils aux entreprises, administrations et collectivités sur la cybersécurité et aider à la gestion des incidents cybernétiques.
- **Certification** : Délivrer des certifications de sécurité pour les technologies et les systèmes d'information utilisés en France, notamment pour les solutions cloud souverain.

3. Secrétariat d'État chargé de la transition numérique et des communications électroniques

Ce secrétariat, sous l'égide du **ministère de l'Économie, des Finances et de la Relance**, est dédié à la mise en œuvre de la politique numérique en France.

Rôles principaux :

- **Coordination des initiatives numériques** : Ce secrétariat coordonne les différentes actions et programmes liés à la transition numérique, notamment en ce qui concerne l'économie, l'inclusion et la sécurité.
- **Régulation des communications électroniques** : Il veille à la régulation du secteur des télécommunications et au bon déploiement des infrastructures numériques (fibre optique, 5G).

4. Programmes et initiatives clés du numérique en France

a. France Num

Lancée par la DGE, **France Num** est une initiative destinée à aider les TPE et PME françaises à réussir leur transition numérique. Elle offre un accompagnement et des solutions concrètes pour encourager l'adoption des technologies numériques (e-commerce, gestion digitale, cybersécurité).

b. Stratégie nationale pour l'intelligence artificielle

La France a lancé en 2018 une **Stratégie nationale pour l'intelligence artificielle**, avec un plan d'investissement de **1,5 milliard d'euros** pour soutenir la recherche, le développement de talents et l'adoption de l'IA dans les secteurs stratégiques tels que la santé, la défense, les transports et l'environnement.

Les objectifs clés incluent :

- **Formation aux compétences en IA** : Renforcer la formation et les compétences en intelligence artificielle au sein des universités et des centres de recherche.
- Innovation et soutien à l'industrie : Promouvoir l'innovation dans l'industrie en utilisant des technologies basées sur l'IA, tout en respectant les normes éthiques et de sécurité.

c. Plan France Très Haut Débit

Le **Plan France Très Haut Débit** vise à garantir l'accès au très haut débit (fibre optique) pour tous les Français d'ici 2025. Ce programme, lancé en 2013, représente un investissement de près de **20 milliards d'euros** et associe des partenariats entre acteurs publics et privés.

d. Cloud souverain

La **stratégie française pour un cloud souverain** a pour objectif de renforcer l'indépendance numérique de la France en matière de stockage et de traitement des données. Cela inclut la promotion des **solutions cloud certifiées** par l'ANSSI, qui garantissent une localisation des données en France et une protection contre les lois extraterritoriales (comme le **Cloud Act américain**).

e. France Relance (Numérique)

Le plan de **relance économique post-COVID-19**, lancé en 2020, inclut un volet numérique important :

- **1 milliard d'euros pour la transformation** numérique des entreprises.
- Soutien aux startups et aux PME pour accélérer l'adoption des outils numériques.
- Digitalisation des services publics : Faciliter l'accès aux démarches administratives via des services numériques.

5. Inclusion numérique et compétences

L'inclusion numérique est un axe majeur de la politique numérique en France pour garantir que chacun ait accès aux services en ligne et puisse les utiliser efficacement.

a. Pass numérique

Le **Pass numérique** est un dispositif de formation destiné aux personnes éloignées du numérique. Il permet à ces citoyens de bénéficier de cours ou de formations pour apprendre à utiliser les outils numériques de manière basique (navigation sur Internet, utilisation de logiciels).

b. Cohésion numérique des territoires

Ce programme vise à réduire la fracture numérique entre les zones rurales et urbaines en soutenant le déploiement d'infrastructures dans les régions moins connectées. Cela inclut :

- **Aides financières** pour les collectivités qui souhaitent accélérer la couverture Internet de leur territoire.

- **Formation aux compétences numériques** pour les citoyens dans les zones rurales.

c. Stratégie nationale pour une éducation numérique

La France déploie également une **stratégie d'éducation numérique** pour intégrer les outils numériques dans les établissements scolaires. Cela inclut la formation des enseignants, le déploiement de plateformes d'apprentissage en ligne, et la dotation en matériel informatique pour les écoles.

6. Régulation et souveraineté numérique

La France est un acteur clé dans la promotion d'une régulation du numérique, notamment en matière de protection des données et de régulation des grandes plateformes.

a. Réglementation des plateformes numériques

La France soutient des initiatives européennes comme le **Digital Services Act (DSA)** et le **Digital Markets Act (DMA)**, qui visent à réguler les grandes plateformes en ligne, en garantissant la transparence de leurs algorithmes, la protection des utilisateurs et une concurrence loyale.

b. Protection des données personnelles (RGPD)

Le **Règlement général sur la protection des données (RGPD)**, adopté par l'Union européenne en 2018, est une pièce maîtresse de la régulation numérique en France. La **Commission nationale de l'informatique et des libertés (CNIL)** est l'autorité de contrôle qui veille au respect de ce règlement, garantissant ainsi la protection des données personnelles des citoyens français.

Conclusion : La stratégie numérique de la France est axée sur la **transition numérique des entreprises et des administrations**, la **protection de la souveraineté numérique**, l'**inclusion numérique** et la **cybersécurité**. Diverses agences comme la **DGE**, l'**ANSSI**, et la **CNIL** travaillent de concert pour mettre en œuvre les politiques publiques nécessaires pour faire de la France un leader en matière de numérique tout en veillant à l'équité et à la sécurité dans cette transformation technologique.

L'Allemagne

...

Les régions

L'Île-de-France

La région Île-de-France est un acteur clé du développement numérique en France, et elle a mis en place plusieurs initiatives et dispositions qui contribuent à une politique publique du numérique. L'objectif est de faire de la région un leader en matière de transformation numérique, d'innovation technologique, et de réduction des fractures numériques. Voici les principaux axes et initiatives de cette politique publique :

1. Transformation numérique des services publics

L'Île-de-France s'est engagée à moderniser les services publics par le numérique pour les rendre plus accessibles et efficaces :

- **Dématérialisation des services publics** : La région a accéléré la digitalisation de ses services pour permettre aux citoyens d'accéder à des démarches administratives en ligne (demande d'aides, gestion des transports, inscriptions scolaires, etc.).
- **Plateformes numériques pour les citoyens** : Des plateformes telles que Mes aides Île-de-France ou Île-de-France Mobilités permettent aux habitants de la région de gérer leurs démarches, de planifier leurs trajets, et d'accéder aux services régionaux en ligne.

2. Développement des infrastructures numériques

L'Île-de-France soutient le déploiement d'infrastructures numériques performantes pour garantir l'accès au très haut débit et réduire les disparités territoriales.

- **Fibre optique** : La région s'est engagée dans un plan de déploiement de la fibre optique pour que tous les territoires franciliens, y compris les zones rurales et périurbaines, puissent bénéficier d'un accès au très haut débit.
- **Réseaux 5G** : L'Île-de-France encourage également le déploiement de la 5G sur son territoire, afin de soutenir l'innovation technologique, notamment dans des secteurs tels que la mobilité intelligente, la santé numérique, et l'industrie du futur.

3. Inclusion numérique

Pour éviter les inégalités d'accès au numérique, la région met en place des politiques d'inclusion numérique visant à former les citoyens et à faciliter leur accès aux outils numériques :

- **Pass numérique** : Ce dispositif permet aux personnes éloignées du numérique de bénéficier de formations adaptées à leurs besoins (bureautique, navigation sur Internet, démarches administratives en ligne, etc.), afin de réduire la fracture numérique.
- **Espaces numériques** : La région soutient la création et le maintien d'espaces numériques dans les communes et quartiers moins bien desservis, où les habitants peuvent accéder à des ordinateurs, à Internet, et à des services d'accompagnement.

4. Soutien à l'innovation et à l'écosystème numérique

L'Île-de-France est un centre important d'innovation technologique en Europe, avec plusieurs initiatives visant à soutenir les startups, les PME, et la recherche dans le domaine du numérique :

- **Soutien aux startups** : La région finance plusieurs incubateurs et accélérateurs de startups spécialisées dans le numérique (Station F, Partech Shaker, etc.), et octroie des subventions pour soutenir les projets innovants. Le programme INNOV'UP finance des projets innovants liés aux nouvelles technologies.

- **Clusters numériques** : L'Île-de-France soutient le développement de clusters numériques, tels que Cap Digital, un pôle de compétitivité dédié à l'économie numérique. Ces clusters favorisent l'innovation et les partenariats entre startups, grandes entreprises, et institutions de recherche.
- **Intelligence artificielle (IA)** : La région se positionne comme un hub pour le développement de l'IA, en finançant la recherche et en soutenant des projets comme Paris Region AI Challenge, un concours destiné à promouvoir l'intelligence artificielle dans l'industrie.

5. Smart City et transition écologique

La région a intégré des solutions numériques pour soutenir la transition écologique et la gestion urbaine intelligente.

- **Smart City** : L'Île-de-France investit dans des projets de ville intelligente en utilisant des capteurs, l'intelligence artificielle, et des plateformes numériques pour améliorer la gestion des ressources urbaines (énergie, eau, déchets) et la mobilité (optimisation des flux de trafic, déploiement de véhicules autonomes).
- **Transition énergétique** : Le numérique joue un rôle clé dans la gestion des réseaux d'énergie de la région. Des technologies de suivi en temps réel permettent de mieux gérer la consommation et la distribution d'énergie dans une perspective de durabilité.

6. Éducation et compétences numériques

La région Île-de-France fait de la formation aux compétences numériques une priorité pour répondre aux besoins du marché du travail et accompagner la transition numérique.

- **Formation numérique** : En partenariat avec des acteurs publics et privés, la région soutient des programmes de formation au numérique pour les jeunes et les personnes en reconversion professionnelle. Des initiatives telles que Écoles du numérique sont mises en place pour former aux métiers du développement web, de la cybersécurité, et des technologies émergentes.
- **FabLabs éducatifs** : L'Île-de-France soutient la création de FabLabs (laboratoires de fabrication) et d'espaces créatifs pour permettre aux jeunes d'apprendre à coder, à utiliser des imprimantes 3D, et à expérimenter avec des technologies innovantes.

7. Cybersécurité et souveraineté numérique

La région a aussi un intérêt particulier pour la sécurité des infrastructures numériques et la protection des données des citoyens :

- **Cybersécurité** : L'Île-de-France finance des initiatives visant à améliorer la sécurité des systèmes informatiques des administrations publiques et des entreprises locales. Des formations en cybersécurité sont également mises en place pour les PME afin de les protéger contre les cyberattaques.
- **Souveraineté numérique** : Dans le cadre de la souveraineté numérique, l'Île-de-France encourage l'utilisation de solutions cloud françaises ou européennes, conformes aux exigences de protection des données (RGPD), et promeut le développement d'une infrastructure cloud souveraine.

Conclusion : La région Île-de-France déploie une politique publique numérique ambitieuse visant à renforcer ses infrastructures, promouvoir l'innovation, et réduire les inégalités d'accès au numérique. En soutenant à la fois le développement économique, l'inclusion numérique et la transition écologique via les technologies numériques, la région se positionne comme un acteur clé de la transformation digitale en Europe.

La Suisse

(pas dans l'UE, mais dans l'AELE)

La souveraineté numérique est une préoccupation centrale pour la Suisse, notamment en raison de sa position en tant que centre financier mondial et son engagement en matière de neutralité. La Suisse met l'accent sur la cybersécurité, la protection des données, et l'autonomie technologique.

Politiques publiques suisses

Stratégie Suisse numérique 2023–2027 : Cette stratégie, publiée par la Confédération, vise à intégrer les technologies numériques dans tous les aspects de la vie sociale, économique et politique. Elle repose sur les principes de durabilité, de sécurité et de souveraineté numérique. L'accent est mis sur :

- **La cybersécurité** : Le Centre national pour la cybersécurité (NCSC) joue un rôle clé pour protéger les infrastructures critiques et sensibiliser les entreprises et la population aux cybermenaces. La Suisse cherche à minimiser sa dépendance envers des technologies étrangères potentiellement vulnérables.
- **Protection des données** : La Suisse a adopté une loi sur la protection des données en ligne avec le RGPD de l'Union européenne. Les données sensibles doivent être stockées sur des serveurs nationaux ou européens, réduisant la dépendance aux services étrangers comme les clouds américains.
- **Neutralité technologique** : La Suisse soutient l'usage de technologies open-source, notamment dans le secteur public, pour maintenir une indépendance vis-à-vis des grandes multinationales technologiques américaines ou chinoises.
- **Centres de données souverains** : La Suisse mise sur son image de "bastion de sécurité" pour attirer des centres de données internationaux tout en développant ses propres infrastructures sécurisées.
- **Neutralité de l'Internet** : Le gouvernement suisse soutient le principe de neutralité de l'Internet, ce qui garantit un accès ouvert et non discriminatoire aux ressources numériques.
- **Partenariats internationaux** : En tant que nation neutre, la Suisse coopère activement avec l'Union européenne, même si elle ne fait pas partie de l'UE. Elle participe à des initiatives de cybersécurité régionales et globales pour renforcer sa souveraineté numérique sans perdre son autonomie.

Défis pour la Suisse

- **Dépendance aux technologies étrangères** : Malgré ses efforts pour promouvoir les technologies locales et européennes, la Suisse reste dépendante des infrastructures numériques (systèmes d'exploitation, cloud) étrangères.
- **Cybermenaces croissantes** : En tant que centre financier, la Suisse est particulièrement vulnérable aux attaques cybernétiques sophistiquées.

L'Irlande

L'Irlande, bien qu'intégrée à l'Union européenne, a une approche singulière en matière de souveraineté numérique. Elle se positionne comme un hub technologique mondial, en hébergeant les sièges européens de nombreuses multinationales du secteur technologique (Google, Facebook, Apple, etc.), tout en développant ses propres politiques pour assurer la sécurité et la résilience numérique.

Politiques publiques irlandaises

National Cyber Security Strategy (2023–2027) : Cette stratégie est axée sur trois piliers principaux :

- **Renforcement des capacités de cybersécurité** : L'Irlande investit dans ses capacités nationales en matière de cybersécurité. Le National Cyber Security Centre (NCSC) est responsable de la protection des infrastructures critiques et de la réponse aux incidents de cybersécurité.
- **Protection des données** : En tant que siège européen de plusieurs géants technologiques, l'Irlande joue un rôle crucial dans l'application du RGPD. L'autorité de protection des données irlandaise (DPC) est l'une des plus influentes en Europe en matière de régulation des entreprises technologiques.
- **Autonomie technologique** : L'Irlande cherche à développer une industrie technologique nationale forte, notamment par des investissements dans l'intelligence artificielle, le cloud computing, et les infrastructures numériques. Cela inclut le soutien à des entreprises locales innovantes dans les domaines des télécommunications et de la cybersécurité.
- **Data Sovereignty and Infrastructure** : L'Irlande s'efforce de maintenir des standards élevés de protection des données, tout en hébergeant de nombreux centres de données pour des entreprises technologiques. L'Irlande promeut la localisation des données en Europe et le développement d'infrastructures cloud européennes. Elle a également rejoint le projet GAIA-X pour soutenir une infrastructure cloud souveraine à l'échelle européenne.
- **Innovation numérique** : L'Irlande investit fortement dans la recherche et le développement de technologies numériques, en collaboration avec l'Union européenne. Le pays est un acteur clé du programme Digital Europe et du Horizon Europe, qui financent l'innovation numérique et la transformation numérique des secteurs publics et privés.

Défis pour l'Irlande

- **Dépendance aux multinationales** : Bien que l'Irlande bénéficie d'investissements massifs de la part des entreprises technologiques, cette dépendance peut également être perçue comme un risque pour sa souveraineté numérique, notamment en matière de protection des données et de contrôle des infrastructures numériques.
- **Conflit entre réglementation et innovation** : L'Irlande doit naviguer entre la protection des données des citoyens et les demandes des entreprises multinationales en matière d'innovation et de traitement des données.

Comparaison entre la Suisse et l'Irlande

- **Cybersécurité** : Les deux pays mettent un accent fort sur la cybersécurité, avec des agences nationales dédiées et des partenariats internationaux pour renforcer leurs capacités.
- **Protection des données** : L'Irlande, en tant que membre de l'UE, applique strictement le RGPD, tandis que la Suisse a sa propre législation similaire mais autonome. Les deux pays cherchent à renforcer leur souveraineté en réduisant leur dépendance aux infrastructures étrangères.
- **Autonomie technologique** : Si la Suisse est plus neutre et se concentre sur l'autonomie et la neutralité, l'Irlande mise davantage sur le développement de son rôle de hub technologique mondial, ce qui peut parfois entrer en tension avec les objectifs de souveraineté.

Ces deux pays, bien que dans des contextes différents, cherchent tous deux à concilier sécurité numérique, innovation technologique et protection de la souveraineté numérique face à des multinationales globales.

Israël

Quelle est la politique publique d'Israël pour le numérique ? Qu'est-ce qui explique son dynamisme ?

La politique publique d'Israël en matière de numérique est largement reconnue pour son dynamisme et son innovation, faisant du pays l'un des leaders mondiaux dans le secteur des technologies de l'information et de la communication. Voici un aperçu des principales composantes de cette politique et des facteurs qui expliquent son succès :

1. Composantes de la Politique Publique Numérique d'Israël

1.1 Stratégie Nationale pour la Cyber-sécurité

- **Infrastructure de Sécurité** : Israël a mis en place une stratégie nationale de cyber-sécurité pour protéger ses infrastructures critiques et ses données contre les cybermenaces. Cela inclut le développement de capacités avancées en matière de sécurité informatique.
- **Collaboration** : Le pays favorise une collaboration étroite entre le gouvernement, l'industrie et les institutions académiques pour renforcer la cyber-résilience.

1.2 Promotion de l'Innovation et des Startups

- **Écosystème de Startups** : Israël est souvent surnommé la "Startup Nation" en raison de son nombre élevé de startups par habitant. Le gouvernement soutient l'innovation par le biais de subventions, de financement de la recherche et d'incubateurs d'entreprises.
- **Investissement en R&D** : Le pays investit massivement dans la recherche et le développement, avec des dépenses de R&D parmi les plus élevées au monde par rapport au PIB.

1.3 Éducation et Formation

- **Formation en Technologies** : Israël met l'accent sur l'éducation et la formation dans les domaines des sciences, de la technologie, de l'ingénierie et des mathématiques (STEM). De nombreuses universités et institutions techniques offrent des programmes de pointe en informatique et en ingénierie.
- **Initiatives de Recrutement** : Le gouvernement encourage également des initiatives pour attirer des talents étrangers et former les travailleurs locaux aux compétences numériques nécessaires.

1.4 Réglementation et Environnement Favorable

- **Réglementation Souple** : Israël a un environnement réglementaire favorable aux entreprises, ce qui permet aux startups de se développer rapidement sans faire face à des contraintes excessives.
- **Collaboration Public-Privé** : Le gouvernement collabore avec le secteur privé pour soutenir des projets d'innovation, faciliter l'accès aux financements et promouvoir des partenariats stratégiques.

2. Facteurs Expliquant le Dynamisme d'Israël

2.1 Historique Militaire

- **Innovation Défensive** : Les avancées technologiques développées pour des besoins militaires ont souvent été transférées vers le secteur civil. Les technologies développées dans l'armée israélienne, notamment dans le domaine de la cyber-sécurité, ont donné naissance à de nombreuses startups.

2.2 Culture de l'Entrepreneuriat

- **Mentalité de Risque** : La culture israélienne valorise l'entrepreneuriat et le risque. Les entrepreneurs sont encouragés à innover et à échouer, ce qui favorise une dynamique d'expérimentation et de croissance.

2.3 Accès aux Investissements

- **Investissement Étranger** : Israël attire des investissements étrangers importants, notamment de la part de fonds de capital-risque et d'entreprises technologiques mondiales. Cette injection de capitaux permet aux startups de se développer rapidement.

- **Partenariats Internationaux** : Le pays a établi des partenariats avec des entreprises et des gouvernements étrangers pour promouvoir l'innovation et l'échange de technologies.

2.4 Réseau d'Innovation

- **Clustérisation** : Le développement de clusters technologiques, comme ceux autour de Tel-Aviv, favorise la collaboration entre startups, investisseurs, et chercheurs, créant un environnement propice à l'innovation.

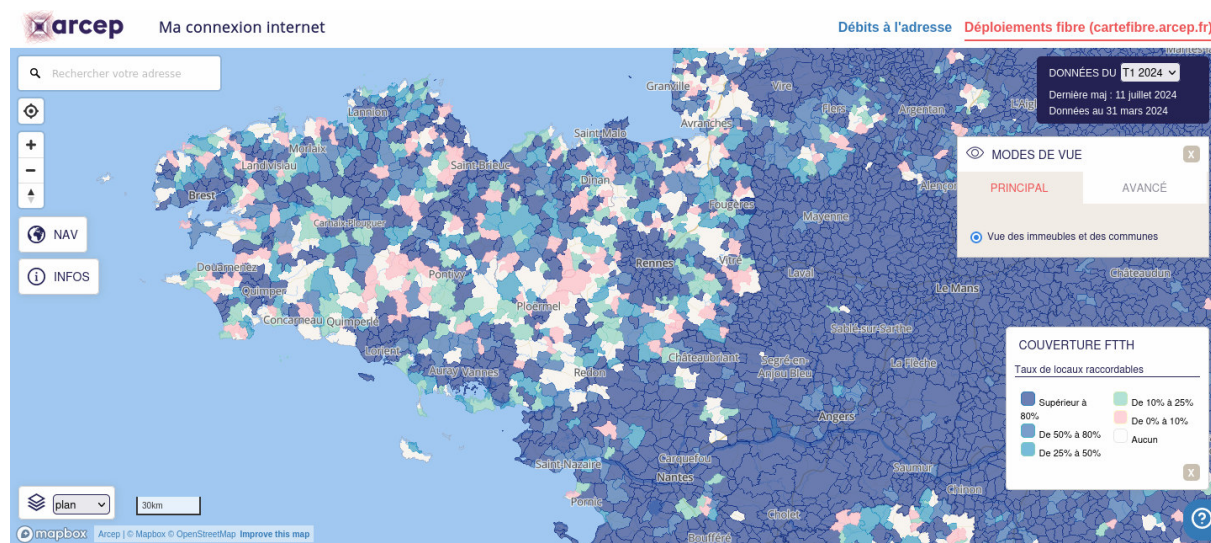
Conclusion

La politique publique d'Israël en matière de numérique est caractérisée par une approche proactive en matière de cyber-sécurité, un soutien fort à l'innovation et aux startups, et un accent sur l'éducation et la formation. Le dynamisme de l'écosystème numérique israélien est renforcé par des facteurs historiques, culturels et économiques qui favorisent l'entrepreneuriat et l'innovation. Grâce à ces éléments, Israël continue de se positionner comme un leader mondial dans le domaine des technologies numériques.

La Bretagne

Internet en Bretagne

La fibre en Bretagne :

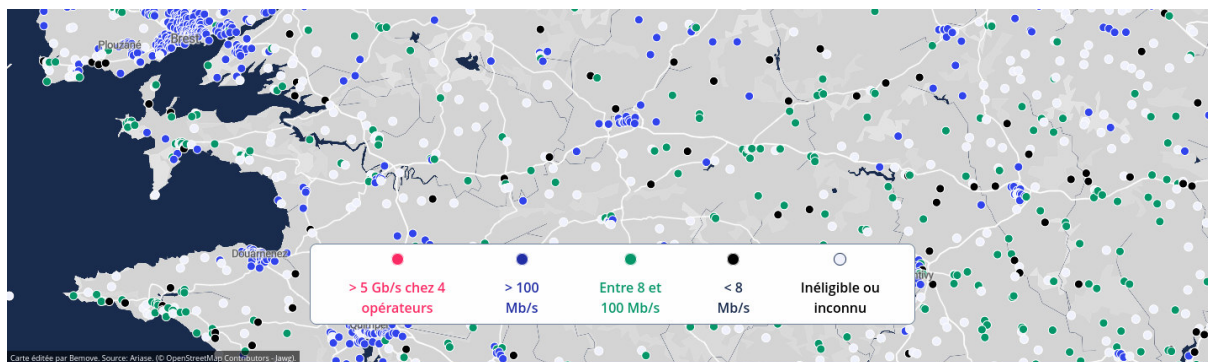


<https://cartefibre.arcep.fr/index.html?lng=-1.9214183377650897&lat=47.96371548630938&zoom=8.075360348671403&mode=normal&legende=true&filter=true&trimestre=2024T1>

Les données avenantes de la carte ci-dessus : <https://www.data.gouv.fr/fr/datasets/le-marche-du-haut-et-tres-haut-debit-fixe-deploiements/>

La carte ci-dessous met en évidence un retard de la Bretagne en termes de déploiement de la fibre. Ce qui pose la question

La carte : <https://www.ariase.com/box/carte-couverture-internet>

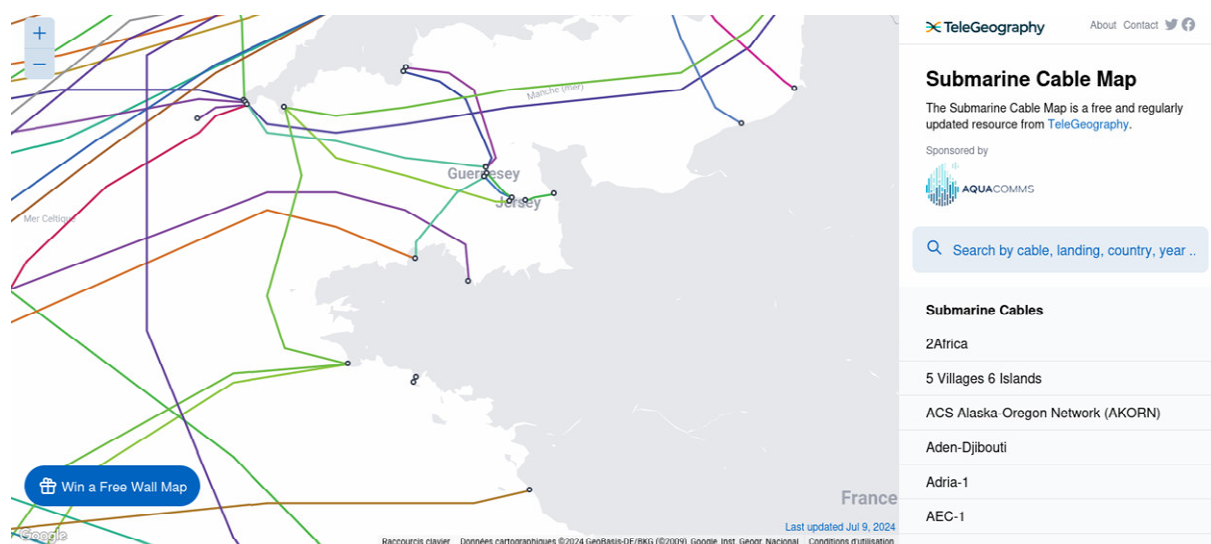


Cette carte est une solution facile et rapide pour [comprendre sa couverture internet](#) et une aide précieuse pour choisir l'offre internet la plus adaptée à votre adresse.

Question : la Bretagne accuse-t-elle un retard préjudiciable à son développement ?

Réponses : oui / non / NSP

Les câbles sous-marins



Les câbles passant par la Bretagne (<https://www.submarinecablemap.com/>) :

Câbles	Point de connexion
Apollo	Lannion
Africa Coast to Europe (ACE)	Penmarc'h
SeaWeMe-3	Penmarc'h
FLAG Atlantic-A (FA-1)	Plerin
Groix-3	Petit-Perello – Port-Nâl

Noter le câble interne vers l'île de Groix

La Bretagne est bien connectée par câbles sous-marins avec la Grande-Bretagne, les USA. On peut imaginer une connexion directe vers l'Amérique du sud. Et dédoublement pour la sécurité.

Brest port câblé : <https://france3-regions.francetvinfo.fr/bretagne/finistere/brest/orange-marine-presente-son-dernier-cablier-brest-591910.html>

L'importance stratégique de câbles sous-marins

ChatGPT : Les câbles Internet sous-marins sont vitaux pour la connectivité mondiale, assurant la transmission rapide et fiable des données entre les continents. Ils offrent des avantages significatifs en termes de vitesse, de capacité, et de stabilité des connexions, tout en jouant un rôle clé dans le soutien aux infrastructures numériques globales. Cependant, leur gestion comporte des défis importants, y compris les coûts élevés, les risques de sécurité, et la vulnérabilité aux dommages physiques. Une connexion robuste et bien gérée par ces câbles est donc essentielle pour maintenir l'efficacité et la résilience du réseau Internet mondial.

Les câbles Internet sous-marins jouent un rôle crucial dans l'infrastructure mondiale des télécommunications et sont essentiels pour le fonctionnement d'Internet tel que nous le connaissons aujourd'hui. Voici pourquoi ils sont importants, ainsi que les avantages et inconvénients de leur utilisation :

Importance des Câbles Internet Sous-Marins

1. Transfert de Données International :

- **Infrastructure de Base** : Les câbles sous-marins sont la principale infrastructure pour le transfert de données entre les continents. Ils transportent environ 99 % du trafic Internet mondial, y compris les communications personnelles, les transactions financières, les contenus multimédias et les services en ligne.
- **Volume de Données** : Ces câbles permettent des volumes énormes de données à travers des distances internationales, facilitant la communication globale en temps réel.

2. Réduction de la Latence :

- **Vitesse de Transmission** : Les câbles sous-marins ont des latences plus faibles par rapport aux alternatives comme les satellites. Cela est crucial pour des services sensibles au temps comme les transactions financières en temps réel, les appels vidéo, et les applications de jeux en ligne.

3. Capacité et Scalabilité :

- **Large Bande Passante** : Les câbles sous-marins modernes offrent une bande passante élevée, permettant le transfert de grandes quantités de données avec une vitesse accrue. Ils sont conçus pour évoluer avec les besoins croissants en données.
- **Technologie de Multiplexage** : Les câbles utilisent des technologies avancées comme la multiplexion en longueur d'onde dense (DWDM) pour maximiser leur capacité de transmission.

4. Fiabilité et Redondance :

- **Connectivité Globale** : En étant connectés à différents points géographiques, les câbles sous-marins offrent des routes de redondance pour le trafic Internet. Si un câble est endommagé, le trafic peut être rerouté via d'autres câbles, minimisant les interruptions de service.
- **Infrastructure Critique** : Leur robustesse est essentielle pour maintenir la continuité des services Internet à l'échelle mondiale, surtout en cas de catastrophes naturelles ou de pannes techniques.

Avantages d'une Connexion Élevée par Câbles Sous-Marins

1. Qualité et Rapidité de Connexion :

- **Haute Vitesse** : Une connexion par câble sous-marin assure une vitesse élevée et une faible latence, améliorant ainsi la qualité des services en ligne et des communications internationales.
- **Stabilité** : Les câbles sous-marins offrent une connexion stable avec peu d'interruptions, ce qui est particulièrement important pour les entreprises multinationales et les services en ligne critiques.

2. Support pour les Infrastructures Numériques :

- **Cloud Computing** : Les entreprises et les services cloud dépendent des câbles sous-marins pour fournir des services à leurs clients à travers le monde, assurant une performance rapide et fiable des applications basées sur le cloud.
- **Services de Streaming et de Contenu** : Les plateformes de streaming, les réseaux sociaux et les services de contenu en ligne utilisent les câbles sous-marins pour diffuser du contenu multimédia de haute qualité à un large public.

Limitations et Défis

1. Coûts et Maintenance :

- **Investissements Élevés** : La construction et la maintenance des câbles sous-marins sont coûteuses. Les entreprises doivent investir dans des infrastructures coûteuses et effectuer des réparations en cas de dommages.
- **Réparations et Réparations** : Les câbles sous-marins peuvent être endommagés par des activités humaines, des tempêtes ou des catastrophes naturelles. Les réparations nécessitent des opérations complexes et coûteuses.

2. Risques Géopolitiques et Sécurité :

- **Vulnérabilités** : Les câbles sous-marins peuvent être vulnérables à des attaques physiques ou à des interceptions, ce qui pose des risques pour la sécurité des données.
- **Conflits Géopolitiques** : Les tensions géopolitiques peuvent affecter la gestion et l'entretien des câbles sous-marins, entraînant des risques pour la continuité des services.

3. Dépendance Technologique :

- **Infrastructure Critique** : La dépendance accrue aux câbles sous-marins signifie que tout problème majeur avec ces infrastructures peut avoir des répercussions significatives sur l'accessibilité et la performance des services Internet à l'échelle mondiale.

Connexion directe

Une connexion directe à Internet par câble sous-marin présente plusieurs avantages et inconvénients par rapport aux réseaux terrestres. Voici une analyse des principaux aspects :

Avantages des Câbles Sous-Marins par Rapport aux Réseaux Terrestres

1. Capacité et Débit

- **Bande Passante Élevée** : Les câbles sous-marins offrent une très grande capacité de bande passante, pouvant supporter des débits de plusieurs téraoctets par seconde. Cette capacité est souvent plus élevée que celle des réseaux terrestres, en raison de la technologie avancée utilisée pour la transmission de données sur de longues distances.
- **Infrastructure à Haute Performance** : Les câbles sous-marins sont conçus pour gérer des volumes importants de données et des connexions internationales à haute vitesse, ce qui est crucial pour les échanges globaux et les services en ligne de grande envergure.

2. Fiabilité et Latence

- **Chemins de Communication Stables** : Les câbles sous-marins offrent des routes de communication relativement stables avec une latence faible, surtout pour les connexions transcontinentales. Ils sont moins affectés par les problèmes liés aux réseaux terrestres tels que les pannes de câbles ou les interruptions causées par des travaux de construction ou des accidents.
- **Diversité des Routes** : Les câbles sous-marins peuvent offrir des chemins alternatifs pour les données, augmentant ainsi la résilience et la fiabilité des connexions internationales.

3. Couverture Globale

- **Interconnexion Internationale** : Les câbles sous-marins relient les continents et permettent une interconnexion directe entre différents points géographiques. Ils sont essentiels pour les communications mondiales, offrant des connexions directes entre les principaux centres de données et les réseaux internationaux.
- **Accès à des Régions Isolées** : Ils fournissent des connexions à des régions insulaires ou éloignées qui peuvent être difficiles à atteindre avec des infrastructures terrestres.

Inconvénients des Câbles Sous-Marins par Rapport aux Réseaux Terrestres

1. Coût et Maintenance

- **Coût Élevé** : Le déploiement de câbles sous-marins est extrêmement coûteux, en raison des défis techniques liés à l'installation en milieu marin et de la nécessité de maintenir et de réparer les câbles en cas de défaillance.
- **Complexité de la Maintenance** : Les réparations et l'entretien des câbles sous-marins peuvent être complexes et nécessitent des équipements spécialisés et des opérations sous-marines coûteuses.

2. Vulnérabilités

- **Risques de Dommages** : Les câbles sous-marins sont vulnérables aux dommages causés par des activités humaines (comme les ancres de navires) et des phénomènes naturels (comme les tremblements de terre sous-marins). Bien que des mesures de sécurité et des protocoles de maintenance existent, ces risques peuvent affecter la disponibilité du service.
- **Sécurité et Souveraineté** : Les câbles sous-marins peuvent être des cibles pour les cyberattaques ou les activités de surveillance, ce qui pose des questions de sécurité et de souveraineté.

3. Latence et Dépendance

- **Latence en Longue Distance** : Bien que les câbles sous-marins aient une faible latence pour les connexions transcontinentales, la distance physique et le nombre de relais peuvent introduire une latence perceptible par rapport aux réseaux locaux terrestres très optimisés.
- **Dépendance à l'Infrastructure Subaquatique** : La dépendance à l'infrastructure sous-marine signifie que des perturbations dans cette infrastructure peuvent avoir des répercussions importantes sur les connexions internationales.

Comparaison avec les Réseaux Terrestres

- **Réseaux Terrestres** : Les réseaux terrestres, tels que les lignes de fibre optique, offrent généralement une flexibilité et une évolutivité plus importantes pour les connexions locales et régionales. Ils sont souvent plus faciles et moins coûteux à installer et à entretenir sur terre, mais peuvent être plus vulnérables aux interruptions locales.
- **Complémentarité** : Les réseaux terrestres et sous-marins sont souvent utilisés en complément pour assurer la continuité et la robustesse des communications. Les câbles sous-marins sont

essentiels pour les connexions internationales, tandis que les réseaux terrestres peuvent fournir des connexions à l'intérieur des continents et des régions spécifiques.

Résumé : Une connexion directe à Internet par câble sous-marin offre des avantages significatifs en termes de capacité, de débit, de fiabilité et de couverture internationale. Cependant, elle présente également des défis en termes de coût, de maintenance, et de vulnérabilités potentielles. Les câbles sous-marins et les réseaux terrestres sont souvent complémentaires, avec les câbles sous-marins assurant la connectivité internationale et les réseaux terrestres fournissant des solutions plus flexibles et économiques pour les connexions locales et régionales.

Les initiatives et les actions

Comment est organisée la région Bretagne pour le numérique : quelles sont les initiatives, les actions ... ?

La **région Bretagne** est un acteur dynamique dans le développement et l'adoption du numérique en France. Elle a mis en place plusieurs initiatives pour faire du numérique un levier de développement économique, social et culturel, avec un accent particulier sur l'inclusion numérique, le déploiement d'infrastructures et le soutien à l'innovation. Voici un aperçu de l'organisation, des actions et des initiatives numériques en Bretagne.

1. Stratégie régionale pour le numérique : Breizh COP

La Bretagne s'appuie sur sa stratégie de développement durable baptisée **Breizh COP**, qui intègre le numérique comme un axe transversal pour répondre aux enjeux de transition écologique, d'inclusion sociale et de dynamisme économique. Les objectifs numériques dans Breizh COP :

- **Réduire la fracture numérique** : S'assurer que tous les habitants de la région, y compris dans les zones rurales, aient accès à des infrastructures numériques performantes.
- **Soutenir l'innovation** : Favoriser l'émergence de nouvelles technologies et entreprises numériques, en particulier dans des secteurs clés comme l'agriculture, la mer, et l'industrie.
- **Transition numérique des entreprises** : Encourager les PME bretonnes à intégrer des solutions numériques dans leurs processus pour améliorer leur compétitivité.

2. Développement des infrastructures numériques

L'un des objectifs principaux de la région est de garantir l'accès à des infrastructures numériques de qualité à l'ensemble de ses habitants, y compris dans les zones rurales.

a. Bretagne Très Haut Débit

Le programme **Bretagne Très Haut Débit**, lancé en 2014, est un des projets phares pour le déploiement de la **fibres optique** dans toute la région. Il vise à équiper l'ensemble des foyers, entreprises, et administrations bretonnes en **fibres optique d'ici 2026**. Ce projet d'envergure, soutenu par des financements publics régionaux, nationaux et européens, vise à :

- **Améliorer la connectivité** dans les zones rurales pour réduire la fracture numérique entre les villes et les campagnes.
- **Faciliter l'accès aux services en ligne** : Assurer que tous les citoyens puissent accéder aux services publics numériques, aux plateformes d'apprentissage, et aux soins de santé numériques.
- **Renforcer la compétitivité des entreprises** en leur offrant un accès à des solutions de cloud et à des outils de communication avancés via des connexions rapides.

b. Déploiement de la 5G

La région Bretagne soutient également le déploiement de la **5G** pour répondre aux besoins croissants des entreprises locales en termes de connectivité et pour favoriser l'émergence de nouveaux services basés sur l'Internet des objets (IoT) et les objets connectés.

3. Soutien à l'innovation numérique

La Bretagne est un pôle d'innovation numérique majeur, avec plusieurs initiatives visant à soutenir les startups, les PME, et les projets de recherche dans le domaine du numérique.

a. Pôle de compétitivité Images & Réseaux

Le **pôle de compétitivité Images & Réseaux**, qui couvre la Bretagne et les Pays de la Loire, est un acteur clé pour l'innovation numérique en France. Ce pôle regroupe plus de 200 acteurs industriels, laboratoires et universités pour promouvoir l'innovation dans les domaines des réseaux, des télécommunications, des images et du multimédia. Le pôle soutient notamment des projets collaboratifs de recherche et développement (R&D) autour de la 5G, de l'IA, du big data, et des réalités immersives.

b. Technopoles et incubateurs

La Bretagne compte plusieurs **technopoles** et **incubateurs** pour soutenir les jeunes entreprises innovantes :

- **Rennes Atalante** : L'une des technopoles les plus dynamiques en France, spécialisée dans les technologies de l'information et de la communication (TIC), les médias, et la cybersécurité.
- **Technopôle Brest Iroise** : Spécialisée dans les technologies marines et les TIC, elle soutient l'innovation dans des secteurs tels que la mer, la défense, et l'environnement.
- **Startup Weekend et concours de startups** : La région soutient également des événements comme les Startup Weekends et les concours de startups pour encourager l'émergence de nouvelles entreprises dans le secteur numérique.

c. Programme Digital Saint-Malo

Digital Saint-Malo est une initiative régionale visant à faire de Saint-Malo un hub de l'innovation numérique, en accueillant des startups, des incubateurs, et des événements numériques dans la région. Le programme soutient le développement des entreprises innovantes, en particulier dans les secteurs du tourisme numérique et des industries créatives.

4. Inclusion numérique

L'inclusion numérique est un enjeu majeur pour la région, notamment pour lutter contre les inégalités d'accès aux technologies.

a. Pass numérique

La Bretagne a déployé le dispositif du **Pass numérique**, qui permet aux personnes éloignées du numérique de bénéficier de formations pour acquérir les compétences nécessaires à l'utilisation des outils digitaux. Ce dispositif est particulièrement utile pour les seniors, les personnes en recherche d'emploi ou les personnes vivant dans des zones rurales.

b. Espaces publics numériques (EPN)

La région finance des **Espaces publics numériques (EPN)**, qui sont des lieux d'accueil pour les personnes souhaitant s'initier ou se perfectionner dans l'utilisation des outils numériques. Ces espaces proposent des ateliers, des formations et un accompagnement individuel pour faciliter l'accès à Internet et aux nouvelles technologies.

c. Programme "Aptitudes numériques"

Ce programme vise à renforcer les compétences numériques de tous les citoyens bretons, en particulier les jeunes et les personnes en reconversion professionnelle. Il met l'accent sur les compétences essentielles pour la vie professionnelle moderne, comme l'utilisation des outils bureautiques, la gestion des réseaux sociaux, et l'apprentissage des bases de la cybersécurité.

5. Transition numérique des entreprises

La région Bretagne accompagne les entreprises dans leur transition numérique via différents programmes et aides.

a. Accélérateur PME

Le programme **Accélérateur PME** est une initiative qui aide les petites et moyennes entreprises bretonnes à passer au numérique, en les accompagnant dans l'adoption de technologies digitales comme l'e-commerce, la gestion en cloud, ou la numérisation de leur chaîne de production.

b. Plateforme Bretagne Grande Vitesse

La **Plateforme Bretagne Grande Vitesse** est un service qui permet aux entreprises d'accéder à des capacités de calcul et de traitement de données à grande échelle, en s'appuyant sur des infrastructures cloud performantes, facilitant ainsi l'innovation numérique dans la région.

6. Cybersécurité

La Bretagne, notamment avec la présence de **Rennes**, est un acteur majeur de la cybersécurité en France. La région a développé des compétences et des infrastructures dédiées à la sécurité numérique, en lien avec le **Pôle d'excellence cyber** basé à Rennes.

a. Pôle d'excellence cyber

Ce pôle regroupe des institutions publiques, des entreprises privées et des centres de recherche pour développer des solutions de cybersécurité, former des experts et soutenir l'innovation dans le domaine de la sécurité numérique.

b. Projets européens de cybersécurité

La région participe à des projets européens pour développer des compétences et des outils en cybersécurité, notamment dans le cadre de programmes comme **Horizon Europe**.

