

Souveraineté numérique et souveraineté des données

Intervention DSI EST – 20/03/2025

An orange speech bubble graphic with a tail pointing downwards, containing the title and subtitle text.

Définitions

Intervention DSI EST – 20/03/2025

La souveraineté des données

« Le principe de la souveraineté des données désigne le droit qu'a un **État de réglementer et de contrôler la collecte, le stockage, et l'utilisation des données personnelles et autres types de données au sein de ses frontières.** »

Le **principe de la souveraineté des données** fait référence à la règle selon laquelle les données créées ou stockées dans un pays sont soumises à la législation de ce pays spécifique. Ce concept émerge comme une réponse aux préoccupations croissantes sur la **protection des données personnelles**, la **sécurité nationale**, et la **gouvernance de l'information** à l'ère où les données circulent librement à travers les frontières numériques.

Source : Avocat Droit International

C'est la capacité d'un état à réglementer et à contrôler :

- La collecte
- Le stockage
- L'exploitation

des données **sur son territoire**

La souveraineté numérique

« **la souveraineté numérique** c'est d'abord la capacité de maîtrise de son territoire numérique. Une fois qu'on a dit ça, la question ensuite c'est qu'est-ce qu'un territoire numérique ? Et pour moi, il ne se limite absolument pas au numérique visible, en tout cas aux logiciels. Les territoires numériques, je le vois vraiment comme la combinaison de ce qui rend possible notre vie numérique, c'est-à-dire notre accès au réseau, nos terminaux, les outils logiciels que nous utilisons, bien-sûr, les données que nous produisons, et du coup, toute la chaîne de valeur dont dépend ce territoire numérique. »

Ophélie COELHO

Doctorant chercheur

Spécialiste de la géopolitique du numérique

La souveraineté numérique est la capacité à maîtriser son territoire numérique, c'est-à-dire :

- Les accès aux réseaux
- Les terminaux et équipements informatiques
- Les couches applicatives
- Les données produits

A graphic featuring a large orange speech bubble on the left containing the text 'Sur quoi repose la souveraineté numérique ?'. To the right of the speech bubble is a bulleted list with three items: 'Les infrastructures (système, réseau, etc.)', 'Les applications', and 'Les données'. The background of the graphic has faint, curved, concentric lines in a light gray color.

Sur quoi repose la souveraineté numérique ?

- Les infrastructures (système, réseau, etc.)
- Les applications
- Les données

On doit aujourd'hui parler de souveraineté numérique en opposition au pouvoir croissant de la BigTech et à la dimension extraterritoriale des lois qui s'appliquent à ces mêmes acteurs de la BigTech.

Chronologie

Intervention DSI EST – 20/03/2025

1953 Small Business Act



Loi du Congrès Américain voté le 30 juillet 1953 permettant de réserver certains marchés publics aux petites et moyennes entreprises nationales.

La loi a également donné naissance à la Small Business Administration : agence fédérale indépendante dédiée à l'aide et au conseil pour protéger les intérêts des PME.

Donne également naissance à l'Office of Advocacy, chargé de se faire l'avocat des PME devant le Congrès.

Objectifs :

- privilégier les entreprises nationales pour les marchés publics*
- permettre à des PME de l'époque de devenir des Grandes Entreprises demain*

« le Gouvernement doit aider, conseiller et protéger dans toute la mesure du possible les intérêts de la petite entreprise, afin de préserver l'esprit de libre concurrence, d'assurer qu'une proportion équitable des marchés publics soit passée avec de petites entreprises, et de maintenir en la renforçant l'économie de la Nation dans son ensemble. »

*On est en 1953 – à cette époque on vient seulement de créer la CECA en Europe (1952).
En 2008 seulement : Small Business Act for Europe (+ Think Small First en 2011)*

1978 Foreign Intelligence Surveillance Act

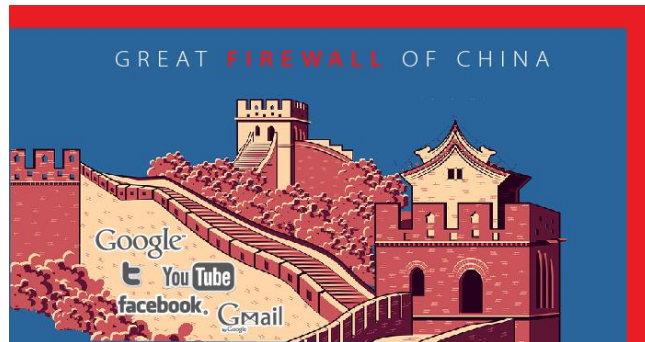


Cette loi américaine régit la surveillance des agents étrangers et des puissances étrangères sur le sol américain. Elle a été adoptée pour fournir un cadre juridique à la surveillance des renseignements étrangers tout en protégeant les droits civils des citoyens américains :

- *création d'une Cour FISA qui est chargée d'examiner et d'approuver les demandes de surveillance présentées par le gouvernement américain*
- *les agences de renseignement américaines doivent obtenir des mandats pour surveiller les communications des agents étrangers ou des puissances étrangères*
- *Protection des droits civils, demande de preuves crédibles*

Au départ, la FISA ne concernait que la surveillance électronique, mais elle a été considérablement modifiée pour traiter de l'utilisation des enregistreurs de numéro et des dispositifs de traçage, des perquisitions physiques et des dossiers commerciaux.

1998
Chine :
The Great Firewall



« The Great Firewall » en référence à la Grande Muraille de Chine, également appelé « Bouclier Doré » est dédié au filtrage du flux entrant mais également du flux sortant.

Portée : surveillance intra-territoriale

Pourquoi ?

