Quentin Guého

LEGAL STUDY OF THE STRATEGIC NECESSITY OF DEVELOPING SOVEREIGN TELECOMMUNICATION SPACE-BASED CAPABILITIES

Why U.S. Data Law Tells Us to Develop Our Own Satellites

INTRODUCTION

"It's not good for Europe to be the permanent security vassal of the United States." For the United States Vice President J. D. Vance, Europe is a vassal of the United States.[1] This is also the conclusion of the latest National Security Strategy of the United States of America, dated November 2025: "Enabling Europe to stand on its own feet and operate as a group of aligned sovereign nations, including by taking primary responsibility for its own defence, without being dominated by any adversarial power."[2] Europe would therefore be lagging behind, unable to steer itself, and the United States would be the unexpected saviour of the Old Continent.[3] The United States is indeed preeminent in many sectors, including the digital and space sectors. Europe – meaning this term in a broad sense, both the European Space Agency (ESA), the European Union (EU) and the states of the European continent (in the narrow sense, excluding Türkiye and Russia) – is struggling to compete. Without focusing on the veracity of such a statement,

1 France 24 2025a.

2 The White House 2025a: 27.

3 This other quote helps to understand the spirit of the document: "But this economic decline is eclipsed by the real and more stark prospect of civilizational erasure" (The White House 2025a: 25).

DOI: https://doi.org/10.36250/01374_11

it must be recognised that in the satellite communications sector, the U.S. mega constellations – namely the two main constellations, Starlink from the company SpaceX and soon Amazon LEO – dominate the world market pending the arrival of Chinese constellations.

At first glance, there is nothing to worry about: not all countries are destined to send such infrastructures into space; Europe is therefore not necessarily threatened by such activities and can even benefit from them, with, for example, the launch of Amazon's future satellites with Ariane 6. At first glance, only because the data that passes through these satellites is not protected. In contrast, U.S. law is designed to prevent legal protection. In this demonstration, we will explain the legal architecture that allows U.S. authorities to access all this data and the vulnerabilities it poses for European countries and their populations. This demonstration can only be complete after an understanding of the place of data and of the U.S. in our contemporary world.

CONTEXT – DATA, SPACE AND EUROPE

To understand the issues surrounding space telecommunications capabilities, it is necessary to explain first why and how data is at the heart of our society. Only once this element is understood and explained will we be able to contextualise the space sector in this environment. Finally, it will be time to show the respective places of the United States and Europe in this world of data.

Digital data at the centre of the world

The term *data* is very broad and can be defined in several ways. We will retain a broad but numerical definition: data is information, such as an image, a message, a document, but also more subtle information, such as the time a user uses an application, or his or her personal information. Metadata, data that provides information about other data, is included in this definition. In

short, everything that is created and/or informed and/or communicated on/by an electronic device is digital data that interests us. Digital data is created by a variety of actors: the average person, through their use of the internet, emails and other applications, but also companies (quotes, invoices, orders, patents, etc.), governments and armies. It is also becoming essential to take into account data generated by artificial intelligence of all kinds.

The numbers are uncertain, but the volume of data created each year continues to increase. In 2025, it is estimated that just over 400 million terabytes (TB) of data will be created each day, which would amount to about 147 zettabytes (ZB) by 2025.[4] For 2029 alone, this figure is expected to reach 527.5 zettabytes.[5] Figures so large that it becomes difficult to realise what they represent.[6] For example, if a film weighed 1 gigabyte (GB), 1 zettabyte would be equivalent to 1,000,000,000,000 films, or 1 trillion films, i.e. a thousand billion films. This impressive amount of data, created and transmitted around the world, has even given its name to the Zettabyte Era.[7] It can be difficult to determine which country generates the most data, as it depends on the parameters chosen: the nationality of the person creating the data, the nationality of the company publishing the software used to create it, and the place of storage. An analysis method considers four criteria: volume, use, accessibility and complexity. Without going into details, the countries that lead in data creation are considered rich and highly developed, with the United States leading the way. France comes sixth.[8] Other European countries are generally at the top of the ranking, with the United Kingdom in second place, Switzerland in fourth, Sweden in eighth, and Germany in thirteenth, ahead of Spain, Ireland, Italy and Portugal, which are ranked 14th to 17th, respectively. And, of course, China ranks third. Software based

4 Duarte 2025.
5 Taylor 2025a.
6 Ionos 2021.
7 For further information see https://en.wikipedia.org/wiki/Zettabyte_Era.
8 Zoox Smart 2020.

on artificial intelligence will further increase the volume of data created,[9] a sector in which the United States excels, even dominates.[10]

Another way is to look at the global distribution of data centres: the United States comes first with more than 45% (5,381 data centres in March 2024), followed by Germany, the United Kingdom, China, Canada and France in sixth place.[11] However, this does not reveal the nationality of the data centre's owner, which may differ. It is therefore interesting to note that the companies with the most data centres in the world are mainly American: Amazon Web Services (AWS) in first place, followed by Microsoft Azure, Google Cloud and Meta[12] – four of the five GAFAMs.[13]

This data represents significant potential for exchanges around the world, including online. However, not all of the data stored necessarily passes through the internet: some is used as a backup or archive or is rarely consulted. It should also be added that some data is stored on so-called local networks, which are therefore not directly connected to the internet.[14] According to the International Telecommunication Union (ITU), global traffic will reach about 9 zettabytes in 2025, a figure that continues to grow.[15]

This data can take various forms: a video accessible online, a message posted on a social network or sent *via* a connected application, or a document sent by email. Data, as such, does not necessarily have great value, except

9 Foley 2024.

10 Koetsier 2025.

11 Lu 2025. The ranking is therefore slightly different from the previous one, but developed countries remain at the top, demonstrating the link between wealth, digital usage and control of infrastructure.

12 Jackson 2024.

13 It should be noted here that we are focusing on GAFAM, but U.S. companies are present everywhere, all the time, at all levels. The problem is therefore systemic and requires global awareness, not just digital awareness. We are thinking, for instance, of McKenzie Wark's work on the vectorialist class, which refers to economic agents who own and/or control the vectors through which information and emotions circulate between us in digital form. Guillaud 2025: 132–133.

14 It is estimated that half of the data is stored on servers that are not directly connected to the network, but it is obviously impossible to know. Edge Delta 2024.

15 ITU 2025.

for the creator and the recipient. In other cases, the data may have great intrinsic value, such as plans for a new technological innovation.

First of all, it should be noted that data can be produced by different categories of people: private individuals, companies, governments, institutions and armies. The importance of the data and its level of protection depend on the data itself: an individual's medical data is highly sensitive, as is the document describing a state's military strategy or the merger plan of two companies. The value of the data, therefore, depends greatly on the creator of the data and on the person who wants to use it: the personal messages of a private person may be of little importance to an army, but of great importance to a government or a company. Military strategic documents, on the other hand, are of no use to a private person, while a foreign government will know how to make good use of them. So, depending on where the data comes from, where it is going, and what it can be used for, the value of the data changes. Therefore, data accessibility is also a criterion to consider when evaluating its value.

Data, no matter what it is, is at the centre of our capitalist[16] society,[17] but data is never neutral, nor is the algorithm that processes it.[18] For this demonstration, we will focus on two uses of data: commercial exploitation and a use that could be described as *regalian,* encompassing both governmental and military aspects. Regarding the commercial use of data, it is accepted that companies selling goods and services seek to maximise their profits *at all costs.* This requires a massive accumulation of data from private individuals – sometimes through problematic methods[19] – to analyse the preferences and behaviours of the greatest number. This analysis then makes it possible, through many means such as advertising and marketing, to orient

16 The concept of "capitalism" is multifaceted. We will not enter into the debate, but will retain an element of the IMF's definition that we believe is sufficient for our demonstration: "The essential feature of capitalism is the motive to make a profit" (Jahan – Saber Mahmud s. a.).

17 Sadowski 2019.

18 Guillaud 2025: 28.

19 European Commission 2018: 67–87.

the consumption of the masses.[20] This is a surprising phenomenon at first glance, but it has been demonstrated: the behaviour of individuals can be largely influenced by companies.[21] This accumulation of data, combined with in-depth analysis, also allows these companies to influence public policies through intensive lobbying.[22] Through this lobbying, companies now have access to the highest levels of power to keep their interests at the top of the state's priorities.

Regarding the sovereign use of data, States have an obvious – but not necessarily legitimate – interest in accumulating the private data of their nationals (private or legal persons) or foreigners.[23] The state, and therefore the government, seeks to maintain its stability, civil peace and coherence, and thus its economic growth, a high employability rate, and a decent standard of living; in short, the prosperity of its inhabitants. The control and surveillance of the said inhabitants make it possible to achieve this goal in part. Data surveillance helps guard against both internal and external threats.[24] The government and its authorities, therefore, have every interest in accessing as much data as possible.[25] The best example remains the mass surveillance of civilian populations by the U.S. Government and some of its allies.[26] Furthermore, beyond the simple survival of the state, a government may seek to acquire more power. Armies, constantly preparing for the possibility of conflict, have just as much interest in accumulating this data and predicting future conflicts, as well as their form and nature.[27]

These two examples of data use[28] serve as a basis for reflection to demonstrate the importance of maintaining a certain degree of sovereignty over our data.

20 Zuboff 2019: 25–30.

21 Zuboff 2019: 271–314.

22 HATVP 2025; Zandt 2022; Thuy D. 2025; Vou 2020; Sieraczek-Laporte 2025.

23 Tambou – Barbou des Places 2020.

24 SGDSN 2016; Garrigou 2025.

25 SGDSN 2025.

26 Untersinger 2022.

27 Koch 2018; Droff–Malizard 2024; Hardy 2021.

28 Data can be used in many ways, and sometimes positively. For example, space data is also being used to combat climate change.

The space sector's place in this world of data

The vast amount of data generated and exchanged every day requires a dense, global infrastructure. As we have seen, online data is stored in data centres. Most – almost half – are in the United States, and the rest are spread around the world, mostly in Asia and Europe. Data centres are at the heart of this global network. These multiple cores are accessible anywhere in the world thanks to a network of cables and waves. The vast majority of countries worldwide are connected by submarine cables: more than 99% of data traffic passes through them.[29] Then the land cables take over. All these cables connect continents, countries, and data centres to enable data transfers. Today, the last few meters are often made by Wi-Fi or 5G, waves generated by antennas connected to the cable network.[30]

The user – regardless of whether it is a private person, a company or a state – creates, consumes and transfers data, thanks to an electronic device – *hardware* – and one or more *software.* To access the network, the user needs a device (computer, smartphone) connected, either via cable (e.g. Ethernet) or wirelessly (e.g. 5G or Wi-Fi). These waves are emitted by devices (such as internet boxes or antennas) that are themselves connected to the local cable network, which is in turn connected to the global cable network. Service providers (e.g. Orange or Vodafone) act as intermediaries at the local level between data centres and users, *via* this network of cables and other ground infrastructure. Users consume data stored in data centres around the world and store their own data in those same centres. While users choose for themselves which services – and *software* – to use, and even which service provider to subscribe to, they generally do not decide exactly which data centre their data is stored in, or which submarine cable it travels through.

[29] Gaur 2026; International Telecommunication Union 2026.

[30] International Telecommunication Union 2025.

