THE CITY LAW SCHOOL
CITY, UNIVERSITY OF LONDON
EST 1894

Academic excellence for business and the professions

City Law School Research Paper 2022/08

The strengthening of European technological sovereignty and its legal bases in the Treaties

Elaine Fahey & Sara Poli

ELAINE FAHEY & SARA POLI
The City Law School

The City Law School Working Paper Series are published by The City Law School, City University London, Northampton Square, London, EC1V 0HB.

An index to the working papers in The City Law School Working Paper Series is located at:
www.city.ac.uk/law/research/working-papers

THE STRENGTHENING OF EUROPEAN TECHNOLOGICAL SOVEREIGNTY AND ITS LEGAL BASES IN THE TREATIES

Published in Eurojus 02/2022

ISSN 2384-9169 rivista.eurojus.it

Elaine Fahey & Sara Poli*

Abstract

We show how the European technological sovereignty is evoked to argue that the EU should be more competitive in the global market and fill in its technological gaps. At the same time, this concept has an assertive and defensive dimension in its framing which raises many questions, particularly as to its concreteness and the realisability of its objectives. There are also not inconsiderable legal issues possibly arising from its application in light of its extensive scope. The article demonstrates the complexities of the span of the legal base for technological sovereignty when subjected to scrutiny from a legal perspective. We consider whether the achievement of a Sovereignty Union in the field of technology may or may not face legal obstacles. We examine two Commission proposals for amendments of measures on network security systems and critical infrastructures and show how they aim at enhancing security even if they are adopted pursuant to Article 114 TFEU (internal market harmonisation). Legal challenges to acts of this kind are possible when they are adopted in their legally binding form. We argue that should the Court of Justice confirm their validity, this would imply that the European integration process is advancing.

Keywords: Technological sovereignty; EU Competence; Internal market; CJEU; legal basis

* Elaine Fahey is Jean Monnet Chair of Law & Transatlantic Relations and Professor of Law at the Institute for the Study of European Law (ISEL), the City Law School, City, University of London; Sara Poli is full professor of EU law at the University of Pisa (Italy), Department of Political Science.

Introduction

Recently, many institutional actors, in particular the European Commission and the Council[1] and have referred to the need to enhance "European technological sovereignty" in various documents[2]. What is striking is that in none of the policy documents in which Europe's technological sovereignty is evoked, there is any definition of this concept or its legal basis. In most of these usages, the overall implication appears to be that the EU is sovereign in making decisions. In abstract terms the expression "European technological sovereignty" refers to the process of transforming the Union into a state entity capable of managing technology independently from others. Such an ambitious objective goes beyond that of strengthening the EU's strategic autonomy[3]; indeed, the latter goal may be achieved without changing the legal nature of the EU, in contrast with the former one. It is therefore necessary to examine what are the legal foundations that are available to the EU institutions in order to advance the European integration process to such an extent. Should the EU be able to fully exploit its powers, a structural change in the nature of the EU may occur. Indeed, the EU is an organisation with attributed competences which is characterised by a unique level of integration amongst Member States. Yet, it is not a State. The current need to strengthen Europe's technological sovereignty does not result from a conscious decision by the Master of the Treaties to change the legal status of the organisation; rather, external circumstances/pressure make it necessary for the EU to act as a global actor to face competition and build a word-leading industry. It is possible that its level of integration will further deepen and the change of its status from an international organisation to something more akin to a State will consolidate. In other words, the call for a digital/technology

[1] The Council referred to the concept of "European technological sovereignty" in 2019. See Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, 3 December 2019, OJ [2019] C 414/7.