- *surveiller les utilisateurs du réseau*
- *de recueillir les données personnelles des citoyens*
- *de bloquer l'accès à certains services étrangers*
- *maintenir la sécurité publique en identifiant rapidement les éventuels mouvements politiques dissidents*

Par ailleurs, il a créé les conditions nécessaires au développement des grandes entreprises chinoises : Baidu, Alibaba, Huawei, etc. qui ont pu se développer sans avoir à subir la concurrence des entreprises occidentales.

2001
Attentats aux
USA le 11 sept.



4 attentats perpétrés par Al-Qaïda : WTC 1, WTC2, le Pentagone, Washington (dans ce dernier cas, le vol s'est finalement écrasé en Pennsylvanie)

Au total, 3 711 morts

2001
PATRIOT Act
voté au congrès
le 26 octobre

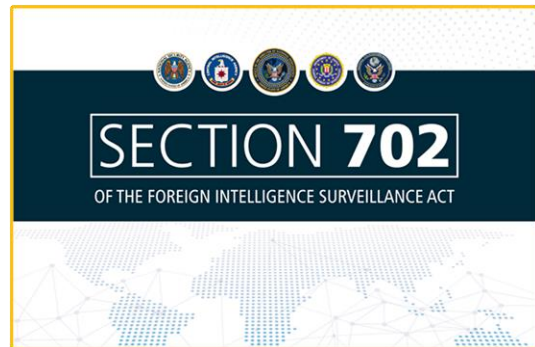


Cette loi a considérablement accru les pouvoirs des agences de sécurité nationale et des forces de l'ordre dans le but de prévenir et de combattre le terrorisme.

- 1. Surveillance accrue des communications électroniques et des communications financières des individus suspectés de terrorisme*
- 2. Facilitation des échanges d'informations entre les agences de renseignement et de sécurité*
- 3. Accès facilité aux dossiers médicaux, financier, et personnel des individus suspectés de terrorisme*

On est à ce stade, encore sur une surveillance individuelle.

2008 Amendement de la Loi FISA



Disposition législative qui autorise la surveillance ciblée des communications électroniques des personnes non-américaines situées en-dehors des USA :

- elle vise à permettre de collecter, sans mandat, des informations de renseignement étranger (via la NSA par ex) concernant des menaces pour la sécurité nationale (ex : terrorisme international ou prolifération d'armes de destruction massive)
- Elle permet aux agences américaines d'obtenir directement les données auprès des fournisseurs de services internet et de communication (Google, Microsoft, Apple, AT&T, etc.)
- interdiction de cibler un citoyen américain

Elle questionne sur 3 points :

- **La massification de la surveillance**
- **Le contournement des garde-fous juridique car dorénavant sans mandat**
- **l'utilisation réelle des données qui sont collectées ?**

Amendement renouvelé par Joe Biden en 2024 jusqu'en 2026

2011
Première
définition de la
souveraineté
numérique



« La souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques »

Pierre BELLANGER – PDG Groupe Skyrock

Egalement à l'origine du dispositif Alerte Enlèvement - 2004 (prévenance de l'ensemble des médias) – qui lui vaudra la Légion d'honneur

Publie en 2014 *La Souveraineté Numérique*

2013 L'affaire Snowden



Dans la nuit du 5 au 6 juin 2013, le quotidien britannique The Guardian publie sur son site Internet un document secret inédit, le premier d'une invraisemblable archive soustraite à la National Security Agency (NSA). Derrière cette fuite, la plus importante de l'histoire des services de renseignement américains, un ancien agent de la CIA et sous-traitant de la NSA : l'Américain Edward Snowden.

Performance and Registration Information Systems Management (PRISM)

Au-delà des révélations liées à l'espionnage généralisé des citoyens par les USA et le RU, cette affaire a également mis en lumière le rôle des entreprises privées dans le système et les process mis en place par les USA : DELL, Google, etc.

Agences mises en cause aux USA : CIA et la National Security Agency (NSA)

Agence mise en cause au RU : Government Communications Headquarters (GCHQ)

Les révélations ont aussi montré que les grandes entreprises numériques, lorsqu'elles n'étaient pas victimes des agences de renseignement, en étaient complices. Un statut difficile à assumer vis-à-vis de leurs utilisateurs et clients étrangers. Les révélations Snowden ont donc écorné la relation entre l'administration américaine et les géants américains du numérique, creusant un fossé qui n'a toujours pas été comblé.

Cet affaire a eu le mérite de déclencher une véritable prise de conscience, point de départ d'une réflexion globale en Europe sur la notion de souveraineté des données.

