Working Paper Series No. 3

November 2020

Fostering EU's Digital Autonomy: Different Perspectives in the Transatlantic Community

Laboratory of Intelligence & Cyber-Security

Author: Dr. Andrew Liaropoulos

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

About the Laboratory

The Laboratory of Intelligence & Cyber-Security was founded in 2015 and provides the Department of International and European Studies, in University of Piraeus, with research and expertise on the fields of intelligence studies and the politics of cyberspace. The Laboratory focuses mainly on the topics of intelligence reform, economic espionage, intelligence, democracy and ethics, oversight of intelligence agencies, cyber-security, cyber-terrorism and cyberspace governance. The Laboratory aims to independently or in cooperation with other higher educational and scientific-research institutions, public institutions, enterprises and civil-society organizations to organize and conduct academic and scientific-research activities in the fields of intelligence and cyber-security.

About the Author

Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. He also teaches in the Joint Military Intelligence College, the National Security College and the Air Staff Command College. He earned his Master's Degree in Intelligence and Strategic Studies at Aberystwyth University and his Doctorate Diploma at Swansea University. His research interests include international security, intelligence reform, strategy, foreign policy analysis, European security policy, cyber security and Greek security policy. Dr. Liaropoulos is also a senior analyst in the Research Institute for European and American Studies (RIEAS) and a member of the editorial board of the Journal of Information Warfare (JIW) and of the Journal of European and American Intelligence Studies (JEAIS).

1. Introduction

The coronavirus outbreak in spring 2020 was a devastating experience, but also highlighted the importance of the digital domain. Due to digital technologies, people were able to work from home, connect to friends, family and colleagues. Policymakers around the world realized the power of digital technologies to influence economic, societal and political outcomes. Even as misinformation about the virus spread across social media, governments turned to potential tracking applications and analyses of medical data to find a way out of lockdowns. The virus sharply revealed the differences in governmental approaches to the internet and their citizens. The virus reinforced within Europe the desire for greater digital sovereignty, based on a strong, European-controlled digital infrastructure that will be resilient in the face of disinformation and other disruptions.[1]

It is in this context that the digital autonomy and digital sovereignty became the latest buzzwords in the corridors of the EU.[2] In plain words, if Europe wants to become autonomous, it must gain control of the technologies that play an increasingly important role in the lives of its citizens. There is a global race for technological leadership and the EU, despite its many assets, is falling behind in this race.[3] This means Europe should know who controls these technologies and ensure that their use is compatible with the values and objectives of the Union. Adding to that, the EU must develop its own methodology for collecting evidence of cyber incidents, it must independently identify the source of hostile activity. The quest for digital sovereignty is rooted in a perception that Europe has to date been dominated by non-EU companies, especially US and Chinese firms, in the digital space. This is true. Of the top 20 digital companies, only one EU company (Deutsche Telekom) made the list,[4] while US companies claimed 12 spots; China and Japan two each; and Hong Kong, South Korea, and Taiwan one each.[5] Likewise, in the area of Artificial Intelligence (AI), the EU is lagging behind both the US and China, in terms of private investment and adoption of AI technologies by the private sector and by the public sector.[6] So how can the EU truly achieve the goal of digital autonomy and what are the implications of EU's ambition to become digitally independent in the transatlantic relationship?

2. European policies towards digital autonomy

Over the last years, the EU has responded to the growing economic and political

[1] Rosa, Brunello, 'Data Laws or Data wars?', *Chatham House,* 1 April 2020.

[2] Madiega, Tambiama, 'Digital Sovereignty for Europe', *EPRS - European Parliamentary Research Service*, July 2020.

[3] European Commission, 'Rethinking Strategic Autonomy in the Digital Age', *EPSC Strategic Note*, Issue 30, July 2019.

[4] https://www.forbes.com/top-digital-companies/list/.

[5] European Commission, 'USA-China-EU plans for AI: where do we stand?', *Digital Transformation Monitor*, January 2018.