Conclusion : La région Bretagne est un acteur clé du développement numérique en France, avec des initiatives couvrant l'inclusion numérique, l'innovation, le déploiement d'infrastructures, et la cybersécurité. Avec des projets tels que **Bretagne Très Haut Débit**, des pôles de compétitivité comme **Images & Réseaux**, et des initiatives locales comme **Digital Saint-Malo**, la Bretagne se positionne comme un leader dans l'adoption du numérique, tout en cherchant à assurer que cette transition bénéficie à l'ensemble de ses citoyens et entreprises.

Les Pays de la Loire

Comment est organisée la région Pays-de-la-Loire pour le numérique : quelles sont les initiatives, les actions ... ?

La région **Pays de la Loire** est particulièrement active en matière de développement numérique, avec des initiatives visant à soutenir l'innovation, à renforcer les infrastructures numériques, à promouvoir l'inclusion numérique et à accompagner la transition numérique des entreprises et des administrations. Voici une vue d'ensemble de l'organisation et des principales initiatives numériques dans cette région.

1. Stratégie régionale pour le numérique

La **région Pays de la Loire** a défini une stratégie numérique ambitieuse qui repose sur trois axes principaux :

- **Soutien à l'innovation numérique** : Promouvoir l'innovation technologique et accompagner les startups et PME dans la transformation numérique.

- **Renforcement des infrastructures numériques** : Améliorer l'accès à l'internet haut débit et très haut débit dans toute la région, en particulier dans les zones rurales.
- **Inclusion numérique** : Assurer que tous les citoyens, y compris les plus éloignés du numérique, puissent accéder aux services en ligne et maîtriser les outils numériques.

2. Développement des infrastructures numériques

a. THD Pays de la Loire

Le programme **THD (Très Haut Débit) Pays de la Loire** vise à connecter l'ensemble des foyers et entreprises de la région à la **fibre optique** d'ici 2025. Ce projet est l'un des piliers de la stratégie régionale pour réduire la fracture numérique entre les zones rurales et urbaines. En collaboration avec les opérateurs privés et les collectivités locales, la région assure la couverture en fibre pour les zones moins densément peuplées où les investissements privés sont limités.

b. Déploiement de la 5G

La région encourage également le **déploiement de la 5G** pour permettre aux entreprises et aux citoyens de bénéficier de la dernière génération de réseaux mobiles. Cela est particulièrement important pour des secteurs comme l'industrie, la santé et la logistique, où la 5G permet d'améliorer la connectivité et d'introduire des technologies comme l'Internet des objets (IoT).

3. Soutien à l'innovation numérique et aux entreprises

a. Pôle de compétitivité Images & Réseaux

Le **pôle de compétitivité Images & Réseaux**, partagé avec la Bretagne, est un acteur majeur dans le soutien à l'innovation numérique en Pays de la Loire. Il regroupe des entreprises, des laboratoires de recherche et des institutions académiques pour développer des projets autour des TIC (technologies de l'information et de la communication), de la 5G, de la réalité virtuelle, et de l'intelligence artificielle (IA).

b. Digital Innovation Hub (DIH) des Pays de la Loire

Les **Digital Innovation Hubs (DIH)** sont des plateformes régionales qui offrent aux entreprises des services de soutien pour faciliter leur transformation numérique. Le DIH des Pays de la Loire propose :

- **Accompagnement des PME** dans l'adoption de nouvelles technologies.
- **Formations aux compétences numériques** pour les entreprises.
- **Projets collaboratifs** entre entreprises, universités, et laboratoires de recherche pour innover dans le domaine numérique.

c. Startup Palace

Startup Palace, basé à Nantes, est un incubateur et accélérateur de startups qui soutient l'innovation numérique en Pays de la Loire. Il offre des services d'accompagnement, des événements de réseautage et des programmes de mentorat pour aider les jeunes entreprises à se développer dans le secteur numérique.

d. La Cantine Numérique

Basée à Nantes, **La Cantine Numérique** est un lieu d'innovation qui réunit entrepreneurs, chercheurs, développeurs et créatifs autour de projets technologiques. Elle propose des événements, des hackathons, et des ateliers pour stimuler l'innovation numérique locale.

4. Transition numérique des entreprises

La région soutient activement la **transition numérique des PME et des industries** à travers des dispositifs spécifiques.

a. Industrie du Futur

Le programme **Industrie du Futur** aide les entreprises manufacturières de la région à moderniser leurs processus en adoptant des technologies numériques. Ce programme vise à améliorer la compétitivité des entreprises grâce à des outils comme l'**automatisation**, l'**intelligence artificielle**, et les **objets connectés** (IoT).

b. Pays de la Loire Investissement Numérique

Ce fonds d'investissement régional soutient les PME et les startups qui développent des technologies numériques innovantes. Il finance des projets de développement dans des domaines comme le cloud computing, l'intelligence artificielle, et la cybersécurité.

c. Initiative "Ambition numérique"

Cette initiative propose des **formations aux entreprises** pour les accompagner dans leur transition numérique, notamment dans l'e-commerce, la gestion des données, et la digitalisation des processus métiers. Elle inclut également un soutien financier pour les investissements numériques.

5. Inclusion numérique

La **région Pays de la Loire** place un accent particulier sur l'inclusion numérique afin que tous les citoyens, y compris les personnes âgées, les jeunes, et ceux en milieu rural, puissent accéder aux services en ligne.

a. Pass numérique

Comme dans d'autres régions, le **Pass numérique** permet aux personnes en difficulté numérique de bénéficier de formations adaptées pour apprendre à utiliser les outils numériques et accéder aux services en ligne (administration, banque, emploi, etc.).

b. Espaces publics numériques (EPN)

La région soutient le développement des Espaces publics numériques (EPN), qui sont des lieux d'accueil pour les citoyens souhaitant s'initier aux outils numériques. Les EPN proposent des ateliers de formation, des conseils pratiques et un accompagnement pour aider les personnes à mieux comprendre et utiliser les technologies numériques.

c. Mission numérique locale

La **mission numérique locale** a pour objectif de former les jeunes aux compétences numériques essentielles pour améliorer leur insertion professionnelle. Des dispositifs d'accompagnement et de formation sont mis en place pour permettre aux jeunes en recherche d'emploi ou en reconversion de se familiariser avec les technologies numériques.

6. Éducation et compétences numériques

a. Campus des métiers et des qualifications du numérique

La région a créé des **campus des métiers et des qualifications** spécialisés dans le numérique pour offrir aux jeunes des formations adaptées aux besoins de l'économie numérique. Ces campus forment aux métiers du développement web, de la cybersécurité, de la gestion de données, et bien d'autres secteurs en forte croissance.

b. Éducation numérique dans les écoles

Les **lycées et collèges des Pays de la Loire** sont progressivement équipés de matériel numérique (tablettes, ordinateurs) pour faciliter l'apprentissage des élèves. Des plateformes d'apprentissage en ligne sont également déployées pour permettre un enseignement numérique interactif.

7. Cybersécurité

La cybersécurité est une priorité pour la région, qui encourage les entreprises à adopter des bonnes pratiques en matière de protection des données.

a. Atlanpole Cyber

Atlanpole Cyber, basé à Nantes, est un pôle d'innovation dédié à la cybersécurité, qui travaille en étroite collaboration avec des entreprises, des laboratoires de recherche, et des institutions académiques. Il propose des solutions de cybersécurité pour les entreprises locales et soutient la formation d'experts dans ce domaine.

b. Accompagnement des entreprises

La région propose un accompagnement aux PME et aux industries pour les aider à renforcer leurs défenses contre les cyberattaques, avec des ateliers de sensibilisation, des diagnostics de sécurité, et des formations en cybersécurité.

Conclusion : La région **Pays de la Loire** est bien organisée pour soutenir le développement numérique à travers des infrastructures modernes, des initiatives d'inclusion numérique, et des programmes d'accompagnement pour les entreprises et les citoyens. Avec des projets comme **THD Pays de la Loire**, des pôles d'innovation comme **Images & Réseaux**, et des actions en faveur de la **cybersécurité** et de l'inclusion numérique, la région se positionne comme un acteur clé de la transformation numérique en France.

Les départements

Le Morbihan

Comment est organisée le département du Morbihan pour le numérique : quelles sont les initiatives, les actions ... ?

Le **département du Morbihan**, en région Bretagne, s'engage activement dans le développement et la mise en œuvre de politiques numériques, axées sur l'infrastructure, l'innovation, et l'inclusion numérique. Grâce à un ensemble de programmes et d'initiatives locales, le Morbihan cherche à renforcer son attractivité, à soutenir ses entreprises, et à réduire les inégalités numériques. Voici un aperçu de l'organisation, des actions et des initiatives numériques dans le département du Morbihan.

1. Développement des infrastructures numériques

a. Bretagne Très Haut Débit (THD)

Comme les autres départements bretons, le **Morbihan** participe activement au programme Bretagne Très Haut Débit, qui vise à déployer la fibre optique sur l'ensemble du territoire breton. Le projet est cofinancé par la région Bretagne, les départements, les collectivités locales et des partenaires privés, avec pour objectif de connecter tous les foyers et entreprises du Morbihan d'ici 2026.

- **Zones rurales** : L'un des principaux défis du programme est d'apporter le très haut débit aux zones rurales et aux zones moins densément peuplées du Morbihan. Des efforts particuliers sont faits pour connecter les communes isolées.

- **Accès pour les entreprises** : Le déploiement de la fibre permet aux entreprises locales d'avoir accès à des solutions de communication et de services numériques performants, renforçant ainsi leur compétitivité.

b. Amélioration de la couverture mobile

Le Morbihan, en partenariat avec les opérateurs de télécommunication, travaille également à améliorer la **couverture mobile 4G** dans les zones rurales et littorales. Des initiatives sont en place pour que les habitants puissent bénéficier d'une couverture mobile plus performante, facilitant ainsi l'accès à Internet pour tous.

2. Soutien à l'innovation numérique

a. Technopôle de Vannes (VIPE)

Le **Technopôle de Vannes**, également appelé **VIPE**, est un acteur clé de l'innovation numérique dans le Morbihan. Il soutient les startups et les entreprises innovantes à travers plusieurs actions :

Accompagnement des startups : Le technopôle propose des programmes d'incubation pour les jeunes entreprises qui développent des solutions innovantes, en particulier dans les secteurs du numérique, de la santé, et de l'environnement.

Réseautage et partenariats : VIPE facilite les échanges entre les entreprises innovantes, les laboratoires de recherche et les acteurs économiques locaux pour encourager l'innovation numérique et le développement de nouveaux projets collaboratifs.

b. Pôle numérique et cybersécurité à Lorient

Lorient, autre grande ville du Morbihan, a développé un pôle d'innovation axé sur le **numérique** et la **cybersécurité**. Ce pôle soutient les entreprises locales dans l'adoption des nouvelles technologies et la mise en place de solutions numériques sécurisées. Lorient est également impliqué dans des programmes de recherche pour renforcer la cybersécurité des systèmes d'information et protéger les données sensibles des entreprises et des administrations publiques.

c. Pôle Mer Bretagne Atlantique

Le **Pôle Mer Bretagne Atlantique**, bien que principalement orienté vers les technologies marines, intègre de plus en plus de solutions numériques dans ses initiatives, notamment l'utilisation de capteurs, de l'Internet des objets (IoT), et de l'intelligence artificielle pour mieux comprendre et gérer les ressources marines et côtières.

3. Transition numérique des entreprises

a. Actions pour les TPE et PME

Le Morbihan encourage la **transition numérique des entreprises**, notamment des **TPE et PME**, en leur fournissant des outils et un accompagnement adaptés :

Formations numériques : Le département propose des formations pour les chefs d'entreprises et les salariés des petites entreprises afin de les aider à intégrer des outils numériques dans leurs processus de production et de gestion (e-commerce, gestion des données, cybersécurité).

Aides à l'investissement : Le Morbihan propose également des aides pour les entreprises qui souhaitent investir dans des technologies numériques, que ce soit pour moderniser leur infrastructure, passer au cloud, ou améliorer leur présence en ligne.

b. Digitalisation des filières agricoles

Le Morbihan, région à forte composante agricole, soutient l'**adoption de solutions numériques dans l'agriculture**. Cela inclut l'utilisation de capteurs connectés pour la gestion de l'irrigation, l'analyse des sols, ou encore la gestion des troupeaux. Des solutions innovantes sont également développées pour optimiser les circuits de distribution et la vente en ligne de produits locaux.

4. Inclusion numérique et lutte contre la fracture numérique

a. Espaces Publics Numériques (EPN)

Le département met en place des **Espaces Publics Numériques (EPN)** pour favoriser l'inclusion numérique. Ces espaces, accessibles à tous, offrent des ateliers et des formations pour aider les citoyens, notamment les plus éloignés des technologies, à apprendre à utiliser les outils numériques.

Accès à Internet : Les EPN mettent à disposition des ordinateurs, une connexion Internet et un accompagnement personnalisé pour faciliter l'apprentissage des compétences numériques de base.

Formations pour tous : Des ateliers sont proposés pour apprendre à utiliser les services en ligne, réaliser des démarches administratives ou encore protéger ses données personnelles.

b. Pass numérique

Le **Pass numérique** est un dispositif qui permet aux personnes en difficulté avec les outils numériques de suivre des formations adaptées. Le Morbihan propose ces pass pour aider les populations éloignées des technologies, notamment dans les zones rurales, à maîtriser les bases de l'Internet et des services numériques.

5. Compétences numériques et éducation

a. Formations aux métiers du numérique

Le Morbihan encourage également la **formation aux métiers du numérique**. Des programmes de formation sont mis en place pour accompagner les jeunes et les adultes en reconversion professionnelle dans l'apprentissage des compétences numériques avancées, comme le développement web, la cybersécurité ou la gestion de projet numérique.

Centres de formation spécialisés : Le département soutient les centres de formation qui offrent des cursus dans le domaine du numérique, afin de renforcer le bassin d'emploi local dans ce secteur en pleine croissance.

b. Éducation numérique dans les écoles

Les établissements scolaires du Morbihan intègrent de plus en plus le numérique dans leurs enseignements. Le département, en collaboration avec les communes et les académies, équipe les

écoles de **tablettes** et d'**ordinateurs** pour permettre aux élèves de se familiariser avec les outils numériques dès le plus jeune âge. Des programmes d'apprentissage du **codage** et des **sciences numériques** sont également développés dans les collèges et lycées.

6. Cybersécurité

a. Ateliers de sensibilisation à la cybersécurité

La **sécurisation des systèmes informatiques** est un enjeu clé pour les entreprises et les collectivités locales. Le Morbihan, en partenariat avec des organismes régionaux et des experts en cybersécurité, propose des **ateliers de sensibilisation** pour aider les entreprises et les administrations à mieux comprendre les risques cybernétiques et à se protéger contre les cyberattaques.

Formation des TPE/PME : Des formations spécifiques sont offertes aux TPE et PME pour les aider à mettre en place des mesures de protection simples et efficaces, comme la gestion des mots de passe, la sécurisation des réseaux ou la mise en place de pare-feu.

Conclusion : Le Morbihan s'efforce de devenir un territoire connecté et innovant grâce à une politique numérique axée sur le déploiement d'infrastructures modernes (fibre optique, 4G/5G), le soutien à l'innovation dans des secteurs clés (technologies marines, cybersécurité, agriculture connectée), et la réduction de la fracture numérique. En investissant dans l'éducation numérique, l'inclusion numérique, et la transition numérique des entreprises, le Morbihan se positionne comme un acteur régional important dans la transformation numérique de la Bretagne et au-delà.

La ville, les communes

La ville de Lorient

Comment est organisée la ville de Lorient pour le numérique : quelles sont les initiatives, les actions ... ?

La **ville de Lorient**, située dans le département du Morbihan, en Bretagne, est particulièrement active en matière de développement numérique. Elle met en place plusieurs initiatives pour promouvoir l'innovation technologique, améliorer l'accès au numérique pour tous les habitants, et soutenir la transition numérique des entreprises locales. Voici un aperçu des principales actions et initiatives numériques à Lorient.

1. Infrastructures numériques et accès au Très Haut Débit

a. Déploiement de la fibre optique

Lorient participe au programme régional **Bretagne Très Haut Débit**, qui vise à déployer la **fibre optique** dans toute la région. Ce programme permet aux habitants de Lorient d'accéder à des connexions Internet à très haut débit, soutenant ainsi le développement des services numériques dans la ville.

Accès pour tous : La fibre optique est déployée aussi bien dans les zones urbaines que dans les quartiers moins densément peuplés, pour offrir à tous les habitants un accès à des services Internet performants.

Support aux entreprises : Le déploiement de la fibre est un levier important pour le développement des entreprises locales, leur permettant d'accéder à des outils numériques avancés et de participer à l'économie numérique.

b. Déploiement de la 5G

Lorient est également concernée par le déploiement de la **5G**, ce qui permet d'améliorer la connectivité mobile et de favoriser l'émergence de nouveaux services numériques, notamment dans les secteurs du tourisme, de la santé, et de l'industrie.

2. Soutien à l'innovation numérique

a. Technopôle de Lorient

Lorient dispose d'un **technopôle**, un espace dédié à l'innovation numérique et au développement des entreprises technologiques. Ce **pôle d'innovation** soutient la création de startups et le développement de projets numériques dans plusieurs domaines :

Transition numérique des entreprises : Le technopôle accompagne les entreprises locales dans l'adoption de technologies numériques, les aide à passer au commerce en ligne, et soutient leur intégration de l'intelligence artificielle et des objets connectés.

Recherche et développement (R&D) : Le technopôle collabore avec des universités et des laboratoires de recherche pour développer des solutions innovantes, en particulier dans les secteurs liés à la **mer** et à l'**environnement**, domaines clé pour l'économie locale de Lorient.

b. Lorient Technopole Métropole

Le programme **Lorient Technopole Métropole** vise à promouvoir le développement des entreprises et des projets innovants dans le numérique. Des incubateurs de startups sont proposés pour soutenir les entreprises émergentes dans leurs projets numériques, en particulier dans les domaines du **numérique vert** et de l'**économie maritime**.

c. Pôle de cybersécurité

Lorient joue un rôle important dans le domaine de la **cybersécurité**, en lien avec le pôle d'excellence régional basé à Rennes. Des programmes de formation et de **recherche** en cybersécurité sont proposés pour répondre aux besoins des entreprises locales en matière de protection des données et de sécurité des systèmes d'information.

3. Inclusion numérique

a. Espaces publics numériques (EPN)

La ville de Lorient met en place des **Espaces Publics Numériques (EPN)** pour favoriser l'**inclusion numérique**. Ces espaces permettent aux habitants, notamment ceux éloignés du numérique (personnes âgées, chômeurs, etc.), d'accéder à des formations et à un accompagnement personnalisé pour apprendre à utiliser les outils numériques.

- **Accès à Internet pour tous** : Les EPN mettent à disposition des ordinateurs et des connexions Internet pour les habitants qui n'ont pas accès à ces services à domicile.

- **Ateliers d'initiation** : Des ateliers sont organisés pour apprendre aux habitants à utiliser des logiciels, réaliser des démarches administratives en ligne, et protéger leurs données personnelles.

b. Pass numérique

Le **Pass numérique** est un dispositif mis en place par la ville pour permettre aux personnes en difficulté numérique de bénéficier de **formations gratuites**. Il vise à former les citoyens aux compétences numériques de base, telles que l'utilisation de l'e-mail, la navigation sur Internet, ou la gestion des outils bureautiques.

4. Transition numérique des entreprises

a. Programme Lorient Numérique

Le programme **Lorient Numérique** est une initiative visant à accompagner les entreprises locales dans leur transformation digitale. Il propose :

- **Conseils et accompagnement** : Les entreprises peuvent bénéficier de l'accompagnement d'experts pour intégrer des solutions numériques dans leur processus de production et de gestion (e-commerce, gestion des données, automatisation, etc.).

- **Aides à l'investissement** : La ville de Lorient offre des **subventions** et des **prêts** aux petites et moyennes entreprises (PME) pour les aider à financer leur transformation numérique.

b. Soutien aux startups

Lorient soutient également les **startups** à travers des **incubateurs** et des **programmes d'accélération**, leur offrant un cadre propice à l'innovation numérique. La ville collabore avec des partenaires académiques, des investisseurs et des associations pour offrir un écosystème dynamique aux entrepreneurs.

5. Éducation et compétences numériques

a. Initiation au codage pour les jeunes

La ville de Lorient encourage les jeunes à développer des compétences numériques dès le plus jeune âge en mettant en place des **ateliers d'initiation au codage** et à la programmation informatique. Ces ateliers sont organisés dans les écoles, les bibliothèques, et les centres culturels.

- **Formation au numérique dans les écoles** : Les établissements scolaires de Lorient sont équipés de **tablettes** et d'**ordinateurs** pour permettre aux élèves de se familiariser avec les outils numériques.

b. Formations professionnelles

La ville propose également des programmes de **formation continue** pour les adultes, notamment en ce qui concerne les compétences numériques avancées (gestion de projet numérique, cybersécurité,

développement web). Ces formations visent à répondre aux besoins du marché du travail local et à renforcer l'employabilité des habitants.

6. Cybersécurité

a. Sensibilisation des entreprises

La cybersécurité est une priorité pour Lorient, qui organise des ateliers de sensibilisation à destination des entreprises locales. Ces sessions visent à informer les dirigeants et les salariés des PME sur les risques liés aux cyberattaques et à leur fournir des solutions pratiques pour protéger leurs données et systèmes.

Programmes de formation en cybersécurité : Lorient propose des formations spécifiques en **cybersécurité** pour former des experts locaux capables de répondre aux besoins croissants de ce secteur.

b. Développement de solutions locales

Lorient travaille en partenariat avec des entreprises spécialisées en cybersécurité pour développer des solutions innovantes destinées aux entreprises locales. Cela inclut des services de conseil, de protection contre les cybermenaces, et de mise en conformité avec les normes de sécurité.

Conclusion : La ville de **Lorient** s'engage activement dans la transformation numérique, en mettant en place des infrastructures performantes (fibre, 5G), en soutenant l'innovation à travers des **technopôles** et des **pôles de cybersécurité**, et en favorisant l'inclusion numérique de tous ses habitants. En accompagnant les entreprises locales dans leur transition digitale et en offrant des formations numériques aux citoyens, Lorient se positionne comme un acteur clé du développement numérique en Bretagne.

Addendum :

- diverses formations à l'informatique pour les associations à la Maison des associations
- Accolades
- ...

Les Etats-Unis, la Chine et l'Union européenne

Les Etats-Unis

Le numérique aux Etats-Unis

Comment sont organisés les Etats-Unis pour le numérique : quelles sont les initiatives, les actions ... ?

Les **États-Unis** sont l'un des principaux leaders mondiaux en matière de numérique, avec un écosystème technologique puissant et une infrastructure numérique avancée. L'organisation du numérique aux États-Unis repose sur une multitude d'agences fédérales, d'acteurs privés, et de collaborations entre les niveaux fédéral, étatique, et local. Les États-Unis adoptent une approche souvent décentralisée, avec des initiatives à plusieurs niveaux, que ce soit pour l'innovation, la régulation des technologies, la cybersécurité, ou l'inclusion numérique. Voici comment le numérique est organisé aux États-Unis, avec des exemples d'initiatives et d'actions.

1. Organisation fédérale : agences et stratégies nationales

Le gouvernement fédéral joue un rôle crucial dans l'élaboration des stratégies et des politiques numériques des États-Unis. Plusieurs agences et départements fédéraux sont impliqués dans la gouvernance et le développement du secteur numérique.

a. National Telecommunications and Information Administration (NTIA)

La **NTIA**, sous la supervision du **Département du Commerce**, est l'agence fédérale principale responsable de l'élaboration des politiques et des réglementations relatives aux télécommunications et à l'économie numérique. Elle travaille à garantir que les infrastructures numériques (Internet, 5G) restent sûres, accessibles et ouvertes.

Rôles et responsabilités :

- **Gestion du spectre radioélectrique** : La NTIA coordonne l'utilisation du spectre pour les agences fédérales, un élément clé pour le développement de la 5G et des réseaux de communication.
- **Politique numérique** : Elle développe des recommandations et des politiques pour promouvoir une **Internet ouverte** et la protection de la vie privée en ligne.
- **Inclusion numérique** : La NTIA joue également un rôle dans la réduction de la fracture numérique par des initiatives visant à augmenter l'accès à Internet à haut débit dans les régions mal desservies.

b. Federal Communications Commission (FCC)

La **FCC** est une autre agence clé dans la régulation des télécommunications et du numérique aux États-Unis. Elle régule l'accès aux télécommunications et à l'Internet, supervise le déploiement de la 5G, et garantit que les communications (fixes, mobiles et Internet) respectent les lois fédérales.

Rôles et responsabilités :

- **Accès à Internet haut débit** : La FCC met en place des programmes comme le **Rural Digital Opportunity Fund (RDOF)** pour soutenir le déploiement du haut débit dans les régions rurales.
- **Neutralité du net** : La FCC a été au cœur du débat sur la **neutralité du net** aux États-Unis, un principe qui vise à garantir un accès égal à tous les services Internet sans discrimination par les fournisseurs.

- **Régulation du secteur des télécommunications** : La FCC régule les opérateurs télécoms pour s'assurer qu'ils respectent les normes de concurrence et de protection des consommateurs.

c. Department of Homeland Security (DHS) et Cybersecurity and Infrastructure Security Agency (CISA)

La **CISA**, une agence du **Department of Homeland Security (DHS)**, est responsable de la **cybersécurité** aux États-Unis. Elle joue un rôle central dans la protection des infrastructures critiques numériques du pays contre les cyberattaques.

Rôles et responsabilités :

- **Cybersécurité nationale** : La CISA collabore avec des agences gouvernementales, des entreprises privées et des gouvernements locaux pour sécuriser les infrastructures essentielles (énergie, télécommunications, transport, etc.) contre les cyberattaques.
- **Sécurité des élections** : Elle a également pour mission de sécuriser les systèmes de vote et de protéger les élections américaines contre les cyberinterférences.
- **Programme de sensibilisation** : CISA mène des campagnes de sensibilisation auprès des entreprises et des citoyens pour les informer des menaces numériques et des bonnes pratiques de cybersécurité.

d. National Institute of Standards and Technology (NIST)

Le **NIST**, rattaché au **Département du Commerce**, établit des normes et des directives pour les technologies émergentes, comme l'intelligence artificielle (IA), la cybersécurité, et les communications sans fil.

Rôles et responsabilités :

- **Normes de cybersécurité** : Le NIST développe des **guidelines** en matière de cybersécurité pour les entreprises et les administrations, comme le célèbre **Cybersecurity Framework**, largement utilisé dans le secteur public et privé.
- **Technologies émergentes** : Il soutient la recherche et le développement sur des technologies avancées comme la **blockchain**, les **réseaux quantiques**, et les technologies de pointe pour la fabrication.

e. National Science Foundation (NSF)

La **NSF** finance la recherche et l'innovation dans le domaine des sciences et des technologies, y compris les technologies numériques. Elle soutient des projets d'intelligence artificielle, de big data, et d'Internet des objets (IoT) à travers des bourses et des subventions.

Rôles et responsabilités :

- **Recherche et innovation** : La NSF finance la recherche universitaire et les projets innovants en matière de **technologies numériques** et de **télécommunications**.
- **Soutien à l'éducation** : La fondation soutient les initiatives éducatives visant à former la prochaine génération de professionnels du numérique, notamment en IA et en cybersécurité.

2. Initiatives fédérales et nationales

a. American Broadband Initiative

L'**American Broadband Initiative** vise à combler la **fracture numérique** en accélérant le déploiement du **haut débit** dans les zones rurales et mal desservies. Cette initiative coordonne les efforts des agences fédérales pour lever les obstacles réglementaires et favoriser les investissements dans les infrastructures de télécommunications.

b. 5G Fast Plan

Le **5G Fast Plan** est une initiative de la FCC visant à accélérer le déploiement de la **5G** à travers les États-Unis. L'objectif est de libérer plus de spectre pour les opérateurs de télécommunications,

simplifier les procédures réglementaires pour installer les infrastructures, et encourager l'investissement privé dans les réseaux de nouvelle génération.

c. National AI Initiative

Le **National AI Initiative** coordonne les efforts du gouvernement fédéral pour promouvoir le développement responsable de l'**intelligence artificielle** (IA) tout en s'assurant que les États-Unis conservent leur leadership mondial dans ce domaine. Cette initiative englobe plusieurs agences (NSF, NIST, DARPA) et vise à développer des normes éthiques, soutenir la recherche et former les talents dans le domaine de l'IA.

3. Niveau étatique et local : initiatives numériques

Aux États-Unis, les États et les collectivités locales jouent un rôle majeur dans la mise en œuvre des politiques numériques. Chaque État, et parfois chaque ville, développe ses propres stratégies numériques adaptées à ses besoins spécifiques.

a. État de la Californie

La **Californie**, en tant que centre névralgique de l'innovation technologique, mène plusieurs initiatives pour soutenir le secteur numérique. Par exemple, l'État finance des **programmes d'accélération de startups** dans la Silicon Valley et soutient le développement d'une **infrastructure 5G**.

b. New York City

New York City s'est concentrée sur l'**inclusion numérique** à travers son initiative **NYC Connected**. Cette initiative vise à fournir un accès Internet à haut débit à faible coût dans les quartiers défavorisés de la ville, ainsi qu'à offrir des programmes de formation aux compétences numériques pour les citoyens et les entreprises locales.

c. Texas

Le **Texas** investit massivement dans le déploiement des **infrastructures numériques**, notamment dans les zones rurales. Le gouvernement de l'État travaille avec des partenaires privés pour développer des solutions locales de **cybersécurité** et de **télécommunication** adaptées aux besoins des entreprises et des services publics.

4. Partenariat public-privé et rôle des entreprises technologiques

Les **entreprises privées** jouent un rôle central dans l'écosystème numérique des États-Unis. Les partenariats entre les secteurs public et privé sont essentiels pour promouvoir l'innovation, développer les infrastructures, et assurer la cybersécurité.

a. GAFAM (Google, Apple, Facebook, Amazon, Microsoft)

Les grandes entreprises technologiques américaines, souvent appelées GAFAM, sont des moteurs de l'innovation numérique mondiale. Elles collaborent fréquemment avec le gouvernement pour :

- **Investir dans les infrastructures** (notamment pour le déploiement de la 5G et l'extension du haut débit).
- **Développer des solutions de cybersécurité**.
- **Soutenir la recherche et l'éducation** à travers des partenariats avec des universités et des laboratoires.

b. Initiatives de connectivité

Des entreprises comme **Google Fiber** et **SpaceX** (avec son projet **Starlink**) participent activement aux efforts de déploiement du haut débit, notamment dans les régions rurales mal desservies, en utilisant des technologies innovantes comme les satellites ou la fibre optique à grande vitesse.

Conclusion

Les **États-Unis** adoptent une approche décentralisée du numérique, avec une coordination au niveau fédéral pour les grandes stratégies et une forte implication des **États, villes** et entreprises privées dans la mise en œuvre des politiques numériques. Les agences fédérales, comme la **FCC**, la **NTIA**, et la **CISA**, définissent des normes,

La comparaison USA-UE

Comment se comparent les États-Unis et l'Union européenne en termes de numérique : leurs initiatives, leurs organisations, leurs objectifs ?

Les **États-Unis** et l'**Union européenne** (UE) sont deux grandes puissances dans le domaine du numérique, mais leurs approches, organisations et objectifs diffèrent en raison de leurs systèmes de gouvernance, de leurs priorités économiques, et de leurs visions sur la régulation des technologies. Voici une comparaison détaillée de leurs initiatives, organisations, et objectifs numériques.

1. Approches de la gouvernance numérique

a. États-Unis : approche décentralisée et axée sur le secteur privé

Les États-Unis adoptent une approche plus **décentralisée** dans la gouvernance du numérique, où le **secteur privé** joue un rôle clé dans le développement et l'innovation technologique. L'intervention gouvernementale se concentre principalement sur des aspects comme la régulation des infrastructures et la cybersécurité, tout en laissant une grande marge de manœuvre aux **entreprises privées** pour innover.

- **Décentralisation** : Les initiatives numériques aux États-Unis sont souvent lancées à différents niveaux, du **fédéral** aux **États** et **municipalités**. Cela permet une grande flexibilité mais peut aussi conduire à des disparités en termes d'accès aux technologies et de régulation.
- **Dominance du secteur privé** : Les grandes entreprises technologiques américaines, comme les **GAFAM** (Google, Apple, Facebook, Amazon, Microsoft), jouent un rôle majeur dans le développement des infrastructures numériques, l'innovation, et la collecte de données. Elles collaborent parfois avec le gouvernement, mais influencent fortement l'écosystème numérique.
- **Régulation légère** : L'intervention de l'État est généralement limitée à la régulation des infrastructures (par la **FCC** et la **NTIA**), la gestion du spectre, et la cybersécurité (avec la **CISA**). Les États-Unis ont une approche plus **libérale** et **moins réglementée** en matière de protection des données et de régulation des grandes entreprises technologiques comparée à l'Europe.

b. Union européenne : approche plus centralisée et régulée

L'UE, en revanche, adopte une approche plus **centralisée** et **régulée** en matière de numérique, avec un fort accent sur la **protection des droits des citoyens**, la **concurrence équitable** et la **souveraineté numérique**. L'Union s'efforce de créer un **marché unique numérique** tout en limitant l'influence des grandes entreprises technologiques à travers des régulations strictes.

- **Coordination centralisée** : La Commission européenne, à travers des directions comme la **DG CONNECT**, joue un rôle central dans l'élaboration des politiques numériques pour l'ensemble des États membres. Les régulations européennes s'appliquent à tous les pays membres, garantissant ainsi une **harmonisation** des règles.
- **Régulation forte** : L'UE met l'accent sur une **régulation stricte**, notamment avec des lois comme le Règlement général sur la protection des données (RGPD), qui impose des normes élevées en matière de protection des données personnelles. De plus, des initiatives comme le Digital Services Act (DSA) et le Digital Markets Act (DMA) visent à encadrer les pratiques des grandes plateformes numériques pour garantir une concurrence loyale et protéger les droits des utilisateurs.

- **Souveraineté numérique** : L'UE met de plus en plus l'accent sur la **souveraineté numérique**, cherchant à limiter la dépendance vis-à-vis des entreprises technologiques non européennes et à promouvoir des solutions technologiques locales, comme avec le projet **GAIA-X** pour un **cloud européen souverain**.

2. Infrastructures et innovation technologique

a. États-Unis : leadership dans les infrastructures et technologies émergentes

Les États-Unis sont en tête dans le développement des **infrastructures numériques** avancées et des **technologies émergentes**, notamment grâce à l'**implication massive du secteur privé**.

- **Infrastructures numériques avancées** : Les États-Unis ont un fort engagement dans le déploiement de la **5G**, avec le **5G Fast Plan** et des investissements massifs des opérateurs privés pour rendre cette technologie accessible dans tout le pays.
- **Technologies émergentes** : Les entreprises américaines sont leaders dans le développement des **technologies de pointe** comme l'**intelligence artificielle (IA)**, le cloud computing, la blockchain, et les réseaux de communication spatiaux (par exemple, **Starlink** de **SpaceX**). Ces innovations sont souvent portées par des acteurs privés, soutenus par des investissements publics limités mais stratégiques, via la National Science Foundation (NSF) et d'autres agences.
- **Cybersécurité** : La **CISA** et le **NIST** sont à la pointe des initiatives pour sécuriser les infrastructures critiques, mais la coordination avec le secteur privé est essentielle pour protéger les infrastructures technologiques.

b. Union européenne : focus sur l'inclusion et la résilience numérique

L'UE met davantage l'accent sur le **développement équilibré des infrastructures**, l'**inclusion numérique** et la **souveraineté technologique** pour réduire sa dépendance vis-à-vis des entreprises étrangères.

- **Marché unique numérique** : L'une des grandes priorités de l'UE est de créer un **marché unique numérique** où les biens et services peuvent circuler librement à travers les États membres, avec des réglementations harmonisées. Cela permet aux entreprises de se développer plus facilement au sein de l'UE.
- **Souveraineté technologique** : Avec des initiatives comme **GAIA-X**, l'UE tente de promouvoir des solutions technologiques européennes (cloud, IA) pour réduire la dépendance à l'égard des géants technologiques non européens, en particulier américains et chinois.
- **Investissement dans la recherche** : L'UE **soutient** l'innovation numérique à travers des programmes de financement comme **Horizon Europe** et le **Programme pour une Europe numérique**, qui financent des projets en IA, en cybersécurité, et dans les **supercalculateurs**.
- **Inclusion numérique** : L'UE met un fort accent sur l'**inclusion numérique**, avec des initiatives comme **Connecting Europe** et **Digital Skills and Jobs Coalition**, visant à réduire la fracture numérique et à former les citoyens aux compétences numériques nécessaires.
- Régulation et protection des données
- États-Unis : régulation limitée, forte dépendance au secteur privé
- **Protection des données** : Les États-Unis n'ont pas de régulation centralisée en matière de protection des données équivalente au RGPD. La gestion des données est souvent laissée à l'appréciation des entreprises, avec des législations variables selon les États. Cependant, des États comme la Californie ont adopté des réglementations similaires au RGPD, comme la California Consumer Privacy Act (CCPA).
- **Régulation des grandes entreprises technologiques** : Les grandes entreprises américaines bénéficient d'une régulation relativement souple. Bien que des enquêtes antitrust aient été

ouvertes contre des géants comme Google et Facebook, la régulation reste plus permissive par rapport à l'Europe.

b. Union européenne : régulation stricte et protection des droits numériques

- **RGPD** : Le **Règlement général sur la protection des données (RGPD)** est l'un des cadres les plus stricts au monde en matière de protection des données personnelles. Il impose des règles strictes aux entreprises opérant en Europe pour garantir la transparence, la sécurité et le consentement des utilisateurs.
- **Digital Markets Act (DMA) et Digital Services Act (DSA)** : Ces **législations** visent à réguler les grandes plateformes numériques et à limiter leur pouvoir sur le marché, garantissant une concurrence équitable et protégeant les consommateurs contre les abus de pouvoir.

4. Cybersécurité

a. États-Unis : focus sur les infrastructures critiques

Les États-Unis mettent fortement l'accent sur la protection des **infrastructures critiques** (énergie, défense, télécommunications) contre les cyberattaques. La **CISA** coordonne les efforts de cybersécurité avec le secteur privé et d'autres agences fédérales pour répondre aux menaces croissantes.

b. Union européenne : approche multilatérale

L'UE, avec la création de l'**ENISA** (Agence de l'UE pour la cybersécurité), adopte une approche multilatérale en matière de **cybersécurité**, en imposant des normes communes à tous les États membres. La directive **NIS2** harmonise les exigences en matière de cybersécurité dans l'ensemble des infrastructures critiques de l'UE, renforçant ainsi la résilience numérique.

5. Objectifs numériques futurs

a. États-Unis

- **Leadership technologique mondial** : Les États-Unis cherchent à maintenir leur leadership dans les technologies émergentes, notamment l'IA, la 5G, la blockchain, et l'espace.
- **Déploiement des infrastructures** : L'objectif est d'étendre la 5G et de combler la fracture numérique dans les zones rurales.

Cybersécurité : Renforcer la cybersécurité des infrastructures critiques tout en travaillant avec le secteur privé pour améliorer les défenses numériques.

b. Union européenne

Souveraineté numérique : L'UE vise à réduire sa dépendance aux technologies non européennes avec des projets comme

La Chine

Le numérique en Chine

Comment est organisée la Chine pour le numérique : quelles sont les initiatives, les actions ... ?

La **Chine** est devenue un acteur central dans le domaine du numérique, avec une stratégie de développement numérique particulièrement ambitieuse. Le gouvernement chinois contrôle et encadre strictement le secteur numérique à travers des initiatives stratégiques, une régulation rigoureuse et des investissements massifs dans l'infrastructure et les technologies de pointe. Voici un aperçu de l'organisation du numérique en Chine, ainsi que des principales initiatives et actions mises en place par le gouvernement.

1. Organisation centrale et contrôle gouvernemental

En Chine, le **gouvernement central** joue un rôle prépondérant dans la régulation et le développement du secteur numérique. Contrairement aux États-Unis ou à l'Union européenne, la **gouvernance numérique en Chine** est très centralisée, et l'État intervient à la fois dans le développement des technologies et dans la régulation des acteurs privés.

a. Cyberspace Administration of China (CAC)

La **Cyberspace Administration of China (CAC)** est l'agence principale chargée de réguler et de surveiller l'Internet en Chine. Elle contrôle les politiques en matière de **cyberespace**, régule les contenus en ligne, et s'assure que les entreprises respectent les règles imposées par le gouvernement.

- **Censure de l'Internet** : Le CAC est responsable de la surveillance et de la censure du contenu en ligne, ce qui inclut la suppression de contenus jugés inappropriés ou critiques envers le gouvernement. La **Grande Muraille numérique (Great Firewall)** est le mécanisme principal utilisé pour filtrer et censurer l'accès à certaines plateformes internationales (Google, Facebook, Twitter, etc.).
- **Protection des données** : Le CAC supervise également la collecte et la gestion des données personnelles par les entreprises. La Chine a mis en place des réglementations strictes sur la gestion des données, via la **Loi sur la protection des informations personnelles (PIPL)**, pour encadrer l'utilisation des données et assurer un contrôle gouvernemental sur celles-ci.

b. Ministère de l'Industrie et des Technologies de l'Information (MIIT)

Le **Ministère de l'Industrie et des Technologies de l'Information (MIIT)** est l'organisme gouvernemental en charge de la politique industrielle et technologique dans le secteur des télécommunications, de l'Internet, et des technologies émergentes.

- **Développement des infrastructures numériques** : Le MIIT est **responsable** de la mise en place des infrastructures numériques comme les réseaux 5G, la fibre optique, et l'Internet des objets (IoT).
- **Planification industrielle** : Le ministère élabore des stratégies **industrielles** pour renforcer la compétitivité chinoise dans des domaines clés comme l'intelligence artificielle (IA), la cybersécurité, et les semi-conducteurs.

c. National Development and Reform Commission (NDRC)

La **NDRC** est l'organisme central qui coordonne la **planification économique** du pays, y compris dans le domaine du numérique. Elle supervise l'allocation des ressources dans des secteurs prioritaires comme le **cloud computing**, l'**intelligence artificielle**, et les **technologies de l'information**.

2. Principales initiatives et stratégies numériques en Chine

a. Made in China 2025

Le plan **Made in China 2025** est une stratégie nationale lancée en 2015 pour transformer la Chine en une puissance manufacturière de haute technologie. Le numérique joue un rôle crucial dans cette initiative, notamment avec l'adoption de technologies numériques dans l'industrie pour moderniser la production.

- **Numérisation des industries** : Le plan vise à numériser et automatiser les processus de production à travers l'utilisation de robots, de systèmes d'intelligence artificielle, et de l'Internet des objets (IoT).
- **Souveraineté technologique** : L'un des objectifs est de réduire la dépendance de la Chine aux technologies étrangères, notamment dans des secteurs stratégiques comme les semi-conducteurs, les télécommunications, et les technologies de l'information.

b. Plan de développement de l'intelligence artificielle (IA)

La Chine a publié en 2017 un Plan de développement de l'intelligence artificielle, avec l'objectif de devenir le leader mondial de l'IA d'ici 2030.