2020
Crise Covid-19

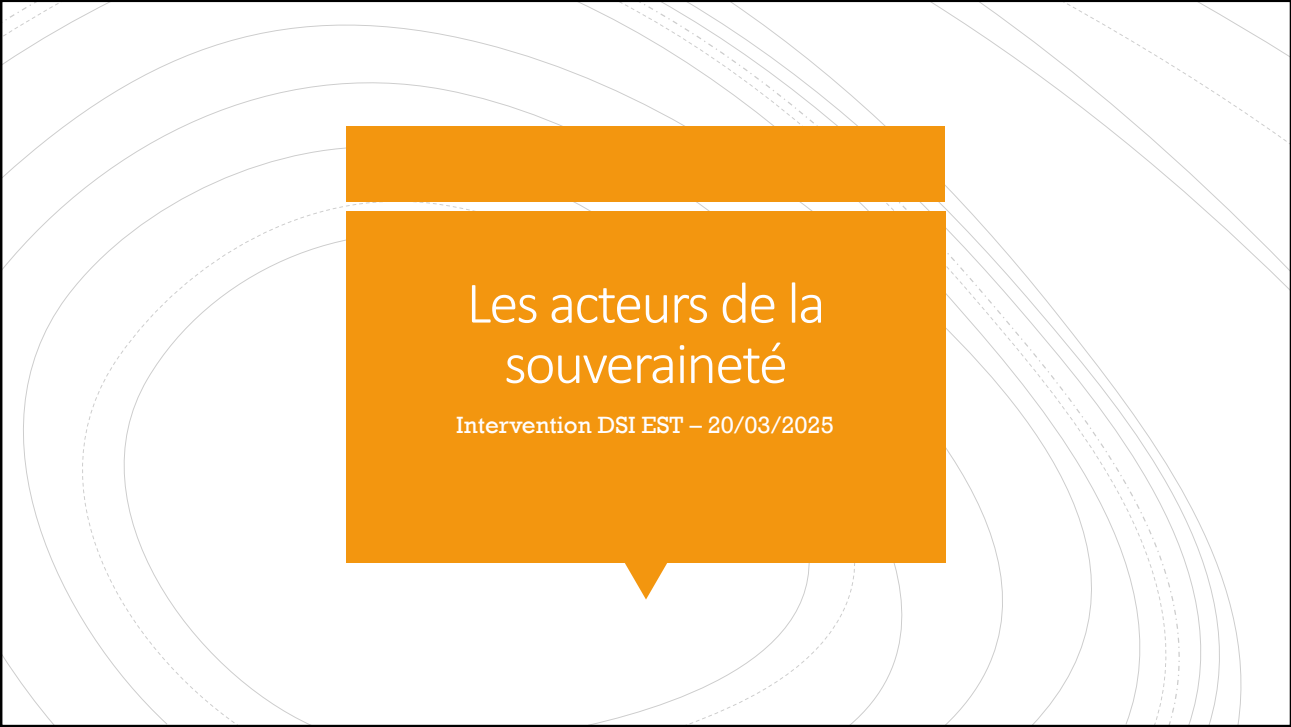


Télétravail : qui a principalement bénéficié aux éditeurs américains, Microsoft en tête

L'accélération de la migration des infrastructures vers le cloud

Cette crise a mis en lumière notre dépendance par rapport aux fournisseurs de services et éditeurs américains, mais elle a aussi mis en évidence notre dépendance à la filière des semi-conducteurs et à l'industrie chinoise.

Crise semi-conducteurs : les USA ont fait un pont d'or à TSMC pour son implantation sur le territoire et la Chine est allée plus loin : financement des entreprises à hauteur de 45 milliards d'euros (ex : YMTC et SMIC) et Pekin impose aux entreprises nationales d'acheter une part croissante de leur production auprès d'acteurs chinois. Ce modèle lui permet de sécuriser une demande locale, d'accélérer la montée en compétence de ses fabricants et de structurer un écosystème intégré. En garantissant un volume de commandes suffisant, elle réduit sa dépendance à TSMC et Samsung, tout en consolidant son autonomie technologique.



Les acteurs de la souveraineté

Intervention DSI EST – 20/03/2025



Les acteurs de la souveraineté

- Les acteurs de la réglementation (Commission européenne, Parlement Européen, Conseil de l'UE, etc.)
- Les institutions publiques (ex : CNIL, ANSSI, DINUM, ISN, etc.)
- Les acteurs économiques
- Les agents de communication (presse, scientifiques, influenceurs, etc.)



Les enjeux de la souveraineté numérique

Intervention DSI EST – 20/03/2025

Les enjeux

- La perte d'autonomie politique, économique, industrielle, etc.
- L'instrumentalisation des technologies,
- La capacité d'innovation,
- La compétitivité des entreprises,
- L'emploi,
- La normalisation (dans le sens de la définition de normes au niveau international) et le formatage des usages
- Le pouvoir des majors privés qui aujourd'hui dépasse celui des états (déterritorialisation des champs d'action des acteurs de la Big Tech)

Instrumentalisation des technologies : à des fins politiques par ex (Starlink en ukraine)

An orange speech bubble graphic with a tail pointing downwards, containing the title and subtitle text.

Quelques chiffres et illustrations

Intervention DSI EST – 20/03/2025

Au total, 113 millions d'euros
dépensés par les entreprises
de la tech en lobbying pour
l'UE

Les 10 premières entreprises
de la tech représentent plus
d'un tiers des
investissements totaux en
lobbying

Vue ci-contre filtrée sur la
catégorie « Groupes privés
et entreprises »

Pour information, Huawei
dépense environ 2 M € / an.

Source :
<https://www.lobbyfacts.eu>

EU Transparency Register data as of: 17 Mar 2025. A total of 3700 results.

#	Name	Head office in	Lobby costs	EP passes	Lobbyists (FTE)	Meetings with EC
1	Veracel Celulose SA	BRAZIL	10,000,000€ +		0.1	1
2	Meta Platforms Ireland Limited and its various subsidiaries	IRELAND	9,000,000€	10	18.45	244
3	Microsoft Corporation	UNITED STATES	7,000,000€	7	6.7	226
4	Amazon Europe Core SARL	LUXEMBOURG	7,000,000€		7.85	137
5	Apple Inc.	UNITED STATES	6,500,000€	10	8.3	120
6	Google	UNITED STATES	6,000,000€	16	7.15	392
7	Bayer AG	GERMANY	6,000,000€	10	22.05	61
8	Trinomics B.V.	NETHERLANDS	5,000,000€		25	3
9	Shell Companies	UNITED KINGDOM	4,500,000€	7	12.5	134
10	QUALCOMM Incorporated	UNITED STATES	4,000,000€	3	2.95	67

Capitalisation sectorielle des marchés boursiers mondiaux

Part du secteur IT :