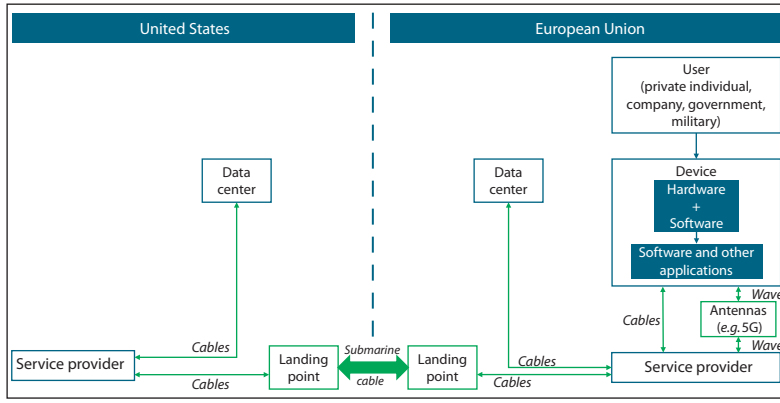

Figure 1. *Network connecting a European user to data centres in Europe and the United States (excluding the space sector)*
Source: Compiled by the author.

What is the place of space infrastructure in this network? Historically, satellites have been used to provide intercontinental television services (e.g. sports broadcasts or news channels).[31] Private satellite communications were also possible, but rarer because they were very expensive.[32] Of course, generously endowed armies had access to these technologies.[33] The New Space phenomenon has radically changed the space telecommunications sector: the falling cost of access to space and the miniaturisation of technologies have enabled the rise of low-Earth orbit mega constellations, allowing the provision of satellite telecommunications services to a wide range of consumers at a much more affordable cost:[34] in 1998, Iridium offered calls costing $6 for 30 minutes from a $3,000 phone, while Starlink offers

31 Cité de Télécoms s. a.; Saillant 1994.
32 CNES 2025a.
33 Lacomia 2025; Guillou 2013; Paolini 1987.
34 CNES 2025b; Rainbow 2024; Fernholz 2024; Croshier 2022.

high-speed internet access for a subscription starting at €29 per month and an antenna costing a few hundred euros.[35] The Starlink constellation is the most emblematic and developed to date, but others exist or are in development, including OneWeb, Amazon Leo, and many Chinese projects.[36]

These satellite networks can be inserted into the global network in different ways. In the first scenario, the satellites simply replace the submarine cable. The information passes from the data centre to the satellites via a ground station. It is then transmitted via another ground station to the user or another data centre *via* the existing network.

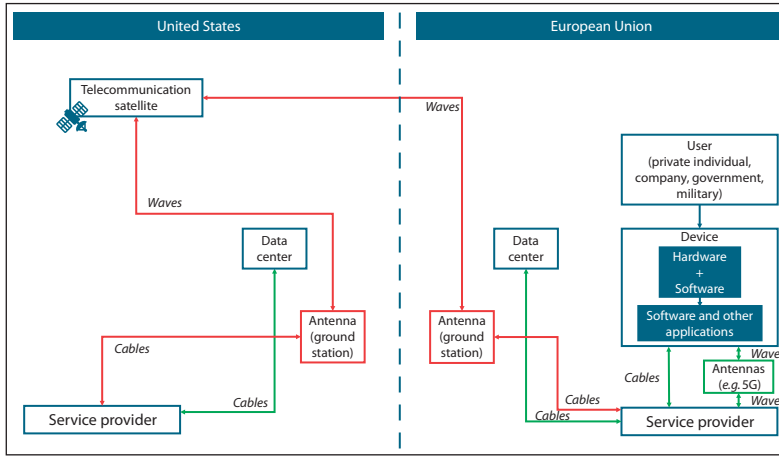

Figure 2. *Satellite network connecting a European user to data centres in Europe and the United States via a ground station*
Source: Compiled by the author.

35 Heijmann 2022; Starlink s. a.
36 McDowell 2026.

In a second scenario, the user has a private antenna that acts as an individual ground station. The satellite network acts directly as a network provider here. This integration is particularly indicated in rural areas not connected to the grid.

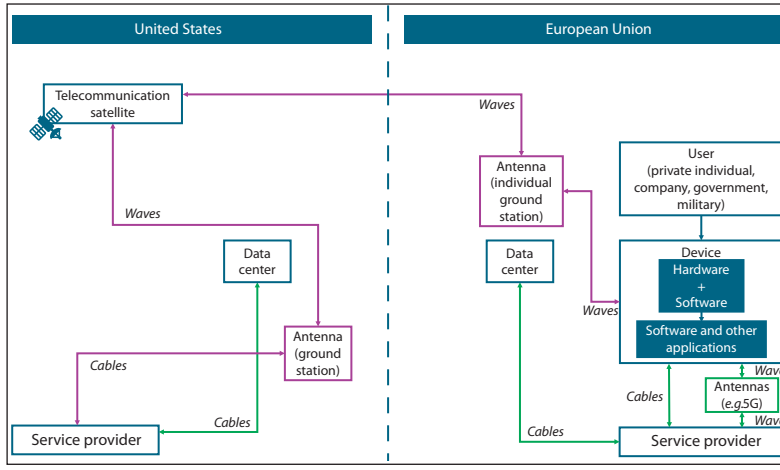

Figure 3. *Satellite network connecting a European user to data centres in Europe and the United States via an individual ground station*
Source: Compiled by the author.

The third scenario connects the satellite network directly to the user's device: this is the direct-to-device. There is no longer a need for antennas; the user is directly connected to the satellites. On the other hand, we typically find a ground station connected to the data centres and, more generally, to the network.

Satellite telecommunications are therefore part of a broader system of users, devices, data centres and submarine cables. The question of infrastructure control, therefore, arises.

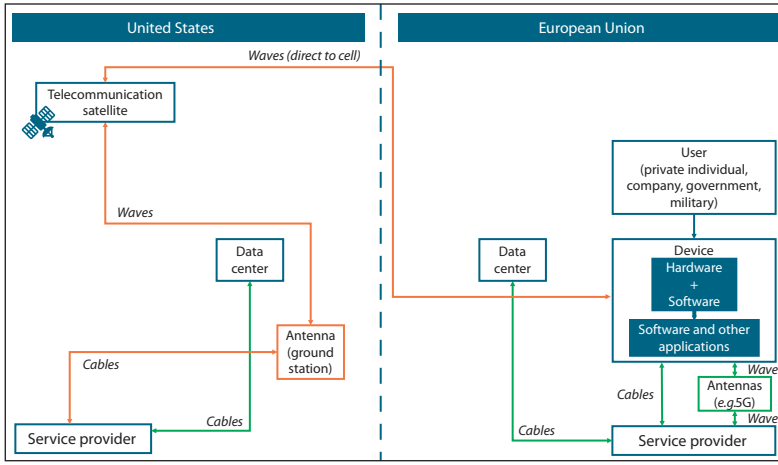

Figure 4. *Satellite network connecting a European user to data centres in Europe and the United States via direct to cell*
Source: Compiled by the author.

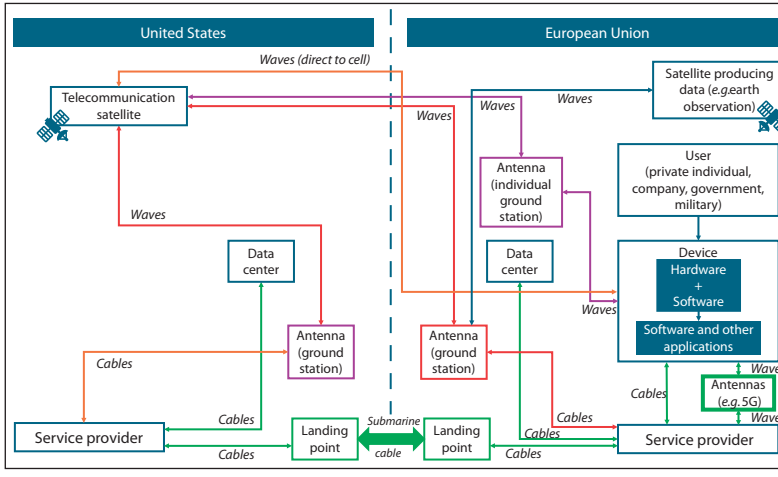

Figure 5. *Network connecting a European user to data centres in Europe and the United States (including the space sector)*
Source: Compiled by the author.

The United States: An unmissable digital space superpower for Europe

The United States is at the centre of the global network. In particular, companies in the digital and space sectors are omnipresent. Social networks, submarine cables, mega constellations of telecommunications satellites, cloud: these private players are everywhere and are massively supported by the state. Before dwelling on U.S. regulations, it is first necessary to study the place of these U.S. private actors in our global network scheme.

Let us take the elements of our diagram one by one. First of all, as far as electronic devices – *hardware* – are concerned, while most of them are built in Asia,[37] the responsible companies are often American. With a few foreign exceptions – Samsung in South Korea,[38] Huawei in China[39] and, far behind, Nokia in Norway[40] – American companies have a good share of the market (Apple, Dell, Microsoft, Google, HP).[41] Not to mention the software used on these devices: mainly Android (Google), Windows (Microsoft) and Apple systems.[42] Users, both in the professional and personal spheres, therefore use American hardware and software solutions. These devices connect to antennas, which again mostly come from American companies, although Chinese (Huawei, ZTE) and European (Nokia, Ericcson) companies are also present.[43] In the cloud, U.S. companies are taking over the market, with Amazon having nearly one-third of the market share, with Microsoft, Google, and other U.S. and foreign companies competing for the remainder.[44] Submarine cables are largely financed and owned by U.S.

37 Lu 2023.
38 Companies Marketcap 2026a.
39 Goh–Pan 2025.
40 Companies Marketcap 2026b.
41 Encelot 2024.
42 Global Stats 2026.
43 Statista 2025; Taylor 2025b; Taylor 2025c.
44 Richter 2025.

companies.[45] The same is true for mega constellations, a sector that is nevertheless undergoing a major transformation.[46]

Some of these mega companies – the largest – are grouped under the acronym "GAFAM" for Google–Apple–Facebook–Amazon–Microsoft.[47] Each of these five companies focuses on the activities mentioned above, except for the mega constellations, which are then forced to form partnerships: Google Cloud hosts SpaceX's Starlink ground stations,[48] and Microsoft Azure also works with SpaceX.[49]

These giant companies are therefore concentrating their digital activities on applications and software that enable users to create data, as well as on data transfer and storage solutions. In short, they are present at each stage, often concurrently. It therefore becomes difficult not to use their services, voluntarily or involuntarily. The data, from its creation to its storage and transmission, is often controlled by a U.S. company, even when a European user is involved. In addition to the GAFAMs, the company SpaceX should now be added. Originally a simple launch company, the ecosystem that its boss, Elon Musk, is building is gradually getting closer to these digital giants: the Starlink mega constellation (equivalent to an underwater cable), the X social network, Tesla self-driving cars, the Grokipedia website, rumours about devices (phone,[50] robot[51]). Data control is at the heart of this empire.[52] Should we now talk about the GAFAMS?[53]

45 The Economist 2017; Mauldin 2024; Qiu 2019; McMahon 2025.

46 Knott et al. 2025; Julienne 2023.

47 Géoconfluences 2025.

48 Google Cloud Press Corner 2021.

49 Sokolowsky 2020.

50 Tesla Pi Phone 2026.

51 Robot Tesla Optimus (https://fr.wikipedia.org/wiki/Tesla_Optimus).

52 Iulian Florea 2025.

53 It is possible to find a few blogs in this direction on the internet. Beyond the traditional GAFAMs, we often consider the "magnificent seven", an expression that refers to the seven technology companies with exceptional performance: Nvidia, Meta (Facebook), Tesla, Amazon, Alphabet (Google), Microsoft, Apple. We notice the presence of Tesla, owned by Elon Musk. SpaceX is still unlisted on the stock exchange, but that could well change.