- **Recherche et développement** : La Chine investit massivement dans la recherche sur l'IA, à la fois dans le secteur public et privé, en encourageant les partenariats entre universités, laboratoires de recherche et entreprises.
- **Applications industrielles** : Le gouvernement chinois soutient activement l'intégration de l'IA dans des secteurs clés comme la santé, la finance, l'éducation, et la sécurité nationale. La technologie est utilisée pour améliorer l'efficacité dans ces domaines, mais aussi pour des applications de surveillance.
- **Surveillance et sécurité** : L'IA est également utilisée pour des technologies de reconnaissance faciale, des systèmes de surveillance de masse, et la gestion des réseaux de sécurité publique.

c. Déploiement de la 5G

La Chine est un leader mondial dans le déploiement de la 5G, avec des acteurs comme Huawei et ZTE qui jouent un rôle clé dans le développement des infrastructures 5G, tant en Chine qu'à l'international.

- **Investissements massifs** : La Chine a déployé plus de **1,6 million de stations de base 5G** d'ici fin 2021, bien en avance par rapport à d'autres pays. La couverture 5G vise à atteindre les zones urbaines, rurales, et industrielles, pour soutenir l'IoT et l'automatisation industrielle.
- **Applications industrielles** : La 5G est également déployée pour des **usines intelligentes**, la **santé connectée**, les **villes intelligentes**, et des applications dans les transports comme les véhicules autonomes.
- d. Souveraineté numérique : le cloud chinois et les semi-conducteurs

La Chine met l'accent sur la **souveraineté numérique**, en réduisant sa dépendance vis-à-vis des technologies et infrastructures étrangères.

- **Cloud souverain** : Le gouvernement soutient des entreprises locales comme **Alibaba Cloud**, **Tencent Cloud**, et **Huawei Cloud**, qui dominent le marché chinois du cloud computing. Ces plateformes cloud sont également déployées à l'international dans le cadre de l'initiative des **Nouvelles Routes de la Soie numériques**.
- **Semi-conducteurs** : En réponse aux sanctions américaines limitant l'accès aux semi-conducteurs, la Chine investit massivement dans la **production de puces** locales et encourage la création de championnes nationales dans la fabrication des **semi-conducteurs** (comme SMIC).

3. Contrôle des données et cybersécurité

a. Loi sur la cybersécurité

La **Loi sur la cybersécurité**, adoptée en 2017, impose des règles strictes sur la manière dont les entreprises collectent, stockent, et utilisent les données en Chine.

- **Stockage des données** : Les entreprises qui opèrent en Chine sont tenues de stocker les données des utilisateurs chinois sur des serveurs localisés en Chine.
- **Accès aux données par le gouvernement** : Les entreprises doivent fournir un accès aux données au gouvernement chinois en cas de besoin, ce qui soulève des préoccupations en matière de **confidentialité** et de **surveillance**.

b. Protection des données personnelles

La **Loi sur la protection des informations personnelles (PIPL)**, entrée en vigueur en 2021, est similaire au **RGPD européen** en ce sens qu'elle régule la collecte et l'utilisation des données personnelles en Chine. Cependant, elle garantit également un **contrôle étatique** important sur ces données.

Contrôle gouvernemental : Bien que cette loi protège les citoyens contre l'abus des données par les entreprises, elle renforce également la capacité du gouvernement à **accéder aux informations personnelles** à des fins de sécurité nationale.

4. Surveillance numérique et contrôle social

a. Système de crédit social

La Chine a mis en place un **système de crédit social**, qui utilise des technologies numériques pour surveiller et évaluer le comportement des citoyens et des entreprises. Ce système repose sur la collecte de données massives via des caméras, des applications mobiles, et des bases de données gouvernementales.

- **Sanctions et récompenses** : En fonction de leurs comportements (respect des lois, paiements de dettes, infractions mineures), les citoyens et les entreprises peuvent être récompensés (accès à des services publics, prêts avantageux) ou pénalisés (restrictions de déplacement, accès limité à certains services).
- **Surveillance massive** : Des technologies comme la reconnaissance faciale, l'intelligence artificielle et l'analyse de données sont utilisées pour suivre les déplacements et les interactions des citoyens, dans le but de maintenir l'ordre social.

b. Reconnaissance faciale et surveillance de masse

La **reconnaissance biométrique** en Chine, notamment la **reconnaissance faciale**, est un outil central dans les systèmes de **surveillance de masse** déployés par le gouvernement. Utilisée dans les grandes villes et régions sensibles, cette technologie permet d'identifier des individus en temps réel et d'assurer le **contrôle social**.

- **Applications de sécurité publique** : Le gouvernement chinois utilise des caméras **intelligentes** couplées à des systèmes de reconnaissance faciale pour surveiller les citoyens, maintenir l'ordre public, et détecter des comportements suspects. Ces technologies sont couramment utilisées pour suivre les déplacements des citoyens, surveiller les rassemblements publics, et identifier rapidement des personnes recherchées par les forces de l'ordre.
- **Surveillance des minorités** : La **reconnaissance biométrique** en Chine a suscité des préoccupations internationales, notamment concernant l'utilisation de cette technologie dans les régions où vivent des minorités ethniques, comme les **Ouïghours** dans le Xinjiang. Il est rapporté que ces systèmes de surveillance sont utilisés pour suivre, contrôler, et opprimer ces populations, conduisant à des violations des **droits de l'homme**. Des rapports indiquent que des millions d'Ouïghours sont suivis et surveillés en temps réel, et que les systèmes de reconnaissance faciale peuvent identifier une personne non seulement en fonction de son apparence, mais aussi de son appartenance ethnique.
- **Contrôle social et crédit social** : En lien avec ces technologies de surveillance, la Chine a développé un système de **crédit social**, qui attribue aux citoyens une note en fonction de leur comportement. Cette note peut affecter leur accès à certains services, comme les prêts bancaires, l'emploi, ou les voyages. Les technologies de reconnaissance biométrique permettent de surveiller et de sanctionner les citoyens en cas de non-respect des lois ou de comportements jugés inappropriés par l'État.

Défis et controverses autour de la surveillance biométrique en Chine

Le modèle chinois de **surveillance biométrique** suscite de nombreuses critiques à l'international, notamment en ce qui concerne le respect de la vie privée et les libertés individuelles.

- **Préoccupations en matière de droits de l'homme** : Les organisations de défense des droits de l'homme accusent la Chine d'utiliser la reconnaissance faciale pour **restreindre les libertés** civiles, opprimer les minorités ethniques, et surveiller les dissidents politiques. Ces technologies posent la question de l'équilibre entre sécurité publique et **liberté individuelle**, notamment dans les régimes autoritaires.

- **Déploiement mondial** : Les technologies chinoises de reconnaissance faciale et de surveillance sont également exportées vers d'autres pays, en particulier dans des États autoritaires ou en développement, alimentant les inquiétudes sur l'utilisation de ces systèmes à des fins de contrôle et de répression des populations.

En conclusion, la **reconnaissance biométrique** en Chine est un exemple de l'utilisation de la technologie pour un contrôle strict de la société. Bien qu'elle soit présentée comme une avancée en matière de sécurité publique, son utilisation à des fins de **surveillance de masse** soulève des questions fondamentales sur les **droits humains** et la **vie privée** dans une société de plus en plus technologique.

La comparaison Chine-USA

Comment se comparent les États-Unis et la Chine en termes de numérique : leurs initiatives, leurs organisations, leurs objectifs ?

Les **États-Unis** et la **Chine** sont les deux plus grandes puissances mondiales dans le domaine du numérique, mais leurs approches en matière de gouvernance, d'initiatives, d'organisations et d'objectifs diffèrent considérablement. Voici une comparaison de leurs stratégies numériques, de la manière dont leurs gouvernements et entreprises privées gèrent ce secteur, et de leurs objectifs à long terme.

1. Approche générale : État contre secteur privé

a. États-Unis : un leadership basé sur l'innovation privée

- **Organisation décentralisée** : Aux États-Unis, la **gouvernance numérique** repose largement sur un modèle **décentralisé** où le **secteur privé** joue un rôle de premier plan. Les grandes entreprises technologiques comme **Google**, **Apple**, **Microsoft**, **Facebook** et **Amazon** (GAFAM) sont les principaux moteurs de l'innovation numérique. Le gouvernement intervient principalement pour la **régulation des infrastructures** (télécoms, spectre) et la **cybersécurité**, tout en laissant une grande marge de manœuvre au secteur privé.
- **Régulation légère** : Les États-Unis adoptent une approche **moins régulée** que la Chine, surtout en matière de **protection des données** et de régulation **des grandes plateformes technologiques**. Des régulations existent, mais elles varient selon les États (par exemple, la **California Consumer Privacy Act - CCPA**) et ne sont pas aussi centralisées que les lois chinoises. Les entreprises ont une grande flexibilité dans leur gestion des données personnelles et des technologies.
- **Innovation technologique** : Les États-Unis sont leaders dans les **technologies émergentes** comme l'**intelligence artificielle (IA)**, le **cloud computing**, les **réseaux spatiaux** (SpaceX et Starlink), et les **semi-conducteurs**. L'innovation est surtout soutenue par des initiatives privées et des fonds d'investissement en capital-risque, avec un soutien gouvernemental limité via des agences comme la **National Science Foundation (NSF)**.

b. Chine : une gouvernance centralisée avec un contrôle étatique fort

- **Organisation centralisée** : En Chine, la gouvernance numérique est **hautement centralisée** et **étatisée**. Le gouvernement joue un rôle **dominant** dans l'orientation et le développement du numérique. Les entreprises chinoises comme **Alibaba**, **Tencent**, **Huawei**, et **Baidu** sont puissantes, mais elles opèrent sous une **surveillance étroite** de l'État et doivent se conformer aux directives du Parti communiste chinois (PCC).
- **Contrôle gouvernemental strict** : Contrairement aux États-Unis, la **régulation en Chine** est beaucoup plus stricte. Des agences comme la **Cyberspace Administration of China (CAC)** et le **Ministère de l'Industrie et des Technologies de l'Information (MIIT)** surveillent de près les activités en ligne, les contenus et les entreprises technologiques. La **surveillance des**

citoyens et la **censure** de l'Internet sont des éléments essentiels de cette régulation, à travers des mécanismes comme la **Grande Muraille numérique** et le **système de crédit social**.

- **Souveraineté numérique** : La Chine se concentre fortement sur la **souveraineté numérique**, cherchant à réduire sa dépendance vis-à-vis des technologies étrangères, notamment dans les secteurs des semi-conducteurs, du **cloud computing**, et de la **5G**. Des initiatives comme **Made in China 2025** et le **Plan de développement de l'IA** visent à faire de la Chine un leader mondial des technologies numériques tout en assurant un contrôle strict de l'État.

2. Infrastructures numériques et technologies émergentes

a. États-Unis : leadership dans les technologies de pointe, infrastructure avancée

- **5G et haut débit** : Les États-Unis investissent massivement dans le déploiement de la **5G** et dans l'amélioration des infrastructures de télécommunication grâce à des initiatives comme le **5G Fast Plan** et le **American Broadband Initiative**. Toutefois, le déploiement de la 5G est principalement mené par des **opérateurs privés** comme **Verizon**, **AT&T**, et **T-Mobile**.
- **Technologies émergentes** : Les États-Unis sont en avance dans le développement de **l'intelligence artificielle (IA)**, de la **réalité augmentée/virtuelle**, du **big data**, et des **réseaux spatiaux** (avec SpaceX et Starlink). Ces innovations sont souvent portées par des géants technologiques privés avec un **soutien modéré du gouvernement** via des financements à la recherche (NSF, DARPA).

b. Chine : leadership dans le déploiement de la 5G et les applications industrielles

- **5G** : La Chine est le **leader mondial dans le déploiement de la 5G**, avec plus de **1,6 million de stations de base 5G** installées en 2021. Les entreprises comme **Huawei** et **ZTE** jouent un rôle crucial dans ce développement. La 5G est **intégrée** dans l'industrie pour soutenir des applications comme **l'Internet des objets (IoT)**, les **usines intelligentes**, et la **santé connectée**.
- **Technologies émergentes** : La Chine investit massivement dans des technologies émergentes comme **l'IA**, la **blockchain**, et les **semi-conducteurs**. Le **Plan de développement de l'IA** de 2017 vise à faire de la Chine le leader mondial de l'IA d'ici 2030, avec un fort soutien de l'État à la **recherche et au développement (R&D)** et une mise en œuvre rapide de ces technologies dans des secteurs stratégiques (industrie, santé, défense, surveillance).

3. Régulation et cybersécurité

a. États-Unis : cybersécurité axée sur les infrastructures critiques et le secteur privé

- **Cybersécurité** : Les États-Unis, via la **Cybersecurity and Infrastructure Security Agency (CISA)** et le **National Institute of Standards and Technology (NIST)**, adoptent une approche axée sur la protection des **infrastructures critiques** (énergie, transport, télécommunications) contre les cyberattaques. Le secteur privé collabore avec le gouvernement pour mettre en place des solutions de sécurité, mais il conserve une grande autonomie.
- **Protection des données** : Contrairement à la Chine, les États-Unis n'ont pas de régulation centralisée pour la **protection des données personnelles**. Des lois existent à l'échelle des États (comme la **CCPA** en Californie), mais il n'y a pas d'équivalent national au **RGD** européen. Le secteur privé dispose donc de plus de latitude dans la collecte et la gestion des données.

b. Chine : cybersécurité et contrôle strict des données

- **Cybersécurité** : En Chine, la **Loi sur la cybersécurité** impose des règles strictes à la fois pour la protection des infrastructures numériques et pour le contrôle **gouvernemental** des activités en ligne. Le **CAC** surveille de près les contenus et impose une censure stricte via la **Grande Muraille numérique**, bloquant l'accès à de nombreux services étrangers (Google, Facebook, etc.).

- **Protection et contrôle des données** : La **Loi sur la protection des informations personnelles (PIPL)**, entrée en vigueur en 2021, impose des règles sur la collecte, le stockage, et l'utilisation des données personnelles, mais elle donne également au gouvernement un **contrôle étendu** sur ces données. Contrairement aux États-Unis, les entreprises chinoises doivent fournir un accès aux données des utilisateurs si le gouvernement le demande, renforçant le cadre de **surveillance de masse**.

4. Objectifs à long terme

a. États-Unis : maintenir le leadership technologique mondial

Les États-Unis visent à **maintenir leur leadership** dans les **technologies de pointe**, notamment l'IA, la cybersécurité, les semi-conducteurs, et les infrastructures spatiales. Ils cherchent à :

- **Soutenir l'innovation privée** : Grâce à un écosystème **de startups** dynamique et des financements privés abondants, les États-Unis s'appuient sur la créativité des acteurs du secteur technologique pour innover.
- **Renforcer les infrastructures numériques** : Les initiatives de **déploiement de la 5G** et de réduction de la **fracture numérique** (American Broadband Initiative) sont des priorités pour garantir que le pays reste connecté et compétitif.
- **Cybersécurité** : La **protection des infrastructures critiques** face aux menaces cybernétiques est une priorité croissante, avec une collaboration public-privé renforcée.

b. Chine : devenir le leader mondial des technologies numériques et de l'IA

La Chine a des objectifs ambitieux pour devenir le leader mondial dans les technologies numériques :

- **Souveraineté technologique** : Le gouvernement chinois cherche à réduire sa dépendance aux technologies étrangères, en particulier dans les **semi-conducteurs** et le cloud computing. L'objectif est de développer une **industrie technologique indépendante**.
- **Leadership mondial en IA** : Le Plan de développement de l'IA vise à faire de la Chine le ...

Les microprocesseurs

Les différents microprocesseurs

L'évolution des microprocesseurs peut être caractérisée par les différents types de processeurs qui ont émergé pour répondre aux besoins spécifiques des technologies modernes. Les principaux types de microprocesseurs sont les CPU (Central Processing Unit), les GPU (Graphics Processing Unit), et les NPU (Neural Processing Unit). Voici une description de chacun et une vue d'ensemble de leur évolution :

1. CPU (Central Processing Unit)

Caractéristiques et Évolution

- **Fonction** : Le CPU est le cœur du système informatique, responsable de l'exécution des instructions des programmes. Il gère les calculs, les opérations logiques, et le contrôle des autres composants du système.
- **Architecture** : Traditionnellement, les CPU sont conçus avec un nombre limité de cœurs (deux à plusieurs dizaines) capables de traiter des instructions de manière séquentielle et simultanée.
- **Évolution** :
 - Monocœur à Multicœurs : Les premiers CPU étaient monocœurs, traitant une seule instruction à la fois. L'évolution vers les architectures multicœurs (deux, quatre, huit cœurs ou plus) a permis une meilleure gestion du multitâche et une augmentation des performances globales.
 - Augmentation de la Fréquence : Au fil du temps, les CPU ont vu une augmentation de la fréquence d'horloge, permettant des calculs plus rapides.
 - Optimisation pour l'Hyper-Threading : Les technologies telles que l'hyper-threading ont permis à chaque cœur de traiter plusieurs threads simultanément, améliorant l'efficacité du traitement.
 - Consommation Énergétique et Miniaturisation : Les CPU modernes sont conçus pour être plus efficaces énergétiquement tout en intégrant de plus en plus de transistors sur des puces de plus petite taille grâce à des technologies de fabrication avancées (par exemple, 7 nm, 5 nm).

2. GPU (Graphics Processing Unit)

Caractéristiques et Évolution

- **Fonction** : Les GPU sont spécialisés dans le traitement parallèle des données, particulièrement efficace pour les calculs graphiques et les opérations vectorielles. Ils sont essentiels pour le rendu des graphismes en 3D, les jeux vidéo, et les applications nécessitant une intensité de calcul parallèle.
- **Architecture** : Les GPU possèdent des milliers de cœurs de traitement plus petits, conçus pour exécuter des tâches simultanées en parallèle, ce qui les rend très efficaces pour des opérations massivement parallèles.
- **Évolution** :
 - **Des GPU Basés sur des Shaders** : Les premiers GPU étaient optimisés pour des tâches graphiques fixes. Avec l'évolution, les GPU modernes sont dotés de shaders programmables, permettant des calculs plus flexibles et personnalisables.
 - **CUDA et OpenCL** : L'introduction des architectures CUDA (NVIDIA) et OpenCL a permis l'utilisation des GPU pour des calculs généraux (GPGPU - General-Purpose computing on

GPU), ouvrant la voie à des applications dans le domaine de l'intelligence artificielle, de l'analyse de données, et plus encore.

- **Ray Tracing et IA** : Les GPU récents intègrent des capacités avancées telles que le ray tracing pour le rendu réaliste et des unités dédiées à l'intelligence artificielle pour améliorer les performances dans les tâches d'apprentissage automatique.

3. NPU (Neural Processing Unit)

Caractéristiques et Évolution

- **Fonction** : Les NPU sont des processeurs spécialement conçus pour l'exécution efficace des opérations liées à l'apprentissage automatique et à l'intelligence artificielle, notamment les réseaux neuronaux. Ils sont optimisés pour les calculs de type tensoriel et les inférences AI.
- **Architecture** : Les NPU intègrent des architectures qui permettent des opérations de matrice et des calculs de grande envergure avec une efficacité énergétique élevée, souvent en utilisant des unités de traitement spécialisées pour les calculs tensoriels.

Évolution :

- **Des Solutions Dédiées aux Réseaux Neuronaux** : Les premiers processeurs AI étaient souvent des GPU adaptés. L'évolution vers des NPUs dédiés permet une optimisation accrue pour les tâches d'apprentissage profond et d'inférence.
- **Intégration dans les SoC** : De nombreux fabricants intègrent désormais des NPUs directement dans leurs System-on-Chip (SoC), notamment dans les smartphones et les dispositifs IoT, pour offrir des capacités AI locales avec une faible consommation énergétique.
- **Optimisation et Performances** : Les NPUs modernes sont conçus pour optimiser non seulement la vitesse des calculs mais aussi l'efficacité énergétique, ce qui est crucial pour les applications en temps réel et les dispositifs embarqués.

Résumé :

- **CPU** : Optimisé pour le traitement séquentiel et multitâche généraliste. Son évolution a porté sur l'augmentation du nombre de cœurs, de la fréquence, et de la miniaturisation des transistors.
- **GPU** : Conçu pour le traitement parallèle massif, particulièrement efficace pour les graphiques et les applications AI. L'évolution a vu l'intégration de capacités de calcul général et de traitement avancé pour les graphismes et l'IA.
- **NPU** : Spécialisé dans le traitement des algorithmes d'IA et d'apprentissage automatique. Son évolution se concentre sur l'optimisation des calculs tensoriels et l'intégration dans des dispositifs pour des performances AI localisées et efficaces énergétiquement.

Chacun de ces types de processeurs joue un rôle crucial dans l'écosystème technologique moderne, avec des spécialisations qui répondent à des besoins différents en matière de traitement des données.

La position de l'Union européenne dans les microprocesseurs

Quelle position occupe l'Union européenne pour les microprocesseurs ?

L'Union européenne (UE) joue un rôle important dans le domaine des microprocesseurs, bien que son positionnement et ses capacités soient marqués par des défis et des opportunités spécifiques. Voici un aperçu de la position actuelle de l'UE dans le secteur des microprocesseurs :

1. Position Actuelle et Rôle Global

Fabrication et Conception

- **Dépendance Importante** : L'UE est largement dépendante des importations de microprocesseurs. La majorité des puces utilisées en Europe sont fabriquées par des entreprises non-européennes, principalement en Asie (notamment en Taiwan avec TSMC et en Corée du Sud avec Samsung) et aux États-Unis (comme Intel et AMD).
- **Industrie Européenne** : L'UE possède des entreprises telles que STMicroelectronics et Infineon Technologies, qui sont des acteurs clés dans la conception et la fabrication de certains types de puces, notamment pour l'automobile, les équipements industriels, et les solutions de sécurité. Cependant, leur part de marché globale dans la production de microprocesseurs est limitée par rapport aux grands leaders mondiaux.

Recherche et Développement

- **Investissements en R&D** : L'UE investit de manière significative dans la recherche et le développement des technologies de microprocesseurs, avec des initiatives telles que le programme Horizon Europe et des projets de collaboration public-privé pour avancer dans les technologies de semi-conducteurs.
- **Projets Européens** : Des initiatives comme EuroHPC visent à développer des supercalculateurs et des infrastructures de calcul de haute performance en Europe, ce qui nécessite des avancées en microprocesseurs.

2. Initiatives et Stratégies Européennes

Stratégie de Sécurité des Approvisionnements

- **Souveraineté Technologique** : Pour réduire la dépendance vis-à-vis des fournisseurs étrangers, l'UE a lancé des initiatives pour renforcer sa capacité de production locale de semi-conducteurs. Le plan "Chips Act" vise à augmenter la capacité de production de semi-conducteurs en Europe, en visant à produire 20% des puces mondiales d'ici 2030.
- **Infrastructures de Fabrication** : Le Chips Act inclut des investissements dans la construction de nouvelles usines de fabrication en Europe et le soutien à la recherche et à l'innovation dans le domaine des semi-conducteurs.

Collaboration Internationale

- **Partenariats** : L'UE collabore avec des partenaires internationaux pour renforcer ses chaînes d'approvisionnement en semi-conducteurs. Des alliances avec des entreprises américaines, asiatiques et d'autres régions sont en place pour sécuriser l'accès aux technologies et aux matériaux critiques.
- **Normes et Régulations** : L'UE joue un rôle actif dans la définition des normes et des réglementations pour les semi-conducteurs à l'échelle mondiale, influençant les pratiques de l'industrie.

3. Défis et Opportunités

Défis

- **Compétition Mondiale** : L'UE fait face à une compétition intense de la part des géants de l'industrie des semi-conducteurs, qui dominent le marché en termes de volume de production, d'innovation et de ressources.
- **Complexité de la Chaîne d'Approvisionnement** : Les chaînes d'approvisionnement en semi-conducteurs sont complexes et vulnérables aux perturbations, comme l'a montré la pénurie mondiale de puces en 2020-2021.

Opportunités

- **Innovation et Leadership** : En mettant l'accent sur des technologies avancées et des applications critiques comme les semi-conducteurs pour l'IA, les voitures autonomes, et les infrastructures de calcul haute performance, l'UE peut jouer un rôle de leader dans certaines niches de marché.

- **Soutien Politique** : Les initiatives politiques et les investissements en R&D fournissent une base solide pour la croissance de l'industrie des microprocesseurs en Europe, offrant une opportunité de renforcer la capacité de fabrication locale et d'améliorer la compétitivité globale.

Résumé : L'Union européenne se positionne comme un acteur important dans le secteur des microprocesseurs, bien que son rôle soit principalement axé sur l'innovation, la recherche et le développement, ainsi que sur des initiatives visant à augmenter sa capacité de production locale. La dépendance vis-à-vis des fournisseurs non-européens reste significative, mais les efforts récents, tels que le Chips Act, montrent une volonté de renforcer la souveraineté technologique et d'améliorer la capacité de production européenne. L'UE continue d'investir dans des projets de recherche et de développement et de collaborer avec des partenaires internationaux pour sécuriser son avenir dans le domaine des microprocesseurs.

Conception et production

Les microprocesseurs ou puces électronique sont-ils conçus dans l'Union européenne et fabriqués à Taïwan ?

Les microprocesseurs et les puces électroniques sont un élément essentiel de la technologie moderne, et leur conception et fabrication impliquent souvent un réseau complexe de chaînes d'approvisionnement internationales. Voici un aperçu de la situation en ce qui concerne la conception des microprocesseurs en Union européenne et leur fabrication à Taïwan :

1. Conception des Microprocesseurs en Union Européenne

Acteurs Clés : L'Union européenne abrite plusieurs entreprises et institutions qui participent à la conception de microprocesseurs et de puces électroniques. Parmi les acteurs notables, on trouve :

- **STMicroelectronics** : Basée en France et en Italie, STMicroelectronics est l'un des principaux fabricants de semi-conducteurs en Europe, concevant des puces pour divers secteurs, y compris l'automobile, l'IoT, et l'électronique grand public.
- **Infineon Technologies** : Entreprise allemande spécialisée dans les semi-conducteurs, Infineon développe des solutions pour l'automobile, la sécurité et les technologies de puissance.
- **ARM Holdings** : Bien que la société soit désormais détenue par des investisseurs japonais et américains, ARM a des liens forts avec l'Europe et est un leader dans la conception de architectures de microprocesseurs, notamment pour les dispositifs mobiles.

2. Fabrication à Taïwan

- **Taiwan Semiconductor Manufacturing Company (TSMC)** : Taïwan est le leader mondial de la fabrication de semi-conducteurs, avec TSMC étant l'un des plus grands fabricants de puces au monde. TSMC produit des microprocesseurs pour de nombreuses entreprises, y compris Apple, NVIDIA, et Qualcomm, ainsi que pour des entreprises européennes qui conçoivent leurs puces.
- **Chaînes d'Approvisionnement** : La fabrication des microprocesseurs nécessite des technologies avancées et des processus de production spécialisés qui sont principalement concentrés en Asie, notamment à Taïwan. Cela crée une dépendance pour de nombreux concepteurs européens qui externalisent la production de leurs puces.

3. Défis et Perspectives pour l'Europe

- **Souveraineté Numérique** : L'UE cherche à renforcer sa souveraineté numérique et sa capacité à produire ses propres semi-conducteurs. Cela inclut des initiatives pour augmenter la fabrication de puces en Europe, comme le programme European Chips Act, visant à investir dans la production de semi-conducteurs sur le continent.

- **Investissements dans l'Infrastructure** : L'UE prévoit d'encourager des investissements dans des usines de fabrication de semi-conducteurs pour réduire la dépendance vis-à-vis des fournisseurs étrangers, notamment en Asie.

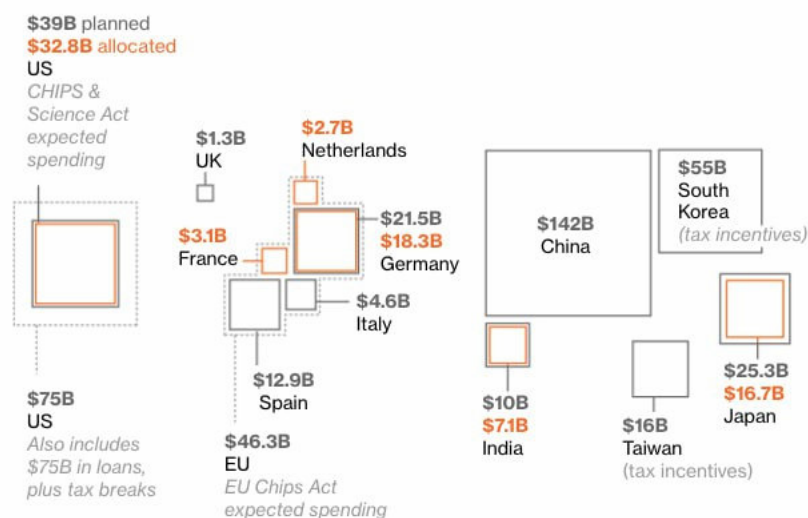
Conclusion : En résumé, la conception de microprocesseurs a lieu en Union européenne grâce à des entreprises comme STMicroelectronics et Infineon, mais la fabrication de ces puces est souvent réalisée à Taïwan, principalement par TSMC. Ce modèle soulève des préoccupations en matière de souveraineté numérique et d'approvisionnement, incitant l'UE à développer ses propres capacités de fabrication pour garantir une indépendance technologique.

Economie des microprocesseurs

Compléments :

Global Chips Investments

Funding allocated or planned for semiconductors, in US dollars



Sources: Bloomberg reporting and research, Semiconductor Industry Association

Figure 4 -Trouvé sur Telegram, chaîne : Guerre économique ! (année ? ...).

Les microprocesseurs russes

Est-ce que la Russie a mis en place une politique de semi-conducteurs consistant à produire d'anciennes puces (avec un écart entre transistors plus grand que les derniers modèles fabriqués à Taïwan), illustrant ainsi une politique de souveraineté numérique dans ce domaine ?

La Russie a entrepris des initiatives pour renforcer sa souveraineté numérique en développant sa propre production de semi-conducteurs. Cependant, en raison de sanctions internationales et de limitations technologiques, la production russe se concentre principalement sur des puces avec des technologies de fabrication plus anciennes, caractérisées par des espacements de transistors plus larges que ceux des modèles les plus récents produits à Taïwan.

Contexte et Initiatives Russes :

- **Souveraineté Numérique** : La Russie a mis en place des politiques visant à réduire sa dépendance vis-à-vis des technologies étrangères, notamment dans le domaine des semi-conducteurs. Ces efforts s'inscrivent dans une stratégie plus large de souveraineté numérique.
- **Production Nationale** : Des entreprises russes, telles que Mikron et Angstrom, ont été impliquées dans la production de semi-conducteurs. Mikron, par exemple, est capable de fabriquer des puces avec des technologies de 65 à 250 nanomètres. □ □cite□turn0search9□

Limitations Technologiques :

- **Sanctions Internationales** : Les sanctions imposées par les pays occidentaux ont restreint l'accès de la Russie aux technologies avancées nécessaires à la production de semi-conducteurs de pointe. Cela a conduit à une concentration sur des technologies plus anciennes.
- **Dépendance Technologique** : La Russie dépendait auparavant de fournisseurs étrangers pour des équipements et des technologies de fabrication avancées. Les restrictions actuelles compliquent la mise à niveau de ses capacités de production.

Conclusion : En résumé, bien que la Russie ait pris des mesures pour développer sa propre production de semi-conducteurs dans le cadre de sa politique de souveraineté numérique, les contraintes technologiques et les sanctions internationales ont limité sa capacité à produire des puces de dernière génération. Ainsi, la production russe se concentre principalement sur des technologies plus anciennes, avec des espacements de transistors plus larges que ceux des modèles les plus récents fabriqués à Taïwan.

Sources :

- **Sciences Po** - Interview : La souveraineté numérique russe en 5 questions avec Kevin Limonier [Sciences Po](#)
- **FranceSoir** - Circuits intégrés et semi-conducteurs : la Russie réalise et teste sa première [FranceSoir](#)
- **Siècle Digital** - La Russie dans une impasse pour produire ses semi-conducteurs [Siècle Digital](#)

Les entreprises russes :

- Mikron : <https://www.mikron.com/en>
- Angstrom : <https://museum.angstrom.ru/>

La 5G

La 4G et la 5G

La 5G est la cinquième génération de réseaux mobiles, succédant à la 4G (LTE). Elle promet de transformer les communications sans fil en offrant des vitesses de connexion beaucoup plus élevées, une latence réduite, et une capacité améliorée. Voici un aperçu des principaux avantages et inconvénients de la 5G :

La 5G est conçue pour améliorer les performances des réseaux mobiles en utilisant des technologies avancées. Elle repose sur trois principaux piliers :

- **Vitesses de Données Accrues** : Les vitesses de téléchargement et de téléversement sont nettement supérieures à celles de la 4G.
- **Latence Réduite** : La latence, c'est-à-dire le délai entre l'envoi et la réception des données, est beaucoup plus faible.
- **Capacité de Connexion** : La 5G peut gérer un nombre beaucoup plus élevé de connexions simultanées par unité de surface, ce qui est crucial pour les environnements densément peuplés et les applications IoT (Internet des Objets).

Avantages de la 5G

1. Vitesse de Connexion Élevée :

- **Débits Supérieurs** : La 5G offre des vitesses de téléchargement allant jusqu'à 10 Gbit/s, bien au-delà des capacités de la 4G. Cela permet des téléchargements de fichiers plus rapides et une diffusion en continu de haute qualité.
- **Expérience Utilisateur Améliorée** : Les applications gourmandes en bande passante, comme les jeux en ligne, les vidéos en haute définition et la réalité virtuelle, bénéficient d'une expérience utilisateur plus fluide.

2. Latence Réduite :

- **Réactivité Instantanée** : La 5G réduit la latence à environ 1 milliseconde (ms), contre 30-50 ms pour la 4G. Cela est essentiel pour les applications nécessitant des réponses en temps réel, comme la conduite autonome et les opérations médicales à distance.
- **Applications Critiques** : La faible latence est cruciale pour des applications comme la chirurgie robotique et les systèmes de contrôle industriels.

3. Capacité et Efficacité :

- **Support pour IoT** : La 5G peut connecter des millions de dispositifs IoT par kilomètre carré, facilitant le déploiement massif de capteurs et d'appareils intelligents.
- **Gestion des Charges** : Elle améliore la gestion des charges dans les zones à forte densité, comme les stades ou les centres-villes, où la 4G peut devenir saturée.

4. Amélioration des Réseaux :

- **Utilisation de Nouvelles Fréquences** : La 5G utilise des fréquences plus élevées (ondes millimétriques) et des technologies avancées comme le MIMO (Multiple Input Multiple Output) pour augmenter les performances du réseau.
- **Réseaux Plus Flexibles** : La 5G permet le découpage de réseau (network slicing), offrant des réseaux virtuels personnalisés pour des besoins spécifiques, comme les applications de mission critique ou les services grand public.

5. Avantages Économiques et Sociaux :

- **Innovation** : La 5G stimule l'innovation dans divers secteurs, y compris les transports, la santé, l'industrie, et les services publics.
- **Création d'Emplois** : Elle favorise la création d'emplois dans les domaines de la technologie, de la construction et des services.

Inconvénients de la 5G

1. Coûts Élevés :

- **Infrastructure** : Le déploiement de la 5G nécessite des investissements considérables dans de nouvelles infrastructures, y compris la construction de nombreuses stations de base et la mise à niveau des équipements existants.
- **Dispositifs Compatibles** : Les consommateurs doivent remplacer leurs anciens dispositifs par des appareils compatibles avec la 5G, ce qui peut représenter un coût supplémentaire.

2. Couverture Limitée :

- **Propagation des Signaux** : Les ondes millimétriques utilisées par la 5G ont une portée plus courte et une pénétration plus faible à travers les obstacles (murs, bâtiments), nécessitant une densité plus élevée de stations de base.
- **Disponibilité** : Dans certaines régions, surtout rurales, la couverture 5G peut être limitée ou inexistante, ce qui peut créer des disparités en termes d'accès à la technologie.

3. Questions de Santé et Environnement :

- **Exposition aux Radiations** : Bien que les recherches n'aient pas conclu à des risques pour la santé publique, certaines personnes expriment des préoccupations concernant l'exposition accrue aux radiations RF (radiofréquences).
- **Impact Environnemental** : La construction et le déploiement d'infrastructures 5G peuvent avoir un impact environnemental, notamment en ce qui concerne la consommation d'énergie et l'utilisation des ressources.

4. Sécurité et Confidentialité :

- **Nouveaux Risques** : La complexité accrue des réseaux 5G peut introduire de nouveaux risques de cybersécurité. Les réseaux devront être conçus avec des mesures de sécurité renforcées pour protéger contre les menaces potentielles.
- **Protection des Données** : Avec une augmentation des connexions IoT, la gestion et la protection des données personnelles et sensibles deviennent encore plus importantes.

5. Interférences et Compatibilité :

- **Interférences** : Les fréquences plus élevées de la 5G peuvent potentiellement interférer avec d'autres dispositifs ou technologies qui utilisent des fréquences similaires.
- **Compatibilité** : Les transitions vers la 5G peuvent présenter des défis en termes de compatibilité avec les technologies existantes et d'intégration avec les réseaux 4G.

Résumé : La 5G offre des avantages significatifs en termes de vitesse, de latence, de capacité, et d'efficacité des réseaux, stimulant ainsi l'innovation et améliorant les services numériques. Cependant, elle présente également des défis importants, tels que les coûts élevés de déploiement, les préoccupations de santé et de sécurité, ainsi que les problèmes de couverture et de compatibilité. La réussite de l'adoption de la 5G dépendra de la gestion efficace de ces défis tout en maximisant les avantages pour les consommateurs et les entreprises.

Comparativement à la 4G, la 5G présente-t-elle des avantages déterminants ?

Oui / non / NSP

Proposition de réponse par ChatGPT : Oui, la 5G présente plusieurs avantages déterminants par rapport à la 4G, qui ont un impact significatif sur les performances, les capacités et les applications des réseaux mobiles. Voici une comparaison détaillée des avantages clés de la 5G par rapport à la 4G :

1. Vitesse de Connexion

- **5G** : La 5G offre des vitesses de téléchargement qui peuvent atteindre jusqu'à 10 Gbit/s (gigabits par seconde) dans des conditions idéales, ce qui est jusqu'à 100 fois plus rapide que la 4G. Cela permet des téléchargements et des téléversements de données beaucoup plus rapides, ainsi qu'une diffusion en continu de haute qualité.
- **4G** : La 4G LTE (Long Term Evolution) offre des vitesses de téléchargement maximales autour de 100 Mbit/s (mégabits par seconde) dans les meilleures conditions, ce qui est considérablement plus lent par rapport à la 5G.

2. Latence

- **5G** : La 5G réduit la latence à environ 1 milliseconde (ms), ce qui est bien inférieur aux 30 à 50 millisecondes typiques de la 4G. Cette faible latence est essentielle pour les applications nécessitant une réponse en temps réel, telles que les jeux en ligne, la réalité augmentée (AR) et la réalité virtuelle (VR).
- **4G** : La 4G a une latence plus élevée, ce qui peut affecter les performances des applications sensibles au temps et provoquer des délais perceptibles dans les communications et les interactions.

3. Capacité et Efficacité du Réseau

- **5G** : La 5G peut gérer un nombre beaucoup plus élevé de connexions simultanées par unité de surface grâce à une capacité accrue. Elle est conçue pour supporter des environnements densément peuplés, comme les stades, les centres-villes et les grandes manifestations.
- **4G** : La 4G a une capacité limitée en termes de nombre de connexions simultanées, ce qui peut entraîner une congestion du réseau et une baisse des performances dans des zones à forte densité d'utilisateurs.

4. Support pour l'Internet des Objets (IoT)

- **5G** : La 5G est optimisée pour le déploiement massif de dispositifs IoT. Elle peut connecter des millions de dispositifs par kilomètre carré, ce qui est crucial pour les villes intelligentes, les réseaux de capteurs, et les systèmes automatisés dans divers secteurs.
- **4G** : La 4G peut également supporter les dispositifs IoT, mais elle est limitée en termes de nombre de connexions simultanées et de bande passante disponible pour ces dispositifs.

5. Flexibilité et Réseaux Virtuels

- **5G** : La 5G permet le découpage de réseau (network slicing), une technologie qui crée des réseaux virtuels distincts sur une même infrastructure physique. Cela permet de personnaliser les réseaux pour des applications spécifiques, comme les services critiques ou les besoins particuliers des entreprises.
- **4G** : La 4G n'a pas la capacité de découpage de réseau, limitant ainsi la personnalisation des services et des applications.

6. Efficacité Spectrale

- **5G** : La 5G utilise des bandes de fréquence plus élevées, notamment les ondes millimétriques (24 GHz et plus), ce qui permet une utilisation plus efficace du spectre radioélectrique et des débits plus élevés. Elle utilise également des technologies avancées comme le MIMO massif (Multiple Input Multiple Output) pour améliorer les performances.

- **4G** : La 4G utilise des bandes de fréquence plus basses et a une efficacité spectrale inférieure par rapport à la 5G, limitant ainsi les débits et la capacité globale du réseau.

7. Applications Avancées

- **5G** : La 5G ouvre la voie à des applications avancées telles que la conduite autonome, la télémédecine (y compris la chirurgie à distance), la réalité augmentée et virtuelle de haute qualité, et des systèmes de contrôle industriel intelligents. Ces applications bénéficient de la haute vitesse, de la faible latence et de la capacité élevée de la 5G.
- **4G** : La 4G peut prendre en charge certaines applications avancées, mais elle est limitée en termes de vitesse et de latence, ce qui peut restreindre l'implémentation et la qualité de ces applications.

Résumé : En résumé, la 5G offre des avantages déterminants par rapport à la 4G, notamment en termes de vitesse de connexion, de latence, de capacité du réseau, et de support pour des applications avancées et l'IoT. Ces améliorations permettent une performance nettement supérieure et ouvrent la voie à de nouvelles possibilités dans divers secteurs. Cependant, la mise en œuvre de la 5G nécessite des investissements importants et présente des défis en termes de couverture, de coûts, et de sécurité.

Commentaire : cette proposition de réponse par ChatGPT porte surtout sur des aspects techniques, mais globalement pour l'utilisateur final, la différence est peut-être moins tranchée.

Délai de mise en place de la 5G

L'implémentation de la 5G doit-elle être immédiate ou peut-elle être différée de quelques années ?

Immédiate / différée / NSP

L'implémentation de la 5G est un sujet complexe qui peut varier en fonction des besoins, des priorités, des ressources disponibles, et des contextes régionaux. Voici une analyse des arguments pour une mise en œuvre immédiate versus différée de la 5G :

Arguments pour une Implémentation Immédiate de la 5G

1. Avantages Technologiques et Économiques :

- **Innovation et Compétitivité** : La 5G permet des vitesses de connexion élevées, une faible latence, et une capacité améliorée, ce qui peut stimuler l'innovation dans divers secteurs comme la télémédecine, l'industrie 4.0, et les villes intelligentes. Une adoption rapide peut offrir un avantage compétitif aux pays et aux entreprises qui la mettent en œuvre en premier.
- **Croissance Économique** : La mise en œuvre rapide de la 5G peut accélérer la transformation numérique, créer des emplois, et favoriser la croissance économique en permettant le développement de nouveaux services et applications.

2. Réponse aux Besoins Croissants :

- **Densité d'Utilisateurs** : Dans les zones urbaines à forte densité, les réseaux 4G peuvent devenir saturés. La 5G peut décharger le réseau en augmentant la capacité et en offrant une meilleure couverture.
- **Demandes de Données** : L'augmentation continue de la consommation de données et des exigences des utilisateurs nécessite des réseaux plus performants, que seule la 5G peut efficacement gérer.