USA – 29,6%

Canada / Australia / New Zealand : 9,1%

Europe : 7,8%

Japon : 13,1%

Marchés émergents : 13,2%

Source : Aswath Damodaran



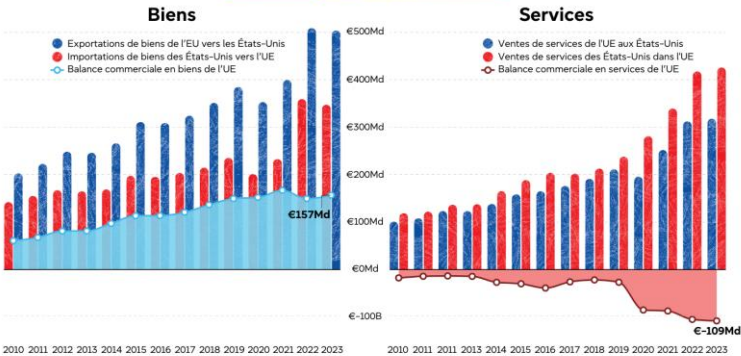
Échanges de biens et de services entre l'UE et les États-Unis
2010-2023, en milliards d'euros



Balance commerciale
USA <> EU en 2023

Source : Parlement Européen
[Commerce entre l'UE et les États-Unis : l'impact des droits de douane sur l'Europe | Thèmes | Parlement européen](#)

Source des données : Eurostat



Source: Eurostat [ds-059331, bop_it6,.det]

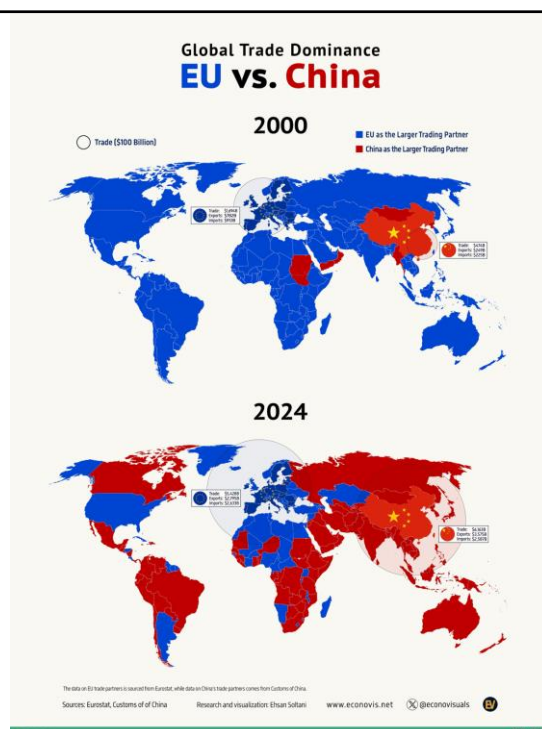


En 2020, l'UE était le principal partenaire commercial de la plupart des pays du monde, à l'exception d'Oman, de la Mongolie, du Myanmar, de la Corée du Nord, du Soudan et du Yémen. Cependant, en 2024, la Chine est devenue le partenaire commercial dominant pour la quasi-totalité de l'Asie et du Moyen-Orient, environ la moitié de l'Afrique, la plupart des Amériques (à l'exclusion des États-Unis, de l'Argentine et de quelques petites économies), ainsi que de la Russie et de l'Océanie.

Source graphique : Voronoi

[Global Trade Dominance: EU vs. China in 2000 & 2024 - Voronoi](#)

Source des données : World Trade Organization



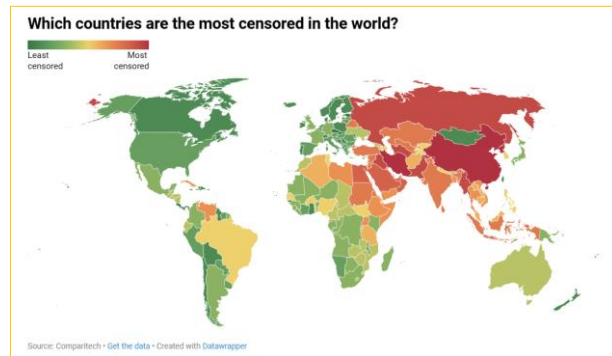
De 2000 à 2024, le commerce total de biens (exportations + importations) est passé de 1,69 billion de dollars à 5,43 billions de dollars pour l'UE (TCAC de 4,1 %) et de 474 milliards de dollars à 6,16 billions de dollars pour la Chine (TCAC de 11,3 %). En 2024, le volume total des échanges commerciaux de la Chine a dépassé celui de l'UE de 14 %, avec des exportations supérieures de 28 %, tandis que les importations étaient presque identiques. En conséquence, l'excédent commercial de la Chine était supérieur de 510 % à celui de l'UE. En 2024, le commerce en pourcentage du PIB s'élevait à 33 % pour la Chine et à 28 % pour l'UE

Top 3 des pays où l'Internet est le plus contrôlé / censuré : Corée du Nord, Chine, Iran avec une note de 12/12.

La Russie quant à elle à une note de 11/12.