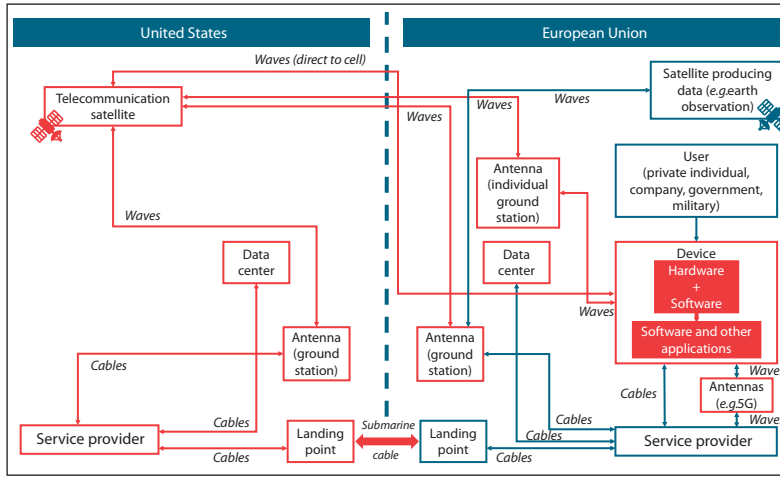

Figure 6. *U.S. pre-eminence in telecommunications (in red)*
Note: Other elements (in blue) may be non-European and non-U.S.
Source: Compiled by the author.

European users who want to use sovereign services, therefore, could feel trapped: they use American services, both personally and professionally, every day or almost every day. In itself, one could argue that it is not a serious issue. This could be true, at least if U.S. law were data protective. In fact, the legal framework governing GAFAMS is not data-protective.

LAWFARE: WHEN THE UNITED STATES USES ITS LAW AGAINST EUROPE

One of the foundations of international society is the possibility for each State to determine its own domestic law. Each state, including the United States, decides on the rules governing data, including its protection: how it is collected, who can access it, and under what conditions. Because the real challenge of data is its protection: the user wants to protect their privacy and prevent third parties from accessing it; these same third parties, public

authorities (States) and companies, want to have access to it to exploit it. The key is to find a happy medium between protecting users and economic and security interests (including national ones).

The European Union is a pioneer in the field, with its regulations protecting Europeans' personal data, even when collected by foreign companies: the famous GDPR (General Data Protection Regulation).[54] Other countries do not protect data as much: this is the case in the United States, as we will see in this section. A notion, therefore, appears in the background, that of lawfare, i.e. war by law. It is not a war as it is generally understood, with weapons and fighting, but rather a search for power through national regulations.[55] Some countries have integrated this tactic into their broader strategy, such as China.[56] In our case, U.S. regulations do not provide sufficient data protection, enabling both the U.S. Government and companies to gain relative power over European users. The data is therefore first collected, controlled, and transmitted in bulk by companies, including GAFAM and others, and then U.S. law allows U.S. authorities to consult this data.

Stored data: The cloud, a giant reserve of data legally accessible by U.S. authorities

Several criteria must be taken into account: the nationality of the company storing the data; where the data is stored; the nationality and nature of the person storing the data (physical or legal, civil, military or governmental); what the U.S. authorities can do with the data; and finally, the reasons justifying such an action.

Starting with the Stored Communications Act (SCA),[57] which allows authorities to access data stored by American companies. The authorities can thus obtain a warrant to recover the content of the communications of interest:

54 European Commission 2022.

55 Deveaux-Moncel 2025; Férey 2022.

56 Kosuke 2025.

57 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703.

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued [...] by a court of competent jurisdiction.[58]

For requests concerning "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days",[59] the authorities may obtain

> [a] court order for disclosure [...] issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[60]

To obtain such legal authorisations from a judge, the authorities must generally justify probable cause.[61]

In addition to content, the authorities can demand "a record or other information about a subscriber to or customer of such service (not including the contents of communications)"[62] thanks to a warrant[63] or thanks to the consent of the interested party.[64] Finally, the U.S. authorities can obtain data if they request it from service providers and the latter, "in good faith, believes that an emergency involving danger of death or serious physical

58 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(a).
59 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(a).
60 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(d).
61 Congress 2022.
62 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(c)(1).
63 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(c)(1)(A) and (B).
64 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(c)(1)(C).

injury to any person requires disclosure without delay of communications relating to the emergency".[65]

The U.S. authorities can therefore access certain data if authorised by a judge. The judge is the guarantor of the protection of private data managed by American companies, by extension of the Fourth Amendment.[66] But when reading the SCA, the uncertainty surrounding the location of the data is noticeable: what if the American company stored the data of its foreign customers… abroad? It would then probably be impossible for the authorities to recover them without violating the sovereignty of this foreign state. The judges came to the same conclusion, pushed by the American company Microsoft, which refused to communicate data stored on an Irish server: "§2703 of the Stored Communications Act does not authorise courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers."[67]

The Clarifying Lawful Overseas Use of Data Act of 2018,[68] better known as the CLOUD Act, closes the gap by amending the SCA and requiring U.S. companies to communicate data stored abroad:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[69]

So if the service provider is subject to U.S. jurisdiction and the authorities have the legal authority to retrieve the data, the fact that the data is stored

65 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2702(b)(8).
66 Congress 2026: Constitution of the United States 1787, 4th Amendment.
67 Justia U.S. Law 2016.
68 Congress 2018.
69 Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2713.

abroad is no longer an obstacle. But the judge remains the custodian of this data, and the U.S. authorities must absolutely go through this step to access it.

However, a clarification:

> A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes – (i) that the customer or subscriber is not a United States person and does not reside in the United States; and (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.[70]

A company that is asked to transmit data of a non-U.S. person who violates foreign law (e.g. European) may contest such a request by authorities.[71] It is then up to the judge to decide whether or not the request is justified in the light of the "interests of justice". A rather weak measure, therefore, which looks more like an attempt to reassure economic partners than a real protection of foreigners and their data stored abroad. It does not matter what the GDPR or any other European or domestic law says: U.S. law is superior and extra-territorial. Europeans must trust the American judge.

In parallel with these texts allowing *classic* surveillance in the context of legal cases, the U.S. authorities can demand data from foreign persons, stored abroad, as part of foreign intelligence. This is permitted by the Foreign Intelligence Surveillance Act (FISA),[72] updated several times:

> Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this

[70] Legal Information Institute 2026b: 18 U.S. Code Chapter 121, § 2703(h)(2)(A).

[71] It should be remembered, on the subject of personal data, that the CNIL considers the United States to be a "country in partial compliance" with European regulations. Commission Nationale de l'Informatique et des Libertés 2025.

[72] Legal Information Institute 2026d: 50 U.S. Code Chapter 36.

> subchapter to acquire foreign intelligence information for periods of up to one year;[73]
>
> the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[74]

The judge is completely bypassed here: nothing and no one protects the data and interests of Europeans anymore.

The surveillance of foreign persons using the services of American companies is therefore legally organised. It would then be strategic for these people not to use this type of service to protect the confidentiality of their data. But the SCA applies to any company under U.S. jurisdiction; as this term has not been defined by the texts concerned, it seems coherent to consider the classic rules of personal jurisdiction applicable in the United States, the minimum contact test: a foreign entity is subject to U.S. jurisdiction if the 'minimum contacts' with the U.S. threshold is met in such a way that exercising jurisdiction seems reasonable.[75] A European company with data centres in the United States could be concerned and subject to the SCA. In any case, the GAFAM(S) are fully concerned.

Data transfer: The open door for U.S. telecommunications services

For the moment, we have studied the question of the U.S. authorities' capture of data stored on U.S. territory or abroad. Another key measure complements the United States' legal arsenal: the authorities can directly intercept communications during their transfer, without waiting for them to be stored. Starting with the Wire and Electronic Communications Interception and

73 Legal Information Institute 2026d: 50 U.S. Code Chapter 36, §1802(a)(1).
74 Legal Information Institute 2026d: 50 U.S. Code Chapter 36, §1881a(a).
75 Justia U.S. Supreme Court 2012.

Interception of Oral Communications (Wiretap Act),[76] including section 2511,[77] which states that "providers of wire or electronic communication service"[78] can "intercept wire, oral, or electronic communications or to conduct electronic surveillance"[79] if the authorities provide a warrant[80] or a written attestation that a warrant or court order is not required.[81] It should be noted that the definitions are very broad:[82]

"electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;[83]

"electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;[84] – the important notion here is again jurisdiction.

The authorities can also set up a "pen register or trap and trace device",[85] but only to obtain metadata, without the content of the telecommunications.[86] Finally, the FISA, of course, concerns both stored and transmitted data, once again without any particular control by the judge.[87] This analysis of U.S. law shows that U.S. authorities can access data transmitted and/or stored by U.S. companies, both inside and outside the United States, and potentially data stored by foreign companies on U.S. territory. These texts

76 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I.
77 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2511.
78 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2511(2)(a)(ii).
79 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2511(2)(a)(ii).
80 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2511(2)(a)(ii)(A).
81 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2511(2)(a)(ii)(B).
82 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2510.
83 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2510(14).
84 Legal Information Institute 2026a: 18 U.S. Code Chapter 119 Part I, §2510(15).
85 Legal Information Institute 2026c: 18 U.S. Code Chapter 206 Part II.
86 Legal Information Institute 2026c: 18 U.S. Code Chapter 206 Part II, §3121(c).
87 It should be noted that the Verizon telephone information retrieved by the NSA and revealed by Edward Snowden was obtained through a court order obtained under FISA. Greenwald 2013.

also concern data of space origin or transmitted by space: they are, therefore, necessary to consider them when consuming U.S. space services.

In summary, U.S. companies have positioned themselves in such a way that European users are instinctively drawn, if not forced, to use their services, both in their personal and professional lives. These same users, in order to use the global network, also unknowingly use U.S. services. These services are now complemented by satellite constellations. On the one hand, these U.S. companies can directly exploit the data provided by users. On the other hand, the U.S. authorities also have access to this data through the extraterritorial legal framework in place in the United States. Control infrastructures and services to control data and use it for various purposes. Faced with this, Europe must react.

European law: Protective, but insufficient?

The European Union is also responding through its legislation. Aware of the dominance of U.S. digital services, two key pieces of legislation have recently come into effect, establishing a framework for the provision of internet services within the European Union: the Digital Services Act (DSA) and the Digital Markets Act (DMA). These two pieces of legislation have different objectives, and we will not take the time to examine them in detail here, but it is still worth understanding the motivations behind them.

The DSA applies to all companies, but the most significant obligations primarily target the largest platforms identified by the European Commission. The DSA imposes transparency requirements on companies regarding the management of online content, algorithms and advertising; enhanced protection for minors; improved traceability of online sellers; and a design intended to exert less control over consumers.[88] It is difficult to assess the legislation's actual impact on the sector after only a few years of implementation, but it has enabled European authorities to launch investigations.[89] National courts can also apply the DSA: this was the case

88 Vie Publique 2025a; European Commission s. a.a; European Commission 2026a.

89 Directorate-General for Communication of the European Commission 2026.

with a Dutch court, which ruled that Meta did not comply with the rules regarding users' choice to use Facebook and Instagram in chronological order rather than via the algorithm.[90] As for the DMA, it aims to combat anti-competitive practices by internet giants and address the imbalances in their dominance of the European digital market. This legislation targets so-called "systemic" services. It should allow European users to benefit from a wider choice of digital services by stimulating competition – thanks, among other things, to service interoperability – and, at the same time, reduce the power held by large companies such as GAFAM.[91] Its success has yet to be proven, and difficulties appear to have already been identified.[92]

Thus, European consumers could be better protected thanks to these regulations. However, their data remains at the mercy of U.S. authorities, regardless of where it is stored, if a U.S. company gains access to it. EU Member States are now exploring "sovereign cloud" solutions, which offer specific safeguards for governments and their agencies. One player in this market is Amazon Web Services. While promising security measures that offer complete data security,[93] one cannot help but question the effectiveness of such a solution, given the extraterritorial reach of U.S. law, a concern also raised by the French Parliament.[94] Other players, this time European ones such as OVHCloud, offer sovereign solutions.[95] Governments must choose the best solution for themselves and the EU, without compromising on data security and, ultimately, their independence.