3. Développement d'Applications Avancées :

- **Applications Critiques** : La 5G est essentielle pour des applications comme la conduite autonome, la réalité augmentée/virtuelle de haute qualité, et les systèmes de contrôle industriel, qui nécessitent la haute vitesse et la faible latence de la 5G.

4. Avantages Concurrentiels :

- **Leadership Technologique** : Être à la pointe de la technologie 5G peut positionner un pays ou une entreprise comme leader technologique, attirant ainsi des investissements et des partenariats internationaux.

Arguments pour une Implémentation Différée de la 5G

1. Coûts et Investissements :

- **Investissements Élevés** : Le déploiement de la 5G nécessite des investissements importants dans l'infrastructure, y compris la construction de nouvelles stations de base et la mise à niveau des équipements. Différer la mise en œuvre peut permettre une planification financière plus prudente et une gestion des coûts.
- **Accessibilité** : Le coût des dispositifs 5G pour les consommateurs et les entreprises peut être élevé, et un déploiement différé peut permettre une réduction progressive des coûts et une adoption plus large.

2. Couverture et Accessibilité :

- **Inégalités Régionales** : La 5G peut initialement ne pas être disponible dans les zones rurales ou moins développées. Différer la mise en œuvre permet de se concentrer d'abord sur les zones urbaines et de planifier l'expansion vers les régions moins desservies.
- **Mise en Réseau Gradualisée** : Un déploiement échelonné permet d'évaluer et d'ajuster les technologies en fonction des retours d'expérience et des besoins spécifiques des différentes régions.

3. Questions de Sécurité et de Confidentialité :

- **Risques de Sécurité** : La 5G introduit de nouveaux défis en matière de sécurité et de confidentialité des données. Un déploiement différé permet de résoudre ces préoccupations et de renforcer les protocoles de sécurité avant une adoption plus large.
- **Protection des Données** : Les risques potentiels liés à la gestion des données et à la cybersécurité peuvent être mieux compris et atténués avec le temps.

4. Évaluation des Impacts Environnementaux et de Santé :

- **Études et Réglages** : La mise en œuvre différée peut offrir le temps nécessaire pour mener des études approfondies sur les impacts environnementaux et de santé potentiels associés à la 5G, garantissant ainsi une adoption plus responsable.

Conclusion : L'implémentation de la 5G peut être bénéfique à court terme pour ses avantages technologiques, économiques, et d'innovation, mais elle implique également des coûts élevés, des défis en matière de sécurité, et des préoccupations de couverture et de santé. La décision de déployer immédiatement ou de différer la 5G dépendra de divers facteurs, y compris les priorités locales, les ressources disponibles, et les besoins spécifiques des régions ou des marchés concernés.

Une approche équilibrée pourrait consister à un déploiement progressif de la 5G, en commençant par les zones à forte densité et les applications critiques, tout en planifiant une expansion future pour garantir une couverture complète et une gestion des risques adéquate.

La 5G chinoise

Faut-il craindre la 5G chinoise ?

La question de savoir s'il faut craindre la 5G chinoise est complexe et touche à divers aspects de la sécurité nationale, de la souveraineté technologique, et des relations internationales. Voici une analyse détaillée des principaux aspects à considérer :

1. Sécurité et Souveraineté

Risques Perçus

- **Propriétaires de Technologie** : Huawei et ZTE, deux grandes entreprises chinoises, sont des fournisseurs majeurs de technologie 5G. Il y a des préoccupations selon lesquelles ces entreprises pourraient être soumises à des lois chinoises qui leur imposeraient de coopérer avec les services de renseignement chinois, ce qui pourrait potentiellement compromettre la sécurité des données et des communications.
- **Vulnérabilités de Sécurité** : Les craintes incluent la possibilité d'interceptions ou d'espionnage des communications, ainsi que l'insertion de portes dérobées (backdoors) dans les équipements de réseau qui pourraient permettre un accès non autorisé aux données sensibles.

Réponses et Contre-Mesures

- **Évaluations de Sécurité** : De nombreux pays ont mis en place des processus rigoureux pour évaluer et auditer les équipements de télécommunications afin d'assurer leur conformité avec les normes de sécurité.
- **Exclusion de Fournisseurs** : Certains pays, comme les États-Unis et plusieurs membres de l'Union européenne, ont pris des mesures pour limiter ou exclure les fournisseurs chinois de leurs réseaux 5G, en faveur de fournisseurs jugés plus sûrs ou en développant des alternatives locales.

2. Impact sur les Relations Internationales

Influence Géopolitique

- **Concurrence Technologique** : Le déploiement de la 5G par la Chine est souvent perçu comme une tentative d'accroître son influence technologique mondiale. Les technologies de télécommunications peuvent jouer un rôle clé dans le renforcement de la position géopolitique d'un pays.
- **Tensions Diplomatiques** : Les préoccupations concernant la 5G chinoise ont conduit à des tensions diplomatiques entre la Chine et d'autres pays. Les restrictions imposées par certains pays peuvent affecter les relations économiques et commerciales internationales.

Partenariats et Alliances

- **Coalitions Technologiques** : Certains pays forment des coalitions ou des alliances pour développer des alternatives à la technologie 5G chinoise, favorisant des fournisseurs jugés plus fiables et garantissant des normes de sécurité élevées.

3. Questions Économiques

Coût et Accessibilité

- **Coût des Technologies** : Les équipements de 5G fournis par des entreprises chinoises peuvent être plus compétitifs en termes de coût, ce qui peut influencer les décisions d'achat des pays en développement ou des pays à budget limité.
- **Soutien au Développement** : La Chine offre également un soutien financier et technique à certains pays pour le déploiement de la 5G, ce qui peut renforcer les relations économiques et politiques bilatérales.

4. Innovations et Opportunités

Avantages Technologiques

- **Performance et Avancées** : Les technologies de 5G développées par des entreprises chinoises peuvent offrir des avantages significatifs en termes de performance et d'innovation, ce qui peut bénéficier à la croissance économique et au développement technologique mondial.
- **Collaboration et Partage de Connaissances** : Les collaborations internationales dans le domaine de la 5G peuvent favoriser l'échange de connaissances et l'innovation, même en tenant compte des préoccupations sécuritaires.

Conclusion : Faut-il craindre la 5G chinoise ?

La réponse dépend du contexte et des priorités spécifiques de chaque pays ou organisation. Les préoccupations majeures incluent les risques pour la sécurité nationale, les enjeux géopolitiques, et les implications économiques. La 5G chinoise offre des avantages en termes de coût et d'innovation, mais elle suscite également des préoccupations sur la sécurité et la souveraineté.

Pour gérer ces risques, il est crucial d'adopter une approche équilibrée :

- **Évaluations Rigoureuses** : Mettre en place des évaluations de sécurité rigoureuses et des contrôles pour assurer la protection des données et des infrastructures.
- **Diversification des Fournisseurs** : Explorer une diversification des fournisseurs pour réduire la dépendance vis-à-vis d'un seul fournisseur ou d'une région spécifique.
- **Collaborations et Normes** : Favoriser les collaborations internationales et les normes de sécurité élevées pour garantir une mise en œuvre sécurisée et fiable de la technologie 5G.

Les décisions concernant l'adoption de la 5G chinoise doivent être basées sur une évaluation complète des avantages et des risques, en tenant compte des considérations de sécurité, d'économie, et de politique internationale.

Linux

Linux est un système d'exploitation « libre » (licence GPL) dont le code est public.

Question : Faut-il favoriser et même imposer Linux pour les administrations, les entreprises et les personnes ?

Réponses : oui / non / NSP

Android

Dans la mesure où il existe une version « degooglisée » d'Android : <https://e.foundation/> :

Question : Faut-il favoriser et même imposer Linux pour les administrations, les entreprises et les personnes ?

Réponses : oui / non / NSP

Le smartphone

Par exemple, en termes de smartphone : <https://shop.fairphone.com> qui sous-traite à l'entreprise bretonne Cordon (<https://www.cordongroup.com/fr/index.html>)

La bureautique

En termes de bureautique, quelles alternatives à Microsoft office ? Open office (<https://www.openoffice.org> ...), WPS (<https://www.wps.com/> de Kingsoft, d'origine chinoise...

Les alternatives à Microsoft office

Il existe plusieurs alternatives à Microsoft Office pour la bureautique, chacune avec des caractéristiques distinctes en matière de fonctionnalités, d'origine et de compatibilité. Voici un aperçu des principales options :

1. OpenOffice

- **Origine et développement** : OpenOffice est un logiciel open source développé par la fondation Apache, conçu pour être une alternative gratuite à Microsoft Office. Il inclut des applications pour le traitement de texte, les tableurs, les présentations et plus.
- **Fonctionnalités** : Bien que basique comparé à Microsoft Office, OpenOffice couvre l'essentiel des fonctionnalités nécessaires pour la bureautique, notamment avec Writer (équivalent de Word), Calc (Excel) et Impress (PowerPoint).
- **Compatibilité** : OpenOffice prend en charge plusieurs formats, y compris les formats de Microsoft, mais il peut parfois rencontrer des problèmes de mise en page avec des fichiers complexes d'Office.
- **Points forts** : Gratuit, sans licence propriétaire, et pris en charge sur Windows, Mac, et Linux, avec une forte communauté de développeurs.

2. LibreOffice

- **Origine et développement** : LibreOffice est une branche d'OpenOffice, créée par The Document Foundation et se développe plus activement qu'OpenOffice.
- **Fonctionnalités** : LibreOffice offre une suite bureautique complète (Writer, Calc, Impress, et Draw pour les diagrammes) et des fonctionnalités avancées, avec une meilleure compatibilité avec les formats Microsoft.
- **Compatibilité** : LibreOffice est généralement plus performant qu'OpenOffice dans la gestion des fichiers Microsoft, surtout pour les documents complexes.
- **Points forts** : Gratuit, plus riche en fonctionnalités qu'OpenOffice, avec une interface plus moderne et des mises à jour régulières.

3. WPS Office

- **Origine et développement** : WPS Office, développé par Kingsoft, une entreprise chinoise, est conçu pour concurrencer directement Microsoft Office, avec une interface très proche.
- **Fonctionnalités** : WPS propose des applications similaires à Word, Excel, et PowerPoint, et ajoute des outils comme le PDF Editor. Il est également compatible avec Windows, Mac, Linux, Android, et iOS.
- **Compatibilité** : WPS offre une compatibilité solide avec les formats Microsoft Office et se distingue par sa capacité à convertir et éditer des fichiers PDF.
- **Points forts** : Interface intuitive, gratuit dans sa version de base, mais avec des fonctionnalités premium payantes, notamment l'absence de publicités et des options avancées.

4. Google Workspace (Google Docs, Sheets, Slides)

- **Origine et développement** : Développé par Google, Google Workspace fonctionne entièrement dans le cloud, permettant un accès aux documents depuis n'importe quel appareil avec une connexion internet.

- **Fonctionnalités** : Workspace inclut Google Docs, Sheets, et Slides, avec des fonctions collaboratives très avancées, permettant à plusieurs utilisateurs de travailler en temps réel.
- **Compatibilité** : Google Workspace offre une compatibilité de base avec les formats Microsoft, mais certaines fonctionnalités complexes d'Office peuvent ne pas être reproduites à l'identique.
- **Points forts** : Gratuit pour une utilisation de base, sans besoin d'installation, avec une synchronisation cloud intégrée et une sécurité solide.

5. OnlyOffice

- **Origine et développement** : OnlyOffice est développé par Ascensio System SIA, une entreprise européenne, et offre une alternative open source qui peut être hébergée sur des serveurs privés ou dans le cloud.
- **Fonctionnalités** : OnlyOffice inclut des outils de traitement de texte, de feuilles de calcul, et de présentation, tout en se concentrant sur la collaboration d'équipe et la compatibilité avec Microsoft.
- **Compatibilité** : Très bonne compatibilité avec Microsoft Office, souvent proche des formats originaux.
- **Points forts** : Interface moderne, options cloud et auto-hébergement pour les entreprises, sécurité renforcée pour la collaboration d'équipe.

6. Zoho Office Suite

- **Origine et développement** : Développée par la société indienne Zoho, cette suite bureautique est entièrement basée sur le cloud et fait partie de l'offre plus large de Zoho, qui inclut des applications CRM, gestion de projets, etc.
- **Fonctionnalités** : Zoho offre un traitement de texte, un tableur, un outil de présentation et des fonctions collaboratives.
- **Compatibilité** : Compatibilité de base avec les formats Office, mais, comme Google Workspace, certaines fonctionnalités avancées d'Office peuvent manquer.
- **Points forts** : Intégration étroite avec l'écosystème Zoho, tarifs compétitifs pour les entreprises, idéal pour les petites et moyennes entreprises cherchant un écosystème complet.

Résumé d'efficacité :

- Pour une **compatibilité forte avec Microsoft Office**, LibreOffice et OnlyOffice sont recommandés, surtout pour les documents complexes.
- Pour la **collaboration en temps réel** et un accès cloud, Google Workspace et Zoho Office Suite se démarquent.
- Pour une **utilisation légère ou mobile**, WPS Office est une bonne option, notamment pour sa fluidité et sa compatibilité avec les formats Microsoft.

Chaque solution présente donc des atouts distincts selon les besoins spécifiques (interopérabilité, collaboration, sécurité, coût). LibreOffice et OnlyOffice sont souvent considérés parmi les meilleures options open source en termes de compatibilité et de coût, tandis que Google Workspace et Zoho sont bien adaptés aux environnements collaboratifs en ligne.

Les données personnelles

Safe harbor, Privacy shield et Data Privacy Framework

Safe Harbor (Port Sûr)

Mise en place: Cet accord a été mis en place à la fin des années 1990 pour faciliter les transferts de données entre l'UE et les États-Unis tout en garantissant un niveau de protection adéquat des données personnelles.

Principe: Les entreprises américaines devaient s'auto-certifier qu'elles respectaient un ensemble de principes relatifs à la protection des données, similaires à ceux du RGPD européen.

Annulation: En 2015, la Cour de justice de l'Union européenne (CJUE) a invalidé le Safe Harbor, jugeant que le niveau de protection offert n'était pas suffisant au regard des lois européennes.

Privacy Shield (Bouclier de protection des données)

Mise en place: Suite à l'invalidation du Safe Harbor, le Privacy Shield a été négocié et adopté en 2016.

Objectif: Il visait à remplacer le Safe Harbor en offrant de nouvelles garanties pour les transferts de données transatlantiques.

Annulation: Malheureusement, en 2020, la CJUE a également annulé le Privacy Shield, pour les mêmes raisons que celles invoquées pour le Safe Harbor.

Data Privacy Framework (Cadre pour la protection de la vie privée)

Mise en place: Face à ces deux annulations, la Commission européenne a négocié un nouvel accord, le Data Privacy Framework, adopté en 2023.

Nouveautés: Ce cadre introduit de nouvelles garanties, notamment la création d'une cour spéciale pour les litiges et un renforcement des obligations des entreprises américaines en matière de protection des données.

Enjeux: Bien que le DPF soit en vigueur, il fait l'objet de critiques et pourrait à nouveau être contesté devant la CJUE.

Les principales raisons de ces annulations sont liées aux lois américaines sur la surveillance, qui permettent aux services de renseignement américains d'accéder aux données personnelles des citoyens européens transférées aux États-Unis. La CJUE a jugé que ces lois ne garantissaient pas un niveau de protection suffisant et étaient donc incompatibles avec le droit européen.

Quelles sont les conséquences pour les entreprises ?

Ces annulations successives créent une grande incertitude juridique pour les entreprises qui souhaitent transférer des données vers les États-Unis. Elles doivent mettre en place des mécanismes alternatifs, tels que les clauses contractuelles types (CCT), pour assurer la licéité de ces transferts.

Le Privacy Shield

BENJAMIN BAYART : INTELLIGENCE ARTIFICIELLE, BULLSH*T, PIPOTRON ?

4 avril 2024 / Interviews, Internet / Technologies, Société

Benjamin Bayart, Président du FDN, cofondateur de la Quadrature du Net.



SOURCEZ, VERIFIEZ LES FAITS :

[CaptainFact.io/videos/](https://captainfact.io/videos/) | S'inscrire à CaptainFact

(<https://www.laquadrature.net/2022/03/25/pourquoi-sopposer-a-la-creation-de-mon-espace-sante/>)

Le 16 juillet 2020, la Cour de justice de l'Union européenne invalide le Privacy Shield, soit le régime de transfert de données avec les Etats-Unis adopté en 2016. Les conséquences de cette décision sont toujours en cours d'examen. La protection de la vie privée des citoyens européens garantie du seul point de vue juridique par cet accord international n'existe donc plus.

Le Privacy Shield était un cadre de protection des données entre l'Union européenne (UE) et les États-Unis, conçu pour encadrer le transfert des données personnelles des citoyens européens vers les entreprises américaines. Il a été mis en place pour remplacer le précédent accord, le Safe Harbor, qui avait été invalidé en 2015 par la Cour de justice de l'Union européenne (CJUE). Voici un aperçu du Privacy Shield, des questions liées à son respect et des enjeux en cours :

1. Présentation du Privacy Shield

Objectif

- Le Privacy Shield visait à assurer un niveau de protection des données personnelles équivalent à celui offert par la législation de l'UE lors du transfert de données vers les États-Unis, facilitant ainsi les échanges commerciaux tout en protégeant la vie privée des citoyens européens.

2. Mécanismes de Protection :

- **Engagement des Entreprises** : Les entreprises américaines participantes s'engageaient à respecter les principes du Privacy Shield en matière de traitement des données personnelles.

- **Recours et Surveillance** : Le cadre prévoyait des mécanismes de recours pour les citoyens européens, ainsi qu'une surveillance par le Département du Commerce des États-Unis et la Commission européenne.
- **Protection des Données** : Des garanties de sécurité et des engagements concernant l'accès des autorités américaines aux données étaient inclus.

Questions et Défis liés au Respect du Privacy Shield

1. Validité et Protection Juridique :

- **Décision de la CJUE** : Le 16 juillet 2020, la CJUE a invalidé le Privacy Shield dans l'affaire **Schrems II**, citant des préoccupations sur la capacité des États-Unis à offrir une protection adéquate des données personnelles en raison de la surveillance étendue par les agences de renseignement américaines, qui pourrait ne pas être conforme aux normes de l'UE.
- **Égalité de Protection** : La Cour a jugé que les protections offertes aux citoyens européens par le Privacy Shield n'étaient pas suffisantes pour répondre aux exigences du Règlement général sur la protection des données (RGPD).

2. Surveillance et Accès aux Données :

- **Législation Américaine** : Les lois américaines, comme le Patriot Act, permettent une surveillance étendue par les agences de renseignement, ce qui a été considéré comme incompatible avec les normes de protection des données exigées par l'UE.
- **Absence de Recours Effectif** : Le cadre ne prévoyait pas suffisamment de recours juridiques pour les citoyens européens en cas de violation de la protection des données.

3. Impact sur les Entreprises :

- **Incertitude Juridique** : L'invalidation du Privacy Shield a créé une incertitude pour les entreprises qui dépendaient de cet accord pour transférer des données personnelles entre l'UE et les États-Unis. Elles doivent maintenant s'appuyer sur d'autres mécanismes de transfert, comme les Clauses Contractuelles Types (CCT), tout en adaptant leurs pratiques de conformité aux nouvelles exigences.
- **Adaptation aux Règles** : Les entreprises doivent adapter leurs politiques et leurs pratiques pour garantir la conformité avec le RGPD et les exigences des autorités européennes en matière de protection des données.

4. Nouveaux Développements :

- **Négociations en cours** : Les autorités de l'UE et des États-Unis ont travaillé sur un nouveau cadre pour remplacer le Privacy Shield, afin de répondre aux préoccupations soulevées par la CJUE. Cependant, ce nouveau cadre doit encore être finalisé et approuvé.
- **Clauses contractuelles types** : Les clauses contractuelles types (CCT) sont actuellement utilisées comme alternative pour les transferts de données, mais elles nécessitent des ajustements et des garanties supplémentaires pour être conformes aux exigences du RGPD.

5. Défis en Matière de Conformité :

- **Complexité Juridique** : La conformité aux exigences de protection des données dans le contexte des transferts internationaux reste complexe et nécessite une vigilance continue pour éviter les violations des réglementations.
- **Coûts et Ressources** : Les entreprises doivent investir des ressources considérables pour mettre en place des mesures de conformité et gérer les risques liés aux transferts de données.
- **Résumé** : Le Privacy Shield a été mis en place pour faciliter les transferts de données personnelles entre l'UE et les États-Unis tout en garantissant une protection adéquate des données. Cependant, son invalidation par la CJUE en 2020 a révélé des lacunes significatives, notamment en ce qui concerne la protection contre la surveillance étendue aux États-Unis. Les

entreprises doivent maintenant naviguer dans un environnement de conformité plus complexe, en s'appuyant sur d'autres mécanismes comme les Clauses Contractuelles Types et en attendant la mise en place de nouveaux accords.



<https://siecledigital.fr/2022/03/25/un-accord-de-principe-pour-le-successeur-de-privacy-shield-a-ete-trouve/>

Le Privacy Shield a-t-il été respecté lors de l'accord entre les Etats-Unis et l'Union européenne ?

Oui / non / NSP

L'Accord entre les Etats-Unis et l'Union européenne est-il réciproque en termes d'accès aux données personnelles ?

Oui / non / NSP

Les données de santé aux USA

<https://www.it-connect.fr/la-cnll-autorise-microsoft-a-heberger-les-donnees-de-sante-des-francais/>

https://www.lemonde.fr/pixels/article/2024/03/18/donnees-de-sante-francaises-chez-microsoft-nouveau-recours-devant-le-conseil-d-etat_6222758_4408996.html :

Le Monde avec AFP Publié le 18 mars 2024 à 19h57

Données de santé françaises chez Microsoft : nouveau recours devant le Conseil d'Etat

Les requérants attaquent l'autorisation accordée par la Commission nationale de l'informatique et des libertés (CNIL) fin décembre à un projet d'entrepôt de données de santé pour la recherche qui sera hébergé par Microsoft.

https://www.lemonde.fr/pixels/article/2024/03/18/donnees-de-sante-francaises-chez-microsoft-nouveau-recours-devant-le-conseil-d-etat_6222758_4408996.html

Des entreprises et des associations françaises ont déposé un nouveau recours devant le Conseil d'Etat contre l'hébergement de données de santé françaises chez l'américain Microsoft, ont-elles annoncé, lundi 18 mars, lors d'une conférence de presse. Les requérants sont les entreprises Nexedi, Clever Cloud, Cleyrop, concurrents potentiels de Microsoft, et des ONG comme l'Open Internet Project ou l'Institut de la souveraineté numérique.

Le recours doit être examiné à 11 heures mardi par le Conseil d'Etat, a précisé l'avocat des requérants, Jean-Baptiste Soufron.

Les requérants attaquent l'autorisation donnée par la Commission nationale de l'informatique et des libertés (CNIL) fin décembre à un projet d'entrepôt de données de santé pour la recherche qui sera hébergé par Microsoft.

Cet entrepôt, baptisé « EMC2 », associera les données des patients de quatre grands hôpitaux français avec les données les concernant (remboursements de consultations et de soins, parcours hospitaliers...) détenues par l'Assurance-maladie. Il est géré par le Health Data Hub (plate-forme de données de santé), dans le cadre d'un programme de recherche en pharmacovigilance de l'Agence européenne des médicaments.

Lire aussi | « L'exploitation de données de santé sur une plate-forme de Microsoft expose à des risques multiples »

Un appel d'offres en bonne et due forme

Les requérants estiment qu'un opérateur de cloud américain comme Microsoft ne peut héberger des données aussi sensibles que les données de santé françaises, pour des raisons de sécurité et de souveraineté.

En 2020, des associations et des professionnels avaient saisi le Conseil d'Etat pour tenter d'empêcher le Health Data Hub d'héberger les données de santé chez Microsoft, et pour demander un appel d'offres en bonne et due forme. Leur procédure avait échoué, mais le gouvernement avait promis qu'un appel d'offres serait lancé dans les années suivantes pour choisir l'hébergeur informatique. Aucun appel d'offres n'a été lancé à ce jour.

Lire aussi | Nous devons « modifier nos normes de protection des données de santé »

Les requérants espèrent, par ailleurs, obtenir que le Conseil d'Etat saisisse la Cour de justice de l'Union européenne sur la validité du nouvel accord transatlantique sur les données, adopté en juillet 2023 par l'UE et les Etats-Unis. « Nous souhaitons obtenir une question préjudicielle » sur ce sujet, a déclaré Me Soufron.

Deux accords UE/Etats-Unis sur les transferts de données transatlantiques ont été cassés par la justice européenne ces dernières années, à la suite de recours déposés par le militant autrichien des droits numériques Max Schrems.

Les militants européens pour la souveraineté des données pensent que la Cour européenne de justice cassera à nouveau l'accord UE/Etats-Unis, les nouvelles garanties données par les Etats-Unis étant insuffisantes selon eux pour garantir les droits des Européens.

Les données de santé peuvent-elles être gérées par Microsoft ?

Oui / non / NSP

Le crédit social

Ou la surveillance généralisée de la population

Le crédit social chinois est un système de surveillance et de notation mis en place par le gouvernement chinois pour évaluer et influencer le comportement des citoyens et des entreprises. Ce système attribue des scores basés sur des critères variés, tels que le respect des lois, les comportements sociaux et les engagements financiers. Les citoyens et les entreprises ayant un score élevé bénéficient de privilèges tels que des crédits plus avantageux, un meilleur accès aux services

publics, et des opportunités d'emploi, tandis que ceux avec un score bas peuvent faire face à des restrictions telles que des limitations de voyage, des interdictions d'achat de biens de luxe ou des difficultés pour obtenir des crédits.

Le crédit social Chinois

Le crédit social Chinois est un système mis en place par le gouvernement chinois pour évaluer et classer les citoyens, les entreprises et les organisations sur la base de leurs comportements et de leurs interactions avec les autorités et les institutions. Son objectif principal est d'encourager les comportements conformes aux normes sociales, éthiques et légales tout en décourageant les comportements jugés nuisibles ou non conformes.

Les comportements observés et notés sont :

- Les comportements légaux et sociaux le respect des lois, les obligations fiscales, le paiement des amendes, les comportements sociaux (par exemple, respect des règles de circulation, interactions en ligne), les données Financières : Historique de crédit, emprunts, remboursements.
- Les activités commerciales : respect des règlements commerciaux, interactions avec les partenaires d'affaires.
- Les informations proviennent des autorités gouvernementales, des institutions financières, des entreprises privées, et parfois des plateformes en ligne.

Les notations :

- La notation individuelle : les citoyens reçoivent un score basé sur un ensemble de critères. Ce score peut influencer divers aspects de leur vie, tels que l'accès aux prêts, les opportunités d'emploi, et la capacité de voyager.
- La notation des entreprises : Les entreprises sont évaluées en fonction de leur conformité aux réglementations, leur transparence, et leur performance. Cela peut influencer leur capacité à obtenir des contrats gouvernementaux ou à faire des affaires.

Les conséquences des scores :

- score élevé : accès facilité à des services financiers, crédits avantageux, opportunités d'emploi, reconnaissance sociale. Les personnes et les entreprises avec un score élevé peuvent également bénéficier de traitements préférentiels dans divers domaines.
- score bas : des restrictions telles que limitations de voyage (par exemple, interdiction de prendre des vols ou des trains), difficultés d'accès à des services financiers, limitations d'opportunités d'emploi, restrictions dans la participation à des activités publiques ou sociales.

Les mesures et les interdictions :

- voyage : Les personnes avec un faible score peuvent être interdites de prendre des vols ou des trains à grande vitesse.
- éducation et emploi : Difficultés pour obtenir des postes dans des institutions publiques ou des entreprises privées, ainsi que des restrictions dans l'accès à certaines institutions éducatives.
- services publics : Restrictions dans l'accès à certains services publics ou subventions gouvernementales.
- Le système est surveillé par des agences gouvernementales et, dans certains cas, des entreprises privées. Il s'appuie sur une combinaison de technologies de surveillance, y compris la collecte de données numériques et les systèmes de reconnaissance faciale.

Les controverses et les critiques portent sur :

- vie privée : Inquiétudes concernant la vie privée et la surveillance intrusive, notamment la collecte extensive de données personnelles.

- libertés individuelles : Crainte d'une atteinte aux libertés individuelles et à l'autonomie des citoyens en raison des mesures de contrôle et des sanctions associées aux scores faibles.
- discrimination : Risque que le système soit utilisé de manière discriminatoire, favorisant certains groupes au détriment d'autres.

Le système évolue en fonction des retours d'expérience et des critiques. Le gouvernement chinois a mis en place des mécanismes pour ajuster le système et répondre aux préoccupations exprimées par les citoyens et les observateurs internationaux.

Le crédit social chinois est un système complexe et intégré qui vise à influencer et à réguler les comportements des citoyens et des entreprises à travers des scores basés sur une vaste collecte de données. Bien qu'il vise à promouvoir la conformité et l'ordre social, il soulève des questions significatives sur la vie privée, la liberté individuelle et l'équité.

Les similitudes avec le pass sanitaire⁶ et l'accès aux zones des Jeux olympiques

Utilisation de Données pour Contrôler l'Accès :

- Crédit Social : Les données collectées sur les citoyens sont utilisées pour influencer leur accès à divers services et privilèges.
- Pass Sanitaire : Pendant la pandémie de COVID-19, le pass sanitaire a utilisé des données médicales (test COVID-19, vaccination) pour déterminer l'accès à des espaces publics, des événements et des voyages.
- Jeux Olympiques de Paris : L'accès aux zones restreintes lors des Jeux Olympiques est régulé par des critères spécifiques, comme les billets et les autorisations de sécurité, qui utilisent des données personnelles pour gérer les flux de spectateurs et les mesures de sécurité.

Contrôle et ségrégation basés sur des critères :

- Crédit social : le système segmente les citoyens selon leur score, avec des avantages ou des restrictions spécifiques.
- Pass sanitaire : les personnes sont séparées en fonction de leur statut de vaccination ou de test, avec des restrictions pour ceux qui ne répondent pas aux critères.
- Jeux Olympiques de Paris : les spectateurs sont catégorisés selon leurs billets et autorisations, avec des accès limités en fonction de ces critères.

3. Objectifs de gestion des comportements et des flux :

- Crédit social : vise à influencer le comportement des citoyens pour qu'ils respectent les normes sociales et légales.
- Pass sanitaire : cherche à protéger la santé publique et à limiter la propagation du virus en contrôlant l'accès aux lieux publics.
- Jeux Olympiques de Paris : Utilise des critères d'accès pour garantir la sécurité et la fluidité des événements tout en gérant les flux de personnes.

Différences Notables

Nature et Objectifs :

- Le crédit social est un système systématique et permanent avec des objectifs de contrôle social et économique à long terme.

⁶ « Green Pass » ou pass sanitaire européen : https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr

- Le pass sanitaire et les restrictions pour les Jeux Olympiques sont des mesures temporaires liées à des circonstances spécifiques (pandémie et événements sportifs) et visent principalement la sécurité et la santé publique.

Durée et Échelle :

- Le crédit social est un système en place de manière continue avec un impact global et à long terme sur la vie quotidienne.
- Les pass sanitaires et les restrictions d'accès pour les Jeux Olympiques sont des mesures ponctuelles avec une durée limitée et une portée spécifique.

Bien que le crédit social chinois et les mesures comme le pass sanitaire ou les accès aux zones des Jeux Olympiques partagent des mécanismes de gestion et de contrôle via des données, ils diffèrent dans leurs objectifs, leur portée et leur durée.

Question : Existe-t-il à moyen ou à long termes un risque d'évolution vers un « crédit social » à la chinoise dans l'Union européenne ?

Réponses : oui – non – NSP

Les données de santé

Nature particulièrement sensible des données de santé: Les données de santé sont considérées comme des données à caractère personnel particulièrement sensibles en raison des implications qu'elles peuvent avoir sur la vie privée et la santé des individus.

Bien qu'il ait été conçu pour offrir un cadre plus solide pour les transferts de données entre l'UE et les États-Unis, le Data Privacy Framework (DPF) ne garantit pas une protection absolue, notamment en raison des lois américaines sur la surveillance. En tant qu'entreprise américaine, Microsoft est soumise aux lois de son pays, ce qui peut potentiellement poser des problèmes de conformité avec le RGPD et le DPF.

La Commission nationale de l'informatique et des libertés (CNIL) a autorisé, dans certains cas, l'hébergement de données de santé sur des serveurs de Microsoft, mais en imposant des garanties supplémentaires.

Lorsque des données à caractère personnel, en particulier des données de santé, sont transférées vers un pays tiers comme les États-Unis, des garanties supplémentaires sont souvent exigées pour s'assurer que le niveau de protection des données reste conforme au RGPD. Ces garanties peuvent varier en fonction de la nature des données, du destinataire et de l'évaluation des risques.

Voici quelques exemples de garanties supplémentaires qui peuvent être mises en place:

- **Clauses contractuelles types (CCT):** Ces clauses contractuelles standardisées, approuvées par la Commission européenne, précisent les droits et obligations des parties impliquées dans le transfert de données. Elles doivent notamment garantir que le destinataire des données s'engage à respecter les principes du RGPD.
- **Codes de conduite:** Les entreprises peuvent adopter des codes de conduite certifiés qui définissent des règles strictes en matière de protection des données. Ces codes peuvent être reconnus par les autorités de contrôle comme offrant des garanties suffisantes.
- **Certifications:** Certaines certifications, comme la certification ISO 27001, peuvent attester de la mise en œuvre de mesures de sécurité robustes au sein d'une organisation.
- **Mesures techniques et organisationnelles:** Des mesures spécifiques peuvent être mises en place pour sécuriser les données, telles que le chiffrement, les contrôles d'accès, la pseudonymisation ou l'anonymisation.

- **Mécanismes de réclamation:** Des procédures doivent être mises en place pour permettre aux personnes concernées de faire valoir leurs droits et de déposer des réclamations en cas de violation de leurs données.
- **Autorisations spécifiques:** Dans certains cas, une autorisation préalable des autorités de contrôle peut être nécessaire, notamment pour les transferts de données à grande échelle ou vers des pays présentant un risque élevé pour les droits fondamentaux.

Dans le cas de données de santé transférées vers Microsoft, il est probable que des garanties supplémentaires spécifiques aient été négociées, notamment:

- Des engagements contractuels forts de la part de Microsoft pour garantir la confidentialité, l'intégrité et la disponibilité des données.
- Des mesures techniques renforcées pour protéger les données contre les accès non autorisés et les cyberattaques.
- Des audits réguliers pour vérifier la conformité de Microsoft aux engagements pris.
- Des mécanismes de résolution des litiges en cas de différend.

Il est important de noter que:

- L'évaluation de ces garanties est effectuée au cas par cas par les autorités de contrôle, telles que la CNIL en France.
- La nature exacte des garanties peut varier en fonction de la sensibilité des données, du contexte du transfert et des risques identifiés.
- Les garanties doivent être régulièrement revues et mises à jour pour s'adapter à l'évolution du contexte technologique et juridique.
- En conclusion, les garanties supplémentaires mises en place pour les transferts de données de santé vers un pays tiers visent à assurer un niveau de protection adéquat des données et à préserver les droits des personnes concernées. Bien que ces garanties puissent sembler complexes, elles sont essentielles pour garantir la confiance dans les traitements de données à caractère personnel à l'ère du numérique.

Le recours au Conseil d'Etat

https://www.lemonde.fr/pixels/article/2024/03/18/donnees-de-sante-francaises-chez-microsoft-nouveau-recours-devant-le-conseil-d-etat_6222758_4408996.html Publié le 18 mars 2024

Données de santé françaises chez Microsoft : nouveau recours devant le Conseil d'Etat

Les requérants attaquent l'autorisation accordée par la Commission nationale de l'informatique et des libertés (CNIL) fin décembre à un projet d'entrepôt de données de santé pour la recherche qui sera hébergé par Microsoft.

Des entreprises et des associations françaises ont déposé un nouveau recours devant le Conseil d'Etat contre l'hébergement de données de santé françaises chez l'américain Microsoft, ont-elles annoncé, lundi 18 mars, lors d'une conférence de presse. Les requérants sont les entreprises Nexedi, Clever Cloud, Cleyrop, concurrents potentiels de Microsoft, et des ONG comme l'Open Internet Project ou l'Institut de la souveraineté numérique.

Le recours doit être examiné à 11 heures mardi par le Conseil d'Etat, a précisé l'avocat des requérants, Jean-Baptiste Soufron.

Les requérants attaquent l'autorisation donnée par la Commission nationale de l'informatique et des libertés (CNIL) fin décembre à un projet d'entrepôt de données de santé pour la recherche qui sera hébergé par Microsoft.

Cet entrepôt, baptisé « EMC2 », associera les données des patients de quatre grands hôpitaux français avec les données les concernant (remboursements de consultations et de soins, parcours hospitaliers...) détenues par l'Assurance-maladie. Il est géré par le Health Data Hub (plateforme de données de santé), dans le cadre d'un programme de recherche en pharmaco-vigilance de l'Agence européenne des médicaments.

...

<https://www.publicsenat.fr/actualites/non-classe/cedric-o-bouscule-au-senat-sur-le-choix-de-microsoft-pour-heberger-le-health> Publié le 03/02/2022 à 16:24

Cédric O bousculé au Sénat sur le choix de Microsoft pour héberger le Health Data Hub

Sujet sensible à l'orée de l'élection présidentielle. La commission d'enquête sénatoriale sur l'influence des cabinets de conseil a interrogé le secrétaire d'Etat au Numérique sur la phase de préfiguration de la plateforme des données de santé. Des consultants de Capgemini ont été appelés en 2019, quelques mois avant que le gouvernement fasse le choix de Microsoft pour héberger les données.

Pétition en ligne : <https://www.mesopinions.com/petition/politique/sortons-nos-donnees-sante-microsoft/227401>

Sortons nos données de santé de chez Microsoft !

Question : l'attribution du marché d'hébergement des données de santé à Microsoft sans appel d'offres et mise en concurrence doit-il être annulé ?

Oui / non / NSP

Question : l'hébergement des données de santé peut-il être confié à une entreprise américaine ?

Oui / non / NSP

Question : le Data Privacy Framework entre les Etats-Unis et les Etats-Unis garantit-il les données personnelles des citoyens européens ?

Oui / non / NSP

Question : des entreprises européennes (de Gaia-X) sont-elles capables d'héberger les données de santé des citoyens européens ?

Oui / non / NSP

Les données des citoyens doivent-elles être partitionnées et physiquement hébergées dans les Etats membres et les régions, sans accès externes à ces données ?

Oui / non / NSP

<https://www.lesnumeriques.com/vie-du-net/ecoutant-la-cnild-cedric-o-ne-veut-finalement-plus-confier-nos-donnees-de-sante-a-microsoft-n155493.html>

Écoutant la Cnil, Cédric O ne veut finalement plus confier nos données de santé à Microsoft

Par Mathieu Chartier - Publié le 09/10/20 à 12h35

Les réseaux sociaux

Tik Tok

La question de l'accès aux données personnelles des utilisateurs européens de TikTok par la Chine est un sujet d'inquiétude légitime et fait l'objet de nombreux débats.

- TikTok a reconnu que des employés basés en Chine avaient accès aux données des utilisateurs européens. Cette information a été révélée lors d'enquêtes journalistiques et a suscité de vives réactions.
- TikTok justifie cet accès en affirmant qu'il est strictement limité à des besoins spécifiques liés au fonctionnement de la plateforme, tels que la modération de contenu, le dépannage technique ou l'analyse de données.
- Cependant, les garanties offertes par TikTok ne sont pas toujours jugées suffisantes par les autorités européennes et les organisations de défense des droits de l'homme. En effet, il existe des craintes que ces données puissent être transmises aux autorités chinoises, notamment dans le cadre de la loi sur le renseignement national chinoise, qui oblige les entreprises chinoises à coopérer avec les services de renseignement.
- De nombreuses enquêtes sont en cours pour faire la lumière sur les pratiques de TikTok en matière de protection des données. Les autorités européennes, notamment la Commission européenne et certaines autorités nationales de protection des données, ont ouvert des enquêtes pour vérifier si TikTok respecte bien le Règlement général sur la protection des données (RGPD).

Les risques potentiels liés à cet accès aux données sont multiples :

- Censure et manipulation de l'information : Les autorités chinoises pourraient être tentées de censurer certains contenus ou de manipuler l'information présentée aux utilisateurs européens.
- Surveillance de masse : Les données collectées par TikTok pourraient être utilisées pour établir des profils détaillés des utilisateurs et les surveiller.
- Profilage à des fins commerciales : Les données pourraient être exploitées à des fins commerciales par des entreprises chinoises.

En conclusion, la question de l'accès aux données personnelles des utilisateurs européens de TikTok par la Chine est complexe et ne peut être résolue simplement. Il est essentiel que TikTok mette en place des garanties solides pour protéger les données de ses utilisateurs et qu'un cadre réglementaire clair soit établi au niveau européen pour réguler les activités des entreprises technologiques chinoises.

https://www.lemonde.fr/pixels/article/2023/03/04/soft-power-espionnage-donnees-personnelles-que-reproche-t-on-a-tiktok_6164148_4408996.html

Que reproche-t-on à TikTok ? Soft power, espionnage, données personnelles...

L'application star des adolescents est menacée d'interdiction par plusieurs gouvernements, qui craignent qu'elle ne soit utilisée par la Chine pour espionner ses utilisateurs.

<https://www.cnil.fr/fr/cookies-la-cnile-sanctionne-tiktok-hauteur-de-5-millions-deuros>

Cookies : la CNIL sanctionne TIKTOK à hauteur de 5 millions d'euros

12 janvier 2023

Entre mai 2020 et juin 2022, la CNIL a effectué plusieurs missions de contrôle en ligne sur le site web « tiktok.com » et sur pièces, c'est-à-dire sur la base de documents demandés à la société par la CNIL.

Les contrôles ont uniquement porté sur le site web de TIKTOK, dans un espace non authentifié, et non sur l'application mobile.

Sur la base des constatations effectuées lors des contrôles, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a considéré que les sociétés TIKTOK INFORMATION TECHNOLOGIES UK LIMITED (TIKTOK ROYAUME-UNI) et TIKTOK TECHNOLOGY LIMITED (TIKTOK IRLANDE) avaient manqué aux obligations prévues par l'article 82 de la loi Informatique et Libertés.

Le montant de cette amende a été décidé au regard des manquements retenus, du nombre de personnes concernées – notamment des mineurs - et des nombreuses communications antérieures de la CNIL sur le fait qu'il doit être aussi simple de refuser les cookies que de les accepter.

https://www.lemonde.fr/pixels/article/2024/04/24/tiktok-les-questions-que-pose-sa-possible-interdiction-aux-etats-unis_6229649_4408996.html

Le Congrès américain a adopté mardi 23 avril un projet de loi controversé pour forcer ByteDance à vendre son réseau social, sous peine de le voir interdit sur le territoire américain.

Une sanction est-elle suffisante ?

Faut-il interdire Tik Tok dans l'Union européenne ?

Oui / non / NSP

L'Inde a interdit Tik Tok pour des questions de souveraineté numérique (Institut Montaigne : <https://www.institutmontaigne.org/expressions/tik-tok-enjeux-pour-lue>)

Faut-il interdire Facebook dans l'Union européenne ?

Oui / non / NSP

Faut-il promouvoir l'application de messagerie Treebal dans l'Union européenne ?

