December 2025
Main Chair, Deputy Chair,
Leiden Model United Nations 2025

Digital autonomy of the European Union

European Council for Foreign Affairs (ECf)

Table of Contents

Introduction **3**
Definition of key terms **4**
Term in alphabetical form 4
General Overview **5**
description 5
description 5
Description 6
description

6
Major parties involved **7**
European Union (EU) 7
China 7
USA 7
Party 4 7
Party 5 8
Timeline of events 9
Possible solutions **10**
References **11**

Introduction

In an increasingly interconnected and digitised world, most affairs nowadays are handled using rapidly advancing, modern technology such as online networks, and complex computer systems. The European Union is no exception to these technological advances, thus Digital Autonomy has become a critical priority in the EU's strategy. Similarly to Strategic Autonomy, Digital autonomy is the ability to make independent choices in the digital realm. Digital Autonomy is all about ensuring that Europe can develop and rely on its own technology without being overly reliant on foreign services. For example, cybersecurity is a significant threat that the EU faces, and is a problem that can be mitigated through the development of technology, and digital autonomy. Digital autonomy in the EU has emerged as a much more recent issue. Due to the novelty of this concept, digital autonomy has not yet quite established a particular definition for itself. With both China and the USA competing for technological supply chains, the EU has struggled to keep up with defining Europe's digital autonomy, while also maintaining good relations with the two great powers in its current geopolitical position in between them.

The EU lacks a coherent rendering of its approach to the issue to ensure and guide Europe's course of action in achieving digital autonomy. Control over technology also gives the EU more control over data, meaning that data can be stored and processed in ways which are more in line with the EU's policies and values. With China and the US as competitors, (and especially with Donald Trump's current tensions with the EU), the necessity for digital autonomy has surged. This acknowledgement that relying on foreign providers poses a bigger strategic/security threat has winded digital autonomy into the midst of European policy debates. This concept involves collaboration, creating legal frameworks, and investing strategically to further advance tech.

Definition of key terms

Artificial Intelligence (AI) regulation

Artificial Intelligence, or AI is a rapidly growing technology. The EU has taken measures for the regulation of AI as part of its digital strategy.

Cybersecurity

Cybersecurity is the protection of online systems, infrastructure, and data from cyber threats. Cybersecurity is essential for economic welfare and security, and therefore a key driver in the EU's desire to further develop digital autonomy.

Data governance

Data governance is the managing of an organisation's data assets, overseeing its quality, security, and compliance with policies. It is a political concept that establishes how data is created, stored, protected, deleted, etc.

Digital infrastructure

Digital infrastructure is the combination of software, hardware, and data centers which serve as the foundation of an organisation's digital operations.

European Security Strategy (ESS)

The European Security Strategy is the document containing the EU's strategy for security. The document explicates how the EU aims to achieve a more secure Europe, by identifying threats and defining strategic objectives including both Strategic Autonomy and Digital Autonomy.

External Action

This refers to the EU's actions regarding international affairs and their relationship with foreign states and organisations.

Power

The ability to do something or act in a certain way. To have power over someone or something means to be able to influence the course of their actions.

Digital Sovereignty

Digital Sovereignty is the authority of a state to govern its own (or another state's) digital environment, including data and infrastructure without interference from any other actors.

Strategic Autonomy

Strategic Autonomy (in the context of the EU) refers to the capacity of EU member states to act independently of any other power for its defense and security.

General Overview

The EU is not autonomous in any sense currently. The Union relies heavily on energy imports from the US, the Middle East, Norway, and even Russia in certain cases. It imports agricultural products from all over the world, especially South America and Northern Africa. Compared to other major global players (China, US, Russia), the EU is arguably the most dependent first-world entity.

Technology-wise, the EU is behind in three major categories: development, production, and implementation. For the "digital" part, 70% of cloud technology used within the European Union originates from the United States. If you have a minute, consider your phone: how many applications/software were fully developed in the EU? Aside from Spotify, most apps are from the United States, your phone was designed in China, South Korea, or the US, and manufactured in China or Vietnam.