In addition to this structural weakness of European law compared to U.S. law, U.S. companies and authorities are working to undermine the legal framework established at the EU level.[96] Through aggressive lobbying, they might well succeed.[97] If the European Union wants to protect its

90 Meijer 2025; Sterling 2026.
91 Vie Publique 2024; European Commission s. a.b; European Commission s. a.c.
92 EDRi 2025.
93 Terwellen 2025.
94 Lopez-Liguori 2025.
95 OVHCloud s. a.
96 Pamuk 2025.
97 Soares 2026.

data and strategic independence from the United States, it must develop its own infrastructure.

VULNERABLE EUROPE: THE DEVELOPMENT OF SOVEREIGN EUROPEAN SPACE INFRASTRUCTURES AS A SOLUTION

American companies are therefore at the heart of the data sector, and particularly in space telecommunications. However, U.S. law is structured so that U.S. authorities can access the data of these companies, even if the owner (private or state person, including armies) is European. This poses two main risks: the first concerns our sovereignty and thus security, the second concerns our economy.

A loss of sovereignty and therefore of independence: A risk for our security

European countries, including France, are very fond of the notion of sovereignty, and their inhabitants are very attached to it. A central and sacred notion in international law, enshrined in particular by the Charter of the United Nations, it is, according to Jean Bodin, a famous French thinker of the sixteenth century, defined as "absolute and perpetual power".[98] More prosaically, sovereignty is the power of the state (an abstract figure, a legal fiction represented by its government or head of state) to do what it wants on its territory – in other words, internal sovereignty. This also translates into independence from other states – this is external sovereignty. Each State decides on its own laws, and, more generally, on its internal behaviour and responses to the international community, in compliance with international law.

[98] Bodin 1576.

Above all other criteria, independence is military – meaning that military capabilities enable independence, and therefore these capabilities must not depend on another state, because despite the prohibition of the use of force,[99] some states still use their armies not exclusively to maintain their integrity, but also to conquer new territories. The Russian invasion of Ukraine in 2022 is an example,[100] as is Israel's colonisation policy,[101] as well as U.S. threats to Greenland[102] or Panamá.[103] A state must preserve its military capacity to act and defend itself, which translates into the total independence of its army. Telecommunications are at the heart of any armed conflict. Plans, strategies, objectives, operational organisation, troop strength, arms control and drones; the transmission and storage of this data are sensitive operations that must be protected to ensure military independence. This U.S. control of data could eventually prevent European armies from being independent. Data control is also inseparable from infrastructure control; a rumour has it that Elon Musk, founder of SpaceX, has cut off connectivity to the Starlink mega constellation to prevent Ukraine from attacking Russia.[104] Italy, before backtracking due to concerns about national security, announced it wanted to use Starlink for its armed forces.[105] The risk here is twofold: the deletion of the service as such, as well as the risk of spying on all data that passes through American services. While the United States has historically been our ally, espionage was not a problem back then. Still, the situation has changed, and the protection of European sovereignty cannot rest on a *status quo* that is all the more fragile today.

The hesitation regarding military aid to Ukraine[106] or the U.S. administration's criticism of European policies regarding the conflict in Iran[107]

99 Charter of the United Nations 1945: 2.4.
100 Clarke 2025.
101 UN News 2025.
102 Bryant 2026.
103 Franceinfo 2024.
104 Creamer 2023.
105 Amante 2025.
106 Green et al. 2025.
107 Wälde 2026.

points to a growing danger for European countries of a shift in international relations. Let us also recall the conclusions of the Draghi Report:

> European collaborative procurement accounted for less than a fifth of spending on defence equipment procurement in 2022. Member States also do not favour competitive European defence companies. Between mid-2022 and mid-2023, 78% of total procurement spending went to non-EU suppliers, out of which 63% went to the US.[108]

The EU is militarily dependent on the United States even as it can no longer rely on this ally. Yet, in the event of a conflict with the United States, the consequences are threefold: our data will be siphoned off by the U.S.; U.S. services will cease to function; and the armed forces of EU Member States will no longer receive U.S. weapons, ammunition, or military technology. The consensus is nearly unanimous:[109] the EU must regain its full independence from the U.S.[110] NATO currently provides a significant portion of Europe's military deterrence; yet "alliances are no longer secure",[111] and at least a portion of European public opinion would like to see the EU play a greater role in this common defence.[112] The European Commission's 2026 Work Program embodies this commitment: "To be able to take care of its own defence and security";[113] as does the Strategic Agenda 2024–2029: "We will invest substantially more and better together, reduce our strategic dependencies, scale up our capacities and strengthen the European defence technological and industrial base accordingly."[114]

[108] European Union 2025a: 8.

[109] It should be noted that while the EU appears unanimous in its strategies regarding its desire for independence from the United States, the perception of these issues in Eastern Europe is different, partly due to the region's proximity to Russia, but also because of its internal political landscape. Dell'Anna–Yilmaz 2025; Krastev–Leonard 2025.

[110] Hutagalung 2025.

[111] Vie Publique 2025b.

[112] Kubilius 2026.

[113] European Commission 2025a.

[114] European Council 2024: 4.

Beyond this necessary military independence, which cannot be subject to any exceptions, European states must also maintain their infrastructural independence. Because the use of foreign constellations, cables and equipment represents an intrinsic risk: the cessation or limitation of the services provided, the software made available, the hardware, the spare parts, up to the extraction, refining and, more generally, the availability of resources and raw materials. If it is impossible to produce all this infrastructure nationally and provide all these services, then a state concentrating its infrastructure to such a large extent poses a disproportionate risk. It is now tempting to take this risk, because it often amounts to savings at least in the short term,[115] but it is a guaranteed loss of sovereignty in the long term. The Draghi Report urges European policymakers to break free from external industrial dependencies,[116] a call that is beginning to bear fruit through several funding programs.[117] Defence budgets across the EU have risen significantly between 2021 and 2024 and continue to rise.[118]

Let us look at two examples to illustrate this point. First, China dominates the production, refining and exportation of rare earth elements, which are essential for new technologies.[119] However, the country is increasingly taking steps to limit these exports, putting pressure on global supply chains.[120] The second example concerns the U.S. practice of imposing an embargo not on a country but on an individual. For if an individual anywhere in the world behaves in a way that displeases the U.S. Government, the U.S. Government can prevent them from using any services provided by U.S. companies. Windows, Outlook, Visa, Mastercard, Google: the targeted individual finds themselves unable to use services they previously used frequently. This was the case for several judges and prosecutors at the International Criminal Court (ICC), who were targeted for their involvement in proceedings

115 Casanova Tormo 2025.
116 European Union 2025b: 159–171.
117 European Commission 2024.
118 Council of the European Union 2026.
119 Pitron 2023: 187–210, 323; Feng 2025.
120 Szczepański 2025; France 24 2025b.

concerning U.S. and Israeli nationals.[121] Thierry Breton, a former European Commissioner and a leading figure in the fight against the unchecked power of GAFAM and efforts to regulate them, along with other high-ranking European officials, are also being targeted by sanctions.[122] Some leaders of Member States are protesting, calling this an unacceptable interference in the EU's internal affairs;[123] Emmanuel Macron has contacted Donald Trump to request that the sanctions be lifted.[124] No one is safe, then; a French judge reportedly received a visit from U.S. diplomats regarding a case involving Marine Le Pen, leader of the far-right political party Rassemblement National.[125] The White House is said to have considered sanctions against the judges handling this case.[126] The solution, therefore, lies partly in sovereign infrastructure and partly in the diversity of foreign services, so as not to depend on a single third country.

The independence to be protected is also political in the broad sense: the protection of our democracies, but also of our societies as such, our values, our fundamental rights, our social protection and the functioning of our societies. Controlling data, especially access to it, means knowing exactly what the masses of individuals in a society think. It is therefore necessary to understand how this society works, to know how to influence it, and to disrupt and *ultimately* control it.[127] U.S. lobbying efforts aimed at dismantling the European Union – particularly its digital regulations – are significant in terms of the resources they deploy.[128] This *ideological war*[129] in which the United States is attempting to circumvent European regulations is perfectly illustrated by a U.S. website project: *freedom.gov,* where it is alleged that Europeans could access banned – illegal – content on the

121 The White House 2025b; International Criminal Court 2025a; International Criminal Court 2025b.
122 France 24 2025c.
123 Clavier 2025.
124 Le Monde 2026.
125 Franceinfo 2026.
126 Mazuir 2026.
127 Zuboff 2019: 657–695.
128 Pollet 2025.
129 Van Middelaar 2026.

European internet.[130] The principled fight that European countries should have waged decades ago is now a matter of civilisational survival.[131] The European Union is aware of this,[132] and the 2019–2024 agenda reflects it: "The EU needs to pursue a strategic course of action and increase its capacity to act autonomously to safeguard its interests, uphold its values and way of life, and help shape the global future."[133]

Finally, our independence must be economic, because the main challenge for digital companies is to monetise this data. But the monetisation of data is not the only issue: the economic threat manifests at different levels. First of all, it is a threat to European companies, which cannot develop in the digital sector because of this almost impossible-to-beat competition. As for the U.S. mega constellations, their use by European users prevents both ground operators (using cables and antennas) from maintaining themselves and investing, but also European constellations from developing. Secondly, American companies offering services through applications and other software exert significant influence on users (including Europeans) through algorithms.[134]

Developing Europe's own satellites and other sovereign infrastructures

SpaceX's Starlink constellation now represents more than half of the satellites in orbit.[135] According to its availability map, the company provides telecommunications on all five continents. It is therefore interesting to take the service provider as an example to illustrate this need to develop our own infrastructure.

130 Down 2026. The concept of freedom of expression in the United States and Europe is radically different, and that's okay: sovereignty allows each country to develop its own values, laws and systems. The fact that a country seeks to circumvent this is simply interference.

131 Sutherland 2026.

132 Barigazzi 2019.

133 European Council 2019: 6.

134 Piccardi 2025; Sée 2019; Bertail et al. 2019; Girardot 2017.

135 Orbital Radar 2026; Robinson-Smith 2026.

Figure 7. *Accessibility map of Starlink services around the world as of the 26th of March 2026*
Source: https://starlink.com/map

If SpaceX registers its satellites abroad,[136] the company, under its real name, Space Exploration Technologies Corp., is legally American. Initially incorporated in Delaware,[137] a U.S. state, the company has recently moved to Texas,[138] another U.S. state; the jurisdictional link is obvious. Starlink is a constellation of telecommunications satellites, and as such, SpaceX is a telecommunications service provider. Regarding data storage, SpaceX's Starlink does not normally store data: it is not a cloud or online storage, but a way to connect users to the internet. Starlink *gateways,* which connect the satellite network to the internet,[139] do not store data. On the other hand, SpaceX does transmit data, which is therefore vulnerable to the indiscretions of the American authorities. It should also be remembered, as we have seen, that SpaceX works hand in hand with American cloud providers, thereby increasing the risks. The Starlink telecommunications network is therefore particularly vulnerable to the U.S. legal spider's web, which should encourage European states not to use this service to protect their data. However, not every country receiving the Starlink signal today has made this choice.

136 De Selding 2023.
137 United States Securities and Exchange Commission 2017.
138 Shetti–Khushi 2024.
139 Starlink Insider 2025; Linkson 2025.