Source :

<https://www.comparitech.com>



Cartographie interactive des câbles sous-marins

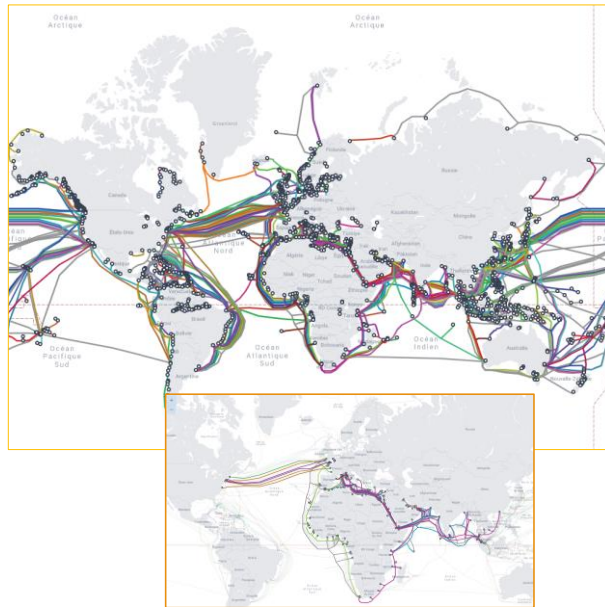
99% des échanges intercontinentaux

70% des infrastructures sous-marines sont détenues par les GAFAM

Sources :

[Submarine Cable Map](#)

[La France et son réseau de câbles sous-marins : enjeux et risques des infrastructures vitales du cyberspace](#)



Double dynamique sectorielle : émergence des acteurs privés (GAFAM) et recul des acteurs étatiques historiques (sociétés publiques).

La centralisation des propriétaires de câbles accroît la dépendance à leurs infrastructures, et donc le risque sur le secteur.

Deux entreprises françaises (Orange Maritime et ASN) semblent bien implantées parmi les fleurons de l'industrie mondiale, de plus en plus structurée par l'intense compétition entre les États-Unis (GAFAM) et la Chine (BATX).

Marseille : hub numérique mondial (11 câbles) et point de transit majeur sur l'axe Est-Ouest, avec une ouverture sur le Sud.

An orange speech bubble graphic with a tail pointing downwards, containing the title and subtitle text.

Le cadre réglementaire

Intervention DSI EST – 20/03/2025

« Les Etats-Unis innovent, la Chine copie, l'Europe régule ... »

À nuancer ...



ECPA
Electronic Communications Privacy Act
(1986)

TR Act
Telecom Reform Act (1996)

COPPA
Children's Online Privacy Protection Act
(2000)

Chips ACT
(2024)

...



DMA
Digital Markets Act (Mai 2023)

DSA
Digital Services Act (Août 2023)

GDRP ou RGPD
General Data Protection Regulation
(Mai 2018)

AI ACT
(2024)

...



CSL
Loi de Cybersécurité Chinoise
(2017)

Loi e-commerce
(2018)

PIPL
Personal Information Protection
Law (2021)

DSL
Data Security Law (2021)

...

RGPD : texte européen qui réglementaire qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne (droit d'accès / droit de rectification / droit d'opposition).

DMA : La législation sur les marchés numériques (DMA) vise à lutter contre les pratiques anticoncurrentielles des géants d'internet et corriger les déséquilibres de leur domination sur le marché numérique européen. Il est actuellement au cœur de l'actualité et alimente les tensions entre la Chine et l'UE

DSA : le DSA s'attaque quant à lui aux contenus illicites (haineux, pédopornographiques, terroristes...) et aux produits illicites (contrefaits ou dangereux) proposés en ligne. Il cherche notamment à harmoniser les législations nationales déjà en place dans les Etats membres en la matière et a pour mot d'ordre : *"ce qui est illégal hors ligne doit également être illégal en ligne"*. Le DSA interdit par ailleurs de cibler des personnes avec des publicités en ligne basées sur leur religion, leurs préférences sexuelles, des informations sur leur santé ou leurs convictions politiques. La publicité ciblée est également interdite vis-à-vis des mineurs.

DGA : cherche à créer un climat de confiance pour le partage des données au sein de l'UE afin de favoriser l'innovation et la croissance économique, et de générer des bénéfices sociétaux.

AI Act : destiné à encadrer de manière éthique et responsable le développement et l'utilisation de l'intelligence artificielle, tout en renforçant la compétitivité de l'UE dans ce domaine. Les produits d'intelligence artificielle doivent se voir apposer le marquage CE pour prouver qu'ils sont conformes aux exigences légales de l'Union Européenne.

Retour sur le sommet de l'IA de Paris : L'un des principaux résultats du sommet est l'adoption par 60 pays d'un **“cadre de confiance”** destiné à encadrer l'IA. L'objectif : **éviter la concentration du marché** et garantir un accès équitable à cette technologie.

Pourtant, **les États-Unis et le Royaume-Uni ont refusé de signer** ce texte pourtant non contraignant.

Le vice-président américain J.D. Vance a réaffirmé la priorité donnée aux intérêts nationaux : **“Les États-Unis sont les leaders de l'IA et doivent le rester”**. Londres partage cette position et préfère une approche nationale plutôt que multilatérale.

Aux USA : pas de loi fédérale sur la protection des données – seuls certains états comme la Virginie et le Colorado disposent de lois approchant celles du RGPD

Echanges en cours entre les USA et l'EU sur le DPF – Data Privacy Framework pour harmoniser les règles entre les USA et l'EU.

Le pb actuel principal est l'extra-territorialité des lois américaines pour les données des citoyens et entreprises européennes

Des approches philosophiques et politiques différentes

UE : la protection des droits des citoyens est au cœur des politiques et législations en Europe. Cela se traduit d'abord par des rapports de force inégaux entre les entreprises et les citoyens, les seconds l'emportant clairement sur les premières.

USA : la liberté avant tout ! Politiques et législations des activités numériques américaines se caractérisent par la centralité de la liberté d'entreprendre et la liberté d'expression.

En Chine : la sécurité intérieure d'abord ! Le grand paradoxe en Chine est la coexistence entre une économie numérique dynamique et un cadre politique strict.