Oui / non / NSP

Le cloud

Le cloud consiste à externaliser son infrastructure informatique sur une plate-forme support partagée par plusieurs entreprises. Cette externalisation est plus ou moins complète selon le schéma :

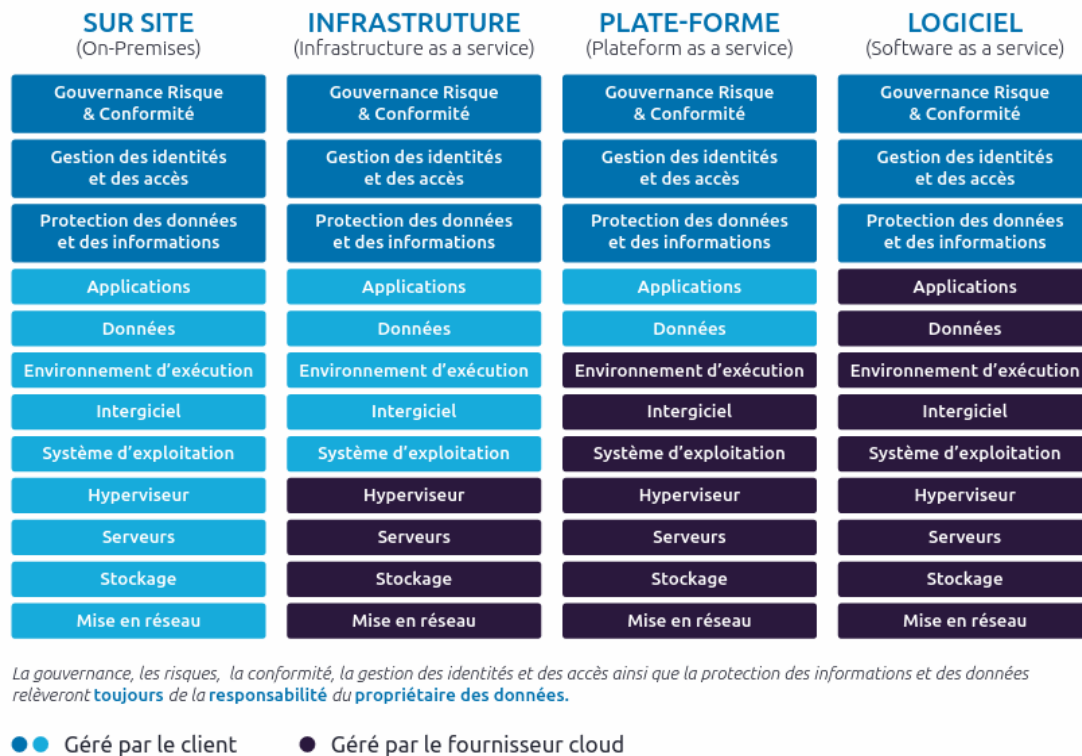


Figure 5 - Les niveaux d'externalisation du cloud (d'après https://www.capgemini.com/fr-fr/wp-content/uploads/sites/6/2022/08/2022-FR-Capgemini_Ebook_Cloud-services-publics-et-securite_-Livres-Blanc.pdf)

L'intérêt du cloud est de s'adapter instantanément aux besoins de l'entreprise sans nécessité d'investir dans une infrastructure interne et d'avoir à investir dans une

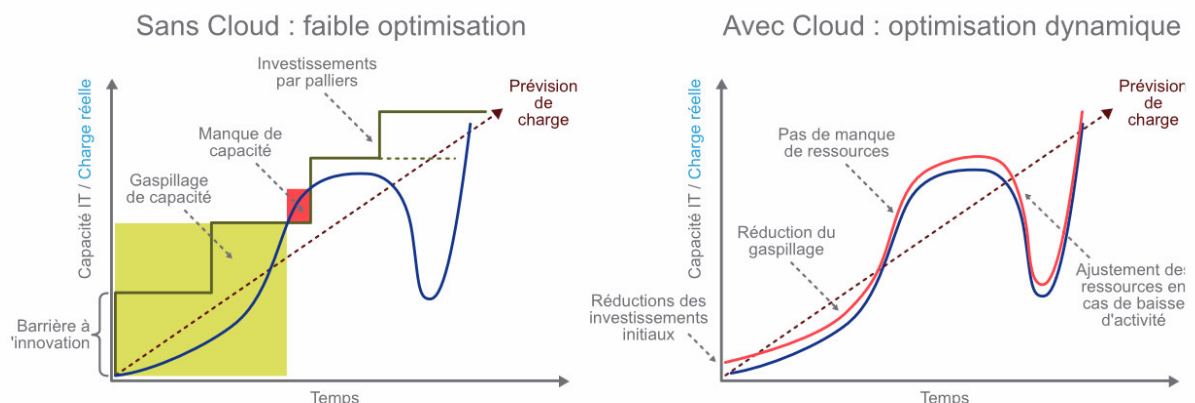


Figure 6 -

<http://www.virtu-desk.fr/medias/files/syntecle-livre-blanc-du-cloud-computing.pdf>

L'Union européenne

La France

L'agence du numérique (2020)

<https://presse.economie.gouv.fr/wp-content/uploads/2020/12/46e6d0f07b047818edf84360acd315c7.pdf>

France 2030 : la stratégie nationale cloud s'enrichit d'un nouvel appel à projets

<https://www.numerique.gouv.fr/espace-presse/france-2030-la-strategie-nationale-cloud-senrichit-dun-nouvel-appel-a-projets/>

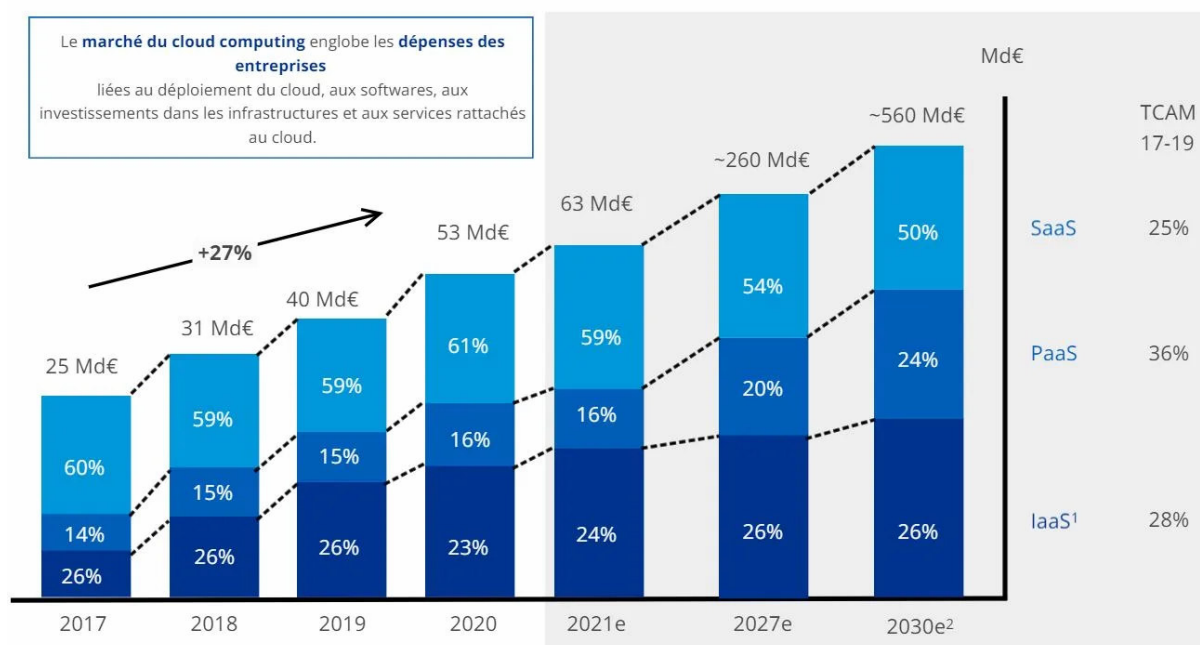
L'enjeu économique

<https://kpmg.com/fr/fr/media/press-releases/2021/05/cloud-europeen-marche-enjeux-economiques.html>

Publié le 4 mai 2021

Un marché de +300 milliards d'euros à l'horizon 2027-2030 dont la moitié du potentiel pourrait échapper à l'Europe ?

<https://kpmg.com/fr/fr/insights/cloud/cloud-europeen.html>



Évolution du marché européen des services cloud IaaS, PaaS et SaaS (2017-2030, Md€)

La Bretagne

<https://www.lejournaldesentreprises.com/article/le-nantais-etix-everywhere-elargit-son-reseau-de-data-centers-de-proximite-en-france-2091036>

https://www.youtube.com/watch?v=NnFUI-k8P_I 1 :40

Dispositions réglementaires pour un cloud souverain

Un cloud souverain se réfère à un environnement de cloud computing contrôlé par des entités nationales ou régionales, visant à garantir la souveraineté des données, la sécurité et la confidentialité. Voici les principales dispositions réglementaires généralement associées à un cloud souverain, souvent en lien avec des initiatives européennes comme GAIA-X :

1. Protection des données

L'élément central d'un cloud souverain est la gestion des données conformément aux lois locales ou régionales, comme le Règlement général sur la protection des données (RGPD) en Europe. Les principales exigences incluent :

- **Localisation des données** : Les données doivent être stockées dans des centres de données situés sur le territoire national ou au sein d'une région particulière (ex. Union européenne) afin d'éviter leur accès par des juridictions étrangères.
- **Conformité au RGPD** : Le cloud doit respecter les principes de minimisation des données, le consentement des utilisateurs, le droit à l'effacement, et la transparence quant à la manière dont les données sont traitées et partagées.
- **Protection des données sensibles** : Des réglementations spécifiques peuvent exiger que certaines catégories de données sensibles (données de santé, bancaires, gouvernementales) soient protégées par des niveaux de chiffrement plus élevés et par des normes de sécurité accrues.

2. Sécurité des infrastructures

La sécurité des infrastructures cloud doit répondre à des normes strictes pour prévenir les cyberattaques et garantir l'intégrité des services hébergés. Cela comprend :

Normes de cybersécurité : Le cloud souverain doit se conformer à des normes reconnues, telles que ISO 27001 (système de gestion de la sécurité de l'information) et ISO 27017 (contrôles de sécurité spécifiques au cloud).

Chiffrement des données : Les données doivent être chiffrées, tant au repos qu'en transit, pour protéger les informations confidentielles contre toute interception ou fuite.

Accès restreint : Les accès aux données et aux systèmes doivent être limités aux personnes autorisées par le pays ou la région, et soumis à des politiques d'audit.

3. Souveraineté juridique

Un des objectifs fondamentaux d'un cloud souverain est de garantir que les données et infrastructures numériques ne sont pas soumises aux lois extraterritoriales. À ce titre :

Exclusion des juridictions étrangères : Les données doivent être à l'abri de l'accès par des gouvernements étrangers, comme sous l'effet de lois telles que le Cloud Act américain (qui permet aux autorités américaines d'accéder à des données stockées dans des centres de données étrangers par des entreprises américaines).

Fournisseurs locaux : Les fournisseurs de cloud souverain doivent être des entreprises locales ou européennes, ou être sous contrôle majoritairement local/ européen afin d'échapper aux influences de juridictions étrangères.

4. Interopérabilité et indépendance technologique

Un cloud souverain doit éviter les situations de dépendance à un seul fournisseur ou à des technologies propriétaires :

Standards ouverts : Promouvoir l'usage de standards ouverts et de solutions interopérables, permettant de passer d'un fournisseur à l'autre sans être contraint par des technologies verrouillées (vendor lock-in).

Logiciels open-source : Encourager l'utilisation de logiciels open-source, notamment pour la gestion des infrastructures, afin de garantir la transparence, la sécurité, et la possibilité d'auditer le code.

5. Gouvernance et contrôle

La gouvernance d'un cloud souverain repose sur des mécanismes de contrôle stricts :

Audit et certification : Des mécanismes réguliers d'audit doivent être mis en place pour vérifier la conformité aux réglementations en vigueur. Cela inclut des certifications par des organismes indépendants, garantissant le respect des normes de sécurité et de protection des données.

Supervision nationale ou régionale : Les autorités nationales ou régionales doivent avoir une capacité de supervision sur les opérations du cloud, garantissant qu'il n'y ait aucune interférence étrangère ou pratique contraire aux lois nationales.

GAIA-X

Site internet : <https://gaia-x.eu/>

GAIA-X est une initiative européenne lancée en 2020 par la France et l'Allemagne, avec pour objectif de créer un écosystème de cloud souverain, sécurisé et interopérable au niveau européen, tout en se basant sur des valeurs de transparence, d'ouverture et de contrôle local. Ce projet vise à renforcer la souveraineté numérique de l'Europe et à réduire la dépendance aux fournisseurs de cloud étrangers (notamment américains comme Amazon AWS, Microsoft Azure, et Google Cloud).

1. Objectifs de GAIA-X

- **Souveraineté des données** : GAIA-X vise à garantir que les données des entreprises et des citoyens européens soient stockées, traitées et gérées en Europe, conformément aux réglementations européennes, comme le RGPD. Cela inclut la création de centres de données européens et la promotion de services de cloud opérés par des entreprises européennes.
- **Interopérabilité et standards ouverts** : GAIA-X repose sur l'idée d'un cloud décentralisé et interopérable. Les différentes solutions cloud doivent être capables de fonctionner ensemble via des interfaces et standards ouverts. Cela permet aux utilisateurs de choisir librement leurs services et de ne pas être enfermés dans des solutions propriétaires.
- **Sécurité et conformité** : GAIA-X impose des critères stricts en termes de sécurité et de protection des données. Toutes les infrastructures et services au sein de l'écosystème GAIA-X doivent répondre à des standards de sécurité et de conformité reconnus au niveau européen.
- **Innovation et compétitivité** : En favorisant un cadre commun pour les services cloud, GAIA-X espère dynamiser l'innovation en Europe et offrir une alternative crédible aux grandes plateformes américaines et asiatiques. L'initiative vise à créer un marché européen compétitif avec de nouveaux acteurs et services tout en soutenant l'économie locale.

2. Architecture de GAIA-X

GAIA-X n'est pas un fournisseur de cloud à proprement parler. C'est une fédération de services opérés par différents acteurs européens (entreprises, centres de données, fournisseurs de services cloud), avec des règles communes de sécurité, d'interopérabilité et de transparence.

- **Catalogue de services** : Les utilisateurs peuvent accéder à un catalogue de services cloud qui répondent aux normes GAIA-X. Chaque service doit respecter les critères de conformité et de sécurité, ce qui permet de choisir des solutions en fonction de la localisation des données, des performances, et des niveaux de sécurité requis.
- **Hub de données** : GAIA-X propose également des hubs de données où les entreprises, les gouvernements et d'autres entités peuvent stocker et partager des données de manière sécurisée, tout en gardant le contrôle sur qui peut y accéder.

3. Partenaires et gouvernance

GAIA-X est soutenu par un large éventail de partenaires européens issus de divers secteurs : technologie, énergie, finance, santé, etc. Les gouvernements de la France et de l'Allemagne ont joué un rôle de premier plan dans la création du projet, mais aujourd'hui, d'autres États membres de l'Union européenne et des entreprises privées y participent également. GAIA-X est géré par une association à but non lucratif, GAIA-X AISBL, basée à Bruxelles.

4. Exemples d'utilisation de GAIA-X

- **Secteur public** : Des gouvernements européens peuvent utiliser GAIA-X pour héberger des services publics critiques et des données sensibles, assurant ainsi leur sécurité et leur conformité avec les réglementations européennes.
- **Industrie** : Les entreprises du secteur manufacturier ou de la santé, par exemple, peuvent s'appuyer sur GAIA-X pour partager des données avec d'autres acteurs européens dans le cadre de chaînes d'approvisionnement, de recherche ou de développement.

Conclusion

GAIA-X représente une tentative européenne de reprendre le contrôle de son infrastructure cloud, tout en garantissant des normes de sécurité, de transparence et d'interopérabilité. Couplée avec des dispositions réglementaires pour un cloud souverain, l'Europe espère ainsi promouvoir une souveraineté numérique tout en restant compétitive sur la scène mondiale.

Les évolutions à venir

Peut-on considérer que le cloud s'est développé et est mature ou est-ce que de nouvelles ruptures technologiques sont anticipables dans ce domaine ?

Le cloud computing a connu un développement spectaculaire au cours de la dernière décennie, et on peut dire qu'il est devenu une technologie mature. Cependant, plusieurs facteurs suggèrent que des ruptures technologiques sont encore anticipables dans ce domaine. Voici une analyse de la situation actuelle et des tendances émergentes :

1. État Actuel du Cloud Computing

1.1 Maturité du Cloud

Adoption Généralisée : De nombreuses entreprises, des startups aux grandes corporations, ont adopté des solutions de cloud, allant des infrastructures cloud (IaaS) aux plateformes cloud (PaaS) et aux logiciels en tant que service (SaaS).

Normes Établies : Le cloud computing a développé des normes et des meilleures pratiques en matière de sécurité, de gestion des données, et d'architecture, ce qui facilite son intégration dans les opérations commerciales.

Services Diversifiés : Les fournisseurs de cloud proposent une gamme variée de services, y compris le cloud public, privé et hybride, ainsi que des solutions spécialisées comme le cloud pour l'IA, le big data, et l'IoT.

1.2 Enjeux et Limitations

Sécurité et Confiance : Bien que les fournisseurs de cloud aient amélioré la sécurité, des préoccupations subsistent concernant la confidentialité des données, la gestion des identités, et la sécurité des applications.

Verrouillage des Fournisseurs (Vendor Lock-In) : Les entreprises craignent d'être dépendantes d'un seul fournisseur de cloud, ce qui limite leur flexibilité et leur capacité à migrer vers d'autres solutions.

2. Anticipation de Nouvelles Ruptures Technologiques

2.1 Edge Computing

Définition : L'edge computing consiste à traiter les données près de leur source (par exemple, sur des appareils IoT) plutôt que de les envoyer vers un cloud centralisé. Cela réduit la latence et permet une prise de décision plus rapide.

Impact Anticipé : À mesure que l'IoT et les dispositifs connectés se multiplient, l'edge computing pourrait devenir une composante essentielle des architectures cloud, créant ainsi une nouvelle approche décentralisée du traitement des données.

2.2 Intelligence Artificielle et Cloud

Intégration de l'IA : L'IA est de plus en plus intégrée aux services cloud, permettant des analyses avancées et une automatisation des processus. Les services de cloud pourraient évoluer pour offrir des outils d'IA prédéfinis et accessibles.

IA Décentralisée : Les modèles d'IA peuvent être exécutés sur des infrastructures distribuées, ce qui pourrait favoriser le développement de solutions plus réactives et adaptées à des besoins spécifiques.

2.3 Multi-Cloud et Interopérabilité

Approche Multi-Cloud : Les entreprises adoptent de plus en plus des stratégies multi-cloud pour éviter le verrouillage des fournisseurs et bénéficier des meilleures fonctionnalités de chaque plateforme. Cela crée un besoin d'interopérabilité entre différents services cloud.

Plateformes d'Interopérabilité : De nouvelles solutions logicielles pourraient émerger pour faciliter la gestion des environnements multi-cloud, permettant aux entreprises de tirer parti de diverses ressources sans complexité excessive.

2.4 Cloud Souverain

Réglementation et Souveraineté : Les préoccupations concernant la souveraineté des données et la conformité aux réglementations (comme le RGPD en Europe) pourraient stimuler la demande pour des solutions de cloud souverain, hébergées et gérées par des acteurs locaux.

Infrastructures Souveraines : Des initiatives pour développer des infrastructures cloud souveraines pourraient émerger, permettant un contrôle accru sur les données et répondant aux exigences réglementaires.

3. Développement Durable et Écologie

Cloud Écologique : Avec l'accent croissant sur le développement durable, les fournisseurs de cloud peuvent être amenés à adopter des pratiques plus respectueuses de l'environnement, notamment en utilisant des énergies renouvelables et en optimisant l'efficacité énergétique de leurs centres de données.

Technologies Vertes : L'intégration de technologies vertes dans l'infrastructure cloud pourrait devenir une exigence pour les entreprises soucieuses de leur impact environnemental.

Conclusion

Bien que le cloud computing soit devenu mature et largement adopté, plusieurs ruptures technologiques sont encore anticipables dans ce domaine. Des concepts tels que l'edge computing, l'intégration de l'IA, les stratégies multi-cloud, et les préoccupations de souveraineté des données pourraient redéfinir l'architecture et l'utilisation du cloud dans les années à venir. Ces développements représentent des opportunités et des défis, et il sera crucial pour les entreprises de s'adapter à ces changements pour rester compétitives.

Un cloud souverain régional

Les États membres de l'Union européenne, ainsi que certaines régions, ont des attentes spécifiques en matière de cloud souverain et par rapport à GAIA-X, car les enjeux de souveraineté numérique, de sécurité des données, et de compétitivité économique sont devenus des priorités stratégiques. Voici quelques exemples d'attentes spécifiques de plusieurs États membres et régions européennes en matière de cloud souverain et de GAIA-X :

1. France

La France a été l'un des principaux moteurs de l'initiative GAIA-X et accorde une importance particulière au développement d'une infrastructure numérique souveraine. Le gouvernement français a des attentes fortes vis-à-vis du cloud souverain, notamment pour renforcer la sécurité et l'indépendance technologique de la France.

Attentes spécifiques :

- **Renforcement de la souveraineté des données** : La France souhaite que GAIA-X assure une protection accrue des données des citoyens et des entreprises françaises, en particulier pour les secteurs stratégiques comme la défense, la santé et l'énergie. Les données doivent rester sous contrôle français ou européen, évitant ainsi la dépendance aux fournisseurs étrangers (américains ou chinois).
- **Cloud de confiance** : La France a introduit la notion de "Cloud de confiance", visant à certifier les solutions cloud qui garantissent la localisation des données en Europe et leur protection contre l'accès extraterritorial. GAIA-X est vu comme un cadre pour assurer cette exigence.
- **Interopérabilité** : La France attend également de GAIA-X qu'il facilite l'interopérabilité entre les solutions cloud publiques et privées, permettant aux entreprises françaises de changer facilement de fournisseur sans risque de verrouillage technologique (vendor lock-in).
- **Soutien à l'innovation européenne** : La France espère que GAIA-X soutiendra la montée en puissance d'acteurs cloud locaux ou européens (comme OVHcloud) et favorisera la recherche et le développement technologique au sein de l'Union européenne.

2. Allemagne

L'Allemagne, cofondatrice de GAIA-X, partage les mêmes préoccupations que la France en matière de souveraineté numérique, tout en mettant l'accent sur l'importance des données industrielles et de l'innovation.

Attentes spécifiques :

- **Cloud industriel** : L'Allemagne, qui possède une base industrielle forte, attend de GAIA-X qu'il offre un cadre sûr et interopérable pour le stockage et le partage des données industrielles. Cela inclut les données issues des secteurs de la production manufacturière, de

l'automobile et de la logistique. La souveraineté sur ces données est essentielle pour préserver la compétitivité des industries allemandes.

- **Souveraineté des infrastructures** : L'Allemagne souhaite garantir que les infrastructures critiques allemandes ne soient pas sous contrôle étranger, et espère que GAIA-X puisse assurer une protection des centres de données et des réseaux cloud sur le sol allemand.
- **Sécurité et conformité** : L'Allemagne attend de GAIA-X une conformité rigoureuse aux normes de sécurité européennes, comme le RGPD, et aux futures normes en matière de cybersécurité. L'objectif est de s'assurer que les données des entreprises et des citoyens allemands restent protégées contre toute tentative d'accès non autorisée, en particulier par des lois étrangères comme le Cloud Act américain.

3. Italie

L'Italie, bien que plus récente dans l'adoption du concept de cloud souverain, voit dans GAIA-X une opportunité de renforcer son infrastructure numérique et de réduire sa dépendance à des fournisseurs cloud étrangers.

Attentes spécifiques :

- **Infrastructures numériques locales** : L'Italie espère utiliser GAIA-X pour développer des infrastructures numériques locales (centres de données, services cloud) qui respectent les normes européennes et garantissent la sécurité des données des citoyens et des entreprises italiennes.

Transition numérique : Le gouvernement italien attend de GAIA-X qu'il aide à moderniser les services publics en Italie, en particulier en permettant une meilleure gestion des données des administrations publiques, tout en garantissant leur protection et leur souveraineté.

- **Collaboration industrielle** : L'Italie souhaite utiliser GAIA-X pour stimuler la collaboration industrielle dans les secteurs de la santé, de la finance et de l'automobile, en offrant un cadre sûr pour le partage de données entre les entreprises italiennes et européennes.

4. Espagne

L'Espagne voit dans GAIA-X une opportunité pour renforcer son écosystème numérique, notamment pour les PME et les startups, qui représentent une part importante de son tissu économique.

Attentes spécifiques :

- **Développement régional** : L'Espagne espère que GAIA-X contribue au développement numérique des régions espagnoles en favorisant l'accès à des infrastructures cloud souveraines, en particulier dans les zones rurales et moins développées économiquement. Cela pourrait passer par des subventions pour installer des centres de données ou des services cloud dans des régions éloignées.
- **Soutien aux PME et startups** : GAIA-X est vu comme une opportunité pour offrir des solutions cloud accessibles, sécurisées et souveraines aux petites et moyennes entreprises espagnoles. Cela permettrait de réduire leur dépendance aux grandes entreprises technologiques étrangères et de stimuler l'innovation locale.
- **Protection des données dans les secteurs critiques** : L'Espagne attend de GAIA-X qu'il offre des garanties solides pour la protection des données dans des secteurs critiques comme l'énergie (particulièrement avec les infrastructures renouvelables), la finance et la santé.

5. Régions européennes : cas de la Bretagne (France)

Certaines régions au sein des États membres développent également des attentes spécifiques en matière de cloud souverain. Prenons l'exemple de la Bretagne, une région française avec une stratégie numérique proactive.

Attentes spécifiques :

- **Développement des infrastructures régionales** : La Bretagne souhaite promouvoir des centres de données régionaux sécurisés et interconnectés, en s'appuyant sur le cadre de GAIA-X. Cela permettrait aux entreprises locales, notamment dans les secteurs de la pêche, de l'agroalimentaire et des télécommunications, de bénéficier d'une infrastructure de cloud souverain.
- **Économie locale** : En encourageant l'utilisation d'un cloud souverain dans le cadre de GAIA-X, la Bretagne espère stimuler l'innovation locale et permettre à des startups de se développer dans des secteurs clés comme l'intelligence artificielle, l'agriculture numérique, et les énergies renouvelables.
- **Souveraineté des données agricoles** : En tant que région à forte tradition agricole, la Bretagne voit un intérêt particulier à protéger les données agricoles (agriculture numérique, capteurs IoT pour la gestion des cultures et du bétail) en s'assurant que ces données restent en Europe et ne tombent pas sous contrôle étranger.

Conclusion

Chaque État membre ou région européenne attend de GAIA-X qu'il réponde à des besoins spécifiques en fonction de leurs priorités économiques, industrielles et sécuritaires. Tous partagent un intérêt commun pour la protection des données, la sécurité des infrastructures critiques et la souveraineté numérique. Cependant, les secteurs d'application prioritaires et les modalités de mise en œuvre peuvent varier : pour certains, il s'agit d'assurer la sécurité des données industrielles, tandis que pour d'autres, il s'agit de développer l'économie numérique locale ou de moderniser les services publics.

Les entreprises bien positionnées

Quelles sont les entreprises bien positionnées pour ces défis ?

Plusieurs entreprises sont bien positionnées pour relever les défis et saisir les opportunités associés aux évolutions du cloud computing, de l'edge computing, de l'intelligence artificielle, et des préoccupations de souveraineté des données. Voici quelques-unes des entreprises clés qui se distinguent dans ces domaines :

1. Fournisseurs de Cloud Public

1.1 Amazon Web Services (AWS)

- **Description** : Leader mondial dans le cloud computing, AWS offre une large gamme de services, y compris le stockage, le calcul, l'intelligence artificielle, et le big data.
- **Positionnement** : Avec des outils avancés pour l'IA et l'analytics, AWS est bien placé pour aider les entreprises à intégrer ces technologies dans leurs opérations.

1.2 Microsoft Azure

- **Description** : Microsoft Azure est une plateforme cloud qui offre des solutions variées, y compris des services de machine learning, d'IoT, et de big data.
- **Positionnement** : Azure se distingue par sa forte intégration avec les logiciels d'entreprise et les services de collaboration, ce qui en fait un choix privilégié pour les entreprises déjà investies dans l'écosystème Microsoft.

1.3 Google Cloud Platform (GCP)

- **Description** : GCP propose des services cloud axés sur l'analyse des données et l'intelligence artificielle, avec des outils comme BigQuery et TensorFlow.

- **Positionnement** : Sa force réside dans l'analyse de données massives et l'apprentissage automatique, ce qui le rend attractif pour les entreprises qui cherchent à tirer parti de l'IA et des données.

2. Fournisseurs de Solutions Edge et Multi-Cloud

2.1 VMware

- **Description** : VMware est un leader dans les solutions de virtualisation et d'infrastructure cloud. Ils offrent des solutions pour gérer des environnements multi-cloud et edge.
- **Positionnement** : Avec des outils pour la gestion des ressources dans des environnements hybrides et multi-cloud, VMware est bien positionnée pour aider les entreprises à naviguer dans des architectures complexes.

2.2 Cisco

- **Description** : Cisco est un acteur majeur dans les technologies de réseau et propose également des solutions pour l'edge computing et la cybersécurité.
- **Positionnement** : Grâce à son expertise en infrastructure réseau, Cisco peut faciliter la transition vers l'edge computing et améliorer la sécurité des données.

3. Entreprises d'IA et de Big Data

3.1 Palantir Technologies

- **Description** : Palantir propose des logiciels de gestion et d'analyse de données, permettant aux entreprises d'exploiter leurs données pour des insights stratégiques.
- **Positionnement** : Avec une forte présence dans des secteurs comme la défense, la finance, et la santé, Palantir est bien positionné pour tirer parti des opportunités dans le big data et l'IA.

3.2 Snowflake

- **Description** : Snowflake est une plateforme de données qui permet le stockage et l'analyse des données dans le cloud. Elle est conçue pour l'intégration des données de plusieurs sources.
- **Positionnement** : Snowflake est particulièrement forte dans l'analyse des données massives et le partage de données, ce qui est essentiel pour les entreprises cherchant à capitaliser sur l'IA et le big data.

4. Acteurs Européens dans le Cloud Souverain

4.1 OVHcloud (France)

- **Description** : OVHcloud est un fournisseur de services cloud basé en France, proposant des solutions d'hébergement et de cloud computing.
- **Positionnement** : En mettant l'accent sur la souveraineté des données et la conformité avec les réglementations européennes, OVHcloud répond à une demande croissante pour des solutions cloud locales.

4.2 Scaleway (France)

- **Description** : Scaleway est un fournisseur de cloud qui propose des solutions d'infrastructure et d'hébergement en France, avec un accent sur la simplicité et l'efficacité.
- **Positionnement** : Scaleway s'efforce de répondre aux besoins des entreprises en matière de cloud tout en garantissant la conformité avec les normes européennes.

5. Startups Innovantes

5.1 DataRobot

- **Description** : DataRobot propose une plateforme d'automatisation de l'apprentissage automatique qui permet aux entreprises de développer et de déployer des modèles d'IA.

- **Positionnement** : En rendant l'IA plus accessible, DataRobot aide les entreprises à intégrer l'IA dans leurs processus décisionnels.

5.2 Mistral AI

- **Description** : En tant que startup européenne, Mistral AI se concentre sur le développement de modèles de langage avancés, cherchant à rivaliser avec des géants comme OpenAI.
- **Positionnement** : Mistral AI s'engage à développer des technologies d'IA tout en respectant les valeurs éthiques et les normes de protection des données.

Conclusion

Il existe de nombreux acteurs, des grandes entreprises établies aux startups innovantes, qui sont bien positionnés pour relever les défis du cloud computing, de l'edge computing, du big data, et de l'intelligence artificielle. Ces entreprises jouent un rôle clé dans l'évolution de ces technologies, et leur succès dépendra de leur capacité à innover et à s'adapter aux besoins changeants du marché, ainsi qu'à répondre aux préoccupations croissantes en matière de sécurité, de souveraineté et d'éthique.

Gaia-X change-t-il fondamentalement la donne en matière de cloud dans l'Union européenne (promotion de solutions cloud ou génération d'entreprises européenne en même temps que suivi des évolutions) ?

Oui / non / NSP

(si oui, continuer, si non, abandonner ?)

Les entreprises bien positionnées en Bretagne

Quelles sont les entreprises bien positionnées dans l'Union européenne pour ces défis ?

En Bretagne et dans les Pays de la Loire, plusieurs entreprises et institutions se distinguent par leur positionnement sur les défis liés à l'intelligence artificielle (IA), au cloud computing, au big data, et à l'edge computing. Voici un aperçu des acteurs clés dans cette région :

1. Entreprises en Bretagne

1.1 Atos (Rennes)

- **Description** : Atos est une entreprise internationale de services numériques qui a des bureaux à Rennes. Elle propose des solutions en cloud, en big data et en cybersécurité.
- **Positionnement** : Atos est engagée dans le développement de solutions numériques et de cloud souverain, contribuant à l'innovation dans le secteur public et privé.

1.2 Elips (Lorient)

- **Description** : Elips est une société spécialisée dans les technologies de l'information et de la communication, fournissant des services liés à l'IA, aux systèmes d'information, et à l'analyse des données.
- **Positionnement** : L'entreprise aide ses clients à tirer parti des données pour optimiser leurs processus opérationnels et améliorer la prise de décision.
- Elips - Adresse : 26 Rue des Potiers, 56100 Lorient, France - Site Web : www.elips.fr (obsolète)

1.3 Kereval (Brest)

- **Description** : Kereval est une startup spécialisée dans l'IoT et l'edge computing, offrant des solutions pour le suivi et la gestion des données en temps réel.
- **Positionnement** : En se concentrant sur l'edge computing, Kereval répond aux besoins des industries pour des applications nécessitant des temps de réponse rapides.
- https://www.kereval.com/a_propos/

1.4 Inria (Bretagne)

- **Description** : Inria est un institut national de recherche en informatique et en automatique, avec des équipes en Bretagne travaillant sur l'IA, la robotique et le traitement de données.
- **Positionnement** : Inria joue un rôle clé dans la recherche fondamentale et appliquée en IA, collaborant avec des entreprises pour développer des solutions innovantes.

2. Entreprises dans les Pays de la Loire

2.1 Apside (Nantes)

- **Description** : Apside est une société de conseil en ingénierie et en technologies numériques, offrant des services dans le développement de logiciels et l'intégration de solutions cloud.
- **Positionnement** : Apside aide les entreprises à s'adapter aux nouvelles technologies et à intégrer des solutions d'IA et de cloud dans leurs opérations.

2.2 Qwant (Nantes)

- **Description** : Qwant est un moteur de recherche qui respecte la vie privée des utilisateurs, utilisant des technologies d'IA pour améliorer les résultats de recherche.
- **Positionnement** : En mettant l'accent sur la confidentialité et l'éthique, Qwant se positionne comme un acteur alternatif dans le paysage numérique, répondant aux préoccupations croissantes concernant les données personnelles.

2.3 Cdiscount (Nantes)

- **Description** : Cdiscount, bien que principalement un acteur du e-commerce, utilise des solutions de big data et d'IA pour optimiser ses opérations et améliorer l'expérience client.
- **Positionnement** : La capacité de Cdiscount à analyser de grandes quantités de données pour personnaliser ses offres et optimiser ses chaînes d'approvisionnement en fait un acteur important dans le domaine.

3. Initiatives et Consortiums

3.1 French Tech Brest+

- **Description** : French Tech Brest+ est un écosystème qui soutient l'innovation et l'entrepreneuriat dans la région de Brest, favorisant la collaboration entre startups, entreprises, et institutions académiques.
- **Positionnement** : Cet écosystème vise à promouvoir des initiatives technologiques, y compris celles liées à l'IA et aux technologies numériques.
- <https://www.ft-brestbretagneouest.bzh/>

3.2 Pôle de compétitivité Images & Réseaux

- **Description** : Ce pôle de compétitivité, basé à Rennes, regroupe des acteurs de l'image, des réseaux et du numérique, soutenant l'innovation dans ces domaines.
- **Positionnement** : Il favorise la collaboration entre entreprises, laboratoires de recherche et écoles pour développer des solutions numériques avancées, y compris en IA et big data.

Conclusion

En Bretagne et dans les Pays de la Loire, plusieurs entreprises et initiatives se distinguent par leur engagement envers l'intelligence artificielle, le cloud computing, et le big data. Des acteurs comme Atos, Elips, et Inria en Bretagne, ainsi qu'Apside et Qwant dans les Pays de la Loire, illustrent la diversité et l'innovation présentes dans la région. Ces entreprises, soutenues par des écosystèmes comme French Tech et des pôles de compétitivité, contribuent à façonner l'avenir numérique de la région, tout en s'attaquant aux défis technologiques et en tirant parti des opportunités émergentes.

Le cloud et Gaia-X

Le cloud est actuellement dominé par les trois grandes entreprises américaines (AWS...) et pour les évolutions du cloud identifiées aujourd'hui, ce sont ces entreprises et d'autres entreprises américaines ou britanniques qui sont bien positionnées, ainsi que quelques entreprises européennes. Le programme ou le consortium européen Gaia-X permettra-t-il de repositionner l'Union européenne dans la course ?

Le programme Gaia-X vise à créer une infrastructure cloud européenne souveraine et interopérable, et il pourrait jouer un rôle clé dans le repositionnement de l'Union européenne (UE) dans le domaine du cloud computing. Voici une analyse des perspectives et des défis associés à Gaia-X :

1. Objectifs de Gaia-X

1.1 Souveraineté Numérique

- **Contrôle des Données** : Gaia-X a pour but de garantir que les données des citoyens et des entreprises européennes soient stockées et traitées sur des infrastructures conformes aux réglementations de l'UE, notamment le RGPD. Cela renforce la souveraineté numérique en évitant le verrouillage des données par des fournisseurs étrangers.
- **Éviter la Dépendance** : En développant des solutions cloud locales, Gaia-X cherche à réduire la dépendance des entreprises européennes vis-à-vis des grandes entreprises américaines et britanniques, comme AWS, Microsoft, et Google.

1.2 Interopérabilité

- **Normes Communes** : Gaia-X promeut l'établissement de normes et d'interopérabilités pour les services cloud, facilitant ainsi la collaboration entre différents fournisseurs de services et l'intégration des systèmes.
- **Partenariats** : L'initiative encourage la coopération entre les entreprises technologiques, les institutions de recherche, et les gouvernements pour créer un écosystème robuste.

2. Perspectives de Repositionnement de l'UE

2.1 Création d'un Écosystème Cloud Européen

- **Infrastructures Locales** : Gaia-X pourrait faciliter le développement d'infrastructures cloud souveraines en Europe, permettant aux entreprises de bénéficier de solutions adaptées à leurs besoins tout en respectant les normes européennes.
- **Soutien à l'Innovation** : En réunissant des acteurs européens, Gaia-X peut encourager l'innovation et le développement de nouvelles technologies dans le cloud computing, stimulant ainsi l'économie numérique en Europe.

2.2 Compétitivité sur le Marché Mondial

- **Alternatives aux GAFAM** : En fournissant des alternatives viables aux solutions de cloud des GAFAM, Gaia-X pourrait aider les entreprises européennes à rester compétitives sur le marché mondial.

- **Attraction des Investissements** : Une infrastructure cloud européenne solide pourrait attirer des investissements, tant locaux qu'internationaux, dans le secteur des technologies.

3. Défis à Surmonter

3.1 Adoption et Participation

- **Engagement des Acteurs** : Pour réussir, Gaia-X a besoin de l'engagement actif des entreprises, des gouvernements et des institutions de recherche. L'adhésion à cette initiative nécessite un changement culturel et des investissements.
- **Confiance et Sécurité** : Les entreprises doivent être convaincues que les solutions offertes par Gaia-X sont sécurisées et fiables, et qu'elles répondent à leurs besoins en matière de performance.

3.2 Coordination et Cohérence

- **Consensus entre les États Membres** : L'UE doit naviguer dans des intérêts divergents parmi ses États membres pour établir des normes et des pratiques communes.
- **Complexité Réglementaire** : L'environnement réglementaire en Europe est complexe, et Gaia-X devra s'assurer que ses solutions respectent les exigences locales tout en restant compétitives.

4. Conclusion

Gaia-X a le potentiel de repositionner l'Union européenne dans la course au cloud computing en développant une infrastructure cloud souveraine et interopérable. En réduisant la dépendance à l'égard des grandes entreprises américaines et en créant un écosystème cloud européen, Gaia-X pourrait favoriser l'innovation, renforcer la souveraineté numérique, et améliorer la compétitivité des entreprises européennes. Toutefois, pour que cette initiative réussisse, elle devra surmonter des défis importants liés à l'engagement des acteurs, à la coordination entre les États membres, et à la création de solutions sécurisées et fiables. La réussite de Gaia-X dépendra également de la capacité à s'adapter aux évolutions rapides du marché technologique.

Le programme Gaia-X permet-il de

Megalis et le cloud

<https://www.megalis.bretagne.bzh/>

Le Syndicat mixte Mégalis Bretagne a été créé en 1999 et a pour compétences :

- D'assurer, en lieu et place de ses membres, la construction et l'exploitation du réseau public régional en fibre optique dans le cadre du projet « Bretagne Très Haut Débit » ;
- De favoriser le développement de l'administration électronique en proposant une offre de services numériques mutualisés et de fournitures annexes associées.

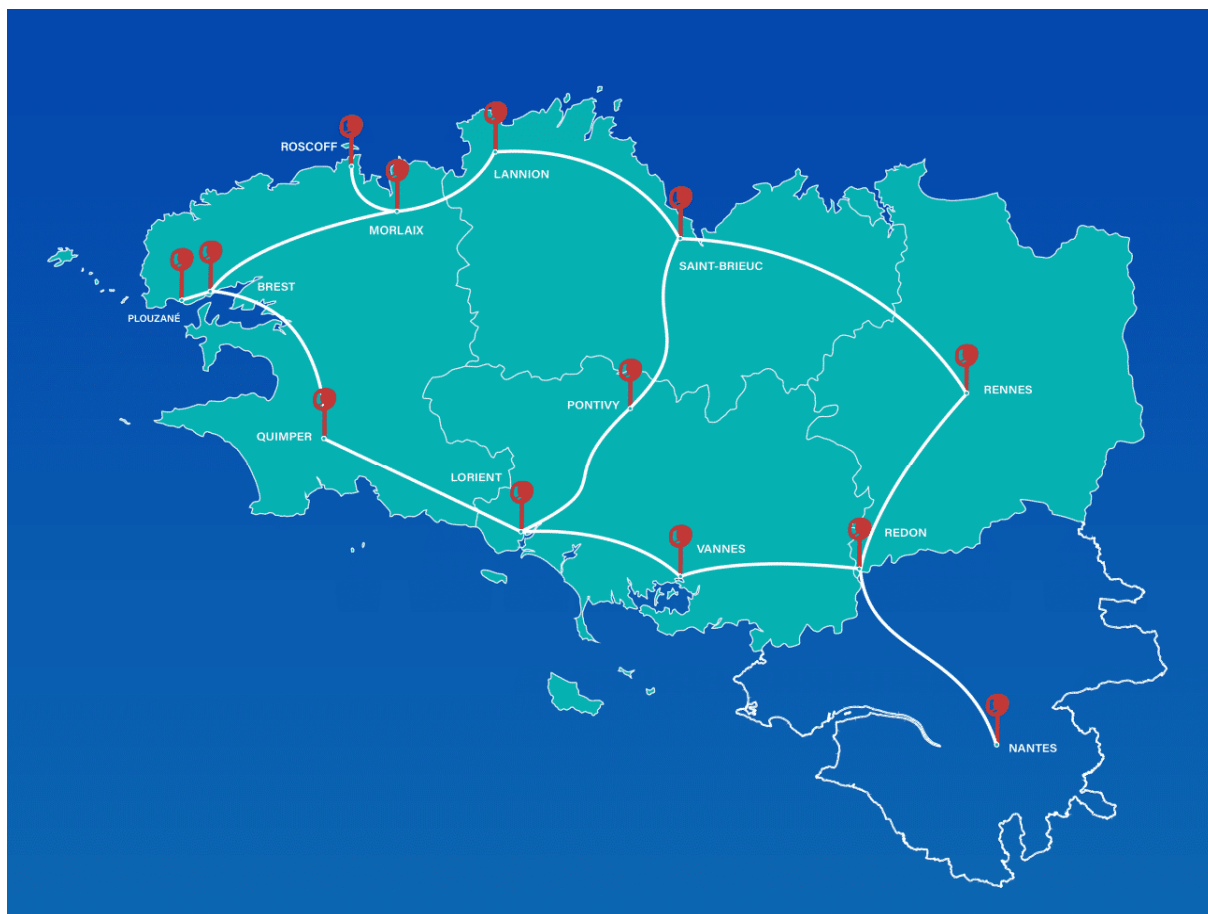


Figure 7 - Le réseau ultra-haut débit (<https://www.megalys.bretagne.bzh/reseau-ultra-haut-debit-ruhd/>)

Le projet Megalis en Bretagne contribue-t-il à l'émergence d'un cloud en Bretagne ?