One could argue that this legal espionage – which is therefore not really espionage, since it is allowed and regulated by law – is not a big deal, especially in Europe. After all, the United States and European countries are allies. However, all the arguments push Europe against using Starlink.

First of all, a government must not use a foreign system to communicate sensitive data *internally,* i.e. to other entities in the same state. To communicate both governmental and military data between national entities, the system should be entirely sovereign; state- or EU-owned. Using a U.S. system means exposing oneself to obvious, announced espionage – written into U.S. law – by U.S. authorities. This strategy must concern not only American companies but also all suppliers of goods and services outside Europe.[140] Regarding external communications, the state should also use sovereign infrastructure, at the risk of sensitive government or military data being spied on by third parties. This is why it is essential that European states develop their own space capabilities.

It is also important to consider the change in the position of the U.S. administration towards Europe and the world to encourage our European leaders to emancipate themselves from services across the Atlantic. The United States has always oscillated between isolationism and interventionism. Still, Donald Trump's second term in office is a real turning point in the United States' relationship with Europe:[141] economic pressure on taxes,[142] military pressure on Greenland, NATO,[143] Ukraine and Iran. European states must interpret the signals as they are – Venezuela as sufficient proof – and seek to emancipate themselves.

This step is precisely to produce, on a European or national scale, the missing systems and operate them at the national or regional level. Of course, developing a mega constellation is not within the reach of all states. Still, Member States are fortunate within the European Union to be a collective of states with the capacity to trust one another enough to develop common sovereign infrastructures: this is the promise of the Iris²

[140] In this respect, we recall the scandal of Chinese 5G antennas. Schmidt 2024.
[141] Gatinois–Ricard 2025.
[142] Clarke 2026.
[143] Cook 2025.

constellation. Galileo[144] is a success story – the world's most widely used and most accurate geolocation system[145] – as is Copernicus,[146] whose data is massively used by researchers around the world.[147] Europe, through its European Space Agency and its joint projects, has succeeded in conceiving, developing, building and operating a sovereign launcher, Ariane.[148] The benefits for the European Union and its members are enormous: total control over infrastructure and its operations, a controlled production chain, data protection, job creation, economic stimulation through the consumption of European services, and strengthening of government and military capacities. On a larger scale, the European Union has launched the Global Gateway program, which aims to make massive investments across various sectors worldwide,[149] including the digital sector[150] and undersea cables.[151] The stated goal is to strengthen ties between the EU and third countries and to enhance the resilience of intra-EU systems. This is a response to China's Belt and Road Initiative,[152] but could also be a way for the EU to reduce its dependence on its American ally. The development of sovereign systems will also enable the EU to set its own technological and strategic agenda, based on its own priorities rather than those of other countries.[153]

144 European Union Agency for the Space Program 2025.

145 European Space Agency 2024.

146 Climate Data Store 2026.

147 European Union 2022.

148 ESA and its Member States have abolished the rule of the single regional launcher: from now on, countries develop private launchers at the national level. Is this the right method to counter U.S. space hegemony?

149 European Commission 2026b.

150 European Commission s. a.d.

151 European Commission 2025b; European Commission s. a.e.

152 Belt and Road Portal s. a.; Bilal et al. 2026.

153 As this article is being finalised, the space sector is being shaken by two announcements from NASA: the Artemis program has been completely overhauled, replacing the lunar orbital station with a lunar surface station; and the ISS will not be replaced by fully independent commercial Earth-orbiting stations. The ESA Member States and the EU, key partners of the U.S., are affected by these changes. Low 2026.

CONCLUSION

The current digital, space and data situation in the European Union is not particularly enviable. Its population massively uses U.S. services, and much of the world's digital architecture is directly owned by U.S. companies. Europe is vulnerable, politically, structurally and economically. Our military independence is, for the moment, generally maintained, but promises of short-term investment savings could well change the situation. This structural dependence is aggravated by U.S. law, which legally allows U.S. authorities to access all data collected, processed, stored and transmitted by U.S. companies. Unequal lawfare, because the American objectives are not the protection of the fundamental rights of the people, but the power of the state. A legal war already lost.

This observation is well known. This article has no merit beyond applying what is already known in digital law to the space sector, and it provides no interlocking vision of the issue. The space solution to this problem is simple: EU Member States need to develop sovereign, national and/or European infrastructures. The Member States are capable of doing so; they have already done so with Galileo and Copernicus. They *might*[154] be on their way to success again with Iris[2]. There is therefore no shortage of skills, nor even political will or cooperation. Funding these projects can be an obstacle, but sovereignty comes at a price. The massive funding of European armies[155] shows that decision-makers are beginning to recognise this, even if it is far from being solved.[156] By the way, the European Commission's work program for 2026 is entitled "Europe's Independence Moment".[157] A message full of hope for the future.[158]

[154] Rugamer – Lo Nostro 2026.

[155] Clapp 2025; Le Monde 2025.

[156] The Economist 2025.

[157] European Commission 2025.

[158] To some European leaders, Donald Trump appears to be a threat. But he can also be seen as a way to recognise the EU's actual dependence on the United States and to act accordingly. For the EU, the second term of Donald Trump could be an opportunity. Coustilliere 2025; Krastev–Leonard 2025.

However, two things must be clarified. First of all, it must be made clear here that the solution does not lie in cutting all ties with the United States or its companies. The European Union must rethink its relations with the United States, interact differently and deny them the central place that the world has allowed them to take. This primarily involves diversifying the services and hardware on which the EU depends, including developing certain sovereign space and digital capabilities, developed and operated by the European Union and/or its Member States. At the same time, it is necessary not to rely on foreign infrastructure to maintain a sufficient market for this new infrastructure. The reasoning applies to the United States but also to any other foreign power. To take just one example, China is currently developing many mega constellations: the stakes are identical, as is the solution. Some space activities can be shared with the United States, such as large-scale international projects like the James Webb telescope or Earth observation constellations for scientific purposes.

This solution, therefore, seems simple. But is it even possible to refuse the use of foreign services on European soil? This is the advantage of sovereignty: each state has the power to prohibit the reception of a service on its territory or the sale of a product. For example, Starlink is only received in Europe because the Member States have individually agreed to receive the signal. States generally have to comply with their domestic competition laws, but protectionism is legally justifiable. It is time for EU Member States to understand the potential of lawfare and to develop their legal framework in this regard.[159]

The second clarification concerns the need to develop such services; we live in a finite world with finite resources. EU must therefore not seek to develop goods and services *only* to have sovereigns, but because there is a demand, a need, on the part of the Member States and/or the European

[159] Member States, within the framework of their national sovereignty, must also take into account the European Union's internal market. If they can coordinate their efforts, this market – the largest in the world – can serve as a lever to compel third countries to comply with European law. The EU Space Act, currently under discussion, holds real potential – though it has yet to be fully realised – with regard to foreign operators such as SpaceX that provide services in Europe. European Space Policy Institute 2025.

Union. This article, therefore, does not argue for the mandatory development of European infrastructures per se. Still, if Member States decide to use them instead of terrestrial infrastructure, they must develop sovereign, sustainable infrastructure. When it comes to digital technology, our societies have already chosen to use these services on a massive scale, so it is high time to become independent. It is not necessary to *develop for the sake of* developing, but to develop well to serve a precise and socially useful objective. At the same time, this should apply to all foreign commercial activities, goods and services. It is also in the field of *soft power* that Europe must present itself and occupy space in its own way, preserving it for future generations, without necessarily following the American model of development. In the meantime, submitting to U.S. extraterritorial law does not seem to be an attractive or desirable solution. Let us build capacity; together, Europeans have the skills and the means to do it. It is at this price that European sovereignty, as well as the future of Earth and space activities, will be preserved.

REFERENCES

Amante, Angelo (2025): Italy Defence Minister Dampens Talk of Starlink Deal for Secure Communications. *Reuters,* 8 January 2025. Online: https://www.reuters.com/technology/space/italy-defence-minister-dampens-talk-starlink-deal-secure-communications-2025-01-08/

Barigazzi, Jacopo (2019): Borrell Urges EU to Be Foreign Policy 'Player, Not the Playground'. *Politico,* 9 December 2019. Online: https://www.politico.eu/article/on-foreign-policy-josep-borrell-urges-eu-to-be-a-player-not-the-playground-balkans/

Belt and Road Portal (s. a.). Online: https://eng.yidaiyilu.gov.cn/

Bertail, Patrice – Bounie, David – Clémençon, Stephan – Waelbroeck, Patrick (2019): Algorithmes: biais, discrimination et équité. *Télécom ParisTech,* February 2019. Online: https://www.telecom-paris.fr/wp-content-EvDsK19/uploads/2019/02/Algorithmes-Biais-discrimination-equite.pdf

Bilal, San – Teevan, Chloe – Hunter, Jonathan (2026): What Is the EU's Global Gateway and How Can It Be Improved? *ECDPM,* 18 March 2026. Online: https://ecdpm.org/work/what-eus-global-gateway-and-how-can-it-be-improved

Bodin, Jean (1576): *Les six livres de la République.* Paris: Jacques du Puy.

Bryant, Miranda (2026): Denmark Reportedly Flew Blood Bags to Greenland in Preparation for a US Attack. *The Guardian,* 19 March 2026. Online: https://www.theguardian.com/world/2026/mar/19/denmark-prepared-for-us-attack-donald-trump-greenland

Casanova Tormo, Jordi (2025): Ensuring a Safe and Sustainable Space: Amazon Kuiper's Perspective on the EU Space Act. In *Third Budapest Conference on Space Law and Policy. European Space Ambitions at a Time of Change.* Budapest, Ludovika University of Public Service, 4 December 2025.

Cité de Télécoms (s. a.): *Premiers satellites. Les télécommunications et la conquête de l'espace.* Online: https://www.cite-telecoms.com/blog/histoire/200-ans-de-telecoms/les-temps-modernes/les-premiers-satellites/

Clapp, Sebastian (2025): EU Member States' Defence Budgets. *European Parliamentary Research Service,* May 2025. Online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772846/EPRS_ATA(2025)772846_EN.pdf

Clarke, Jennifer (2026): What Tariffs Has Trump Introduced and Why? *BBC News,* 24 February 2026. Online: https://www.bbc.com/news/articles/cn93e12rypgo

Clarke, Seán (2025): Which Areas Is Russia Demanding as its Price for Peace in Ukraine? – Visual Explainer. *The Guardian,* 3 December 2025. Online: https://www.theguardian.com/world/ng-interactive/2025/dec/03/which-areas-is-russia-demanding-as-its-price-for-peace-in-ukraine-visual-explainer

Clavier, Henri (2025): Sanctions contre Thierry Breton: l'administration Trump «est moins sur un volet économique que sur un volet idéologique». *Public Sénat,* 26 December 2025. Online: https://www.publicsenat.fr/actualites/international/sanctions-contre-thierry-breton-ladministration-trump-est-moins-sur-un-volet-economique-que-sur-un-volet-ideologique

Climate Data Store (2026): Live dashboards. *Climate Data Store,* 30 January 2026. Online: https://cds.climate.copernicus.eu/live

CNES (2025a): Quand les satellites s'invitent dans notre quotidien. *Centre National d'Études Spatiales,* 3 December 2025. Online: https://cnes.fr/dossiers/applications-satellites

CNES (2025b): Newspace: les nouveaux acteurs du spatial. *Centre National d'Études Spatiales,* 8 December 2025. Online: https://cnes.fr/dossiers/newspace-nouveaux-acteurs-spatial

Commission Nationale de l'Informatique et des Libertés (2025): *La protection des données dans le monde.* Online: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Companies Marketcap (2026a): *Market Capitalization of Samsung.* Online: https://companiesmarketcap.com/samsung/marketcap/