Source – Fondation Robert Schumann :

[Législation numérique : convergence ou divergence des modèles ? Un regard comparatif Union européenne, Chine, États-Unis](#)

USA : les [chercheurs](#) comme [Adam Thierer](#) ont qualifié les approches de l'Union européenne et des États-Unis respectivement de « réglementation prudente » et de « réglementation à autorisation automatique ». Avec la première, les nouvelles technologies ne peuvent être mises en œuvre que lorsqu'il est prouvé qu'elles ne nuisent pas aux citoyens. La seconde suit une logique contraire : les nouvelles technologies sont automatiquement permises sauf si suffisamment de cas démontrent leur nuisance. Très souvent, dans la jurisprudence, les droits des entreprises du numérique prévalent sur ceux des citoyens. Les lobbyings des entreprises du numérique aux USA sont par ailleurs très forts (cf. investiture de Trump : Sam Altman (OpenAI), Sundar Pichai (Alphabet), Jeff Bezos, Shou Zi Chew (Tik Tok))

En Chine : Alors que le versant économique vise à réaliser les objectifs favorables à la société, tels l'innovation technologique, le versant politique est marqué par sa centralisation. Dirigé par le Cyberspace Administration of China depuis 2014, il vise à atteindre en priorité des objectifs favorables au régime : la sécurité nationale, la stabilité sociale et le leadership du Parti dans la sphère idéologique. La Chine partage beaucoup de similitudes avec les démocraties occidentales en matière économique. [Une convergence régulatrice](#) se profile progressivement dans la responsabilisation des sociétés numériques, la législation anti-trust et la protection des données personnelles. Cependant, au cas où la transgression de règles par les sociétés numériques nuirait à la sécurité nationale ou à la stabilité sociale, l'État-parti réagit

promptement en envoyant les régulateurs nationaux en première ligne (ex : Jack Ma – PDG d'Alibaba - en 2020 – disparu pdt 2 mois et qui a fait de rares apparitions publiques - qui vient de réapparaître publiquement le mois dernier aux côtés de Xi Jing Ping)

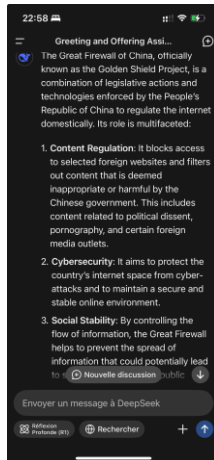
An orange speech bubble graphic with a tail pointing downwards, containing the text 'Et demain?' and 'Intervention DSI EST – 20/03/2025'. The background of the slide features a pattern of concentric circles and curved lines in light gray.

Et demain?

Intervention DSI EST – 20/03/2025

L'Intelligence Artificielle

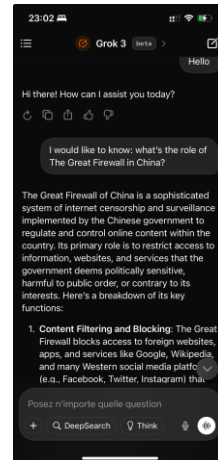
Test IA : DeepSeek / Chat GPT / Grok
« What's the role of The Great Firewall in China? »



DeepSeek



ChatGPT



Grok

Pour DeepSeek : le projet est un ensemble d'actions législatives et techniques destiné à réguler l'Internet domestique, à protéger les utilisateurs, et à garantir la paix social
Pour ChatGPT et Grok, il s'agit très clairement d'un outil de surveillance de masse et de censure destiné à maintenir le parti communiste au pouvoir en contrôlant les moindres mouvements dissidents.

Autre test : « Is China a democracy? »

Les IA ne sont pas neutres, chaque IA présente des biais :

- Des biais culturels (dépendant essentiellement de la culture et des valeurs de ses concepteurs)
- Des biais liés à la collecte initiale des données

NB : attention au données que nous allons injecter dans les LLM qui sont liées à nos activités professionnelles

Sommet de l'IA de PARIS : 2 pays ne l'ont pas ratifié – les USA et le Royaume-Uni

L'espace

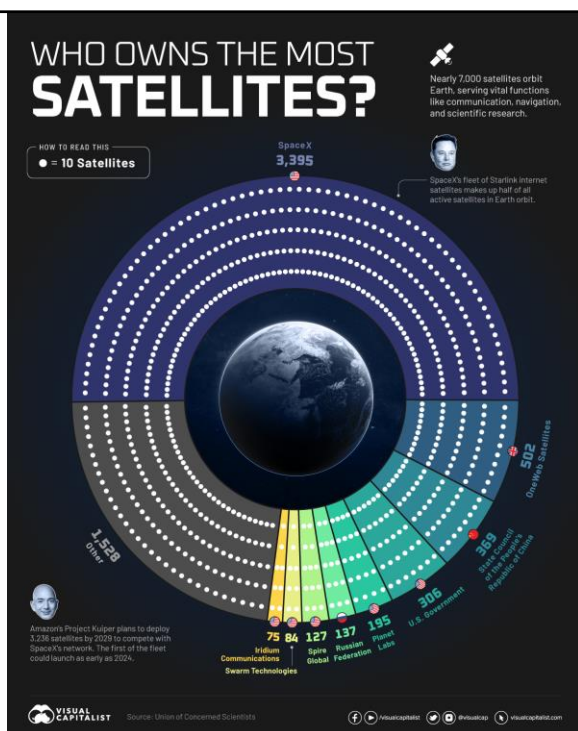
Au total, il y avait plus de 7 500 satellites en orbite autour de la terre en 2023. Il y en a 11 000 aujourd'hui.