[6] Castro, Daniel, Michael McLaughin and Eline Chivot, 'Who is winning the AI Race: China, the EU of the United States?', *Center for Data Innovation,* August 2019.

importance of the digital economy, as well as to the security concerns of its citizens, by launching a series of regulatory initiatives.[7] To begin with, the EU launched the Digital Single Market in 2015, in order to reduce barriers to digital activity between the member-states and improve access to online services and products for citizens and businesses.[8] After the 2013 revelations by Edward Snowden, of significant US government surveillance of European citizens' communications, including German Chancellor Angela Merkel's mobile phone, trust in the US took a significant blow and raised serious concerns regarding the cohesion of the transatlantic partnership. Snowden's global surveillance revelations triggered the debate about data protection within the EU.[9] As a result, the EU passed the General Data Protection Regulation (GDPR)[10]. This privacy legislation imposed strict conditions on the handling of EU citizens' personal information, even if that data or citizen was physically outside the EU. When it came into effect in May 2018, companies around the world found themselves having to comply with GDPR. As a result, the EU is regarded as a standard setter in privacy and data protection, since many countries have incorporated GDPR provisions in their national legislation.[11] Although creating EU digital sovereignty was rarely mentioned at the time, both the Digital Single Market plan and GDPR were clearly intended to enhance EU digital capabilities and provide citizens with a form of control, over their own personal data.[12] Since then, the idea of greater European sovereignty over the digital realm had gained more ground. Indicative of the above is the reference made by Ursula von der Leyen in her statement over her policy priorities, where she called for the EU to "achieve technological sovereignty in some critical technology areas".[13]

The European Commission stressed the importance of technological sovereignty, and the need to ensure that the EU has a secure, high-quality digital infrastructure and the ability to develop and sustain key cutting-edge technologies.[14] In 2019, the EU expressed its concern about the potential reliance of its member-states on Chinese 5G infrastructure.[15] Even though, Huawei was not banned, despite the pressure exercised by the US, certain member-states restrained Huawei's role in their networks.[16] The EU is concerned over the lack of control over data produced in its territory. The global cloud market is dominated by US and Chinese technological giants. Both governments and the private sector in the EU, are concerned about using non-European data services, given the expansive extra-territorial ability granted to US law

[7] Hobbs, Carla (ed), 'Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry', *European Council on Foreign Relations,* July 2020, p.47.

[8] https://eufordigital.eu/discover-eu/eu-digital-single-market/.

[9] Rossi, Augustin, 'How the Snowden Revelations Saved the EU General Data Protection Regulation', *The International Spectator*, 53, 4 (2018).

[10] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

[11] Madiega, 'Digital Sovereignty for Europe', p.3.

[12] Hobbs, 'Europe's Digital Sovereignty', p.47.

[13]https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

[14] Hobbs, 'Europe's Digital Sovereignty', p.48.

[15] NIS Cooperation Group, 'EU coordinated risk assessment of the cybersecurity of the 5G networks', Report, 9 October 2019.

[16] Morris, Ian, 'Europe is showing Huawei the exit', *Light Reading,* 9 September 2020.

enforcement agencies to obtain foreigners' personal data under the 2018 US Cloud Act.[17] As a result, the European Commission highlighted the need to deploy European designed cloud solutions[18] and began discussions with the German and French governments, which had already launched the GAIA-X cloud project.[19] Such initiatives aim to build a resilient digital infrastructure.