Companies Marketcap (2026b): *Market Capitalization of Nokia.* Online: https://companiesmarketcap.com/nokia/marketcap/

Congress (2018): *H.R.4943 – CLOUD Act.* 2 June 2018. Online: https://www.congress.gov/bill/115th-congress/house-bill/4943/text

Congress (2022): *Overview of Governmental Action Under the Stored Communications Act (SCA).* 8 March 2022. Online: https://www.congress.gov/crs-product/LSB10801

Congress (2026): *Constitution of the United States,* effective as of 29 January 2026. Online: https://constitution.congress.gov/constitution/

Cook, Lorne (2025): NATO Is in Disarray after the US Announces that Its Security Priorities Lie Elsewhere. *AP News,* 13 February 2025. Online: https://apnews.com/article/nato-us-europeans-ukraine-security-russia-hegseth-d2cd05b5a7bc3d98acbf123179e6b391

Coustilliere, Arnaud (2025): UE. Quel chemin pour conquérir notre autonomie stratégique numérique? Trump un électrochoc salutaire! *Diploweb,* 5 April 2025. Online: https://www.diploweb.com/UE-Quel-chemin-pour-conquerir-notre-autonomie-strategique-numerique.html

Creamer, Ella (2023): Elon Musk Biographer Admits Suggestion SpaceX Head Blocked Ukraine Drone Attack Was Wrong. *The Guardian,* 12 September 2023. Online: https://www.theguardian.com/books/2023/sep/12/elon-musk-biographer-admits-suggestion-spacex-head-blocked-ukraine-drone-attack-was-wrong

Croshier, Rose (2022): Space and Development: Preparing for Affordable Space-Based Telecommunications. *Center for Global Development,* 19 January 2022. Online: https://www.cgdev.org/publication/space-and-development-preparing-affordable-space-based-telecommunications

Council of the European Union (2026): La défense de l'UE en chiffres. *Council of the European Union,* 7 January 2026. Online: https://www.consilium.europa.eu/fr/policies/defence-numbers/

De Selding, Peter B. (2023): SpaceX Files 29,988-satellite W-band Network, Using Kingdom of Tonga as Regulatory Home. *Space Intel Report,* 12 October 2023. Online: https://www.spaceintelreport.com/spacex-files-29988-satellite-w-band-network-using-kingdom-of-tonga-as-regulatory-home/

Dell'Anna, Alessio – Yilmaz, Mert Can (2025): Europe's Pro-Trump Hotspots: Which Countries Stand Out? *Euronews,* 5 December 2025. Online: https://www.euronews.com/my-europe/2025/12/05/europes-pro-trump-hotspots-which-countries-stand-out

Deveaux-Moncel, Arthur (2025): Le droit contre le droit. Le "lawfare" ou les usages stratégiques de la norme. *Géoconfluences,* 30 September 2025. Online: https://geoconfluences.ens-lyon.fr/informations-scientifiques/dossiers-thematiques/geographie-du-politique/articles/le-lawfare-ou-les-usages-strategiques-de-la-norme

Directorate-General for Communication of the European Commission (2026): Two Years of the Digital Services Act Ensuring Safer Online Spaces. *Directorate-General for Communication of the European Commission,* 17 February 2026. Online: https://commission.europa.eu/news-and-media/news/two-years-digital-services-act-ensuring-safer-online-spaces-2026-02-17_en

Down, Aisha (2026): US Builds Website that Will Allow Europeans to View Blocked Content. *The Guardian,* 19 February 2026. Online: https://www.theguardian.com/technology/2026/feb/19/us-builds-website-that-will-allow-europeans-to-view-blocked-content

Droff, Josselin – Malizard, Julien (2024): Évolution des conflits et reconfiguration de l'industrie de l'armement: l'hypothèse des deux marchés. *Défense & Industries,* 18, 28–34. Online: https://www.frstrategie.org/sites/default/files/documents/publications/defense-et-industries/2024/DefenseIndustries-N18juin2024-JD-JM.pdf

Duarte, Fabio (2025): Amount of Data Created Daily. *Exploding Topics,* 24 April 2025. Online: https://explodingtopics.com/blog/data-generated-per-day

Edge Delta (2024): Data Storage Statistics: Key Figures and Trends. *Edge Delta,* 29 May 2024. Online: https://edgedelta.com/company/blog/data-storage-statistics

EDRi (2025): The DMA Is a Success, It Should Be Strengthened and Expanded. *EDRi,* 16 October 2025. Online: https://edri.org/our-work/the-dma-is-a-success-it-should-be-strengthened-and-expanded/

Encelot, Marjorie (2024): Les États-Unis représentent 65% du marché mondial des actions et 81% du secteur de la « tech », Microsoft est la seule entreprise à figurer dans le Top 10 des capitalisations tout au long du 21e siècle. *Les Echos Investir,* 21 August 2024. Online: https://investir.lesechos.fr/actu-des-valeurs/la-vie-des-actions/les-etats-unis-representent-65-du-marche-mondial-des-actions-et-81-du-secteur-de-la-tech-microsoft-est-la-seule-entreprise-a-figurer-dans-le-top-10-des-capitalisations-tout-au-long-du-21e-siecle-2114519

European Commission (2018): *Behavioural Study on Advertising and Marketing Practices in Online Social Media.* Online: https://commission.europa.eu/system/files/2018-07/osm-final-report_en.pdf#page=88.08

European Commission (2022): *General Data Protection Regulation (GDPR).* Online: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

European Commission (2024): *Chapitre 2: Une Union prospère et compétitive.* Online: https://op.europa.eu/webpub/com/general-report-2024/fr/chapter2.html

European Commission (2025a): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2025) 870 final. *Commission Work Programme 2026.* Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0870&qid=1761126156157

European Commission (2025b): Global Gateway Forum: EU for Strategic Expansion of the Medusa Submarine Cable System to the Middle East. *European Commission,* 10 October 2025. Online: https://north-africa-middle-east-gulf.ec.europa.eu/news/global-gateway-forum-eu-strategic-expansion-medusa-submarine-cable-system-middle-east-2025-10-10_en

European Commission (2026a): *The Impact of the Digital Services Act on Digital Platforms.* Online: https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

European Commission (2026b): *The Global Gateway Strategy.* Online: https://international-partnerships.ec.europa.eu/policies/global-gateway/global-gateway-overview_en

European Commission (s. a.a): *The Digital Services Act.* Online: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

European Commission (s. a.b): *The Digital Markets Act.* Online: https://digital-markets-act.ec.europa.eu/index_en

European Commission (s. a.c): *About the Digital Markets Act.* Online: https://digital-markets-act.ec.europa.eu/about-dma_en

European Commission (s. a.d): *Digital.* Online: https://international-partnerships.ec.europa.eu/policies/global-gateway/digital_en

European Commission (s. a.e): *Northern EU Digital Gateways.* Online: https://international-partnerships.ec.europa.eu/policies/global-gateway/northern-eu-digital-gateways_en

European Council (2019): *A New Strategic Agenda 2019–2024.* Online: https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

European Council (2024): *Strategic Agenda 2024–2029.* Online: https://www.consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf

European Space Agency (2024): Galileo: six faits qui vont vous époustoufler. *European Space Agency,* 22 April 2024. Online: https://www.esa.int/Space_in_Member_States/France/Galileo_six_faits_qui_vont_vous_epoustoufler

European Space Policy Institute (2025): Bold Words, Blurred Lines: A Reflective Look at the EU Space Act. *European Space Policy Institute,* 8 October 2025. Online: https://www.espi.eu/briefs/bold-words-blurred-lines-a-reflective-look-at-the-eu-space-act/

European Union (2022): OBSERVER: A History of Copernicus. *Copernicus,* 9 June 2022. Online: https://www.copernicus.eu/en/news/news/observer-history-copernicus

European Union (2025a): *The Future of European Competitiveness. Part A: A Competitiveness Strategy for Europe.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2872/9356120

European Union (2025b): *The Future of European Competitiveness. Part B: In-depth Analysis and Recommendations.* Online: https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf#page=172.10

European Union Agency for the Space Program (2025): *Constellation Information.* Online: https://www.gsc-europa.eu/system-service-status/constellation-information

Feng, Emily (2025): How China Came to Rule the World of Rare Earth Elements. *NPR,* 23 July 2025. Online: https://www.npr.org/2025/07/23/nx-s1-5475137/china-rare-earth-elements

Férey, Amélie (2022): *Towards a War of Norms? From Lawfare to Legal Operations.* French Institute of International Relations. Online: https://www.ifri.org/en/studies/towards-war-norms-lawfare-legal-operations

Fernholz, Tim (2024): The Cost of Satcom Has Fallen Dramatically Thanks to Starlink. *Payload,* 13 February 2024. Online: https://payloadspace.com/the-cost-of-satcom-has-fallen-dramatically-thanks-to-starlink/

Foley, John (2024): How Much More Data Will AI Generate? 10x, 100x, 1000x? *Cloud Database Report,* 23 August 2024. Online: https://clouddb.substack.com/p/how-much-more-data-will-ai-generate

France 24 (2025a): Vance Urges Europe Not to Be US 'Vassal'. *France 24,* 15 April 2025. Online: https://www.france24.com/en/live-news/20250415-vance-urges-europe-not-to-be-us-vassal

France 24 (2025b): How China Leveraged Its Rare Earths Dominance over the US. *France 24,* 26 November 2025. Online: https://www.france24.com/en/live-news/20251126-how-china-leveraged-its-rare-earths-dominance-over-the-us

France 24 (2025c): Thierry Breton banni des États-Unis, le DSA et la lutte de l'UE contre la désinformation ciblés. *France 24,* 24 December 2025. Online: https://www.france24.com/fr/%C3%A9co-tech/20251224-washington-sanctionne-cinq-europeens-engages-regulation-numerique-tech-dsa-thierry-breton-etats-unis-union-europeenne-visa-desinformation

Franceinfo (2024): Donald Trump menace de reprendre le contrôle du canal de Panama. *Franceinfo,* 22 December 2024. Online: https://www.franceinfo.fr/monde/usa/presidentielle/donald-trump/donald-trump-menace-de-reprendre-le-controle-du-canal-de-panama_6970949.html

Franceinfo (2026): Ingérence américaine: le troublant récit d'une juge française. *Franceinfo,* 22 January 2026. Online: https://www.franceinfo.fr/politique/marine-le-pen/ingerence-americaine-le-troublant-recit-d-une-juge-francaise_7758632.html

Garrigou, Laura (2025): La bataille invisible du renseignement. *Esprit défense,* 17, 26–31. Online: https://www.defense.gouv.fr/bataille-invisible-du-renseignement

Gatinois, Claire – Ricard, Philippe (2025): L'ère Trump, un cauchemar pour la diplomatie européenne, entre flagornerie et humiliations. *Le Monde,* 23 November 2025. Online: https://www.lemonde.fr/international/article/2025/11/23/flagorneries-et-humiliations-donald-trump-met-la-diplomatie-europeenne-a-l-epreuve_6654503_3210.html

Gaur, Sachin (2026): Invisible Highways: The Vast Network of Undersea Cables Powering Our Connectivity. *UN News,* 2 February 2026. Online: https://news.un.org/en/story/2026/02/1166867

Géoconfluences (2025): *GAFA, GAFAM, géants du net.* Online: https://geoconfluences.ens-lyon.fr/glossaire/gafa-gafam

Girardot, Clément (2017): Comment enquêter sur les algorithmes? *La revue des médias,* 29 May 2017. Online: https://larevuedesmedias.ina.fr/comment-enqueter-sur-les-algorithmes

Global Stats (2026): *Operating System Market Share Worldwide Dec 2024 – Dec 2025.* Online: https://gs.statcounter.com/os-market-share

Goh, Brenda – Pan, Che (2025): Face à Nvidia, Huawei dévoile ses projets de puces et de puissance de calcul. *Les Echos Investir,* 18 September 2025. Online: https://investir.lesechos.fr/actu-des-valeurs/la-vie-des-actions/face-a-nvidia-huawei-devoile-ses-projets-de-puces-et-de-puissance-de-calcul-2186952

Google Cloud Press Corner (2021): Google Cloud and SpaceX's Starlink to Deliver Secure, Global Connectivity. *Google Cloud Press Corner,* 13 May 2021. Online: https://www.googlecloudpresscorner.com/2021-05-13-Google-Cloud-and-SpaceXs-Starlink-to-Deliver-Secure,-Global-Connectivity

Green, Erica L. – Schmitt, Eric – Sanger, David E. – Barnes, Julian E. (2025): Trump Suspends Military Aid to Ukraine After Oval Office Blowup. *The New York Times,* 3 March 2025. Online: https://www.nytimes.com/2025/03/03/us/politics/trump-ukraine-military-aid.html

Greenwald, Glenn (2013): NSA Collecting Phone Records of Millions of Verizon Customers Daily. *The Guardian,* 6 June 2013. Online: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Guillaud, Hubert (2025): *Les algorithmes contre la société.* Paris: La fabrique éditions.