Le projet **Megalys**, lancé en Bretagne, vise à renforcer l'infrastructure numérique de la région et contribue effectivement à l'émergence d'un cloud local. Voici un aperçu de ce projet et de son impact potentiel :

1. Présentation du Projet Megalis

1.1 Objectifs

- **Infrastructure Numérique** : Megalis a pour but de développer et de moderniser l'infrastructure numérique en Bretagne, en favorisant l'accès à des services numériques de qualité pour les entreprises, les administrations, et les citoyens.
- **Promotion de la Souveraineté Numérique** : Le projet cherche à offrir des solutions adaptées aux besoins spécifiques de la région, tout en respectant les réglementations sur la protection des données et en renforçant la souveraineté numérique.

1.2 Services Proposés

- **Réseau Numérique** : Megalis met en place un réseau très haut débit pour garantir un accès rapide et fiable à Internet, essentiel pour les services cloud.
- **Solutions Cloud** : Le projet inclut le développement de services cloud, permettant aux entreprises et aux administrations locales de bénéficier de solutions d'hébergement et de gestion des données.

2. Contribution à l'Émergence d'un Cloud en Bretagne

2.1 Infrastructure Localisée

- **Hébergement Souverain** : Megalis permet le développement de centres de données en Bretagne, offrant des solutions d'hébergement de données qui répondent aux besoins locaux et respectent les lois européennes, comme le RGPD.
- **Accessibilité** : En facilitant l'accès à des services cloud pour les entreprises de la région, Megalis contribue à réduire la dépendance vis-à-vis des grands fournisseurs de cloud internationaux.

2.2 Soutien aux Entreprises

- **Accompagnement des PME** : Megalis cible particulièrement les petites et moyennes entreprises (PME) en leur offrant des solutions cloud adaptées, favorisant leur transformation numérique.
- **Innovation Locale** : Le projet encourage l'innovation en soutenant des startups et des entreprises locales dans le développement de solutions numériques basées sur le cloud.

2.3 Écosystème Collaboratif

- **Partenariats** : Megalis favorise les collaborations entre les acteurs locaux, y compris les collectivités territoriales, les entreprises, et les établissements d'enseignement supérieur, pour développer des solutions cloud adaptées aux besoins de la région.
- **Formation et Sensibilisation** : Le projet inclut des initiatives de formation pour sensibiliser les entreprises aux avantages du cloud et à son intégration dans leurs processus opérationnels.

3. Défis à Surmonter

3.1 Adoption des Solutions

- **Sensibilisation** : Il peut être nécessaire de sensibiliser davantage les entreprises locales aux avantages des solutions cloud et de les accompagner dans leur adoption.
- **Investissement** : Le développement d'une infrastructure cloud robuste nécessite des investissements significatifs, et il est crucial de sécuriser des financements adéquats.

3.2 Concurrence avec des Fournisseurs Établis

- **Compétitivité** : Les solutions cloud développées par Megalis devront être compétitives par rapport à celles offertes par les grandes entreprises internationales pour attirer les entreprises locales.

4. Conclusion

Le projet Megalis contribue effectivement à l'émergence d'un cloud en Bretagne en développant une infrastructure numérique locale, en offrant des solutions d'hébergement et de services cloud, et en soutenant les entreprises dans leur transformation numérique. En renforçant la souveraineté numérique et en favorisant l'innovation locale, Megalis pourrait jouer un rôle clé dans le développement de l'écosystème numérique de la région. Cependant, il devra surmonter certains défis pour maximiser son impact et garantir l'adoption des solutions proposées par les entreprises et les administrations locales.

Megalis et La fibre 44

<https://fibre44.fr/>

Megalis et Fibre 44 sont interconnectés ou interconnectables ?

Megalys et **Fibre 44** sont deux initiatives distinctes visant à améliorer l'infrastructure numérique en Bretagne et dans la Loire-Atlantique, respectivement. Voici un aperçu de leur interconnexion potentielle :

1. Megalis

- **Objectif** : Megalis Bretagne est un projet régional qui vise à développer l'infrastructure numérique, y compris le très haut débit, pour améliorer l'accès aux services numériques pour les entreprises et les collectivités en Bretagne.
- **Infrastructures** : Megalis met en place un réseau de fibre optique et d'autres infrastructures numériques pour garantir un accès équitable à Internet de haute qualité.

2. Fibre 44

- **Objectif** : Fibre 44 est une initiative spécifique au département de la Loire-Atlantique, qui se concentre sur le déploiement de la fibre optique pour garantir l'accès à Internet très haut débit, notamment dans les zones rurales.
- **Infrastructures** : Ce projet a pour but de développer un réseau de fibre optique qui dessert les communes et les entreprises de la Loire-Atlantique.

3. Interconnexion et Synergies

3.1 Interconnexion

- **Infrastructure Complémentaire** : Megalis et Fibre 44 peuvent être considérés comme complémentaires, car ils visent à améliorer l'accès au haut débit dans deux régions différentes. Si Megalis se concentre sur la Bretagne et Fibre 44 sur la Loire-Atlantique, il est possible qu'il existe des points d'interconnexion entre leurs infrastructures de fibre optique, facilitant ainsi le transit des données entre les deux régions.

3.2 Collaboration Potentielle

- **Partage de Ressources** : Il pourrait y avoir des opportunités de collaboration pour le partage d'infrastructures, d'expertise ou de meilleures pratiques entre Megalis et Fibre 44, notamment dans le cadre de projets interrégionaux ou de financement commun pour le déploiement des infrastructures.
- **Interopérabilité** : La mise en place de normes communes et de pratiques d'interopérabilité pourrait permettre aux réseaux de Megalis et de Fibre 44 de communiquer efficacement, facilitant l'accès des utilisateurs à des services numériques dans les deux régions.

4. Conclusion

Bien que Megalis et Fibre 44 soient des initiatives distinctes, leur interconnexion est possible grâce à une infrastructure complémentaire et des opportunités de collaboration. En favorisant une approche intégrée et en partageant des ressources, ces projets pourraient améliorer l'accès au haut débit et renforcer l'écosystème numérique dans les deux régions. La coopération entre les différentes initiatives régionales est essentielle pour maximiser l'impact de ces projets sur le développement numérique en France.

Megalys et câbles sous-marins

Megalys est-il interconnecté ou interconnectable avec des câbles sous-marins ?

Megalys en Bretagne peut potentiellement être interconnecté avec des câbles sous-marins, bien que cette interconnexion ne soit pas nécessairement une composante directe de son projet. Voici une analyse de la situation :

1. Importance des Câbles Sous-Marins

- **Connectivité Internationale** : Les câbles sous-marins sont essentiels pour assurer la connectivité Internet à haut débit entre les continents et les pays. Ils transportent la majorité du trafic de données international et sont cruciaux pour les infrastructures numériques modernes.
- **Réduction de la Latence** : En offrant des chemins directs pour les données, les câbles sous-marins peuvent réduire la latence, ce qui est particulièrement important pour des applications sensibles au temps, comme la vidéoconférence, le cloud computing, et les services en ligne.

2. Interconnexion Potentielle de Megalis

2.1 Infrastructure Régionale

- **Accès aux Câbles Sous-Marins** : Si la Bretagne est reliée à des câbles sous-marins, par exemple ceux qui desservent la côte atlantique française, Megalis pourrait bénéficier de cette connectivité pour améliorer l'accès aux services numériques dans la région.
- **Points de Peering** : Megalis pourrait envisager d'établir des points de peering avec des infrastructures qui utilisent ces câbles, permettant aux entreprises locales d'accéder directement à Internet à haut débit et à des services de cloud international.

2.2 Projets en Cours

- **Initiatives Locales** : Certaines initiatives locales ou régionales peuvent déjà travailler sur des projets visant à interconnecter des infrastructures régionales avec des câbles sous-marins. Cela pourrait inclure des collaborations avec des opérateurs de télécommunications pour tirer parti de la connectivité sous-marine.

3. Avantages de l'Interconnexion avec des Câbles Sous-Marins

- **Amélioration de la Connectivité** : L'interconnexion avec des câbles sous-marins renforcerait la connectivité d'un point de vue international et permettrait aux entreprises bretonnes d'accéder à des services numériques de manière plus rapide et efficace.
- **Soutien aux Startups et PME** : Une meilleure connectivité peut soutenir l'innovation et la croissance des startups et des PME en Bretagne, en leur permettant d'accéder à des marchés plus vastes et de bénéficier de services cloud performants.

4. Conclusion

Megalys peut être interconnecté ou interconnectable avec des câbles sous-marins, en fonction de l'infrastructure existante et des projets en cours dans la région. Cette interconnexion pourrait jouer un rôle clé dans l'amélioration de la connectivité numérique en Bretagne, soutenant le développement économique et la transformation numérique des entreprises locales. Pour un impact maximal, il serait judicieux de continuer à explorer des partenariats avec des opérateurs de télécommunications et d'autres acteurs pour faciliter cette interconnexion.

Megalys et les opérateurs internationaux

Megalys peut-il servir de plate-forme numérique pour des opérateurs régionaux ou internationaux pour développer leurs produits ?

Oui, **Megalys** peut potentiellement servir de plateforme numérique pour des opérateurs régionaux ou internationaux souhaitant développer et déployer leurs produits. Voici comment cela pourrait fonctionner et quels avantages cela pourrait offrir :

1. Infrastructure de Base

1.1 Réseau Très Haut Débit

- **Accessibilité** : Megalis met en place un réseau de fibre optique et d'autres infrastructures numériques qui offrent un accès à Internet très haut débit. Cela constitue une base solide pour les opérateurs cherchant à développer des produits numériques.
- **Connectivité** : La connexion rapide et fiable fournie par Megalis permet aux opérateurs d'exploiter efficacement leurs services en ligne et d'interagir avec leurs clients.

2. Plateforme pour le Développement de Produits

2.1 Environnement de Développement

- **Services Numériques** : Megalis pourrait offrir des services tels que des API, des plateformes cloud, ou des outils de développement pour aider les opérateurs à créer et à déployer leurs produits.
- **Soutien à l'Innovation** : En fournissant un cadre de collaboration, Megalis pourrait faciliter l'innovation et le développement de nouvelles solutions numériques par des opérateurs.

2.2 Collaboration avec les Startups

- **Accélération de l'Innovation** : Megalis peut collaborer avec des startups et des entreprises locales pour les aider à développer et à tester de nouveaux produits sur sa plateforme, favorisant ainsi un écosystème d'innovation.
- **Partenariats** : La plateforme pourrait également faciliter des partenariats entre opérateurs régionaux et entreprises technologiques pour co-développer des solutions.

3. Avantages pour les Opérateurs

3.1 Réduction des Coûts

- **Infrastructures Partagées** : Les opérateurs pourraient bénéficier de l'utilisation d'infrastructures partagées, ce qui peut réduire les coûts de développement et d'exploitation.
- **Accès à des Ressources** : En utilisant la plateforme Megalis, les opérateurs peuvent accéder à des ressources numériques, telles que des outils d'analyse et de gestion des données, sans avoir à investir dans des infrastructures coûteuses.

3.2 Accès au Marché

- **Opportunités Commerciales** : Megalis peut fournir une visibilité et un accès aux marchés locaux, permettant aux opérateurs de toucher de nouveaux clients dans la région.
- **Support aux Entreprises** : En soutenant les entreprises locales, Megalis peut également aider les opérateurs à établir des relations solides avec des clients et des partenaires potentiels.

4. Enjeux à Considérer

4.1 Sécurité et Confiance

- **Protection des Données** : Il est essentiel que Megalis assure la sécurité des données et la conformité avec les réglementations en matière de protection des données, ce qui est crucial pour gagner la confiance des opérateurs et des clients.
- **Transparence** : Offrir une transparence sur les services et les processus de développement est également important pour attirer des opérateurs.

4.2 Compétitivité

- **Attractivité de la Plateforme** : Megalis doit veiller à ce que ses services soient compétitifs par rapport à d'autres solutions disponibles sur le marché, tant au niveau régional qu'international.

5. Conclusion

Megalys a le potentiel de servir de plateforme numérique pour des opérateurs régionaux et internationaux cherchant à développer et déployer des produits. En offrant une infrastructure robuste, des services de soutien et un environnement collaboratif, Megalis peut faciliter l'innovation

et aider les opérateurs à atteindre de nouveaux marchés. Toutefois, pour maximiser cette opportunité, il est important de garantir la sécurité, la conformité et la compétitivité des services offerts.

Mégalis et la Normandie

La Normandie a mis en place plusieurs initiatives visant à renforcer son infrastructure numérique, bien que ces projets diffèrent de **Mégalis**, qui est spécifique à la Bretagne.

1. Normandie Connectée Innovante et Durable

La Région Normandie a lancé le programme **Normandie Connectée Innovante et Durable**, visant à faire de la Normandie un territoire de référence pour sa dynamique de développement numérique. Ce programme s'articule autour de deux axes principaux :

- **Équipement du territoire en ressources numériques** : Il s'agit de déployer des infrastructures numériques de qualité pour assurer une couverture optimale du territoire.
- **Transformation numérique des acteurs et des territoires** : Ce volet vise à accompagner les entreprises, les collectivités et les citoyens dans leur transition numérique, en favorisant l'innovation et l'accès aux services numériques.

2. Appel à projets "Normandie Connectée – nouveaux espaces de compétences – Deffinov"

Dans le cadre de ce programme, la Région a lancé un appel à projets intitulé "Normandie Connectée – nouveaux espaces de compétences – Deffinov". Cet appel vise à soutenir des projets portés par des collectifs regroupant des acteurs de la compétence et des tiers-lieux, afin de développer des services numériques innovants et durables.

3. Réseau des Espaces Publics Numériques (EPN) Normandie

La Normandie dispose également d'un réseau d'Espaces Publics Numériques (EPN) labellisés, offrant des services tels que l'accès à Internet, des ateliers informatiques et des espaces de coworking. Ces structures visent à accompagner les normands dans leurs usages numériques et à favoriser l'insertion professionnelle.

Conclusion : Bien que la Normandie ne dispose pas d'un projet équivalent à **Mégalis**, elle a mis en place des initiatives ambitieuses pour renforcer son infrastructure numérique et accompagner la transformation numérique de ses acteurs et territoires.

Sources :

- **Région Normandie** - *Normandie Connectée Innovante et Durable* normandie.fr
- **Normandie Connectée** - *Appel à projets "Normandie Connectée – nouveaux espaces de compétences – Deffinov"* normandie-connectee.fr
- **Normandie Connectée** - *Réseau des Espaces Publics Numériques (EPN) Normandie* normandie-connectee.fr

ERP

Les principaux acteurs

Quels sont les principaux acteurs de l'ERP ?

Google Gemini : Les principaux fournisseurs d'ERP en Europe et aux États-Unis :

En Europe:

- **SAP:** Leader mondial, SAP propose une gamme complète de solutions ERP, de la PME à la grande entreprise. Forte présence en Europe, notamment en Allemagne, son pays d'origine.
- **Oracle:** Autre géant du logiciel, Oracle offre des solutions ERP très complètes, souvent utilisées par les grandes entreprises.
- **Sage:** Spécialisé dans les PME et les ETI, Sage propose des solutions ERP modulaires et adaptables.
- **Microsoft Dynamics:** Intégré à l'écosystème Microsoft, Dynamics 365 offre une solution ERP cloud complète et évolutive.
- **Infor:** Connu pour ses solutions sectorielles (industrie, distribution...), Infor propose des ERP adaptés à des besoins spécifiques.
- **Odoo:** Solution open-source très flexible et personnalisable, idéale pour les entreprises qui souhaitent un ERP sur mesure.

Aux États-Unis:

SAP, Oracle, Microsoft Dynamics: Ces trois géants sont également très présents aux États-Unis, où ils proposent des solutions similaires à celles proposées en Europe.

- **NetSuite:** Solution cloud native, NetSuite est particulièrement populaire auprès des entreprises de croissance.
- **Workday:** Spécialisé dans les ressources humaines et la finance, Workday propose une solution cloud complète et moderne.
- **Epicor:** Connu pour ses solutions sectorielles (industrie manufacturière, distribution...), Epicor est un acteur important du marché américain.

ERP et souveraineté numérique

L'ERP relève-t-il de la souveraineté numérique ?

L'ERP (Enterprise Resource Planning) peut être considéré comme un aspect clé de la souveraineté numérique, et ce pour plusieurs raisons. Voici une analyse des liens entre les systèmes ERP et la souveraineté numérique :

1. Définition de la Souveraineté Numérique

La souveraineté numérique fait référence à la capacité d'un État ou d'une entité à contrôler et à gérer ses propres données, infrastructures numériques, et technologies de l'information, tout en respectant les réglementations et les lois en vigueur. Cela implique également le contrôle sur les processus, les systèmes et les informations au sein d'une organisation ou d'une région.

2. Rôle des ERP dans la Souveraineté Numérique

2.1 Gestion des Données Sensibles

- **Centralisation des Données** : Les ERP intègrent diverses fonctions d'une entreprise (finances, ressources humaines, production, etc.) et centralisent les données. Cela signifie que les données sensibles, y compris les informations clients et les données financières, sont stockées et gérées au sein d'un même système.
- **Contrôle des Données** : Avoir un ERP sous contrôle local (par exemple, hébergé sur des serveurs internes ou dans un cloud souverain) permet à une organisation de garantir que ses données ne sont pas soumises à des lois ou des réglementations étrangères qui pourraient compromettre la confidentialité ou la sécurité.

2.2 Conformité aux Réglementations

- **Réglementations sur la Protection des Données** : Les entreprises doivent se conformer à des réglementations telles que le RGPD en Europe, qui impose des exigences strictes sur la gestion des données personnelles. Les systèmes ERP doivent être conçus pour répondre à ces exigences, ce qui est un aspect important de la souveraineté numérique.
- **Transparence et Traçabilité** : Les ERP permettent un suivi et une traçabilité des données, ce qui est essentiel pour garantir la conformité avec les réglementations et pour assurer la transparence vis-à-vis des parties prenantes.

2.3 Choix des Fournisseurs et Hébergement

- **Souveraineté sur les Fournisseurs** : Les entreprises peuvent choisir de travailler avec des fournisseurs d'ERP qui respectent les lois locales et les normes de sécurité, renforçant ainsi leur souveraineté numérique.
- **Hébergement Local** : En optant pour des solutions ERP hébergées localement ou dans un cloud souverain, les entreprises peuvent mieux contrôler l'accès à leurs données et éviter le verrouillage par des fournisseurs étrangers.

3. Défis Associés

3.1 Intégration avec des Systèmes Tiers

- **Interopérabilité** : Les ERP doivent souvent s'intégrer avec d'autres systèmes, y compris ceux basés à l'étranger. Cela peut poser des défis en matière de souveraineté si les données transitent par des infrastructures qui ne sont pas conformes aux exigences locales.

3.2 Coûts et Ressources

- **Investissement en Infrastructure** : Maintenir un système ERP sous contrôle local peut nécessiter des investissements significatifs en infrastructure et en ressources humaines pour assurer la sécurité et la mise à jour des systèmes.

Conclusion

Les systèmes ERP jouent un rôle crucial dans la souveraineté numérique, car ils permettent aux entreprises de gérer efficacement leurs données sensibles tout en garantissant la conformité avec les réglementations. Le choix de la solution ERP, de son hébergement, et de son intégration avec d'autres systèmes sont des facteurs clés pour assurer la souveraineté numérique des organisations. Cependant, les entreprises doivent également être conscientes des défis associés à l'intégration et à l'investissement nécessaire pour maintenir cette souveraineté.

IA (Intelligence artificielle)

Définition

L'intelligence artificielle (IA) désigne un ensemble de technologies et de systèmes informatiques capables d'effectuer des tâches qui nécessitent normalement l'intelligence humaine. Cela inclut la capacité d'apprendre, de raisonner, de résoudre des problèmes, de comprendre le langage naturel, et de percevoir des informations à partir d'images ou de sons. L'IA peut être classée en deux catégories principales :

1. **IA Faible (ou IA étroite)** : Conçue pour effectuer des tâches spécifiques (par exemple, les assistants vocaux, les recommandations de produits, ou les systèmes de reconnaissance d'images).
2. **IA Forte** : Une forme hypothétique d'IA qui pourrait comprendre, apprendre et appliquer des connaissances de manière générale, comparable à l'intelligence humaine.

Les techniques couramment utilisées dans l'IA incluent l'apprentissage automatique (machine learning), l'apprentissage profond (deep learning), et le traitement du langage naturel (NLP). L'IA est utilisée dans de nombreux domaines, tels que la santé, la finance, l'industrie, et les services, et transforme la manière dont les entreprises et les sociétés fonctionnent.

L'Union européenne

La France

Stratégie nationale pour l'intelligence artificielle

STRATÉGIE NATIONALE POUR L'INTELLIGENCE ARTIFICIELLE – 2^e phase

Conquérir les talents et transformer notre potentiel scientifique en succès économiques

<https://presse.economie.gouv.fr/wp-content/uploads/2021/11/8bcf2b43571df79a59055eab0cc5047e.pdf>



Ministère de l'Économie, des Finances et de l'Industrie
Ministère chargé du Budget et des Comptes publics



Rechercher

Accueil | Particuliers | Entreprises | Les ministres | Ministère

Accueil du portail > Actualités > France 2030 > La stratégie nationale pour l'intelligence artificielle

La stratégie nationale pour l'intelligence artificielle

22/05/2024

Depuis 2017, le Gouvernement a lancé une réflexion autour du développement de l'intelligence artificielle. Celle-ci prend la forme d'une stratégie nationale, divisée en deux phases entre 2018 et 2025. Présentation.

La France aux avant-postes !

Les atouts de la France dans l'IA

- Une **école mathématique** mondialement reconnue
- De nombreux chercheurs français parmi les **stars mondiales de la discipline**
- **Le plus grand nombre de laboratoires IA** parmi les pays européens (81)
- Un **écosystème entrepreneurial** en dynamique croissante
- Des **grandes entreprises** particulièrement sensibilisées aux enjeux de l'IA

Objectifs clés

- **Faire monter la nation en compétences**
- **Faire de la France un leader dans les domaines de l'IA embarquée et de l'IA de confiance**
- **Accélérer le déploiement de l'IA dans l'économie**

IA embarquée : smartphones, véhicules, robots...

Indicateurs de succès à 2025

Compétences et talents

- Former et financer une cible d'au moins 2000 étudiants en DUT / licence / licence pro, 1500 étudiants en master et 200 thèses supplémentaires par an en régime de croisière
- Placer au minimum 1 établissement d'excellence dans les meilleurs rangs internationaux
- Recruter 15 scientifiques étrangers d'envergure mondiale d'ici janvier 2024

IA embarquée, frugale et de confiance

- Capturer de 10 à 15% des parts du marché mondial de l'IA embarquée à horizon 2025 et faire de la France un leader mondial dans le domaine
- Soutenir 10 projets d'IA de démonstrateurs ou de développement technologique d'IA frugale
- Lancer 4 démonstrateurs d'usages de l'IA dans les verticales prioritaires que sont l'automobile, l'aéronautique, l'industrie 4.0 et l'énergie d'ici fin 2022
- Livrer 3 à 4 plateformes logicielles interopérables multi-acteurs, d'envergure européenne, dans les domaines de l'IA embarquée ou décentralisée et de l'IA de confiance

IA de confiance : <https://www.confiance.ai/> (= IA "éthique")

Rapport Vilani

Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne,
Auteur(s) : Cédric Villani ; Marc Schoenauer ; Yann Bonnet ; Charly Berthet ; Anne-Charlotte Cornut ; François Levin ; Bertrand Rondepierre

<https://www.vie-publique.fr/files/rapport/pdf/184000159.pdf>

La Bretagne

Analyse SWOT de la filière IA

Analyse SWOT

...de la filière IA / data science bretonne

■ caractéristiques fournisseurs

○ caractéristiques utilisateurs

► caractéristiques communes

FORCES

- Des **compétences pointues** sur certains maillons de la chaîne IA/data science et des **marchés applicatifs** de prédilection solides
- Une **stratégie** d'adoption par anticipation et une attention à la dimension éthique des projets
- La recherche de collaborations avec la recherche

OPPORTUNITES

- Capitaliser sur la démarche réussie de la **filière cybersécurité** et les synergies avec l'IA/data science
- Exploiter le levier de la dynamique européenne sur le sujet (projets, stratégie européenne de la donnée...)
- Développer des synergies entre « l'IA pour la gouvernance et les citoyens » et le **développement d'une filière économique en Bretagne**, (ex : utilisation de la commande publique comme levier)
- Exploiter l'excellence bretonne sur certains champs d'IA pour adresser de **nouveaux marchés** à fort potentiel

FAIBLESSES

- Un **petit tissu d'entreprises** fournisseuses peu valorisé
- Un manque de prise en compte des **dimensions éthiques** dans les projets d'IA
- Des **marchés d'applications à consolider et étendre**
- Un faible nombre d'entreprises engagées concrètement dans l'IA/Data science

MENACES

- Un **risque de décrochage** si les fournisseurs n'intègrent pas dès maintenant le champ réglementaire (ex : directives EU)
- Une **utilisation captive des outils propriétaires** non européens
- Un **risque de décrochage** des entreprises qui n'auront pas saisi l'opportunité d'exploiter le potentiel de l'IA
- Une utilisation non éclairée de l'IA/data science enfouie dans les fonctionnalités des logiciels métiers

Observatoire de l'intelligence artificielle et de la datascience en Bretagne



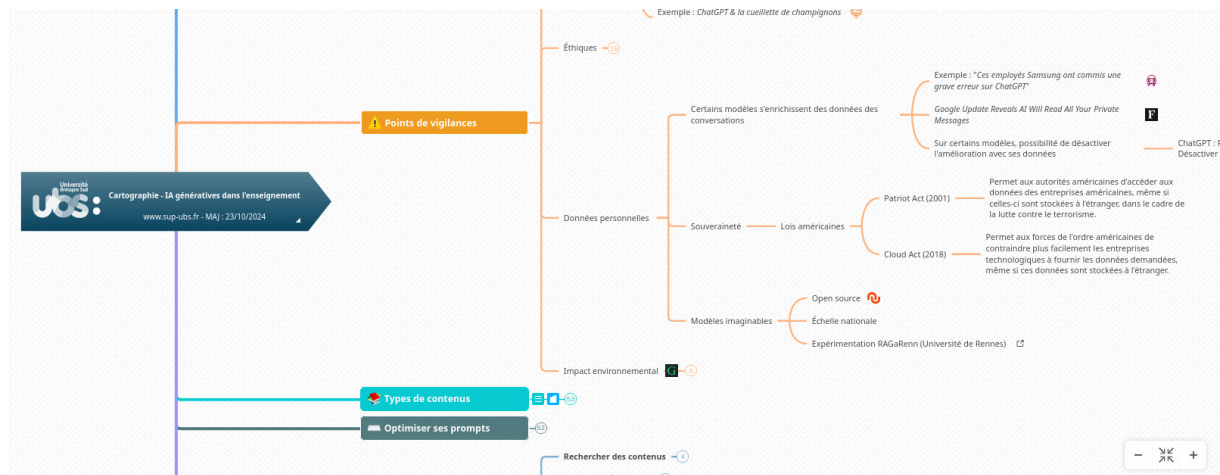
<https://tools.bdi.fr/Etudes/IA/accueil.htm>

Acteurs

Quelques acteurs (liste non exhaustive)

- SequoIA <https://actu.univ-rennes.fr/actualites/le-projet-sequoia-ia-cluster-confiance-et-securite-labellise-pole-dexcellence-en>
- LabSTICC <https://labsticc.fr/fr/lab-sticc/presentation>
- IRISA <https://www.irisa.fr/umr-6074> valorisation@irisa.fr
- <https://www.irisa.fr/equipes/kerdata> Gabriel ANTONIU
- <https://www.irisa.fr/ia-intelligence-artificielle> <http://www.irisa.fr/lande/ridoux/>
- UBS :
- <https://www.univ-ubs.fr/fr/nos-domaines-d-excellence/cyber-intelligence-des-donnees/intelligence-artificielle.html>

<https://www-actus.univ-ubs.fr/fr/index/articles-chroniques/sup/l-intelligence-artificielle-au-service-de-l-enseignement.html>



<https://www.mindomo.com/fr/mindmap/ia-generatives-dans-lenseignement-afe76157fc7d4d3e99d300cbe75596a1>

Pays-de-la Loire

DIVA, pour le développement d'une intelligence artificielle

Les Chambres de Commerce et d'Industrie des Pays de la Loire accompagnent les entreprises de la région dans leur transition digitale.

<https://www.paysdelaloire.cci.fr/diva-pour-le-developpement-dune-intelligence-artificielle>

<https://www.paysdelaloire-eco.fr/ressources-analyses/lintelligence-artificielle/>

Les pionniers

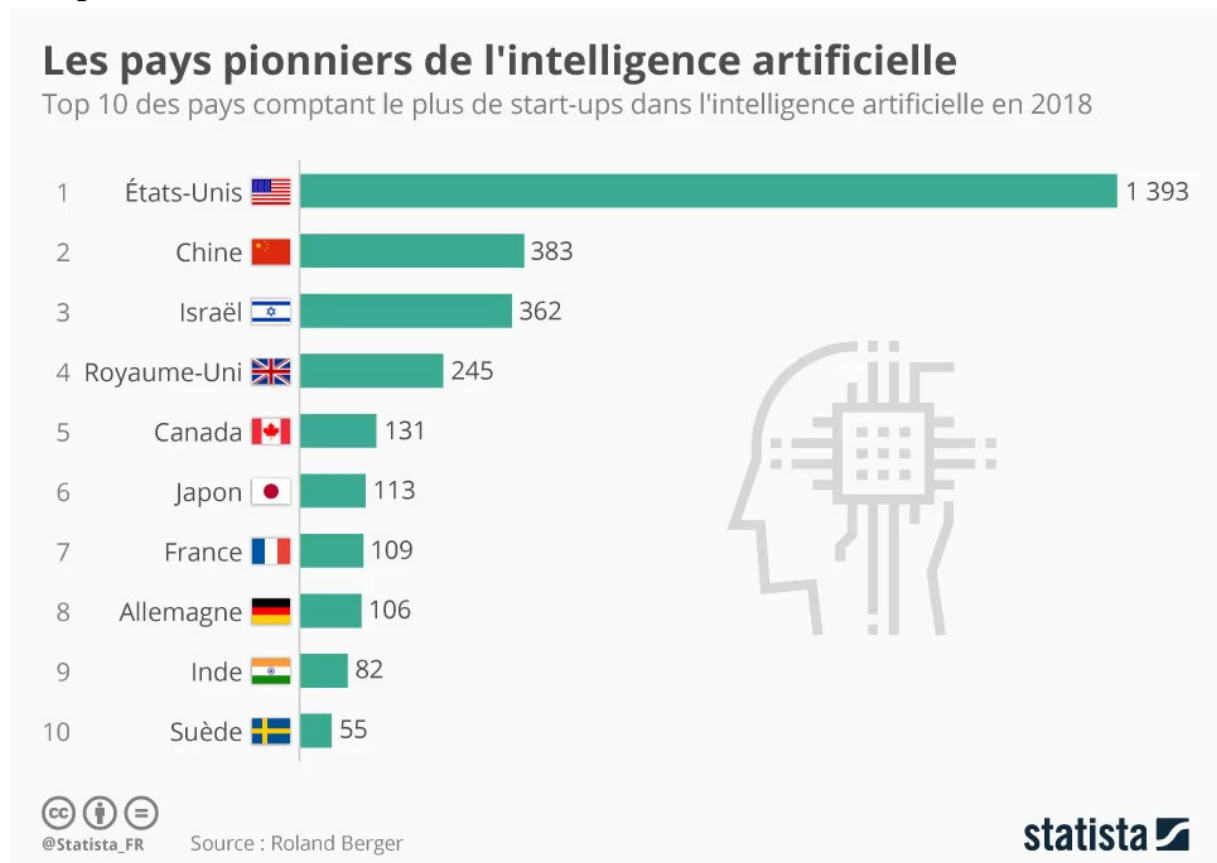


Figure 8 – Les pionniers

AI startups as innovations drivers: Europe must take action to establish a competitive ecosystem (<https://www.rolandberger.com/en/Media/AI-startups-as-innovations-drivers-Europe-must-take-action-to-establish-a-2.html>)

AI strategy for European startups

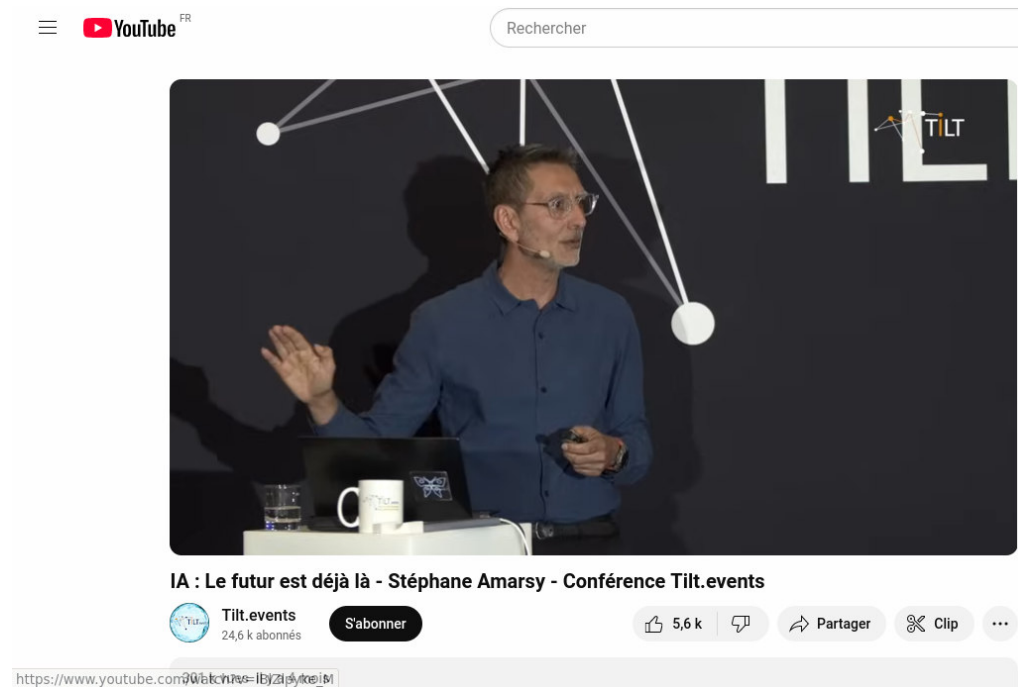
https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf

Les évolutions prévisibles

L'Intelligence artificielle connaît des progrès fulgurants et va encore en connaître davantage. Les applications sont immenses et de nombreuses activités humaines vont être impactées. Les progrès reposeront sur :

- les données
- les Algorithmes
- la puissance de calcul (les microprocesseurs)

A titre d'exemple : <https://www.youtube.com/watch?v=4619HLxbV2A>



L'IA proprement dit et ses domaines d'application :

IA : Le futur est déjà là - Stéphane Amarsy - Conférence Tilt.events

LA CANNIBALISATION DE L'IA

Annonce le 7/12/23 par le gouvernement du Royaume Uni

Exposure to all AI applications	Exposure to large language modelling
1 Management consultants and business analysts*	Telephone salespersons
2 Financial managers and directors	Solicitors*
3 Chartered and certified accountants	Psychologists*
4 Psychologists*	Further education teaching professionals
5 Purchasing managers and directors	Market and street traders and assistants
6 Actuaries, economists and statisticians	Legal professionals n.e.c.*
7 Business and financial project management professionals	Credit controllers*
8 Finance and investment analysts and advisers	Human resource administration occupations*
9 Legal professionals n.e.c.*	Public relations professionals
10 Business and related associate professionals n.e.c.	Management consultant and business analysts*
11 Credit controllers*	Market research interviewers
12 Solicitors*	Local government administrative occupations
13 Civil engineers	Clergy
14 Education advisers and school inspectors*	Higher education teaching professionals
15 Human resources administrative occupations*	Collector salespersons and credit agents
16 Business, research and administrative professionals n.e.c.	Education advisers and school inspectors*
17 Financial accounts managers	Human resource managers and directors
18 Bookkeepers, payroll managers and wages clerks	National government administrative occupations*
19 National government administrative occupations*	Vocational and industrial trainers and instructors
20 Marketing associate professionals	Social and humanities scientists

56:44 / 1:05:11

Faites défiler la page pour afficher plus de détails

Les futures ruptures

Quelles sont les perspectives de nouvelles ruptures en IA ?

Les perspectives de nouvelles ruptures en intelligence artificielle (IA) sont nombreuses et couvrent divers domaines d'application, de recherche et d'impact sociétal. Voici quelques-unes des tendances et des développements potentiels qui pourraient conduire à des ruptures significatives dans le domaine de l'IA dans les années à venir :

1. Améliorations de l'Apprentissage Automatique (Machine Learning)

- **Modèles de Plus en Plus Sophistiqués** : Les avancées dans les architectures de modèles, comme les réseaux neuronaux profonds et les modèles de transformer, continuent de produire des systèmes d'IA capables d'apprendre et de généraliser à partir de données de manière plus efficace.
- **Apprentissage Auto-Supervisé et Non Supervisé** : Ces techniques permettent à l'IA d'apprendre à partir de données non étiquetées, réduisant ainsi le besoin de grandes quantités de données annotées, ce qui pourrait élargir les applications de l'IA à de nouveaux domaines.

2. IA Générative et Créativité

- **Création de Contenus** : Les modèles d'IA générative, tels que GPT-4 ou DALL-E, révolutionnent la création de contenu, de la rédaction à la génération d'images, et même à la composition musicale. Ces technologies pourraient transformer des industries créatives comme le cinéma, la musique, et le design graphique.
- **Applications dans le Design et la Prototypage** : L'IA générative pourrait être utilisée pour concevoir de nouveaux produits, optimiser des designs, ou même créer des prototypes physiques via l'impression 3D.

3. Interactions Humain-IA Améliorées

- **Agents Conversationnels Avancés** : Les progrès en traitement du langage naturel (NLP) permettront de développer des assistants virtuels plus intelligents et empathiques, capables de comprendre et de répondre aux émotions humaines.
- **Interfaces Cognitives** : Les technologies d'interface cerveau-ordinateur (BCI) pourraient permettre une interaction directe entre le cerveau humain et les systèmes d'IA, ouvrant la voie à des applications dans la médecine, le divertissement et d'autres domaines.

4. IA dans le Domaine de la Santé

- **Diagnostics Prédicatifs** : L'IA pourrait révolutionner le diagnostic médical en analysant des données de santé massives pour identifier des maladies à un stade précoce, personnalisant ainsi les traitements pour chaque patient.
- **Découverte de Médicaments** : Les algorithmes d'IA peuvent accélérer la découverte de nouveaux médicaments en simulant et en analysant les interactions moléculaires, ce qui pourrait conduire à des traitements plus efficaces.

5. Automatisation et Robotique Avancées

- **Robots Autonomes** : Les avancées en IA permettront de développer des robots autonomes capables de naviguer dans des environnements complexes, d'effectuer des tâches variées, et d'interagir avec les humains de manière naturelle.
- **Automatisation des Industries** : L'IA continuera à transformer les chaînes d'approvisionnement, la fabrication, et d'autres secteurs en automatisant des processus et en améliorant l'efficacité.

6. Éthique et Régulation de l'IA

- **Régulations Émergentes** : Avec la montée des préoccupations éthiques et des risques associés à l'IA, des cadres réglementaires plus stricts pourraient émerger, influençant le développement et l'application de technologies IA.
- **IA Responsable** : Les efforts pour développer des IA éthiques et responsables, prenant en compte des principes tels que la transparence, l'équité, et la protection des données, pourraient devenir des normes clés dans l'industrie.

7. IA et Développement Durable

- **Optimisation des Ressources** : L'IA peut jouer un rôle crucial dans l'optimisation de l'utilisation des ressources dans des secteurs comme l'agriculture, l'énergie, et les transports, contribuant ainsi à des objectifs de durabilité.

Lutte contre le Changement Climatique : Des modèles prédictifs basés sur l'IA pourraient aider à modéliser et à atténuer les effets du changement climatique en améliorant la gestion des énergies renouvelables et des ressources naturelles.

Résumé

Les perspectives de nouvelles ruptures en intelligence artificielle sont vastes et variées, allant des avancées technologiques dans l'apprentissage automatique à des applications révolutionnaires dans la santé, la créativité, et l'automatisation. Cependant, ces développements s'accompagnent de défis éthiques et réglementaires qui devront être abordés pour garantir que l'IA soit utilisée de manière responsable et bénéfique pour la société. La manière dont ces tendances évolueront dépendra des recherches, des investissements, des politiques publiques et des collaborations entre les secteurs public et privé.

Conditions du positionnement favorables pour les prochaines ruptures

Quels sont les conditions (intellectuelles, universitaires, entrepreneuriales, réglementaires, budgétaires, matérielles, financières...) pour être positionné sur ces futures ruptures ?

Pour se positionner efficacement sur les futures ruptures en intelligence artificielle (IA) et dans d'autres technologies numériques, plusieurs conditions doivent être réunies dans différents domaines, notamment intellectuels, universitaires, entrepreneuriaux, réglementaires, budgétaires, matériels, et financiers. Voici une analyse de ces conditions :

1. Conditions Intellectuelles

- **Culture de l'Innovation** : Promouvoir une culture d'innovation au sein des entreprises et des institutions qui encourage la prise de risque, l'expérimentation, et l'apprentissage continu.
- **Formation et Sensibilisation** : Former les équipes à comprendre les enjeux et les opportunités liés à l'IA et aux technologies numériques, afin de stimuler la créativité et l'adoption de nouvelles idées.

2. Conditions Universitaires

- **Programmes Éducatifs Axés sur l'IA** : Développer des programmes universitaires en IA, machine learning, et data science, intégrant des compétences pratiques et théoriques.
- **Recherche et Développement** : Encourager les collaborations entre les universités et l'industrie pour favoriser la recherche appliquée et la création de prototypes innovants.
- **Partenariats Académiques** : Établir des partenariats entre les institutions académiques, les centres de recherche, et les entreprises pour partager des ressources, des connaissances et des infrastructures.