Another example of exercising digital sovereignty is the fact that the EU is perceived to be a global leader in establishing standards related to online activities that are intended to safeguard its citizens and ensure an ethical approach to the dilemmas posed by the digital world (e.g. the "right to be forgotten" and restrictions regarding hate speech).[20] In particular, the data strategy and the AI proposal include potential rules seeking to ensure that data collected and controlled within the EU, should be managed according to ethical standards that place privacy in the epicenter.[21] Likewise, the Digital Services Act, proposes rules intended to reinforce European norms on content, consumer protection, and platform liability.[22] In parallel, the European data strategy that was adopted in February 2020, aims to create European data spaces that will be used for economic and societal reasons. In these data spaces, EU companies and citizens will be able to control their data.[23] By emphasizing on infrastructure, key industries, creation of data spaces and by promoting a set of European norms for behavior and responsibilities in the digital world, the EU aspires to gain more control over how digital activities are conducted within Europe and therefore how its citizens are treated in the digital realm.

3. Trapped between the US Cloud Act and Chinese 5G providers or examples of EU's digital sovereignty?

Technological giants like Google, Apple, Facebook, Amazon and Microsoft (the so-called GAFAM), are collecting massive amounts of personal data and their economic model (data capitalism) is largely based on the collection and exploitation of online users' data to generate profit.[24] Most EU citizens store their data with US cloud providers, because there are hardly any European alternatives. This is problematic and has raised concerns within the EU, because US intelligence and law enforcement agencies can access this data under the US Cloud Act. Thus, the European Court of Justice overturned in July the so-called "Privacy Shield" agreement, which allowed data transfers between European and US companies, but without providing the legal protection in the US that users enjoy in Europe. Because this data could be tapped by

[17] Madiega, 'Digital Sovereignty for Europe', p.4.

[18] Nextcloud, 'EU governments chose independence from US cloud providers with Nextcloud', 27 October 2019.

[19] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/FAQ/faq-projekt-gaia-x.html.

[20] Hobbs, 'Europe's Digital Sovereignty', p.49.

[21] The EU's approach towards AI is a human centric one, meaning that the EU requires compliance with fundamental rights, regardless of whether these are explicitly protected by EU treaties, such as the Treaty on European Union or by the Charter of Fundamental Rights of the European Union.

[22] https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

[23] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

[24] Madiega, 'Digital Sovereignty for Europe', pp.3-4.

US authorities without EU citizens being able to take effective action against it, the Court declared it invalid. This development is regarded, as a step towards digital sovereignty because the EU had stood up for its values and the rights of its citizens.[25]

As mentioned earlier, a European alternative to the US providers is on the way. GAIA-X, a Franco-German project, is to produce cloud services according to European standards next year. It is a platform where customers can find providers that meet certain criteria, such as compliance with the GDPR. By building cloud services, the EU seeks to keep in Europe data generated on the continent, in order to protect that information from non-European governments.[26] US companies are also welcomed to participate, as long as they comply with these standards.[27] This is an example of how Europe can extend its digital sovereignty, through clear sets of criteria, which companies must meet in order to be allowed to enter the internal market. Some EU member-states, including Belgium, Bulgaria, France, Germany, Greece, Luxembourg, the Netherlands, Poland, Romania, and Sweden have taken a further step, by enacting data localization measures that exclude certain categories of data from being relocated outside their territory.[28]

Over the last two years, Europe has been discussing whether to commission Chinese producers like Huawei to equip Europe with 5G technology. Even though, Chinese companies offer high quality at a low price, there is a concern that the Chinese government could influence companies like Huawei to monitor or even shut down critical infrastructure whenever it wants.[29] The US sanctioned the company and demanded Europe to follow. Brussels left the decision to the states. For example, Spain hired Huawei, whereas the Czech Republic decided not to. Germany took the middle way, welcoming all companies as long as they adhere to a catalogue of safety criteria. For example, suppliers have to give a declaration of confidence that no information will reach foreign authorities and that they can refuse to disclose confidential information from or about their customers to third parties.[30]

4. Conclusions

To promote European digital sovereignty, the EU member-states should coordinate their policies around the following areas. First, enhance the capacity of EU member-states to defend their networks and to strengthen their digital resilience. Second, develop an autonomous, innovative, effective and diversified industry at the European level, in particular in the fields of cybersecurity and trusted digital products. Third, the member-states should decide in an autonomous way of the level of security for their

[25] Grüll, Philip, 'Geopolitical Europe aims to extend its sovereignty from China', EUACTIV.DE, 11 September 2020, https://www.euractiv.com/section/digital/news/geopolitical-europe-aims-to-extend-its-digital-sovereignty-versus-china/.