Guillou, Michel (2013): Les débuts des télécommunications par satellites (1959–1969). In Griset, Pascal (ed.): *Les ingénieurs des Télécommunications dans la France contemporaine.* Paris: Institut de la gestion publique et du développement économique, 125–137. Online: https://books.openedition.org/igpde/3219?lang=fr

Hardy, Edmond (2021): La stratégie militaire et le champ opérationnel des compétitions technologiques. In Caspar-Fille-Lambie, Thierry (ed.): *Faire face à la recomposition du monde: Regards du CHEM – 70e session.* Paris: Comité d'études de défense nationale, 214–226. Online: https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=384&cidcahier=1264

HATVP (2025): La représentation des intérêts des GAFAM depuis 2020. *Haute Autorité pour la transparence de la vie publique,* 3 April 2025. Online: https://www.hatvp.fr/lobbying/actualites/la-representation-des-interets-des-gafam-depuis-2020/

Heijmann, Tim (2022): Economics behind Satellite Megaconstellations. *E-Shape Sustainability,* 24 November 2022. Online: https://sustainability.e-shape.eu/economics-behind-satellite-megaconstellations/

Hutagalung, Simon (2025): Europe's Push for Independence: Navigating Uncertainty Amid the Trump–Putin Era. *European Times,* 18 April 2025. Online: https://europeantimes.org/europes-push-for-independence-navigating-uncertainty-amid-the-trump-putin-era/

International Criminal Court (2025a): The International Criminal Court Deplores New Sanctions from the US Administration against ICC Officials. *International Criminal Court,* 5 June 2025. Online: https://www.icc-cpi.int/news/international-criminal-court-deplores-new-sanctions-us-administration-against-icc-officials

International Criminal Court (2025b): The ICC Strongly Rejects New US Sanctions against Judges and Deputy Prosecutors. *International Criminal Court,* 20 August 2025. Online: https://www.icc-cpi.int/news/icc-strongly-rejects-new-us-sanctions-against-judges-and-deputy-prosecutors

International Telecommunication Union (2025): Mobile Broadband Traffic Is Growing Faster, but Fixed Networks Still Carry Most of the Internet Data. *ITU,* 15 October 2025. Online: https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-traffic/

International Telecommunication Union (2026): *Submarine Cable Resilience.* Online: https://www.itu.int/digital-resilience/submarine-cables/

Ionos (2021): Zettabyte: tout savoir sur la taille de stockage. *Ionos,* 13 September 2021. Online: https://www.ionos.fr/digitalguide/sites-internet/developpement-web/quest-ce-quun-zettabyte/

Iulian Florea, Alexandru (2025): Elon's Empire Runs on Your Data. Decentralization Is the Escape Plan. *Ice Open Network,* 3 April 2025. Online: https://ice.io/elons-empire-runs-on-your-data-decentralization-is-the-escape-plan

Jackson, Amber (2024): Top 10: Data Centre Companies in the World 2024. *Data Centre Magazine,* 24 January 2024. Online: https://datacentremagazine.com/top10/top-10-data-centre-companies-in-the-world-2024

Jahan, Sarwat – Saber Mahmud, Ahmed (s. a.): *What Is Capitalism?* Online: https://www.imf.org/-/media/files/publications/fandd/back-to-basics/jahan-capital.pdf

Julienne, Marc (2023): La Chine dans la course à l'orbite basse. Perspectives sur la future constellation internet Guowang. *Notes de l'IFRI, Asie. Visions,* (136). Online: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/julienne_chine-constellation-guowang_avril2023.pdf

Justia U.S. Law (2016): *Microsoft v. United States, No. 14-2985 (2d Cir. 2016).* Online: https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html

Justia U.S. Supreme Court (2012): *International Shoe Co. v. Washington, 326 U.S. 310 (1945).* Online: https://supreme.justia.com/cases/federal/us/326/310/

Knott, Michael – Rossbach, Carsten – Teisseyre, Nicolas – De Peretti, Alexis – Shaikh, Jawad (2025): Constellations: Telco Race in Outer Space. *Roland Berger,* 24 March 2025. Online: https://www.rolandberger.com/en/Insights/Publications/Constellations-Telco-Race-in-outer-space.html

Koch, Olivier (2018): Les données de la guerre. Big Data et algorithmes à usage militaire. *Les Enjeux de l'information et de la communication,* 19(2), 113–123. Online: https://shs-cairn-info.ezproxy.universite-paris-saclay.fr/revue-les-enjeux-de-l-information-et-de-la-communication-2018-2-page-113?lang=fr

Koetsier, John (2025): Top 10 AI Nations: Global AI Superpowers Ranked in Industry Report. *Forbes,* 11 September 2025. Online: https://www.forbes.com/sites/johnkoetsier/2025/09/11/top-10-ai-nations-global-ai-superpowers-ranked/

KOSUKE, Takahashi (2025): China Intensifies 'Three Warfares' Targeting Japan Over Takaichi's Taiwan Remarks. *The Diplomat,* 5 December 2025. Online: https://thediplomat.com/2025/12/china-intensifies-three-warfares-targeting-japan-over-takaichis-taiwan-remarks/

KRASTEV, IVAN – LEONARD, Mark (2025): Trump's European Revolution. *European Council of Foreign Relations,* 23 June 2025. Online: https://ecfr.eu/publication/trumps-european-revolution/

KUBILIUS, Andrius (2026): Speech by Commissioner Kubilius at the Forum Europa Event "Ideas to Strengthen the Union". *European Commission Press Release,* 16 March 2026. Online: https://ec.europa.eu/commission/presscorner/detail/en/speech_26_610

LACOMIA, John M. (2025): Space Warfighter Heritage: First Military Communications Satellite Launches. *USSF Combat Forces Command,* 26 June 2025. Online: https://www.ussf-cfc.spaceforce.mil/News/Article-Display/Article/4227603/space-warfighter-heritage-first-military-communications-satellite-launches

Legal Information Institute (2026a): *18 U.S. Code Chapter 119 Part I – Wire and Electronic Communications Interception and Interception of Oral Communications,* effective as of 29 January 2026. Online: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

Legal Information Institute (2026b): *18 U.S. Code Chapter 121 Part I – Stored Wire and Electronic Communications and Transactional Records Access,* effective as of 29 January 2026. Online: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

Legal Information Institute (2026c): *18 U.S. Code Chapter 206 Part II – Pen Registers and Trap and Trace Devices,* effective as of 29 January 2026. Online: https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

Legal Information Institute (2026d): *50 U.S. Code Chapter 36 – Foreign Intelligence Surveillance,* effective as of 29 January 2026. Online: https://www.law.cornell.edu/uscode/text/50/chapter-36

Le Monde (2025): EU Chief Unveils €800 Billion Plan to 'Rearm' Europe. *Le Monde,* 4 March 2025. Online: https://www.lemonde.fr/en/european-union/article/2025/03/04/eu-chief-reveals-800-billion-plan-to-rearm-europe_6738782_156.html

Le Monde (2026): Emmanuel Macron écrit une lettre à Donald Trump pour demander la levée des sanctions contre Thierry Breton et Nicolas Guillou, juge de la CPI. *Le Monde,* 22 February 2026. Online: https://www.lemonde.fr/international/article/2026/02/22/emmanuel-macron-ecrit-une-lettre-a-donald-trump-pour-demander-la-levee-des-sanctions-contre-thierry-breton-et-le-juge-nicolas-guillou_6667798_3210.html

LINKSON, Stella (2025): Starlink Ground Stations: What They Are and How They Work. *Starlink Info,* 11 October 2025. Online: https://www.starlinkinfo.com/starlink-ground-stations

LOPEZ-LIGUORI, Aurélien (2025): Question écrite n° 3330: Lancement du cloud AWS European Sovereign Cloud. *Assemblée nationale,* 3 June 2025. Online: https://www.assemblee-nationale.fr/dyn/17/questions/QANR5L17QE3330

Low, Lauren E. (2026): NASA Unveils Initiatives to Achieve America's National Space Policy. *NASA,* 24 March 2026. Online: https://www.nasa.gov/news-release/nasa-unveils-initiatives-to-achieve-americas-national-space-policy/

Lu, Marcus (2023): Ranked: The World's Top 10 Electronics Exporters (2000–2021). *Visual Capitalist,* 3 December 2023. Online: https://www.visualcapitalist.com/top-10-electronics-exporters-in-the-world/

Lu, Marcus (2025): Ranked: The Top 25 Countries with the Most Data Centres. *Visual Capitalist,* 21 January 2025. Online: https://www.visualcapitalist.com/ranked-the-top-25-countries-with-the-most-data-centers/

Mauldin, Alan (2024): A (Refreshed) List of Content Providers' Submarine Cable Holdings. *Tele Geography,* 27 June 2024. Online: https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new

Mazuir, Manon (2026): Procès en appel de Marine Le Pen: quelle ingérence américaine? *Toute l'Europe,* 9 January 2026. Online: https://www.touteleurope.eu/vie-politique-des-etats-membres/proces-en-appel-de-marine-le-pen-quelle-ingerence-americaine/

McDowell, Jonathan (2026): *Enormous ('Mega') Satellite Constellations.* Online: https://planet4589.org/space/con/conlist.html

McMahon, Liv (2025): Meta Plans Globe-Spanning Sub-Sea Internet Cable. *BBC News,* 17 February 2025. Online: https://www.bbc.com/news/articles/ckgrgz8271go

Meijer, Bart (2025): Dutch Court Gives Meta More Time to Change Timeline Settings. *Reuters,* 28 October 2025. Online: https://www.reuters.com/technology/dutch-court-gives-meta-more-time-change-timeline-settings-2025-10-28/

Orbital Radar (2026): How Many Satellites Are in Orbit in 2026? *Orbital Radar,* 7 March 2026. Online: https://orbitalradar.com/how-many-satellites-in-orbit

OVHCloud (s. a.): *Du cloud souverain au cloud de confiance.* Online: https://www.ovhcloud.com/fr/about-us/sovereign-cloud/

Pamuk, Humeyra (2025): Exclusive: Rubio Orders US Diplomats to Launch Lobbying Blitz against Europe's Tech Law. *Reuters,* 7 August 2025. Online: https://www.reuters.com/sustainability/society-equity/rubio-orders-us-diplomats-launch-lobbying-blitz-against-europes-tech-law-2025-08-07/

Paolini, Jérôme (1987): Politique spatiale militaire française et coopération. *Politique étrangère,* 52(2), 435–449. Online: https://www.persee.fr/doc/polit_0032-342x_1987_num_52_2_3678

Piccardi, Tiziano (2025): Changer les algorithmes des réseaux sociaux suffit à réduire l'hostilité politique. *The Conversation,* 14 December 2025. Online: https://theconversation.com/changer-les-algorithmes-des-reseaux-sociaux-suffit-a-reduire-lhostilite-politique-271879

Pitron, Guillaume (2023): *La Guerre des métaux rares.* Paris: Les liens qui libèrent.