3. Conditions Entrepreneuriales

- **Écosystèmes d'Innovation** : Créer des écosystèmes d'innovation comprenant des incubateurs, des accélérateurs, et des espaces de co-working pour favoriser la collaboration entre startups, PME, et grandes entreprises.
- **Accès au Marché** : Faciliter l'accès des entreprises aux marchés en simplifiant les démarches administratives et en soutenant les initiatives d'exportation.
- **Culture de la Collaboration** : Encourager les collaborations intersectorielles pour développer des solutions innovantes et intégrées.

4. Conditions Réglementaires

- **Régulations Claires et Favorables** : Établir un cadre réglementaire clair qui encourage l'innovation tout en garantissant la protection des données, la sécurité, et l'éthique.
- **Soutien aux Initiatives Éthiques** : Promouvoir des réglementations qui encouragent le développement d'IA éthique et responsable, avec des principes de transparence et d'équité.
- **Harmonisation des Normes** : Travailler à l'harmonisation des normes et des réglementations au niveau national et international pour faciliter la coopération et le commerce.

5. Conditions Budgétaires et Financières

- **Investissements en R&D** : Allouer des budgets suffisants à la recherche et au développement, tant au niveau public que privé, pour stimuler l'innovation.
- **Financement des Startups** : Créer des mécanismes de financement, tels que des fonds de capital-risque, des subventions et des prêts, pour soutenir les startups et les PME innovantes.
- **Partenariats Publics-Privés** : Favoriser les partenariats entre le secteur public et le secteur privé pour partager les coûts et les risques associés au développement de nouvelles technologies.

6. Conditions Matérielles

- **Infrastructure Technologique** : Investir dans des infrastructures technologiques modernes, y compris des centres de données, des réseaux à haut débit, et des équipements de pointe pour soutenir le développement et le déploiement de solutions IA.
- **Accès aux Données** : Garantir un accès sécurisé et éthique aux données nécessaires à l'entraînement des modèles d'IA, tout en respectant les réglementations sur la protection des données.

7. Conditions de Compétence et de Main-d'œuvre

- **Formation de la Main-d'œuvre** : Développer des programmes de formation continue pour renforcer les compétences numériques de la main-d'œuvre existante et préparer les futurs professionnels aux défis de l'IA et des technologies numériques.
- **Attraction des Talents** : Mettre en place des politiques pour attirer et retenir des talents qualifiés dans le domaine de l'IA, tels que des chercheurs, des ingénieurs et des data scientists.

Résumé

Pour se positionner sur les futures ruptures en intelligence artificielle et dans d'autres technologies numériques, il est essentiel de réunir des conditions favorables dans les domaines intellectuels, universitaires, entrepreneuriaux, réglementaires, budgétaires, matériels et financiers. Cela nécessite une approche collaborative entre les secteurs public et privé, un soutien à l'innovation et à la recherche, ainsi que la création d'infrastructures et de politiques favorables à la croissance de l'écosystème numérique. En intégrant ces éléments, les pays et les entreprises peuvent mieux naviguer dans un paysage technologique en constante évolution et saisir les opportunités offertes par les ruptures à venir.

Politiques publiques américaines versus politiques publiques européennes pour l'IA

Pour bien gérer ces ruptures, les politiques publiques américaines semblent plus adaptées que les politiques publiques européennes : pourquoi ?

Les politiques publiques américaines sont souvent perçues comme étant plus adaptées à la gestion des ruptures technologiques que celles de l'Union européenne (UE) pour plusieurs raisons. Voici un aperçu des facteurs qui contribuent à cette perception :

1. Approche Axée sur l'Innovation

1.1 Flexibilité Réglementaire

- **Moins de Régulations** : Les États-Unis ont traditionnellement adopté une approche moins réglementée en matière d'innovation technologique. Cela permet aux entreprises de se développer rapidement et de tester de nouveaux produits et services sans faire face à des contraintes réglementaires lourdes.
- **Encouragement de l'Entrepreneuriat** : La culture entrepreneuriale aux États-Unis favorise la création de startups et l'expérimentation, permettant aux nouvelles technologies d'émerger rapidement et d'être commercialisées.

1.2 Support Institutionnel

- **Agences de Financement** : Des institutions comme la **National Science Foundation (NSF)** et la **Defense Advanced Research Projects Agency (DARPA)** jouent un rôle clé dans le financement de la recherche et développement, soutenant des projets innovants qui peuvent conduire à des ruptures technologiques.

2. Culture de l'Innovation et du Risque

2.1 Acceptation du Risque

- **Culture du Risque** : Les entreprises américaines sont généralement plus disposées à prendre des risques, tant en matière de financement que de développement de nouveaux produits. Cette culture favorise l'innovation rapide et la disruption des marchés existants.
- **Échec comme Apprentissage** : L'échec est souvent considéré comme une étape normale dans le processus d'innovation aux États-Unis, ce qui encourage les entrepreneurs à innover sans crainte de répercussions.

3. Infrastructure Technologique

3.1 Écosystèmes Technologiques

- **Silicon Valley et Autres Pôles** : Les États-Unis possèdent des écosystèmes technologiques matures, comme la Silicon Valley, qui rassemblent des entrepreneurs, des investisseurs, des universités et des entreprises. Ces écosystèmes favorisent l'innovation par la collaboration et le partage de ressources.
- **Investissements en R&D** : Les entreprises américaines investissent massivement dans la recherche et développement, ce qui permet de rester à la pointe des avancées technologiques.

4. Adaptabilité des Politiques

4.1 Politiques de Régulation Adaptables

- **Réponses Rapides** : Les agences gouvernementales américaines peuvent souvent réagir plus rapidement aux changements technologiques en adaptant les réglementations et en créant des cadres réglementaires spécifiques pour les nouvelles technologies.

- **Tests Réglementaires (Regulatory Sandboxes)** : Certaines agences permettent des "sandboxes" réglementaires qui permettent aux entreprises de tester des innovations dans un environnement contrôlé avant de les déployer à grande échelle.

5. Comparaison avec l'Union Européenne

5.1 Approche Plus Prudente

- **Régulations Strictes** : L'UE a une approche plus prudente et réglementée, cherchant à protéger les droits des consommateurs et la vie privée, comme en témoignent des régulations comme le RGPD. Bien que cela soit important, cela peut également ralentir l'innovation.
- **Consensus Nécessaire** : La prise de décision au sein de l'UE nécessite souvent un consensus entre les États membres, ce qui peut rendre le processus plus lent et plus complexe en matière d'adaptation aux nouvelles technologies.

5.2 Divergences d'Intérêts

- **Intérêts Nationaux Variés** : Les États membres de l'UE peuvent avoir des priorités et des intérêts divergents, ce qui complique la mise en place de politiques communes favorables à l'innovation technologique.

Résumé

Les politiques publiques américaines sont souvent perçues comme plus adaptées à la gestion des ruptures technologiques en raison de leur flexibilité réglementaire, de leur culture de l'innovation et du risque, et de leurs écosystèmes technologiques matures. En revanche, les politiques publiques de l'Union européenne, bien que protectrices et axées sur les droits des consommateurs, peuvent parfois ralentir l'innovation en raison de leur approche plus prudente et de la nécessité de consensus parmi les États membres. Cela ne signifie pas que les politiques européennes ne peuvent pas évoluer pour favoriser davantage l'innovation, mais elles devront trouver un équilibre entre la régulation et la promotion de l'innovation pour répondre aux défis technologiques à venir.

Une exception Mistral AI ?

Pour ces ruptures, l'Union européenne semblent souffrir d'un retard difficile à rattraper. Une exception pourrait être celle de Mistral AI (votre concurrente) qui semble se positionner comme un acteur comparable à Open AI, Google Gemini et autres : est-ce bien le cas ?

Mistral AI est effectivement une startup européenne qui a suscité un intérêt considérable en raison de son positionnement dans le domaine de l'intelligence artificielle, en particulier dans le développement de modèles d'IA avancés. Voici un aperçu de Mistral AI et de son positionnement par rapport à d'autres acteurs majeurs de l'IA, tels qu'OpenAI et Google Gemini :

1. Positionnement de Mistral AI

1.1 Objectifs et Produits

- **Modèles de Langage** : Mistral AI développe des modèles de langage similaires à ceux d'OpenAI (comme GPT) et de Google (Gemini). L'objectif est de créer des systèmes d'IA capables de comprendre et de générer du langage naturel de manière efficace et pertinente.
- **Focus sur l'IA Éthique et Responsable** : Mistral AI s'engage à développer des technologies d'IA de manière éthique, en mettant l'accent sur la transparence, la sécurité et la conformité avec les réglementations européennes, notamment le RGPD.

1.2 Écosystème Européen

- **Soutien à l'Innovation Locale** : En tant qu'entreprise basée en Europe, Mistral AI contribue à renforcer l'écosystème d'IA en Europe et à diminuer la dépendance vis-à-vis des géants technologiques américains.
- **Collaborations et Partenariats** : Mistral AI collabore avec des universités et des institutions de recherche pour favoriser l'innovation et le développement de nouvelles technologies.

2. Comparaison avec OpenAI et Google Gemini

2.1 Capacités Technologiques

- **Modèles d'IA Avancés** : Comme OpenAI et Google, Mistral AI vise à développer des modèles de traitement du langage naturel qui rivalisent en termes de performances et de capacité d'apprentissage.
- **Infrastructure et Ressources** : OpenAI et Google disposent de ressources considérables pour le développement et l'entraînement de leurs modèles, ce qui leur permet de mener des recherches à grande échelle. Mistral AI, bien que prometteuse, devra continuer à sécuriser des financements et des ressources suffisantes pour maintenir un rythme de développement compétitif.

2.2 Marché et Adoption

- **Adoption par les Entreprises** : OpenAI et Google ont déjà une forte adoption de leurs technologies par les entreprises et les développeurs à travers le monde. Mistral AI devra travailler sur sa visibilité et ses partenariats pour s'imposer sur le marché.
- **Dynamique de Concurrence** : Le paysage de l'IA est très compétitif, avec de nombreux acteurs, y compris des startups et des entreprises établies, qui cherchent à innover et à capturer des parts de marché. Mistral AI doit donc se différencier et prouver la valeur ajoutée de ses solutions.

3. Défis et Perspectives

3.1 Rattrapage du Retard

- **Accès aux Données** : L'accès à des données de qualité pour l'entraînement des modèles est crucial. Mistral AI devra s'assurer d'avoir des partenariats solides pour l'accès à des ensembles de données diversifiés.
- **Ressources Financières** : Lever des fonds et investir dans la recherche et le développement est essentiel pour soutenir l'innovation à long terme.

3.2 Éthique et Régulation

- **Conformité avec les Régulations** : En tant qu'entreprise européenne, Mistral AI doit naviguer dans un cadre réglementaire plus strict, mais cela peut aussi être un avantage concurrentiel si elle réussit à intégrer des normes éthiques dès le départ.
- **Perception de l'IA** : Travailler sur des initiatives de sensibilisation et de transparence peut aider à bâtir la confiance des utilisateurs et des entreprises vis-à-vis de ses technologies.

Conclusion : Mistral AI se positionne comme un acteur prometteur dans le domaine de l'intelligence artificielle en Europe, avec un potentiel de concurrence face à des géants comme OpenAI et Google Gemini. Bien que des défis subsistent, notamment en matière de ressources, d'adoption et de concurrence, Mistral AI pourrait jouer un rôle clé dans le développement de solutions d'IA éthiques et responsables, tout en contribuant à l'autonomie numérique de l'Europe. La dynamique du marché et l'engagement à innover de manière éthique seront essentiels pour sa réussite future.

La sécurité

Echelon

Les Etats-Unis et la Grande-Bretagne (qui a quitté l'Union européenne) ont mis en place le système de renseignement électronique et numérique Echelon qui espionne les gouvernements, les entreprises et les citoyens européens.

Source : ARTE, *Echelon, le pouvoir secret* (<https://www.youtube.com/watch?v=cX0q-yFFQrQ>).

Question : l'Union européenne a-t-elle mis fin ou peut-elle mettre fin à Echelon ?

Réponses : oui / non / NSP

Microsoft Cowdstrike

Une panne mondiale a frappé les systèmes Microsoft le 19 juillet 2024. L'incident, provoqué par une mise à jour de l'antivirus CrowdStrike, a paralysé de nombreux secteurs : aéroports, médias, Bourses. Des écrans bleus sont apparus sur les ordinateurs d'entreprises utilisant Windows et les solutions Microsoft 365. Quelle leçon tirer de cet événement ?

L'incident du 19 juillet 2024, causé par une mise à jour de l'antivirus CrowdStrike qui a perturbé les systèmes Microsoft, met en évidence plusieurs leçons cruciales sur la dépendance aux solutions centralisées et l'importance de la résilience numérique. Voici les principaux enseignements :

1. Vulnérabilité des systèmes centralisés et dépendance à un fournisseur unique :

La panne a révélé les risques liés à la dépendance envers un fournisseur unique pour des services critiques, en l'occurrence Microsoft pour les systèmes d'exploitation et les suites bureautiques. Lorsqu'une mise à jour défectueuse affecte une infrastructure si centralisée, l'impact est massif, touchant des secteurs divers et sensibles. Une diversification des outils technologiques, avec des alternatives viables à Microsoft, peut réduire le risque d'arrêt global.

2. Importance de la résilience et de la continuité d'activité :

Les organisations doivent évaluer et renforcer leurs plans de continuité d'activité (PCA), en incluant des systèmes de secours et des protocoles d'urgence en cas de panne. Cela peut inclure des sauvegardes régulières, des moyens de communication alternatifs, des solutions de cloud hybride, et des versions de secours pour des services critiques. Les entreprises doivent être prêtes à continuer leurs opérations sans interruption, même en cas de dysfonctionnement des principaux fournisseurs.

3. Repenser la cybersécurité et les mises à jour :

Cet incident montre que même des mises à jour de sécurité, conçues pour protéger les systèmes, peuvent accidentellement causer des dysfonctionnements majeurs. Les entreprises peuvent envisager d'adopter des stratégies de mise à jour progressive ou différée pour tester les nouvelles versions avant leur déploiement global. Des outils comme les environnements de test peuvent être essentiels pour détecter les éventuels effets secondaires d'une mise à jour avant qu'elle ne soit appliquée à l'échelle de l'organisation.

4. Évaluation des solutions de sauvegarde et de secours basées sur le cloud :

La dépendance aux outils en ligne de Microsoft, comme Microsoft 365, qui regroupe emails, documents, et autres services, a montré la fragilité des entreprises sans accès à des solutions alternatives de travail. Un modèle de cloud hybride ou une redondance des services, où certaines

fonctionnalités clés sont disponibles hors ligne ou via des fournisseurs alternatifs, peut atténuer l'impact d'une telle panne.

5. Formation à la gestion de crise et sensibilisation des utilisateurs :

La résilience repose aussi sur la capacité des utilisateurs à réagir efficacement. Une formation régulière des équipes à la gestion de crise technologique peut réduire les temps d'arrêt et améliorer la coordination lors de pannes globales. Savoir passer temporairement à d'autres outils ou à des méthodes de travail manuelles en cas de besoin peut être déterminant pour la continuité des opérations.

En conclusion, cette panne mondiale est un rappel des risques associés à la centralisation des infrastructures technologiques et de la nécessité pour les entreprises d'intégrer la résilience, la diversité des outils, et des protocoles de continuité robustes pour parer aux interruptions de service. Une approche proactive et diversifiée peut limiter les effets d'un tel incident et garantir une meilleure stabilité numérique pour l'avenir.

Faut-il rompre totalement avec Microsoft ?

Oui / non : NSP

Le droit et la réglementation du numérique

Code is law⁷.

Lawrence Lessig

UE : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fr

Le RGPD

Le Règlement Général sur la Protection des Données (RGPD), entré en vigueur le 25 mai 2018, est souvent considéré comme une initiative majeure de l'Union européenne pour protéger la vie privée des individus dans le monde numérique. Voici une évaluation de son succès, en considérant ses impacts positifs, ses défis, et ses implications globales :

1. Objectifs du RGPD

1.1 Protection des Données Personnelles

- **Renforcement des Droits des Individus** : Le RGPD vise à renforcer les droits des individus en matière de protection de leurs données personnelles, en leur donnant plus de contrôle sur la manière dont leurs données sont collectées, stockées, et utilisées.
- **Responsabilité des Organisations** : Les organisations doivent se conformer à des normes strictes pour la gestion des données, y compris la notification des violations de données et la mise en œuvre de mesures de sécurité appropriées.

1.2 Harmonisation Réglementaire

Uniformisation des Règles : Le RGPD a pour but d'harmoniser les lois sur la protection des données à travers l'UE, en fournissant un cadre uniforme qui facilite la conformité pour les entreprises opérant dans plusieurs États membres.

2. Réussites du RGPD

2.1 Amélioration des Pratiques de Protection des Données

- **Sensibilisation Accrue** : Le RGPD a sensibilisé les entreprises et les citoyens à l'importance de la protection des données personnelles, entraînant une meilleure gestion des données et une prise de conscience accrue des droits en matière de confidentialité.
- **Meilleures Pratiques de Conformité** : De nombreuses organisations ont amélioré leurs pratiques en matière de sécurité des données, de gestion des consentements, et de transparence pour se conformer aux exigences du RGPD.

2.2 Impact Global

- **Modèle de Référence** : Le RGPD est devenu un modèle de référence pour les législations sur la protection des données dans d'autres régions, comme la Californie avec le CCPA (California Consumer Privacy Act) et d'autres pays qui s'inspirent du RGPD pour élaborer leurs propres réglementations.
- **Renforcement des Droits des Consommateurs** : Il a renforcé les droits des consommateurs à l'échelle mondiale, même au-delà des frontières de l'UE, car les entreprises mondiales doivent se conformer au RGPD lorsqu'elles traitent des données de citoyens européens.

⁷ And Architecture is politics...

3. Défis et Limites du RGPD

3.1 Mise en Œuvre et Conformité

- **Complexité et Coûts** : La mise en conformité avec le RGPD peut être complexe et coûteuse pour les entreprises, en particulier pour les PME qui peuvent avoir des difficultés à respecter toutes les exigences.
- **Incertitude Juridique** : Certaines entreprises ont signalé une incertitude juridique en ce qui concerne l'interprétation et l'application des règles du RGPD, notamment en ce qui concerne des aspects comme le consentement et le traitement des données transfrontalières.

3.2 Application et Sanctions

- **Incohérence dans l'Application** : L'application du RGPD peut varier d'un État membre à l'autre, ce qui peut entraîner des incohérences dans la manière dont les règles sont appliquées et respectées.
- **Nombre Limité de Sanctions** : Bien que des amendes significatives puissent être imposées, il y a eu des préoccupations concernant le nombre relativement limité d'amendes réellement appliquées jusqu'à présent. Cela peut suggérer que certaines entreprises continuent de fonctionner dans des zones grises ou en retard sur la conformité.

4. Impact Pratique

4.1 Sur les Entreprises

- **Innovation et Adaptation** : Certaines entreprises ont utilisé le RGPD comme une opportunité pour améliorer leurs pratiques en matière de gestion des données et renforcer la confiance des consommateurs.
- **Réactions des Entreprises** : D'autres ont rencontré des difficultés pour se conformer aux exigences du RGPD et ont exprimé des préoccupations concernant les coûts et les charges administratives associés.

4.2 Sur les Consommateurs

- **Amélioration des Droits** : Les consommateurs bénéficient d'un plus grand contrôle sur leurs données personnelles et d'une meilleure transparence concernant leur collecte et utilisation.
- **Renforcement de la Confiance** : Le RGPD a contribué à renforcer la confiance des consommateurs dans la manière dont leurs données sont traitées par les entreprises.

Résumé : Le RGPD peut être considéré comme une réussite en ce sens qu'il a significativement amélioré la protection des données personnelles, sensibilisé le public à la confidentialité, et influencé la législation mondiale en matière de protection des données. Il a introduit des droits renforcés pour les individus et a mis en place des normes rigoureuses pour les entreprises.

Cependant, le RGPD présente aussi des défis, notamment en termes de mise en œuvre complexe et de coûts pour les entreprises, ainsi que d'incohérences dans l'application des règles à travers les États membres. Le succès du RGPD continuera d'être évalué au fil du temps en fonction de son impact sur les pratiques des entreprises, les droits des consommateurs, et son influence internationale.

Globalement, le RGPD a marqué un tournant important dans la régulation de la protection des données personnelles, et ses effets devraient continuer à se faire sentir à mesure que les pratiques de conformité évoluent et que de nouvelles interprétations des règles émergent.

Pas de RGPD aux USA

Aux États-Unis, il n'existe pas de cadre réglementaire unique et centralisé équivalent au Règlement Général sur la Protection des Données (RGPD) de l'Union européenne. Cependant, plusieurs lois et règlements à différents niveaux (fédéral, étatique et sectoriel) traitent de la protection des données personnelles. Voici un aperçu des principales législations et initiatives aux États-Unis qui se comparent au RGPD :

1. California Consumer Privacy Act (CCPA)

- **Description** : La CCPA, entrée en vigueur en janvier 2020, est l'une des lois les plus significatives en matière de protection des données aux États-Unis. Elle accorde aux consommateurs californiens des droits spécifiques concernant leurs données personnelles, y compris le droit de savoir quelles données sont collectées, le droit de demander la suppression de ces données, et le droit de refuser la vente de leurs informations personnelles.
- **Comparaison avec le RGPD** : La CCPA partage certaines similitudes avec le RGPD, notamment en ce qui concerne les droits des consommateurs, mais elle est moins exhaustive et impose moins d'obligations aux entreprises.

2. Virginia Consumer Data Protection Act (VCDPA)

- **Description** : Adoptée en mars 2021, la VCDPA est une autre loi sur la protection des données qui s'applique aux résidents de la Virginie. Elle offre des droits similaires à ceux de la CCPA, tels que le droit d'accès, de correction et de suppression des données personnelles.
- **Comparaison avec le RGPD** : Bien que la VCDPA ait des principes similaires, elle est considérée comme moins stricte que le RGPD et ne couvre pas tous les types de données ou d'entreprises.

3. New York Privacy Act (proposition)

- **Description** : Bien que la New York Privacy Act n'ait pas encore été adoptée, elle propose des protections similaires à celles du RGPD, en offrant aux consommateurs des droits étendus sur leurs données personnelles.
- **Impact potentiel** : Si adoptée, cette loi pourrait renforcer considérablement la protection des données personnelles dans l'État de New York.

4. Health Insurance Portability and Accountability Act (HIPAA)

- **Description** : HIPAA, adopté en 1996, est une loi fédérale qui protège la confidentialité et la sécurité des informations médicales personnelles. Elle s'applique spécifiquement aux données de santé.
- **Comparaison avec le RGPD** : Bien qu'elle offre des protections solides pour les données de santé, HIPAA est limitée à ce secteur et ne couvre pas la protection des données personnelles dans d'autres domaines.

5. Children's Online Privacy Protection Act (COPPA)

- **Description** : COPPA impose des exigences spécifiques concernant la collecte d'informations personnelles auprès d'enfants de moins de 13 ans, notamment en exigeant le consentement des parents.
- **Comparaison avec le RGPD** : Bien qu'elle protège spécifiquement les données des enfants, COPPA est beaucoup plus restrictive dans son application et ne fournit pas une approche globale de la protection des données.

6. Loi sur la protection des données personnelles des consommateurs (propositions diverses)

- **Description** : Plusieurs États ont proposé ou adopté des lois sur la protection des données personnelles qui varient considérablement en termes de droits des consommateurs et d'obligations des entreprises.

- **Comparaison avec le RGPD** : Ces lois peuvent partager des caractéristiques avec le RGPD, mais souvent de manière fragmentaire, sans la cohérence et l'universalité du RGPD.

Conclusion

En résumé, bien qu'il n'existe pas de loi unique équivalente au RGPD aux États-Unis, plusieurs lois étatiques et fédérales abordent la protection des données personnelles. Ces lois, telles que la CCPA et la VCDPA, établissent des droits pour les consommateurs, mais elles manquent souvent de l'universalité et de la rigueur du RGPD. Cela crée un paysage réglementaire fragmenté, où les protections des données varient considérablement d'un État à l'autre, ce qui pose des défis pour les entreprises qui opèrent à l'échelle nationale.

Question : la réglementation européenne est-elle un frein ou un accélérateur du numérique dans l'Union européenne ?

Réponses : un frein / un accélérateur / NSP

La justice

Le RGPD

Le RGPD (Règlement Général sur la Protection des Données) a conduit à l'imposition de plusieurs amendes depuis son entrée en vigueur le 25 mai 2018. Ces amendes visent à encourager la conformité avec les règles de protection des données et à sanctionner les violations. Voici un aperçu des amendes notables imposées sous le RGPD et de leur impact :

1. Amendes Notables Imposées sous le RGPD

1.1 Google (France) - 50 Millions d'Euros

- **Date** : Janvier 2019
- **Motif** : La Commission Nationale de l'Informatique et des Libertés (CNIL) a infligé cette amende à Google pour manquement aux obligations de transparence et d'information concernant le traitement des données personnelles. L'affaire concernait le manque de clarté sur la manière dont Google collecte et utilise les données pour la publicité ciblée.

1.2 British Airways (Royaume-Uni) - 22 Millions d'Euros

- **Date** : Octobre 2020
- **Motif** : L'Information Commissioner's Office (ICO) a infligé cette amende pour une violation de données qui a exposé les informations personnelles de plus de 400 000 clients. L'infraction concernait le manquement aux mesures de sécurité appropriées.

1.3 Marriott International (Royaume-Uni) - 20 Millions d'Euros

- **Date** : Octobre 2020
- **Motif** : L'ICO a imposé cette amende à Marriott pour une violation de données qui a compromis les informations personnelles de millions de clients. L'enquête a révélé des défaillances dans les pratiques de sécurité des données après la fusion avec Starwood.

1.4 H&M (Allemagne) - 35.3 Millions d'Euros

- **Date** : Octobre 2020
- **Motif** : L'amende a été infligée pour la collecte et la gestion illégales de données personnelles des employés. H&M avait mis en place un système de surveillance qui collectait des informations détaillées sur les employés, ce qui était contraire aux exigences du RGPD.

1.5 Amazon (Luxembourg) - 746 Millions d'Euros

- **Date** : Juillet 2021
- **Motif** : La Commission Nationale pour la Protection des Données (CNPD) du Luxembourg a infligé cette amende pour des violations liées à la manière dont Amazon collecte et utilise les données personnelles des utilisateurs, principalement concernant la publicité ciblée.

2. Impact des Amendes

2.1 Conformité des Entreprises

- **Instauration de Pratiques de Conformité** : Les amendes ont incité de nombreuses entreprises à revoir et améliorer leurs pratiques de gestion des données pour se conformer aux exigences du RGPD.
- **Augmentation de la Sensibilisation** : Les amendes ont sensibilisé davantage les entreprises aux obligations du RGPD et ont encouragé une culture de respect de la vie privée.

2.2 Effets sur les Grandes Entreprises

- **Réactions des Entreprises** : Les grandes entreprises, en particulier celles ayant des ressources importantes comme Google et Amazon, ont mis en place des mesures de conformité renforcées pour éviter des amendes futures.
- **Précédents Juridiques** : Les amendes élevées établissent des précédents pour les violations futures et servent de référence pour d'autres enquêtes et actions réglementaires.

3. Défis et Limitations

3.1 Variabilité des Amendes

- **Montants Variables** : Les montants des amendes varient considérablement en fonction de la gravité des violations et de la taille de l'entreprise, ce qui peut entraîner des perceptions d'injustice ou d'incohérence.

3.2 Application des Sanctions

- **Délai d'Application** : L'application des amendes peut prendre du temps en raison des procédures d'enquête et des recours juridiques des entreprises.
- **Recours Juridiques** : Les entreprises peuvent contester les amendes, ce qui peut prolonger les litiges et influencer l'application effective des sanctions.

Résumé : Depuis son entrée en vigueur, le RGPD a conduit à l'imposition de plusieurs amendes importantes à des entreprises pour diverses violations des règles de protection des données. Ces amendes ont eu un impact significatif sur la manière dont les entreprises abordent la conformité et la gestion des données personnelles. Elles ont également renforcé la sensibilisation aux obligations du RGPD et ont établi des précédents importants pour le respect des normes de protection des données.

Toutefois, des défis subsistent en termes de cohérence d'application, de temps de traitement des amendes, et de recours juridiques. Les amendes sous le RGPD continuent de jouer un rôle crucial dans la promotion de la conformité et la protection des données personnelles dans l'UE.

Le Digital Service Act (DSA) and Markets

Le Digital Services Act (DSA) de l'Union européenne vise à améliorer la gestion des contenus illégaux et la transparence des algorithmes de recommandations. Il a introduit des mesures importantes pour accroître la responsabilité des grandes plateformes et fournir aux utilisateurs plus d'informations sur la manière dont leurs données sont utilisées.

Cependant, son efficacité dépendra de la manière dont les plateformes mettent en œuvre ces exigences et de la capacité des autorités à surveiller et à faire respecter les règles. Les défis incluent la complexité des algorithmes, la variabilité dans la mise en œuvre, et les possibles incohérences dans l'application des règles. Le DSA représente un pas important vers une régulation plus stricte et plus transparente des plateformes numériques, mais son succès complet nécessitera une vigilance continue et des ajustements en fonction de l'évolution du paysage numérique.

Le DSA a-t-il déjà conduit à des peines et des amendes ?

Depuis son entrée en vigueur le 1er novembre 2022, le Digital Services Act (DSA) de l'Union européenne a commencé à influencer les pratiques des grandes plateformes numériques, mais les sanctions effectives, comme les peines et les amendes, n'ont pas encore été largement appliquées.

Question : Le Digital Services Act (DSA) de l'Union européenne est-il efficace selon ses objectifs de lutte contre les contenus illégaux et la transparence sur le fonctionnement des algorithmes de recommandations ?

Réponses : oui / non / NSP

Le Digital Market Act (DMA)

L'Union européenne a mis en place la directive sur le Digital Markets Act (DMA) qui a pour but de lutter contre les éventuels comportements abusifs et anticoncurrentiels des « plateformes structurantes » ou « gatekeepers », ce qui semble être adressé directement aux géants du numérique.

Le Digital Markets Act (DMA) de l'Union européenne, entré en vigueur en novembre 2022, vise à réguler les grandes plateformes numériques dites « gatekeepers » (gardiennes), afin de promouvoir la concurrence et de limiter les comportements abusifs dans le secteur numérique. Voici une évaluation de son efficacité jusqu'à présent :

1. Objectifs du DMA

1.1 Lutte contre les Comportements Abusifs

- **Pratiques Évitées** : Le DMA interdit des pratiques jugées anticoncurrentielles, telles que la promotion injuste des propres services des gatekeepers au détriment des concurrents, et les pratiques de verrouillage qui empêchent les utilisateurs de changer de services ou d'accéder à des offres concurrentes.
- **Interdiction des Abus de Pouvoir** : Les gatekeepers ne peuvent pas utiliser leur position dominante pour imposer des conditions déloyales aux entreprises et aux utilisateurs.

1.2 Promotion de la Concurrence

- **Conditions d'Accès Équitable** : Le DMA vise à créer un environnement de marché plus équitable en imposant des obligations aux gatekeepers concernant la transparence, l'interopérabilité et l'accès équitable aux plateformes.
- **Facilitation des Entrées** : Les règles sont conçues pour réduire les barrières à l'entrée pour de nouvelles entreprises et stimuler la concurrence sur le marché numérique.

2. Évaluation de l'Efficacité

2.1 Mesures de Conformité et Impact Initial

Avantages :

- **Cadre Réglementaire Clair** : Le DMA établit des règles claires pour les grandes plateformes, fournissant des directives précises sur les comportements anticoncurrentiels à éviter. Cela aide à créer un environnement plus prévisible pour les entreprises et les utilisateurs.
- **Encouragement à la Concurrence** : Les obligations imposées aux gatekeepers, telles que l'obligation de permettre une plus grande interopérabilité et de ne pas favoriser leurs propres services, devraient, en théorie, encourager une concurrence plus loyale et plus dynamique sur le marché.

Défis :

- **Mise en Œuvre** : La mise en œuvre complète des exigences du DMA est encore en cours. Les régulateurs doivent surveiller et évaluer la conformité des gatekeepers, ce qui peut prendre du temps avant que les impacts concrets ne se manifestent.

- **Résistance des Gatekeepers** : Les grandes plateformes peuvent résister aux nouvelles règles, ce qui pourrait ralentir le processus de mise en conformité. Les litiges et les négociations avec les autorités de régulation peuvent également influencer l'efficacité du DMA.

2.2 Cas Pratiques et Sanctions

Avantages :

- **Sanctions Disuasives** : Le DMA prévoit des amendes importantes pour les gatekeepers en cas de non-conformité, pouvant atteindre jusqu'à 10% de leur chiffre d'affaires mondial. Ces sanctions devraient agir comme un puissant facteur dissuasif contre les pratiques anticoncurrentielles.
- **Exemples d'Application** : Des premières actions d'application pourraient déjà avoir lieu, avec des enquêtes et des demandes de mise en conformité adressées aux principales entreprises concernées.

Défis :

- **Complexité des Enquêtes** : Les enquêtes pour détecter des violations du DMA peuvent être complexes et nécessiter du temps. Les régulateurs doivent démontrer que des comportements anticoncurrentiels se produisent et qu'ils sont directement liés aux pratiques interdites par le DMA.
- **Défis Juridiques** : Les grandes entreprises peuvent contester les sanctions et les exigences du DMA, entraînant des litiges juridiques qui pourraient ralentir l'application effective des règles.

3. Perspectives d'Avenir

Impact à Long Terme :

- **Évolution du Marché** : Le DMA est conçu pour avoir un impact à long terme sur le marché numérique, en stimulant la concurrence et en limitant les abus de pouvoir. Les effets complets du DMA pourraient ne se manifester pleinement qu'après plusieurs années d'application et de surveillance.
- **Adaptation Continue** : Le paysage numérique évolue rapidement, et le DMA devra peut-être être ajusté pour s'adapter aux nouvelles tendances et technologies. Les régulateurs devront rester vigilants pour garantir que les règles restent pertinentes et efficaces.
- Réactions des Acteurs du Marché :
- **Réactions des Plateformes** : Les gatekeepers pourraient adapter leurs stratégies pour se conformer au DMA tout en minimisant son impact sur leur modèle d'affaires. Les entreprises concurrentes pourraient également tirer parti de nouvelles opportunités créées par une concurrence accrue.
- **Évaluation Continue** : Les autorités de régulation devront évaluer régulièrement l'efficacité du DMA et ajuster les mesures en fonction des résultats observés et des retours du marché.

Résumé : Le Digital Markets Act (DMA) de l'Union européenne a le potentiel de promouvoir une concurrence plus équitable sur le marché numérique en limitant les comportements abusifs des grandes plateformes. Les avantages incluent un cadre réglementaire clair, des sanctions dissuasives et une tentative de stimulation de la concurrence. Cependant, les défis incluent la mise en œuvre, la résistance des gatekeepers, et les complexités liées aux enquêtes et aux litiges. L'efficacité complète du DMA se manifesterait probablement au fil du temps, à mesure que les mesures de conformité se stabilisent et que les impacts sur le marché deviennent plus clairs.

Le Digital Markets Act (DMA) qui a pour but de lutter contre les éventuels comportements abusifs et anticoncurrentiels est-il efficace ?

L'environnement

Les infrastructures numériques doivent s'inscrire dans une démarche écologique. Cela passe par l'efficacité énergétique des centres de données, le recyclage des équipements électroniques, et une promotion des pratiques numériques durables auprès des entreprises et des citoyens.

La politique publique du numérique

Comparaison UE-USA

Rédigé à l'aide de : <https://www.perplexity.ai/search/quelle-est-la-difference-de-politique-numerique-entre-l-union-europeenne-et-les-etats-unis>

Quelle est la différence de politique publique pour le numérique entre les États-Unis et l'Union européenne ?

La différence majeure entre les États-Unis et l'Union européenne en matière de politique numérique réside dans leurs approches respectives de la régulation et de la protection des données.

1. Régulation et protection des données personnelles :

Union européenne : L'UE est reconnue pour son approche rigoureuse en matière de protection des données personnelles, surtout avec le RGPD (Règlement général sur la protection des données). Ce cadre réglementaire impose des obligations strictes aux entreprises sur la collecte, le traitement et le stockage des données personnelles. L'UE met l'accent sur les droits des citoyens (accès, portabilité, effacement de leurs données) et vise à instaurer une transparence et une confiance accrues.

États-Unis : En revanche, les États-Unis adoptent une approche plus souple, basée sur la libre entreprise, avec des réglementations spécifiques sectorielles (comme HIPAA pour la santé ou COPPA pour la protection des enfants en ligne). Cependant, le niveau fédéral est moins protecteur pour les droits des utilisateurs, confiant davantage aux entreprises la responsabilité de fixer leurs politiques de confidentialité.

2. Approche du marché et innovation :

États-Unis : Le marché numérique est surtout orienté vers la maximisation de l'innovation et de la compétitivité. Les géants de la tech (Google, Meta, Amazon, Microsoft) dominent le secteur, et le cadre législatif plus permissif soutient cette dynamique. Les États-Unis ont un système d'autorégulation de l'industrie qui leur permet de maintenir leur avance technologique en IA, en cloud, et sur les réseaux sociaux.

Union européenne : L'UE tente de trouver un équilibre entre innovation et protection du consommateur. Des législations comme la DSA (Digital Services Act) et la DMA (Digital Markets Act) visent à réguler les grandes plateformes numériques et limiter les abus de position dominante, en imposant des standards plus élevés en matière de transparence et d'interopérabilité pour promouvoir la concurrence.

3. Vie privée et surveillance :

Union européenne : Très attachée à la vie privée, l'UE limite la surveillance des citoyens, en s'assurant que les technologies de surveillance ou d'analyse de données sont soumises à des contrôles stricts. Cela est aussi marqué par la réticence à accorder un accès sans restriction aux agences de renseignement, même pour des questions de sécurité.

États-Unis : La loi américaine permet aux agences de renseignement de surveiller largement les données, même celles de citoyens étrangers. La surveillance des données est facilitée par des lois comme le Patriot Act et le Cloud Act, qui donnent aux autorités des droits d'accès importants aux données hébergées sur le territoire américain.

En somme, l'UE se concentre davantage sur la protection des droits des citoyens et la régulation des acteurs dominants, tandis que les États-Unis privilégient la liberté d'innovation et une régulation plus légère, laissant davantage de marge de manœuvre aux entreprises tech.

Financements publics : subventions et autres

Les Etats-Unis et l'Union européenne mettent en place des financements publics : subventions, fiscalité, taux d'emprunt... quelles sont les différences et qui est le plus efficace ?

ChatGPT :

Les États-Unis et l'Union européenne adoptent des approches distinctes en matière de financement public pour le numérique, combinant subventions, incitations fiscales et dispositifs de prêts avantageux, mais avec des priorités et des modes de financement variés. Voici les principales différences et les points d'efficacité :

1. Subventions et programmes d'investissement :

États-Unis : Les États-Unis favorisent souvent des subventions directes et des investissements de capital-risque public, en se concentrant sur les technologies stratégiques. Des initiatives comme le **CHIPS Act** offrent d'importantes subventions et crédits pour renforcer la production de semi-conducteurs, et le **National AI Initiative Act** met des fonds publics dans la recherche en IA. Ce modèle vise à renforcer la compétitivité en soutenant des entreprises privées clés, avec une concentration sur la souveraineté technologique.

Union européenne : L'UE privilégie des programmes de subventions et de financement coopératifs, comme **Horizon Europe** pour la recherche et l'innovation, ou le **Digital Europe Programme** qui cible des secteurs comme la cybersécurité, l'IA, et les infrastructures de données. Les subventions européennes se répartissent souvent via des appels à projets auxquels répondent des consortiums publics-privés, renforçant ainsi l'intégration de différents acteurs. Cette approche est davantage orientée vers une coopération transfrontalière et le partage de connaissances, moins vers l'indépendance stratégique directe.

2. Incitations fiscales et crédits d'impôt :

- **États-Unis** : Les États-Unis offrent des crédits d'impôt généreux et des déductions fiscales pour stimuler la R&D dans la tech, l'IA et les infrastructures numériques. Les États américains ajoutent aussi des incitations régionales attractives pour attirer des entreprises technologiques, créant un environnement propice à l'innovation avec une charge fiscale réduite.
- **Union européenne** : L'UE propose des crédits d'impôt pour la R&D, mais ceux-ci sont souvent administrés par chaque État membre avec des règles variées, générant une fragmentation. Certains pays, comme la France avec le **Crédit d'Impôt Recherche**, sont très compétitifs, mais l'absence d'un système unifié dans l'UE peut être moins efficace comparé au modèle coordonné américain.

3. Accès au financement et taux d'emprunt :

- **États-Unis** : Grâce à une politique monétaire plus souple, les entreprises américaines bénéficient souvent de taux d'intérêt plus bas, notamment grâce au financement public et semi-public facilité par des agences comme la **Small Business Administration (SBA)** pour les startups. Cela permet aux petites entreprises d'accéder à des prêts abordables pour développer leurs innovations.
- **Union européenne** : En revanche, l'UE s'appuie davantage sur la **Banque européenne d'investissement (BEI)** pour offrir des taux d'intérêt faibles sur des prêts de long terme. Cependant, l'accessibilité à ces prêts est parfois limitée par les critères stricts d'éligibilité et le temps nécessaire pour approuver les dossiers.

4. Efficacité des financements :

- **États-Unis** : Les États-Unis semblent plus efficaces en termes d'impact direct, car ils concentrent leurs financements sur des entreprises de pointe et visent un retour rapide et

compétitif. La flexibilité des dispositifs et les incitations fiscales jouent également en faveur d'une exécution plus rapide.

- **Union européenne** : L'UE est efficace dans la structuration de financements pour des projets transnationaux et durables, mais la fragmentation des systèmes fiscaux et des modalités d'octroi de subventions peut ralentir l'efficacité globale. Le modèle de subventions européennes permet néanmoins une coopération régionale forte et plus de cohésion, mais parfois au détriment de la compétitivité rapide face aux États-Unis.

En conclusion, les États-Unis ont un modèle d'efficacité à court terme axé sur la compétitivité et l'innovation privée, tandis que l'**Union européenne** mise sur une efficacité à long terme en intégrant des financements plus complexes mais encourageant une croissance régionale et collaborative. Le modèle américain est souvent considéré comme plus efficace dans la course aux innovations de rupture, mais l'UE favorise une approche plus équilibrée et coopérative pour des progrès technologiques et sociaux durables.

Perplexity :

Les approches de financement public pour l'innovation numérique diffèrent entre les États-Unis et l'Union européenne, chacune ayant ses forces et ses faiblesses :

Approche américaine

1. **Financement décentralisé** : Plusieurs agences fédérales (NSF, DARPA, etc.) financent des projets spécifiques.
2. **Focus sur la recherche fondamentale** : Accent mis sur les technologies de rupture et l'innovation de pointe.
3. **Partenariats public-privé** : Forte synergie entre le gouvernement, les universités et l'industrie.
4. **Financement ciblé** : Subventions importantes mais concentrées sur des domaines stratégiques.

Approche européenne

1. **Stratégie coordonnée** : Programmes dédiés comme le "Programme pour une Europe numérique" avec un budget de 7,5 milliards d'euros pour 2021-2027.
2. **Objectifs précis** : Définis dans la "Boussole numérique" pour 2030.
3. **Développement équilibré** : Accent mis sur le soutien aux PME et aux territoires.
4. **Réglementation** : Forte emphase sur la protection des données et la régulation des grandes entreprises technologiques.