Principaux acteurs : SpaceX (Starlink), Amazon (Kuiper)

Date des données : septembre 2023

Source des données : Union of Concerned Scientists

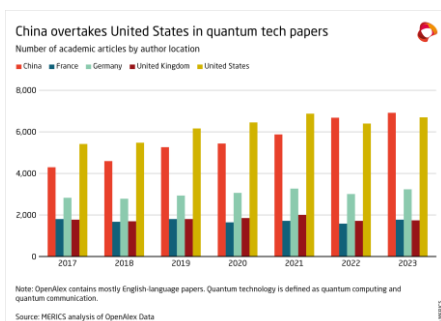
<https://www.ucsusa.org/resources/satellite-database> (visualisation Voronoi)



Objectif d'Amazon : 3 500 satellites d'ici 2029 (pour rattraper Starlink). Avec un prévisionnel de 1 700 satellites environ d'ici quelques mois, le réseau satellitaire d'Amazon devrait être opérationnel en 2026

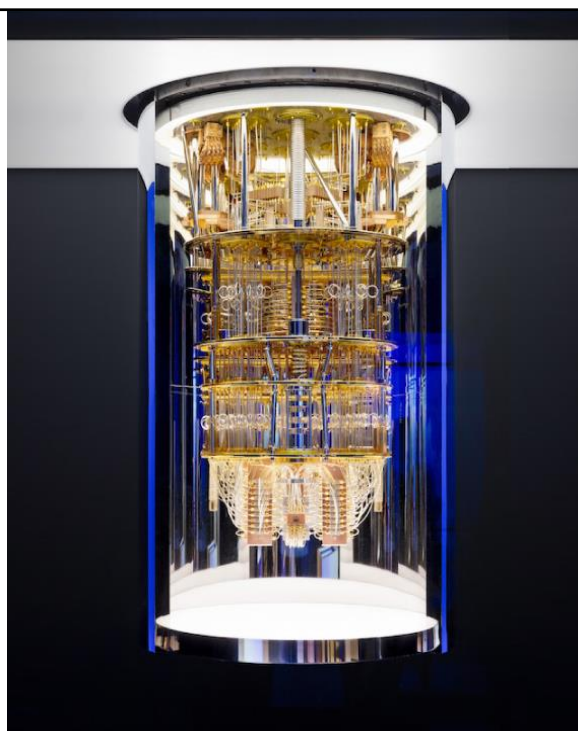
Perte de la neutralité

Le quantique



Source :

<https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch>



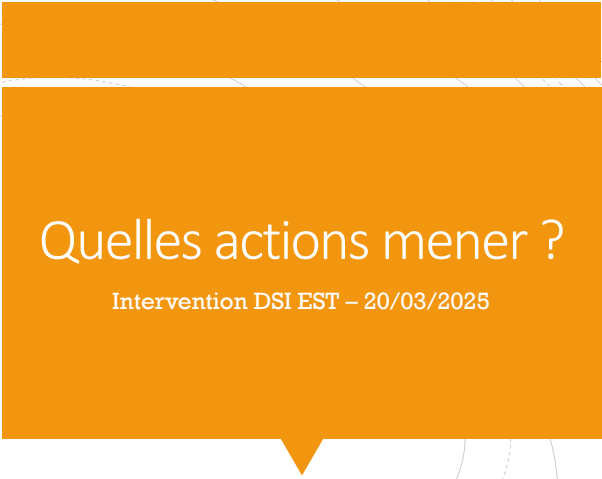
L'informatique quantique est un domaine révolutionnaire qui exploite les principes de la mécanique quantique pour traiter l'information d'une manière dont les ordinateurs classiques ne peuvent pas le faire. Contrairement aux bits traditionnels, qui représentent les données sous la forme de 0 ou de 1, les bits quantiques (qubits) peuvent exister dans plusieurs états simultanément, grâce à la superposition. De plus, l'intrication quantique permet de relier les qubits, ce qui permet de résoudre les problèmes plus rapidement et plus efficacement. Les ordinateurs quantiques ont le potentiel d'avoir un impact significatif sur des domaines tels que la cryptographie, la science des matériaux, l'intelligence artificielle et les simulations complexes. Cependant, ils en sont encore à leurs débuts et doivent surmonter des défis en termes de stabilité et d'évolutivité avant une utilisation pratique généralisée.

Pour l'instant la France fait à priori partie du peloton de tête avec les USA et la Chine.

Les plus gros acteurs du secteur :

- IBM (USA)
- D-Wave Solutions (USA)
- Intel (USA)
- Alphabet (USA)
- Honeywell International (USA)
- Rigetti Computing (USA)

China Telecom Quantum Group – CTQG (Chine)
QuantumCTek (Chine)
IonQ (USA)
Atos
Alice & Bob (FR)
Pasqal (FR)
Quandela (FR)

An orange speech bubble graphic with a tail pointing downwards, containing the title and subtitle text. The background of the slide features a pattern of concentric circles and curved lines in light gray.

Quelles actions mener ?

Intervention DSI EST – 20/03/2025

- Tenir compte de la **perte d'autonomie** lors du choix d'une solution applicative, d'une infrastructure, d'un prestataire
- Réaliser une **cartographie de ses dépendances numériques**
- Réaliser une **matrice des risques**
- S'assurer **du chiffrement des données** (pour transport et stockage en s'assurant de maîtriser les clés)
- Analyser les **conditions juridiques** – CGV / CGU (ex : s'assurer de la réversibilité de ses données, localisation HQ, tribunaux compétents, etc.)
- Penser à **impliquer la Direction Générale** dans les choix liés aux projets structurants en abordant le projet, entre autres bien entendu, sous le prisme de la souveraineté numérique
- Quand nécessaire, possible, sélectionner des **prestataires certifiés** : ISO27001, SecNum, etc.
- S'appuyer sur des **datacenters de proximité** (pour questions de sécurité + RSE)



Conclusion

Intervention DSI EST – 20/03/2025

Un enjeu de souveraineté décisionnelle

- Au-delà de la souveraineté numérique, c'est la capacité à faire des choix libres qui est en jeu
- Les décisions politiques sont aujourd'hui contraintes par nos dépendances numériques
- Nécessité de préserver des marges de manœuvre pour l'avenir
- Se rappeler que la donnée produite par l'entreprise, rapportée à un écosystème global, peut avoir une valeur critique. Vos données doivent par conséquent être protégées (les outils de surveillance US et CH sont clairement utilisés pour l'intelligence économique).