App	Origin Country	Notes about usage in EU
Temu	China	Most-downloaded in many European countries in 2024 (Germany, France, Spain, UK etc.) (Brilliant Maps)
ChatGPT	USA	Top downloaded especially in Central & Southeastern European countries — Austria, Hungary, Romania, Switzerland, etc. (Brilliant Maps)
TikTok	China	Among the top in many EU countries. Frequently appears as a most-used app (Statista)
WhatsApp	USA (Meta)	Very high usage in Southern/Eastern Europe; often used by >90% of smartphone users in Spain, Italy, Romania, Portugal (Statista)
Telegram	Founded in Russia (but global company)	Rising in popularity; among top messenger/social apps in several EU states (youappi.com)
Instagram / Facebook / Messenger	USA (Meta)	Standard in many countries for social media / messaging use (youappi.com)

Such dependence poses significant risks, especially in these unprecedented and unpredictable times. Relying on the United States and China in particular places Europe in a vulnerable position, both strategically and economically. Even with legislation such as the General Data Protection Regulation (GDPR) introduced in 2016, the Union cannot consistently ensure that user data is stored, processed, or secured in alignment with its own values.

The Cambridge Analytica scandal of 2018 further exposed the risks of relying on foreign platforms for sensitive data. The scandal in which improperly harvested data was used by a British analyst group to manipulate the 2016 US elections, highlighted Europe's vulnerability when relying on foreign tech giants for its digital ecosystem. The lawsuit ended with a 700 million euro settlement paid by Facebook (now Meta). It pushed the EU to enforce stricter data laws like the General Data Protection Regulation (GDPR) (which took effect in 2018), making privacy and digital sovereignty a central part of its digital autonomy agenda.

Having recognized these challenges, the EU has begun several initiatives to strengthen digital autonomy. The Gaia-X project, launched in 2019, aims to create a secure, European-based cloud ecosystem, where European files are stored on European servers. The EU Digital Strategy of 2020 laid out priorities for AI, cloud, cybersecurity, and semiconductors. In 2021, the European Data Governance Act was proposed to facilitate secure data sharing while keeping control in European hands. The 2022 EU Chips Act seeks to increase domestic semiconductor production from ~10% to 20% of the global market by 2030, reducing reliance on foreign suppliers.

Artificial intelligence (AI) is an even more urgent issue. While the EU has begun implementing AI legislation, it lags behind in AI technology development and innovation. Most major AI companies are based in the US or China. While a few European AI firms exist, their models are less developed and much less widely used than their transatlantic or transasiatic counterparts.

However, the EU is ahead in certain areas of digital autonomy, mainly digital privacy laws, AI regulation, and broader legislative control over technology. There have been many instances where the EU discovers shady activities performed by US companies, such as non-GDPR handling of data, or slowing older phones without the user's knowledge, to urge them to upgrade.

Major parties involved

European Union (EU)

The main party involved; The EU has passed several laws and a number of regulations for digital security, AI, and the regulation of data. As a distinct branch of strategic autonomy, the EU has deemed digital autonomy as a significant part of their global strategy. Subsequently due to potential cybersecurity threats from the Russian Federation, and the competition for digital power and supplies between the USA and China, the EU has found itself striving for a more self-reliant capacity in the digital realm, particularly in strengthening cybersecurity and continuing to regulate emerging innovations such as AI.

China

China is a major competitor of both the USA and the EU in digital development. China has invested copiously in digital infrastructure, including 5G and AI which have positioned them high up the ladder of digital power. China is a key supplier of digital infrastructure, and aims to expand its technological dominance and global influence.

United States of America (USA)

The USA is a major technological supplier to the EU, with companies like Google, Amazon, and Microsoft dominating Europe's digital infrastructure. With striving to become more autonomous in general, this usually refers to Europe being more independent from the USA, which is the party they currently rely on most for military, trade, and digital resources. The ongoing situation between the USA and the EU presents both opportunity and tension for Europe's economy and security.