POLLET, Mathieu (2025): Big Tech Ups Lobbying Firepower, €€ in Brussels. *Politico,* 29 October 2025. Online: https://www.politico.eu/article/big-tech-lobbying-brussels-digital-markets-act-digital-services-act/

QIU, Winston (2019): Complete List of Google's Subsea Cable Investments. *Submarine Networks,* 9 July 2019. Online: https://www.submarinenetworks.com/en/nv/insights/complete-list-of-google-s-subsea-cable-investments

RAINBOW, Jason (2024): Global Satellite Capacity Prices Tumble in Starlink's Wake. *Space News,* 12 February 2024. Online: https://spacenews.com/global-satellite-capacity-prices-tumble-in-starlinks-wake/

RICHTER, Felix (2025): AWS Stays Ahead as Cloud Market Accelerates. *Statista,* 4 November 2025. Online: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/?srsltid=AfmBOooXCIDiWOKtqea5eMeXZTiPNRARAZ98xbfwvL54_mIakveNEDzp

ROBINSON-SMITH, Will (2026): SpaceX Reaches 10,000 Simultaneous Starlink Satellites in Orbit Following Falcon 9 Launch from California. *Spaceflight Now,* 16 March 2026. Online: https://spaceflightnow.com/2026/03/16/live-coverage-spacex-to-launch-25-starlink-satellites-on-falcon-9-rocket-from-california/

RUGAMER, MARIA – LO NOSTRO, Giancula (2026): Germany Military Satellite Plan Fuels EU Fragmentation Fears. *Reuters,* 24 March 2026. Online: https://www.reuters.com/business/aerospace-defense/german-military-satellite-plan-fuels-eu-fragmentation-fears-2026-03-24/

SADOWSKI, Jathan (2019): When Data Is Capital: Datafication, Accumulation and Extraction. *Big Data & Society,* 6(1). Online: https://doi.org/10.1177/2053951718820549

SAILLANT, Jean-Michel (1994): Point de synthèse XII. Le satellite. In *Passeport pour les médias de demain.* Villeneuve d'Ascq: Presses universitaires du Septentrion, 165–175. Online: https://books.openedition.org/septentrion/114000?lang=fr

SCHMIDT, Milos (2024): Onze pays de l'UE ont pris des mesures de sécurité pour interdire Huawei et ZTE sur la 5G. *Observatoire de l'Europe,* 12 August 2024. Online: https://www.observatoiredeleurope.com/onze-pays-de-lue-ont-pris-des-mesures-de-securite-pour-interdire-huawei-et-zte-sur-la-5g_a37812.html

SÉE, Arnaud (2019): La régulation des algorithmes: un nouveau modèle de globalisation? *Revue française de droit administratif,* 5, 830–843. Online: https://shs.hal.science/halshs-02450617/document

SGDSN (2016): "Renseignement et terrorisme" Discours inaugural prononcé par M. Louis Gautier le 9 décembre 2016 devant les sessions IHEDN-INHESJ. Paris. *Secrétariat général de la défense et de la sécurité nationale,* 9 December 2016. Online: https://www.sgdsn.gouv.fr/publications/renseignement-et-terrorisme

SGDSN (2025): Revue nationale stratégique 2025. *Secrétariat général de la défense et de la sécurité nationale,* 2025. Online: https://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_Actualisation_2025_RNS_FR.pdf

Shetti, Utkarsh – Khushi, Akanksha (2024): Musk Says SpaceX Has Moved Its Incorporation to Texas from Delaware. *Reuters,* 15 February 2024. Online: https://www.reuters.com/technology/space/musk-says-spacex-has-moved-its-incorporation-texas-delaware-2024-02-15/

Sieraczek-Laporte, Manon (2025): La guerre informationnelle des GAFAM pour conserver leur hégémonie numérique en Europe. *Ecole de Guerre Economique,* 19 May 2025. Online: https://www.ege.fr/la-guerre-informationnelle-des-gafam-pour-conserver-leur-hegemonie-numerique-en-europe

Soares, Joana (2026): "Explosive Mix": How US Pressure and Big Tech Lobbying Are Reshaping EU Digital Rules. *EUPerspectives,* 16 February 2026. Online: https://euperspectives.eu/2026/02/explosive-mix-us-pressure-and-lobbying-shape-eu-tech-policy/

Sokolowsky, Jennifer (2020): Azure Space Partners Bring Deep Expertise to New Venture. *Microsoft News,* 20 October 2020. Online: https://news.microsoft.com/source/features/digital-transformation/azure-space-partners-bring-deep-expertise-to-new-venture/

Starlink (s. a.): *Service Plans.* Online: https://starlink.com/service-plans?srsltid=AfmBOor3mJmzNjEJygLzk8_frUr_MV6qsYmr5qrw3HZxSAouhEGaKsAa

Starlink Insider (2025): *Starlink Ground Station Locations.* Online: https://starlinkinsider.com/starlink-gateway-locations/

Statista (2025): Ranking of Telecom Infrastructure Companies by Brand Value in 2025. *Statista,* 27 November 2025. Online: https://www.statista.com/statistics/500041/telecom-infrastructure-brand-value/

Sterling, Toby (2026): Dutch Court Upholds Ruling Forcing Meta to Offer Chronological Feeds. *Reuters,* 10 March 2026. Online: https://www.reuters.com/legal/litigation/dutch-court-upholds-ruling-forcing-meta-offer-chronological-feeds-2026-03-10/

Sutherland, Callum (2026): 'A European Moment:' E.U. Leaders Push Back Against U.S. 'Civilizational Erasure' Claim. *Time,* 16 February 2026. Online: https://time.com/7379005/european-sovereignty-leaders-rally-against-us-erasure-claims/

Szczepański, Marcin (2025): China's Rare-Earth Export Restrictions. *European Parliamentary Research Service,* 24 November 2025. Online: https://epthinktank.eu/2025/11/24/chinas-rare-earth-export-restrictions/

Tambou, Olivia – Barbou des Places, Ségolène (2020): À la recherche d'un régime cohérent de protection des données personnelles contre les mesures de surveillance étatique. *Annuaire Français de Droit International,* 66, 595–606. Online: https://www.persee.fr/doc/afdi_0066-3085_2020_num_66_1_5482

Taylor, Petroc (2025a): Volume of Data or Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2029. *Statista,* 19 November 2025. Online: https://www.statista.com/statistics/871513/worldwide-data-created/

Taylor, Petroc (2025b): Telecommunications Equipment Companies Revenue Share Worldwide in 2024. *Statista,* 27 November 2025. Online: https://www.statista.com/statistics/1614896/telecoms-equipment-market-share/

TAYLOR, Petroc (2025c): Leading Telecommunications Equipment Companies Worldwide as of May 28, 2025, by Market Capitalization. *Statista,* 27 November 2025. Online: https://www.statista.com/statistics/1614671/top-telecoms-equipment-companies-market-cap/

TERWELLEN, Andreas (2025): Exploring the New AWS European Sovereign Cloud: Sovereign Reference Framework. *AWS Security Blog*, 22 December 2025. Online: https://aws.amazon.com/de/blogs/security/exploring-the-new-aws-european-sovereign-cloud-sovereign-reference-framework/

Tesla Pi Phone (2026): *The Definitive Guide to Features, Release Date, Price and Rumors.* Online: https://www.teslapiphone.net/

The Economist (2017): Tech Companies Are Laying Their Own Undersea Cables. *The Economist,* 9 October 2017. Online: https://www.economist.com/graphic-detail/2017/10/09/tech-companies-are-laying-their-own-undersea-cables

The Economist (2025): Europe Needs to Spend More on Defence, Not Just Pretend To. *The Economist,* 20 March 2025. Online: https://www.economist.com/europe/2025/03/20/europe-needs-to-spend-more-on-defence-not-just-pretend-to

The White House (2025a): *National Security Strategy of the United States of America. November 2025.* Online: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

The White House (2025b): Imposing Sanctions on the International Criminal Court. *The White House,* 6 February 2025. Online: https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/

THUY D., Nguyen (2025): Lobbying Expenses of Meta in the European Union (EU) from 2017 to 2023. *Statista,* 25 November 2025. Online: https://www.statista.com/statistics/1321211/lobbying-expenses-of-meta-inc-eu/

UN News (2025): Accélération de la colonisation israélienne: colline après colline, la paix s'éloigne. *UN News,* 16 December 2025. Online: https://news.un.org/fr/story/2025/12/1158098

United States Securities and Exchange Commission (2017): Form D. Notice of Exempt Offering of Securities. *United States Securities and Exchange Commission,* 27 November 2017. Online: https://www.sec.gov/Archives/edgar/data/1181412/000118141217000002/xslFormDX01/primary_doc.xml

UNTERSINGER, Martin (2022): Ce que les « révélations Snowden » ont changé depuis 2013. *Le Monde,* 13 September 2019. Online: https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis-2013_5509864_4408996.html

VAN MIDDELAAR, Luuk (2026): Luuk van Middelaar: 'With Trump, Europe Is Suffering an Ideological Assault from Its Historic Protector'. *Le Monde,* 3 February 2026. Online: https://www.lemonde.fr/en/opinion/article/2026/02/03/luuk-van-middelaar-with-trump-europe-is-suffering-an-ideological-assault-from-its-historic-protector_6750096_23.html

Vie Publique (2024): DMA: le règlement sur les marchés numériques veut mettre fin à la domination des géants du Net. *Vie Publique,* 13 May 2024. Online: https://www.vie-publique.fr/eclairage/284907-dma-le-reglement-sur-les-marches-numeriques-ou-digital-markets-act

Vie Publique (2025a): Le règlement européen sur les services numériques (DSA) vise une responsabilisation des plateformes. *Vie Publique,* 4 August 2025. Online: https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act

Vie Publique (2025b): L'autonomie stratégique européenne en cinq questions. *Vie Publique,* 9 December 2025. Online: https://www.vie-publique.fr/questions-reponses/282035-lautonomie-strategique-europeenne-en-cinq-questions

Vou, Andreas (2020): Comment les GAFAM étendent leur emprise sur l'UE et ses Etats à coups de lobbying. *Voxeurop,* 15 October 2020. Online: https://voxeurop.eu/fr/comment-les-gafam-etendent-leur-emprise-sur-ue-et-ses-etats-coup-de-lobbying/

Wälde, Milena (2026): Trump Warns NATO (Again) of 'Very Bad Future' if Allies Don't Secure Strait of Hormuz. *Politico,* 16 March 2026. Online: https://www.politico.eu/article/donald-trump-warns-nato-very-bad-future-allies-iran-strait-of-hormuz/

Zoox Smart (2020): Which Country Is Leading Data Generation? How Does It Work? *Zoox Smart,* 15 September 2020. Online: https://blog.zooxsmart.com/which-countries-are-leading-data-generation-and-how-does-it-work

Zandt, Florian (2022): Big Tech Goes Big on Lobbying Efforts. *Statista,* 25 January 2022. Online: https://www.statista.com/chart/26673/highest-lobbying-spending-in-the-tech-industry-in-the-us/

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.