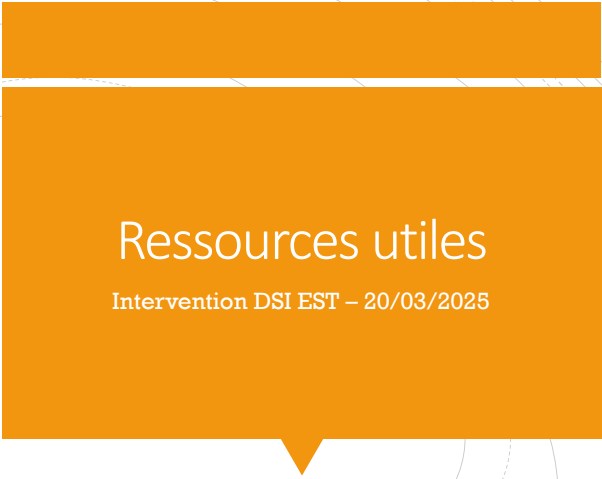
Exemples :

Retrait de Starlink d'Ukraine (couper Internet, y compris les communications militaires)

Arrêt du service de renseignement des USA > Ukraine

Trump a fait pression comme ça sur Zelensky pour l'obliger à accepter l'accord de paix (pour servir ses propres intérêts : Trump vise le prix Nobel de la Paix)

Les États occidentaux sont encore imprégnés de l'idée que seules certaines informations ont besoin d'être protégées. Nous commençons seulement à nous rendre compte que, regroupées avec d'autres ensembles de données et analysées à travers le filtre de l'intelligence artificielle, des données qui, en soi, sembleraient inoffensives, peuvent être très révélatrices – d'une manière que nous ne souhaitons peut-être pas.

An orange speech bubble graphic with a small tail pointing downwards, containing the text 'Ressources utiles' and 'Intervention DSI EST – 20/03/2025'. The background of the slide features a light gray pattern of concentric circles and curved lines.

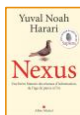
Ressources utiles

Intervention DSI EST – 20/03/2025

- L'Institut de la Souveraineté numérique : [Institut de la souveraineté numérique](#)
- Renaissance Numérique - [Le think tank dédié à la transformation numérique de la société](#)
- Numérique : le feu roulant des USA contre la régulation européenne : https://www.lemonde.fr/economie/article/2025/03/05/numerique-le-feu-roulant-des-etats-unis-contre-la-regulation-europeenne_6576612_3234.html
- Sismique : [Géopolitique du numérique : l'impérialisme à pas de géants](#)
- Deepseek, la souveraineté numérique - <https://www.contretemps.eu/deepseek-ia-souverainete-numerique/>
- Données sur les marchés des télécommunications et des réseaux : <https://www2.telegeography.com/>
- Data Visualization : <https://www.voronoiaapp.com>
- CAIRN Info : [Chapitre IV. L'espionnage économique | Cairn.info](#)
- Polytechnique Insights : <https://www.polytechnique-insights.com/dossiers/economie/la-guerre-technologique-entre-la-chine-et-les-usa/comment-la-chine-veut-gagner-la-course-a-la-suprematie-technologique/>

- Qu'est-ce que l'AI Act : <https://www.info.gouv.fr/actualite/quest-ce-que-lai-act>
- La régulation du numérique : Chine, Etats-unis, France : [226-regulation-fr-2023-07-26-w.pdf](#)
- The Chips Act : <https://www.pwc.com/us/en/library/chips-act.html>
- Prolongement section 702 du FISA : <https://www.lemondeinformatique.fr/actualites/lire-fisa-section-702-les-us-prolongent-son-permis-de-surveillance-a-l-etranger-93552.html>
- Pourra-t-on tendre vers une souveraineté quantique : <https://www.annales.org/enjeux-numeriques/2023/en-2023-09/2023-09-11.pdf>
- Quel est l'état des droits sur Internet aux Etats Unis : [Quel est l'état des droits sur internet aux États-Unis ?](#)
- Sommet de l'IA 2025, ce qu'il faut retenir : [Sommet de l'IA 2025 : ce qu'il faut retenir](#)
- Souveraineté européenne et protection des données, qui mène la danse : [Souveraineté européenne et protection des données : qui mène la danse ?](#)
- Cybersécurité et cyberdéfense – un sujet géopolitique – Guillaume Poupard : <https://www.youtube.com/watch?v=Iw5JztDeSRE>

Bibliographie



« Nexus : A brief History of Information Networks from the Stone Age to AI »

Yuval Noah Harari

Editions Albin Michel - 2024



« Mémoires vives »

Edward Snowden

Editions du Seuil – Collection Points – 2019



« La souveraineté numérique »

Pauline Türk, Christian Vallar

Editions Mare & Martin – 2018



« La souveraineté numérique »

Pierre Bellanger

Stock – 2014



« Géopolitique du numérique »

Ophélie Coelho

Les éditions de l'atelier – 2023

Merci !

Intervention DSI EST – 20/03/2025