Efficacité

Il est difficile de déterminer quelle approche est la plus efficace, car chacune répond à des contextes et des objectifs différents :

1. **Impact économique** : Selon une étude franco-allemande, l'impact macroéconomique des subventions serait minimal dans les deux cas.
2. **Innovation** : Les États-Unis semblent avoir un avantage en termes d'innovation de rupture et de création de géants technologiques.
3. **Protection et régulation** : L'UE est en avance sur les questions de protection des données et de régulation des grandes plateformes.
4. **Adaptation aux enjeux locaux** : L'approche européenne semble mieux adaptée aux spécificités du marché unique et aux besoins des citoyens européens.
5. **Souveraineté numérique** : L'UE met davantage l'accent sur le développement d'une souveraineté numérique européenne.

En conclusion, plutôt que de chercher une approche supérieure, il semble que la coopération et l'apprentissage mutuel entre l'UE et les États-Unis soient bénéfiques. L'approche américaine favorise l'innovation de pointe et la création de leaders mondiaux, tandis que l'approche européenne vise un développement plus équilibré et régulé. L'efficacité dépend largement des objectifs spécifiques poursuivis par chaque région.

Citations:

- [1] <https://bofip.impots.gouv.fr/bofip/4680-PGP.html/identifiant=BOI-BIC-RICI-10-10-30-20-20210713>
- [2] <https://www.lafinancepourtous.com/juniors/lyceens/le-financement-de-lactivite-economique/comment-letat-finance-t-il-son-besoin-de-financement/>
- [3] https://www.financierterritorial.fr/rubrique_financement-du-secteur-public-local_679A4B884DA273BC8E50A577D69A63.html
- [4] <https://tnova.fr/economie-social/territoires-metropoles/quel-avenir-pour-limpot-local-quel-financement-des-services-publics-locaux/>
- [5] <https://www.economie.gouv.fr/entreprises/financement-entreprises-aides-credits-impot>
- [6] <https://entreprendre.service-public.fr/vosdroits/F23533>
- [7] <https://www.epfauvergne.com/epf-auvergne/financement-et-fiscalite/>
- [8] <https://fr.euronews.com/business/2023/02/26/la-guerre-des-subsidies-entre-leurope-et-les-etats-unis>

Réinventer la poudre ?

En termes de politique publique du numérique, l'Union européenne aurait-elle tendance à "réinventer la poudre" par rapport aux États-Unis ?

La question de savoir si l'Union européenne a tendance à "réinventer la poudre" par rapport aux États-Unis en matière de politique publique du numérique est complexe et soulève plusieurs points à considérer :

1. Différences de Philosophies et d'Approches

1.1 Approche Réglementaire de l'UE

- **Précaution et Protection des Données** : L'UE adopte une approche plus prudente et réglementée, centrée sur la protection des données et des droits des consommateurs. Des règlements comme le RGPD (Règlement Général sur la Protection des Données) illustrent cette tendance à privilégier la vie privée et la sécurité des données.
- **Régulations Strictes** : L'UE met en place des régulations pour encadrer les géants du numérique (GAFAM) et promouvoir des pratiques équitables, ce qui peut être perçu comme une "réinvention de la poudre" si l'on considère que ces régulations diffèrent des approches plus laxistes adoptées par les États-Unis.

1.2 Innovation et Agilité aux États-Unis

- **Liberté d'Innovation** : Les États-Unis ont traditionnellement adopté une approche plus libérale envers l'innovation technologique, permettant aux entreprises de développer et de déployer des solutions sans contraintes réglementaires majeures. Cela favorise une culture de l'innovation rapide.
- **Culture Entrepreneuriale** : Le climat d'affaires aux États-Unis encourage le risque et l'expérimentation, ce qui peut mener à des avancées rapides dans le domaine technologique.

2. Réponses aux Défis Numériques

2.1 Anticipation des Problèmes

- **Problèmes Émergents** : L'UE peut être perçue comme plus proactive dans l'anticipation des problèmes associés à l'usage des technologies numériques, tels que la désinformation, la manipulation des données, et la protection des droits des utilisateurs. En ce sens, l'UE ne réinvente pas la poudre, mais cherche à répondre à des enjeux spécifiques qui peuvent ne pas être abordés de manière équivalente aux États-Unis.

2.2 Cohérence et Harmonisation

- **Politique Cohérente** : L'UE cherche à créer un cadre cohérent pour la politique numérique à travers ses États membres, ce qui peut rendre le marché unique plus attractif pour les entreprises. Cela contraste avec les approches disparates adoptées par différents États américains.

3. Collaboration et Apprentissage Mutuel

3.1 Partage de Meilleures Pratiques

- **Coopération Internationale** : L'UE et les États-Unis ont récemment engagé des dialogues pour échanger des meilleures pratiques et s'attaquer ensemble à des défis communs, comme la cybersécurité et la régulation des plateformes numériques.
- **Innovation Responsable** : L'UE propose un modèle d'innovation responsable qui pourrait influencer les États-Unis, notamment en matière de responsabilité des entreprises technologiques.

4. Conclusion

En résumé, plutôt que de "réinventer la poudre", l'Union européenne adopte une approche distincte et parfois complémentaire aux États-Unis en matière de politique publique du numérique. Si les réglementations de l'UE peuvent sembler plus restrictives, elles visent à protéger les droits des citoyens et à répondre à des préoccupations émergentes. Les deux approches ont leurs avantages et leurs inconvénients, et un dialogue ouvert entre l'UE et les États-Unis pourrait permettre d'enrichir les politiques numériques de chaque région.

Le marché unique numérique

Le **marché unique numérique** de l'Union européenne (UE) est une initiative visant à créer un espace numérique intégré qui permet aux biens, services, et données de circuler librement à travers les États membres de l'UE. Ce concept s'inscrit dans une volonté de renforcer l'économie numérique de l'Europe et d'encourager l'innovation et la compétitivité.

La boussole numérique

La **Boussole numérique** de l'Union européenne est une initiative qui vise à définir et à orienter les actions et les politiques de l'UE dans le domaine de la transformation numérique d'ici 2030. Présentée en janvier 2021 par la Commission européenne, la Boussole numérique a pour objectif d'établir un cadre clair pour guider les États membres et les institutions de l'UE vers une transition numérique réussie et inclusive. Voici les principaux éléments qui la composent :

1. Objectifs de la Boussole Numérique

1.1 Une Europe Numérique Durable

- **Transformation Numérique** : La Boussole numérique vise à renforcer la capacité numérique de l'Europe dans divers secteurs, en intégrant des technologies avancées tout en respectant les valeurs européennes, notamment la durabilité et la protection des données.

1.2 Développement des Compétences

- **Compétences Numériques** : L'initiative met l'accent sur le développement des compétences numériques des citoyens, en assurant que tous aient accès à la formation nécessaire pour participer à l'économie numérique.

1.3 Accessibilité et Inclusion

- **Égalité d'Accès** : La Boussole numérique vise à garantir que tous les citoyens de l'UE, y compris les populations marginalisées et les zones rurales, aient accès à des services numériques de qualité.

2. Quatre piliers principaux de la Boussole Numérique

La Boussole numérique est structurée autour de quatre axes principaux, appelés "piliers", qui définissent les domaines prioritaires d'action :

2.1 Compétences numériques

- **Objectif** : 80 % de la population adulte devrait avoir des compétences numériques de base d'ici 2030, et 20 millions de spécialistes en TIC devraient être formés.

2.2 Infrastructure numérique

- **Objectif** : L'UE vise à garantir que toutes les régions aient accès à des réseaux très haut débit et à une couverture 5G.

2.3 Services publics numériques

- **Objectif** : La Boussole numérique promeut la numérisation des services publics, avec l'ambition que 100 % des services publics essentiels soient disponibles en ligne.

2.4 Transformation numérique des entreprises

- **Objectif** : Au moins 75 % des entreprises devraient adopter des technologies numériques, avec un accent particulier sur les PME, pour améliorer leur compétitivité.

3. Suivi et Évaluation

- **Tableau de Bord** : La Boussole numérique est accompagnée d'un tableau de bord qui permettra de suivre les progrès des États membres par rapport aux objectifs fixés, en utilisant des indicateurs clairs et mesurables.

4. Importance Stratégique

- **Réponse aux Défis Mondiaux** : La Boussole numérique est une réponse stratégique aux défis mondiaux croissants liés à la numérisation, à la cybersécurité, et à la compétitivité dans le contexte de la géopolitique numérique.
- **Alignement avec d'autres Initiatives** : Elle s'inscrit également dans le cadre d'autres initiatives de l'UE, telles que le Digital Services Act (DSA) et le Digital Markets Act (DMA), visant à créer un cadre réglementaire robuste pour l'économie numérique.

Conclusion

La Boussole numérique de l'Union européenne représente un engagement fort en faveur d'une transformation numérique inclusive, durable et compétitive. En se concentrant sur les compétences, l'infrastructure, les services publics numériques et la transformation des entreprises, elle vise à positionner l'Europe comme un leader dans l'économie numérique tout en respectant les valeurs fondamentales de l'UE.

Une hybridation ?

Est-il possible d'hybrider les deux systèmes : garder le meilleur des deux et éliminer le moins bon ? Garder les atouts d'une innovation dynamique et flexible aux Etats-Unis et

débureaucratiser l'approche européenne, conserver le souci de la protection de la vie privée et d'un numérique européen « éthique » ?

L'idée d'hybrider les systèmes américain et européen en matière de politique publique du numérique est à la fois séduisante et complexe. Voici quelques éléments à considérer sur la possibilité de combiner les atouts des deux approches tout en atténuant leurs inconvénients :

1. Atouts à Conserver

1.1 Innovation Dynamique et Flexible (Modèle Américain)

- **Encouragement à l'Innovation** : L'approche américaine, qui favorise une culture d'innovation rapide et une grande flexibilité réglementaire, peut être bénéfique. Cela permet aux entreprises de tester et de déployer rapidement de nouvelles technologies.
- **Soutien à l'Entrepreneuriat** : Les États-Unis ont un écosystème entrepreneurial vibrant, soutenu par des investissements en capital-risque et des initiatives publiques, qui peuvent être reproduits dans le cadre européen.

1.2 Protection de la Vie Privée et Éthique (Modèle Européen)

- **Régulations Protectrices** : Les réglementations comme le RGPD mettent l'accent sur la protection des données personnelles et des droits des utilisateurs. Cet aspect est crucial pour maintenir la confiance des citoyens dans le numérique.
- **Numérique Éthique** : La volonté de créer un numérique éthique en Europe, qui respecte les valeurs sociales et environnementales, peut guider le développement de technologies de manière responsable.

2. Éliminer les Moins Bons Aspects

2.1 Débureaucratisation de l'Approche Européenne

- **Simplification des Régulations** : L'UE pourrait travailler à simplifier ses processus réglementaires, réduire la lourdeur bureaucratique et rendre l'environnement plus favorable à l'innovation tout en préservant les protections nécessaires.
- **Flexibilité dans l'Application des Régulations** : Introduire des "sandboxes" réglementaires similaires à celles en vigueur aux États-Unis, permettant aux entreprises de tester leurs innovations dans un cadre contrôlé sans se heurter à une réglementation rigide.

2.2 Régulation Proactive sans Étouffement

- **Équilibre entre Protection et Innovation** : Établir des réglementations qui favorisent l'innovation tout en garantissant la protection des droits des utilisateurs. Par exemple, des réglementations claires sur l'utilisation des données pourraient coexister avec un environnement propice à la créativité.
- **Engagement des Parties Prenantes** : Impliquer les entreprises, les chercheurs et les citoyens dans le processus de réglementation pour s'assurer que les lois reflètent les réalités du marché et des préoccupations sociétales.

3. Collaborations et Échanges

- **Partenariats Public-Privé** : Encourager des partenariats entre les gouvernements et les entreprises technologiques pour co-développer des solutions qui intègrent les meilleures pratiques des deux systèmes.
- **Dialogue International** : Renforcer les échanges entre les États-Unis et l'UE pour partager des expériences et des leçons tirées de l'application de réglementations et de politiques publiques dans le numérique.

4. Conclusion

L'hybridation des systèmes américain et européen en matière de politique publique du numérique est non seulement possible, mais elle pourrait également être bénéfique pour les deux régions. En conservant les atouts de l'innovation dynamique et flexible des États-Unis tout en intégrant les valeurs de protection de la vie privée et d'éthique de l'UE, il est possible de créer un cadre numérique qui favorise à la fois l'innovation et la responsabilité. Cela nécessitera un engagement fort de toutes les parties prenantes et une volonté d'adapter les modèles existants pour mieux répondre aux défis futurs du numérique.

Orienter le financement public vers l'infrastructure publique

Le numérique peut s'appréhender par une infrastructure publique et une superstructure privée. L'infrastructure est d'abord un réseau (Internet) qui assure le transfert de données entre acteurs privés et la superstructure s'appuie sur le réseau pour fonctionner et échanger des données. Les acteurs privés sont les entreprises et les personnes. Le financement est-il logiquement : public pour l'infrastructure public (impôts, taxes) et privé pour la superstructure ?

Votre analyse du numérique en tant que système composé d'une infrastructure publique et d'une superstructure privée est pertinente et reflète une approche classique dans l'étude des infrastructures numériques. Voici quelques réflexions sur le financement de ces deux composantes :

1. Infrastructure Publique

1.1 Rôle et Importance

- **Réseau de Base** : L'infrastructure numérique, qui inclut des éléments tels que les réseaux de télécommunications, l'Internet, et les centres de données, constitue le fondement sur lequel repose l'ensemble des services numériques.
- **Accès Équitable** : Une infrastructure publique de qualité est essentielle pour garantir un accès équitable à Internet pour tous, y compris les zones rurales ou moins desservies.

1.2 Financement Public

- **Sources de Financement** : Le financement de l'infrastructure est logiquement basé sur des ressources publiques, telles que les impôts et les taxes. Les gouvernements investissent dans la construction et l'entretien des réseaux pour s'assurer que l'accès à Internet est généralisé et de qualité.
- **Partenariats Public-Privé** : Dans de nombreux cas, des partenariats public-privé (PPP) sont établis pour développer l'infrastructure. Cela permet de combiner les ressources publiques et privées, d'accélérer les investissements et d'améliorer l'efficacité des projets.

2. Superstructure Privée

2.1 Rôle et Importance

- **Services et Applications** : La superstructure privée englobe les entreprises et les utilisateurs individuels qui exploitent l'infrastructure pour offrir des services, développer des applications, et interagir entre eux.
- **Innovation et Créativité** : Les acteurs privés jouent un rôle crucial dans l'innovation technologique et la création de valeur ajoutée en exploitant les ressources disponibles sur le réseau.

2.2 Financement Privé

- **Investissements Privés** : Le financement de la superstructure provient principalement du secteur privé, que ce soit par des investissements en capital, des revenus commerciaux, ou des

financements d'entreprises. Les entreprises génèrent des revenus en offrant des services qui dépendent de l'infrastructure publique.

- **Modèles Économiques** : Les entreprises peuvent adopter divers modèles économiques, tels que les abonnements, la publicité, ou les ventes de produits, pour financer leurs opérations.

3. Interdépendance des Deux Systèmes

- **Relation Symbiotique** : La superstructure ne peut fonctionner efficacement sans une infrastructure robuste et bien financée. Inversement, l'infrastructure a besoin des acteurs privés pour générer de la demande et justifier les investissements.
- **Évolutions Technologiques** : Avec l'émergence de nouvelles technologies (comme l'IoT, l'IA, et le cloud), la relation entre l'infrastructure et la superstructure peut évoluer, entraînant de nouveaux modèles de financement et de collaboration.

4. Conclusion

Votre proposition selon laquelle le financement de l'infrastructure publique devrait être principalement public, tandis que celui de la superstructure privée devrait être principalement privé, est logique et reflète les réalités du système numérique actuel. Cette séparation des rôles permet de garantir que chacun des niveaux fonctionne de manière optimale, tout en soulignant l'importance d'une collaboration continue entre les secteurs public et privé pour répondre aux défis futurs du numérique.

Efficacité du financement public de la superstructure privée

Tous les Etats (USA, UE, Chine...) encourage les initiatives privées du numérique (subventions, crédits d'impôts, prêt remboursables ou non remboursables...). Ce financement public, quel que soit sa forme, suppose une procédure administrative qui génère lenteur, formalisme réducteur, décision par des élus ou des fonctionnaires qui ne sont pas nécessairement experts du domaine. Le financement public est-il efficace, en particulier dans le cas du numérique, très évolutif comparativement au seul financement privé par capital-risque, autofinancement ... Pouvez-vous produire des liens vers des sites internet qui illustre cette question ?

Le financement public des initiatives numériques, bien qu'il offre des avantages tels que le soutien à l'innovation et la réduction des risques pour les entreprises, présente également des défis spécifiques, notamment en raison de procédures administratives complexes et de lenteurs décisionnelles.

Avantages du financement public :

- **Soutien à l'innovation** : Les subventions et crédits d'impôt permettent aux entreprises de se lancer dans des projets innovants sans supporter l'intégralité des risques financiers. □
- **Réduction des inégalités** : Le financement public peut aider à combler les lacunes de financement, en particulier pour les start-up et les PME qui ont du mal à accéder au capital-risque. □

Défis du financement public :

- **Procédures administratives** : Les démarches pour obtenir des financements publics peuvent être longues et complexes, ce qui peut décourager les entreprises et retarder le lancement de projets.
- **Manque d'expertise sectorielle** : Les décisions de financement sont souvent prises par des fonctionnaires ou des élus qui ne sont pas toujours experts dans le domaine technologique concerné, ce qui peut entraîner des choix moins adaptés aux besoins du marché.

Comparaison avec le financement privé :

- **Flexibilité et rapidité** : Le capital-risque et l'autofinancement offrent une plus grande flexibilité et une prise de décision plus rapide, ce qui est crucial dans le secteur numérique en constante évolution.
- **Alignement avec le marché** : Les investisseurs privés, étant directement concernés par le succès commercial, sont souvent plus en phase avec les tendances du marché et les besoins des consommateurs.

Exemples illustratifs :

- **France 2030** : Ce plan gouvernemental, doté de 54 milliards d'euros, vise à soutenir l'innovation en France. Cependant, des critiques ont émergé concernant la lenteur des procédures administratives et la nécessité d'une plus grande implication du secteur privé pour accélérer le financement de l'innovation.
- **Baromètre 2024 sur le financement de l'innovation en France** : Une étude indique que 68 % des répondants estiment qu'il est facile d'innover en France, grâce à des dispositifs tels que le crédit d'impôt recherche. Cependant, l'accès aux financements privés reste restreint, ce qui souligne la nécessité d'améliorer l'efficacité des financements publics.

En conclusion, bien que le financement public joue un rôle essentiel dans le soutien à l'innovation numérique, il est crucial d'optimiser les procédures administratives et d'encourager une plus grande participation du secteur privé pour assurer une efficacité maximale, en particulier dans un domaine aussi dynamique que le numérique.

Perplexity :

Le financement public du numérique présente à la fois des avantages et des inconvénients par rapport au financement privé. Une analyse nuancée est nécessaire pour évaluer son efficacité.

Avantages du financement public

- **Soutien à l'innovation de long terme** : Le financement public permet de soutenir des projets à plus long terme et plus risqués que le secteur privé, qui recherche généralement des retours sur investissement rapides[1]. Cela est particulièrement important dans le domaine du numérique où certaines innovations peuvent mettre des années à se concrétiser.
- **Orientation vers l'intérêt général** : Les fonds publics peuvent être orientés vers des projets d'intérêt général qui ne seraient pas nécessairement financés par le privé, comme l'accessibilité numérique ou la transition écologique[2].
- **Effet de levier** : Le soutien public peut avoir un effet d'entraînement sur les investissements privés, en réduisant les risques initiaux pour les entreprises.

Inconvénients du financement public

- **Lourdeur administrative** : Les procédures administratives pour obtenir des financements publics sont souvent longues et complexes, ce qui peut freiner l'innovation dans un secteur aussi dynamique que le numérique[3].
- **Manque d'expertise** : Les décideurs publics peuvent manquer d'expertise technique pour évaluer efficacement les projets numériques les plus prometteurs.
- **Rigidité** : Les programmes de financement public peuvent manquer de flexibilité pour s'adapter rapidement aux évolutions technologiques, contrairement au capital-risque privé.

Comparaison avec le financement privé

Le financement privé, notamment par capital-risque, présente plusieurs avantages dans le secteur numérique :

- Rapidité de décision et de mise en œuvre
- Expertise sectorielle des investisseurs
- Accompagnement stratégique des startups
- Flexibilité pour s'adapter aux pivots des projets

Cependant, il tend à se concentrer sur les projets à fort potentiel de rentabilité à court/moyen terme, au détriment parfois de l'innovation de rupture ou des projets d'intérêt général.

Vers un modèle hybride

L'efficacité optimale semble résider dans une approche hybride combinant financement public et privé :

1. Financement public pour la recherche fondamentale et les projets à long terme
2. Partenariats public-privé pour partager les risques sur des projets innovants
3. Capital-risque et autofinancement pour le développement commercial

Cette complémentarité permettrait de bénéficier des avantages de chaque approche tout en limitant les inconvénients.

Pistes d'amélioration du financement public

Pour accroître l'efficacité du financement public dans le numérique, plusieurs pistes peuvent être envisagées :

- Simplification des procédures administratives
- Recours accru à des experts du secteur dans l'évaluation des projets
- Mise en place de mécanismes de financement plus agiles et réactifs
- Renforcement de la collaboration avec le secteur privé

En conclusion, bien que le financement public présente certaines limites dans le secteur numérique, il reste un outil important pour soutenir l'innovation de long terme et les projets d'intérêt général. Son efficacité peut être optimisée en le combinant judicieusement avec des financements privés et en améliorant ses processus pour les adapter aux spécificités du secteur.

Citations:

- [1] <https://aides-territoires.beta.gouv.fr/aides/1bd7-ameliorer-lefficacite-de-laction-publique-par/>
- [2] https://www.budget.gouv.fr/files/files/plf/plf-2024/FR_2024_PLF_BG_PGM_352_STRAT.html
- [3] <https://europe.maregionsud.fr/projets/detail/ameliorer-lefficacite-de-laction-publique-par-sa-transformation-numerique>
- [4] <https://digital-strategy.ec.europa.eu/fr/activities/funding-digital>
- [5] <https://freebalance.com/fr/blog/gouvernement-transformation-numerique/digital-pfm-pourquoi-ca-ne-fonctionne-pas-ce-quon-peut-faire/>
- [6] <https://www.numerique.gouv.fr/espace-presse/numerique-au-service-de-lefficacite-de-laction-publique/>
- [7] <https://www.lagazettedescommunes.com/820524/comment-la-transformation-numerique-rend-le-service-public-plus-efficace/>
- [8] <https://www.economie.gouv.fr/plan-de-relance/mesures/aides-france-num-transformation-numerique>

« sandbox » Bretagne

Connaissez-vous Megalis en Bretagne ? Est-ce que cette infrastructure pourrait être utilisée pour une expérimentation du numérique ?

Perplexity

Oui, je connais Mégalis Bretagne. C'est un syndicat mixte créé en 1999 qui joue un rôle crucial dans le développement numérique de la région Bretagne. Voici les principaux éléments à retenir sur Mégalis Bretagne et son potentiel pour des expérimentations numériques :

Missions principales de Mégalis Bretagne

1. Déploiement de la fibre optique

Mégalis Bretagne est responsable de la construction et de l'exploitation du réseau public régional de fibre optique dans le cadre du projet "Bretagne Très Haut Débit"[1]. Ce projet vise à remplacer le réseau téléphonique actuel basé sur le cuivre par un réseau en fibre optique couvrant l'ensemble du territoire breton.

2. Développement de l'administration électronique

Le syndicat propose une offre de services numériques mutualisés et de fournitures associées pour favoriser le développement de l'e-administration[2].

Potentiel pour l'expérimentation numérique

L'infrastructure déployée par Mégalis Bretagne offre un excellent terrain pour des expérimentations numériques :

1. Couverture étendue

Le réseau de fibre optique en cours de déploiement couvrira à terme l'ensemble du territoire breton, y compris les zones rurales[1]. Cela permet d'envisager des expérimentations à grande échelle, touchant des populations variées.

2. Très haut débit

La fibre optique offre des débits très élevés, ce qui ouvre la voie à des applications innovantes nécessitant une forte bande passante (réalité virtuelle, IoT, etc.).

3. Partenariats existants

Mégalis Bretagne collabore déjà avec de nombreuses collectivités et acteurs locaux[2], ce qui facilite la mise en place de projets expérimentaux impliquant différentes parties prenantes.

4. Expertise technique

L'équipe de Mégalis Bretagne possède une solide expertise dans le domaine des infrastructures numériques, ce qui peut être précieux pour accompagner des projets innovants.

5. Services numériques existants

Les services d'e-administration déjà développés par Mégalis Bretagne peuvent servir de base ou d'inspiration pour de nouvelles expérimentations dans le domaine des services publics numériques.

Exemples d'expérimentations possibles

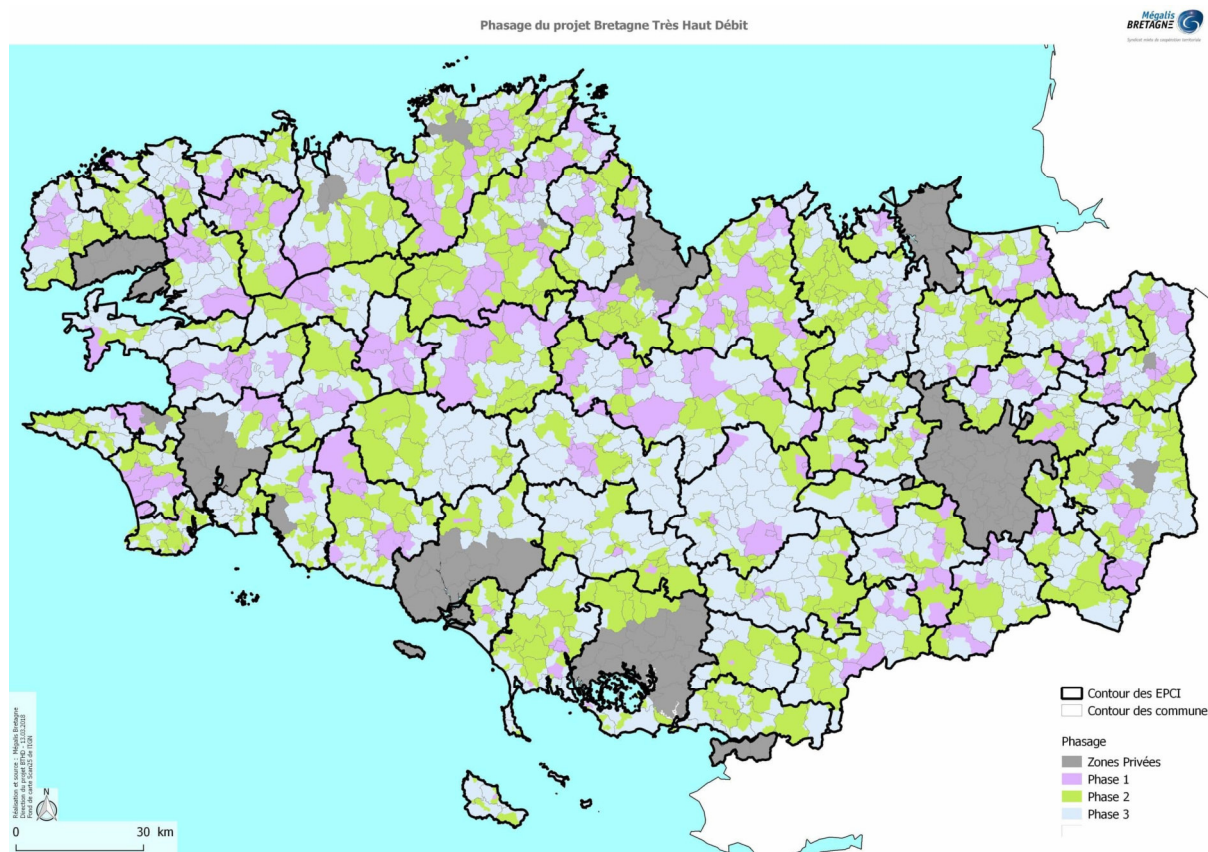
- **Smart cities** : utilisation de l'infrastructure pour déployer des capteurs IoT et améliorer la gestion urbaine.
- **Télémédecine** : expérimentation de nouveaux services de santé à distance, notamment dans les zones rurales.
- **Education** : développement de plateformes d'apprentissage innovantes tirant parti du très haut débit.

- **Mobilité** : mise en place de systèmes de transport intelligents à l'échelle régionale.

En conclusion, l'infrastructure déployée par Mégalis Bretagne offre un terrain propice à l'expérimentation numérique, grâce à sa couverture étendue, ses performances techniques et l'écosystème de partenaires déjà en place. La région Bretagne pourrait ainsi devenir un véritable laboratoire d'innovation numérique à l'échelle nationale.

Citations:

- [1] <https://www.megalis.bretagne.bzh/le-deploiement-concretement/>
- [2] <https://www.megalis.bretagne.bzh/a-propos/>
- [3] <https://www.megalis.bretagne.bzh>
- [4] <https://www.megalis.bretagne.bzh/foire-aux-questions/>
- [5] <https://www.thdbretagne.bzh>
- [6] <https://www.lagazettedescommunes.com/820524/comment-la-transformation-numerique-rend-le-service-public-plus-efficace/>
- [7] <https://europe.maregionsud.fr/projets/detail/ameliorer-lefficacite-de-laction-publique-par-sa-transformation-numerique>
- [8] <https://aides-territoires.beta.gouv.fr/aides/1bd7-ameliorer-lefficacite-de-laction-publique-par/>





Apprentissage innovant et très haut débit

Pouvez-vous expliciter : développement de plateformes d'apprentissage innovantes tirant parti du très haut débit. ?

Le développement de plateformes d'apprentissage innovantes tirant parti du très haut débit offre de nombreuses possibilités pour transformer l'éducation et la formation. Voici quelques exemples concrets de ce que cela pourrait impliquer :

Contenu multimédia immersif

Réalité virtuelle et augmentée

Le très haut débit permet de diffuser en streaming des expériences de réalité virtuelle et augmentée de haute qualité. Les apprenants pourraient ainsi :

- Visiter virtuellement des sites historiques ou scientifiques
- Manipuler des objets 3D complexes (molécules, structures anatomiques, etc.)
- S'entraîner à des procédures techniques dans des environnements simulés

Vidéos 4K/8K et 360°

La bande passante élevée autorise l'utilisation de vidéos ultra-haute définition et à 360 degrés, offrant une expérience visuelle plus riche et immersive.

Apprentissage collaboratif en temps réel

- **Visioconférence haute qualité** : Des sessions de visioconférence en haute définition avec de nombreux participants simultanés deviennent possibles, facilitant les cours à distance et les travaux de groupe.
- **Tableaux blancs collaboratifs** : Les apprenants peuvent travailler ensemble sur des documents partagés ou des tableaux blancs virtuels en temps réel, sans latence.

Personnalisation et adaptabilité

- **Analyse de données en temps réel** : La plateforme peut analyser instantanément les performances et le comportement des apprenants pour adapter le contenu et le rythme d'apprentissage en temps réel.
- **Contenu dynamique** : Le contenu des cours peut être mis à jour et adapté en temps réel en fonction des besoins des apprenants ou de l'actualité.

Accès ubiquitaire

- **Apprentissage mobile** : Le très haut débit mobile (5G) permet d'accéder à des contenus riches et interactifs depuis n'importe où, favorisant l'apprentissage en situation.
- **Cloud gaming éducatif** : Le développement de plateformes d'apprentissage innovantes tirant parti du très haut débit offre de nombreuses possibilités pour transformer l'éducation et la formation. Voici quelques exemples concrets de ce que cela pourrait impliquer :

Contenu multimédia immersif

Réalité virtuelle et augmentée : Le très haut débit permet de diffuser en streaming des expériences de réalité virtuelle et augmentée de haute qualité. Les apprenants pourraient ainsi :

- Visiter virtuellement des sites historiques ou scientifiques
- Manipuler des objets 3D complexes (molécules, structures anatomiques, etc.)
- S'entraîner à des procédures techniques dans des environnements simulés

Vidéos 4K/8K et 360° : La bande passante élevée autorise l'utilisation de vidéos ultra-haute définition et à 360 degrés, offrant une expérience visuelle plus riche et immersive.

Apprentissage collaboratif en temps réel

- **Visioconférence haute qualité** : Des sessions de visioconférence en haute définition avec de nombreux participants simultanés deviennent possibles, facilitant les cours à distance et les travaux de groupe.
- **Tableaux blancs collaboratifs** : Les apprenants peuvent travailler ensemble sur des documents partagés ou des tableaux blancs virtuels en temps réel, sans latence.

Personnalisation et adaptabilité

- **Analyse de données en temps réel** : La plateforme peut analyser instantanément les performances et le comportement des apprenants pour adapter le contenu et le rythme d'apprentissage en temps réel.
- **Contenu dynamique** : Le contenu des cours peut être mis à jour et adapté en temps réel en fonction des besoins des apprenants ou de l'actualité.

Accès ubiquitaire

- **Apprentissage mobile** : Le très haut débit mobile (5G) permet d'accéder à des contenus riches et interactifs depuis n'importe où, favorisant l'apprentissage en situation.
- **Cloud gaming éducatif** : Des jeux éducatifs complexes peuvent être diffusés en streaming, sans nécessiter de matériel puissant côté utilisateur.

Évaluation innovante

- **Simulations complexes** : Le très haut débit permet de réaliser des évaluations basées sur des simulations complexes et réalistes, testant les compétences pratiques des apprenants.
- **Surveillance d'examen à distance** : Des systèmes de surveillance d'examen à distance plus sophistiqués et fiables peuvent être mis en place, utilisant par exemple l'analyse vidéo en temps réel.

En conclusion, le très haut débit ouvre la voie à des plateformes d'apprentissage plus immersives, interactives et personnalisées, transformant profondément l'expérience éducative. Ces innovations

peuvent améliorer l'engagement des apprenants, l'efficacité de l'apprentissage et l'accessibilité de l'éducation.

Citations:

[1] <https://www.formationfibreoptique.fr>

[2] <https://www.lagazettedescommunes.com/820524/comment-la-transformation-numerique-rend-le-service-public-plus-efficace/>

[3] <https://www.entreprises.gouv.fr/fr/actualites/transition-fibre-optique-etat-lance-site-internet-accompagner-usagers>

[4] <https://5glab.orange.com/fr/la-5g-leve-les-freins-de-lapprentissage-a-distance-et-de-lacquisition-de-competences-en-mobilite/>

[5] <https://www.telecom-sudparis.eu/recherche/plateformes-recherche/>

[6] <https://www.purple-campus.com/formation/monteur-installateur-h-f-reseaux-tres-haut-debit/>

[7] <https://digital-strategy.ec.europa.eu/fr/activities/funding-digital>

[8] <https://www.economie.gouv.fr/plan-de-relance/mesures/aides-france-num-transformation-numerique>

Droit à l'expérimentation en Bretagne

Est-il concevable de mener une expérimentation dans une région comme la Bretagne ?

Oui, il est tout à fait concevable et même encouragé de mener des expérimentations dans une région comme la Bretagne. Les informations fournies montrent que la Bretagne a mis en place plusieurs dispositifs pour favoriser l'innovation et l'expérimentation, notamment dans le domaine numérique :

1. Le dispositif INNO Expé Numérique :

Aide les PME bretonnes à déployer leurs solutions numériques innovantes sur de nouveaux marchés[1].

Cible des domaines comme la cybersécurité, les smart grids, la course au large, les transports et la mobilité[1].

Offre un soutien financier sous forme de subventions ou d'avances remboursables[4].

2. Critères d'éligibilité adaptés :

Les projets doivent durer moins de 24 mois et inclure une phase de développement, d'expérimentation (minimum 4 mois) et d'évaluation[4].

Le budget minimum varie selon les territoires (50 000 € pour les métropoles, 30 000 € pour les autres)[1].

3. Exemples concrets d'expérimentations :

Beo Healthcare a obtenu un financement de 150 000 € pour expérimenter son projet Alix MED auprès de patients en chirurgie du genou[2].

Des entreprises comme Defants (cybersécurité) et OSO-AI (santé) ont bénéficié de soutiens régionaux[1].

4. Infrastructures dédiées :

L'INH Lab, un tiers-lieu d'expérimentation en santé numérique dédié au handicap, illustre l'engagement de la région dans ce domaine[3].

5. Écosystème favorable :

La présence de technopoles et d'acteurs comme Biotech Santé Bretagne facilite l'accompagnement des projets innovants[2][3].

6. Stratégie régionale :

La Bretagne a mis en place une Stratégie régionale Recherche et Innovation (S3) qui encourage la transition numérique de l'économie et de la société[1].

Ces éléments démontrent que la Bretagne offre un environnement propice aux expérimentations, particulièrement dans le domaine numérique, avec des dispositifs de soutien financier, un accompagnement structuré et un écosystème favorable à l'innovation.

Citations:

- [1] <https://www.bretagne.bzh/aides/fiches/inno-experimentation-numerique/>
- [2] <https://www.tech-brest-iroise.fr/actualites-beo-healthcare-laureat-inno-experimentation-numerique-de-la-region-bretagne-2872-4740-0-0.html>
- [3] <https://www.biotech-sante-bretagne.fr/agenda/un-an-du-tiers-lieu-dexperimentation-en-sante-numerique-inh-lab/>
- [4] <https://les-aides.fr/aide/aJgv3w/region-bretagne/aide-a-l-innovation-inno-experimentation.html>
- [5] <https://www.francenum.gouv.fr/aides-financieres/guides-et-conseils-financiers/faites-appel-un-pole-europeen-dinnovation-numerique>
- [6] <https://digital-strategy.ec.europa.eu/fr/activities/funding-digital>
- [7] <https://digital-strategy.ec.europa.eu/fr/activities/digital-programme>
- [8] <https://group-gac.com/en/subsidies-innovative-projects-digital-sector/>

Annexes

Le numérique en Bretagne

CCETT

(http://racines.a3c7.fr/a3c7V3/index.php?option=com_content&view=article&id=573:le-livret-des-40ans-du-ccett&catid=83:les-40-ans-du-ccett-2012&Itemid=176)

CELAR (<https://www.defense.gouv.fr/dga/dga-maitrise-linformation>)

Université de Bretagne Sud

Ecole d'ingénieurs : IMT (Ex Télécom), ENSSAT...

BreizhCyber : <http://breizhcyber.bzh/>



<https://www.cyberblog.bzh>

Cybersécurité en Bretagne :

Bretagne développement innovation : <https://www.bdi.fr/fr/publications/annuairecyber/>



Des initiatives remarquables en Bretagne

B-Com

Institut de recherche et de technologie (IRT)

<https://b-com.com/>



Treebal

<https://www.treebal.green/>



Découvrir

Les valeurs de Treebal

Demandez une D  mo

BRETAGNE



Avec Treebal Pro, rejoignez le terrain !



* accessible gratuitement pour le grand public



Icodia

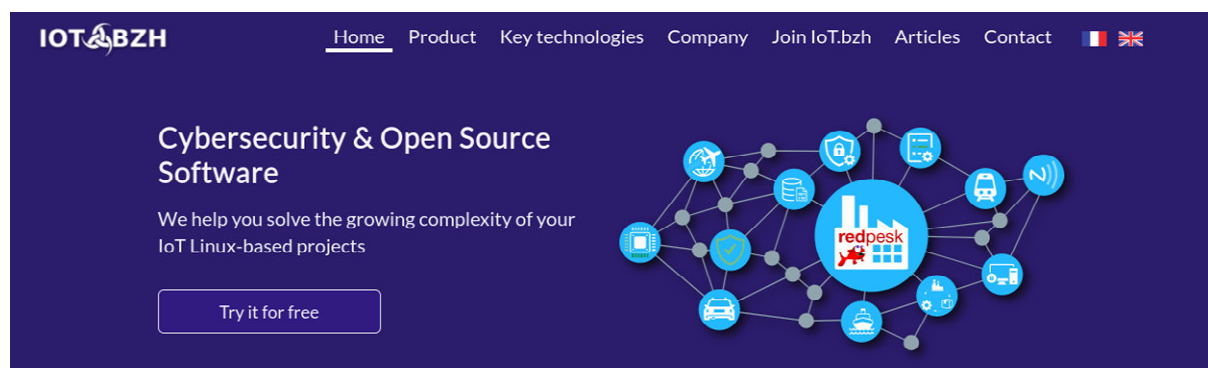
<https://www.icodia.com/>



171 vues 30 sept. 2024 - Conférence de Raphaël ANGLERAUX et Émeric COCAULT / Cofondateurs et dirigeants d'Icodia : « Comment ces Bretons sont-ils restés maîtres à bord de leur datacenter ? » lors du deuxième colloque national de Souveraine Tech, vendredi 20 septembre 2024, Palais du Grand Large de Saint-Malo (<https://www.youtube.com/watch?v=dsxA1--wmNA>) - <https://soveraine.tech/>

iot.bzh

<https://iot.bzh/>



A promotional banner for .bzh domains. It features a smiling woman with long blonde hair wearing a denim jacket, set against an orange background with white wavy lines at the bottom. The text 'UN POINT C'EST TOUT !' is in large white letters, with 'UR PIK, HA MAT PELL ZO !' in smaller black letters below it. At the bottom, a white bar contains the text 'Affichez votre ancrage en Bretagne comme 12000 sites en .bzh !' with 'Bretagne' in orange.

**UN POINT
C'EST TOUT !**
UR PIK, HA MAT PELL ZO !

Affichez votre ancrage en **Bretagne** comme 12000 sites en .bzh !

Anne Kerdi

L'influence Anne Kerdi n'est qu'un avatar ! Sur <https://www.instagram.com/annekerdi/>



A notre demande, Sébastien, le "père" d'Anne, a créé des visuels d'elle en situation d'interview. (DR)

<https://www.bretagne.bzh/actualites/nous-avons-interroge-anne-kerdi-linfluenceuse-la-plus-artificielle-de-bretagne/>

BreizhIA

<https://breizhia.org/>

BreizhIA, une
intelligence artificielle
bretonne, fière de l'être
et souriante !



Des événements du numériques en Bretagne

Connect'in

Mardi 12 novembre 2024 - Lorient

<https://connectin-lorient.fr/>

Breiz dataday

<https://breizhdataday.innozh.fr/>

15 mai 2025 - 9h – 18h > Saint-Brieuc

Glossaires du numérique

https://blogpeda.ac-poitiers.fr/ent-lyc/files/2020/02/Lexique_numerique.pdf

<https://www.grandecolenumerique.fr/metiers-davenir/lexique-du-numerique>

Bibliographie et vidéographie

Livres

Mendès-France Tristan, Leeds Quintin, *Internet – Une infographie*, CNRS Editions, 2021

Sites Internet

Benjamin Bayart, Président du FDN, cofondateur de la Quadrature du Net sur Thinkerviews (<https://www.thinkerview.com/benjamin-bayart-intelligence-artificielle-bullsht-pipotron/>)

Tariq Krim et Bernard Benhamou : Souveraineté numérique, la douche froide ? (<https://www.thinkerview.com/tariq-krim-et-bernard-benhamou-souverainete-numerique-la-douche-froide/>).

Comment les réseaux sociaux ont détruit la démocratie (<https://elucid.media/democratie/fabrice-epelboin-comment-les-reseaux-sociaux-ont-detruit-la-democratie>).

Géopolitique des réseaux sociaux - Le dessous des cartes | ARTE (<https://www.youtube.com/watch?v=hWeksJQQRyU>).

ARTE, *Echelon, le pouvoir secret* (<https://www.youtube.com/watch?v=cX0q-yFFQrQ>).

La quadrature du net : <https://www.laquadrature.net/>