Russia

Russia has shown consistent hostility towards the EU, especially in recent years and today. Russia has been known to be behind multiple cyber attacks, targeting both western and eastern European countries, particularly Ukraine but also countries such as Poland and Ukraine. These attacks, which have a Europe-wide effect, have been condemned by both the EU member states and NATO allies. Russia continues to present itself as a threat to the EU, both

Timeline of events

2016	*Introduction of GDPR*	EU introduces new, one-of-a-kind legislation to battle unlawful digital data use
2018	Cambridge Analytica scandal	Data misuse scandal reinforces EU concerns about reliance on U.S. tech giants, accelerating debates on the need for stronger digital sovereignty.
2019	Gaia-X Project	France launches Gaia-X project
2020	EU Digital Strategy Announced	The European Commission presents its Digital Strategy, emphasizing data sovereignty, AI development, and reducing dependence on foreign technology.
2021	European Data Governance Act Proposed	The EU proposes legislation to facilitate data sharing while ensuring EU-based control, further embedding the principle of digital autonomy in policymaking.
2022	Russian Invasion of Ukraine & Digital Security Concerns	The war in Ukraine heightens EU awareness of cyber vulnerabilities and dependency on external providers, adding urgency to the digital autonomy agenda.
2022	EU Chips Act Proposal	The Commission proposes the EU Chips Act to boost semiconductor production in Europe, with the goal of increasing Europe's global chip production share from ~10% to 20% by 2030.
2023	EU Cloud Market Report Shows U.S. Dominance	Studies reveal that about 70% of the EU cloud market is controlled by U.S. providers (Amazon, Microsoft, Google), highlighting the Union's continued dependence.
2024	Adoption of the AI Act	EU adopts first AI legislation

Possible solutions

Currently, overregulation has created a bureaucratic environment where innovation and production are slowed. Many observers still consider it much easier to start a new company in the US than in the EU, due to faster business registration, more flexible labor laws, and greater access to venture capital. While many EU regulations are crucial to ensure citizens' privacy, the EU's regulatory framework is so daunting that many innovators choose the move and innovate in the US instead. This leaves the EU dependent on foreign entities for all technology and digital innovation.

Expanding access to such financial support, simplifying application processes, and encouraging private investment could help European entrepreneurs compete on a global scale.

Education, financial education, and digital education are also all important areas to strengthen. Improving digital literacy at all levels, training future engineers, data scientists, and AI specialists, and providing entrepreneurs with financial and business skills would create a workforce capable of driving innovation and sustaining a more autonomous European tech ecosystem.

It would be important for the EU to create programmes where receiving education outside of the EU is encouraged and even funded, on the condition that the applicant returns to work and innovate within the Union after graduation. We are like sponges; by surrounding ourselves with those who excel, in this case China and the US we absorb their wisdom and elevate our own abilities.

References

- Codagnone, C., Liva, G., & Gunderson, L. (n.d.). https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf
- Europe Talks Digital Sovereignty – Open Future. (2025). Open Future. https://openfuture.eu/blog/europe-talks-digital-sovereignty/
- European Parliament. (2025, February 19). EU AI Act: First Regulation on Artificial Intelligence. European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
- Follin, A. (2025, February 4). Digital sovereignty in Europe: navigating the challenges of the digital era. ESCP International Politics Society. https://pppescp.com/2025/02/04/digital-sovereignty-in-europe-navigating-the-challenges-of-the-digital-era/
- How can the European Union achieve digital strategic autonomy? Views from future leaders. (2022). CIDOB. https://www.cidob.org/en/publications/how-can-european-union-achieve-digital-strategic-autonomy-views-future-leaders
- Jones, E. (2024, August 30). Data governance. Ibm.com. https://www.ibm.com/think/topics/data-governance
- Space for Infrastructure: Digital Infrastructure. (2024). Esa.int. https://business.esa.int/funding/call-for-proposals-non-competitive/space-for-infrastructure-digital-infrastructure
- Tech sovereignty and a new EU foreign economic policy. (2024). ECDPM. https://ecdpm.org/work/tech-sovereignty-and-new-eu-foreign-economic-policy