[26] Burwell, Frances and Kenneth, Propp, 'The European Union and the Search for Digital Sovereignty: Building Fortress Europe or preparing for the New World?', Atlantic Council, *Future Europe Initiative, Issue Brief,* June 2020, p.9.

[27] Grüll, Philip, 'Geopolitical Europe aims to extend its sovereignty from China'.

[28] Burwell and Propp, 'The European Union and the Search for Digital Sovereignty', p.9.

[29] Grüll, Philip, 'Geopolitical Europe aims to extend its sovereignty from China'.

[30] Ibid.

data, in particular in the context of negotiations of trade agreements. To enhance its digital autonomy and to protect its digital sovereignty, the EU must become resilient and therefore invest in prediction, prevention, detection and response. A comprehensive European cybersecurity strategy is a necessity to achieve digital strategic autonomy, protect Europe’s digital sovereignty and compete on the global market.

The widespread implementation of the GDPR, demonstrated to the EU that it could create regulations with global reach. As the EU galvanizes its digital agenda, US companies are likely to face additional rules, especially on data governance, use of AI, platform liability, and other digital issues. This will affect the ability of US companies to import goods or services that use AI into the EU, or how they manage data pools derived from EU data.[31] It is fair to argue that the EU’s quest for digital sovereignty will put the fragile transatlantic partnership in a serious test over the coming years. After all, from the viewpoint of autonomy, the dominance of US digital platforms is regarded as a critical vulnerability for Europe. The regulatory differences between the US and the EU regarding the definition and protection of privacy rights and personal data, remains unsolved and is a thorny issue in their relationship.

References

- Burwell, Frances and Kenneth, Propp, ‘The European Union and the Search for Digital Sovereignty: Building Fortress Europe or preparing for the New World?’, Atlantic Council, *Future Europe Initiative, Issue Brief,* June 2020.
- Castro, Daniel, Michael McLaughin and Eline Chivot. ‘Who is winning the AI Race: China, the EU of the United States?’, *Center for Data Innovation,* August 2019.
- European Commission, ‘Rethinking Strategic Autonomy in the Digital Age’, *EPSC Strategic Note*, Issue 30, July 2019.
- European Commission, ‘USA-China-EU plans for AI: where do we stand?’, *Digital Transformation Monitor*, January 2018.
- Grüll, Philip, ‘Geopolitical Europe aims to extend its sovereignty from China’, EUACTIV.DE, 11 September 2020, https://www.euractiv.com/section/digital/news/geopolitical-europe-aims-to-extend-its-digital-sovereignty-versus-china/.
- Hobbs, Carla (ed), ‘Europe’s Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry’, *European Council on Foreign Relations,* July 2020.
- Madiega, Tambiama, ‘Digital Sovereignty for Europe’, *EPRS - European Parliamentary Research Service*, July 2020.
- Morris, Ian, ‘Europe is showing Huawei the exit’, *Light Reading,* 9 September 2020.

[31] Hobbs, ‘Europe’s Digital Sovereignty’, p.52.

- Nextcloud, ‘EU governments chose independence from US cloud providers with Nextcloud’, 27 October 2019.
- NIS Cooperation Group, ‘EU coordinated risk assessment of the cybersecurity of the 5G networks’, Report, 9 October 2019.
- Rosa, Brunello, ‘Data Laws or Data wars?’, *Chatham House,* 1 April 2020.
- Rossi, Augustin, ‘How the Snowden Revelations Saved the EU General Data Protection Regulation’, *The International Spectator*, 53, 4 (2018).