[2] European Commission President, Junker, had been talking about "the hour of European sovereignty" since 2018. See European Commission, "State of the Union 2018: The Hour of European Sovereignty" available at: https://ec.europa.eu/info/sites/default/files/soteu2018-speech_en_0.pdf (accessed 30 November 2021)). The current President of the European Commission has stressed the importance of investing in "Our European tech sovereignty" in her speech "2021 State of the Union address by President Von Der Leyen", available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 and in her political guidelines of 2019 she had stated that it was not too late to achieve technological sovereignty in some critical technology areas. See 'A Union That Strives For More: My Agenda for Europe (Political Guidelines for the Next European Commission 2019-2024)', 2019, available at: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf (Accessed: 30 November 2021).

[3] The EU sought to enhance its strategic autonomy in a number of policy areas in recent years, where being autonomous means on the one hand, achieving independence from others and on the other being able to react to unilateral measures taken from third countries. The objective of attaining "strategic autonomy" was defined for the first time by the Council Conclusions on Common Security and Defence Policy of 25-26 November 2013, doc. n. 15992/13, par 30. It refers to the EU's ability to be military capable of defending its member States, upon request and to intervene in third countries for the purpose of protecting peace and security and to assist its partners to strengthen their defence capacities. In this case, the EU seeks to reduce dependence on others (NATO) and be able to perform a role which is complementary to that of the military organization. In order to do so, the EU needs to develop its own defence industry, without seeking to achieve autarky in defence matters which is extremely difficult to achieve. See D. FIOTT, *Strategic autonomy: towards European sovereignty in defense?*, *EUISS Brief* no. 12, 2020, p. 7 ss. "Open strategic autonomy" was also invoked by the EU in relation to "critical raw materials" (tungsten, gallium and indium, silicon metal, platinum group metals) which are necessary for the production of many goods. The EU is dependent on the supply of these materials from third countries and advocates for undistorted access to these materials. See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability, COM(2020) 474 final.

sovereignty may turn into a catalyst for the European integration process.

We show how there is an assertive and aggressive dimension to digital sovereignty in its framing which raises many questions, particularly as to its concreteness and the realisability of its objectives.[4] At the same time, this concept is evoked to argue that the EU should be more competitive in the global market and fill in its technological gaps. There are also, however, not inconsiderable legal issues possibly arising from its application in light of its extensive scope. The article demonstrates the complexities of the span of the legal base of the terms when subjected to scrutiny from a legal perspective. We consider whether they have or may have inherent weaknesses considering that in many of the areas affected by the pursuit of the EU's sovereignty the EU Member States have exclusive competence or the Union has only complementary competences.

As a preliminary step, we will examine the reasons that justify the need to strengthen the European technological sovereignty to the detriment of that of Member States; secondly, we will explore definitions of digital/technological sovereignty and thirdly the legal foundations in the Treaty to achieve this ambitious objective are identified. Then, the way the EU competences were exercised in the practice so far will be scrutinised. In the various policy documents published by the Commission on technological sovereignty there is a limited attention to the EU competence to act so as to enhance technological sovereignty. Critical comments can be made on the legal bases underpinning the measures (or proposed EU measures) taken to strengthen European technological sovereignty. So far the legal instruments derive from supplementary, complementary competences and the internal market and here is a trend to stretch the use of art. 114 TFEU beyond the limits allowed by the principle of conferral. This is shown by three proposals for amendments of Directives concerning cybersecurity of network and information systems and other critical infrastructures. It may be questioned whether the legal bases used are sufficient to effectively pursue the objective of enhancing technological sovereignty. We thus argue that the EU frequently

[4] É. KELLY, *Decoding Europe's new fascination with "tech sovereignty"*, 2020. Available at: https://sciencebusiness.net/news/decoding-europes-new-fascination-tech-sovereignty (Accessed: 30 November 2021); E. AMIOT *et al*., *European Digital Sovereignty Syncing values and value*, 2020. Available at: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf (Accessed: 30 November 2021); F. G. BURWELL, AND K. PROPP, *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?*, 2020. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf (Accessed: 30 November 2021); J. POHLE, Digital sovereignty: A new key concept of digital policy in Germany and Europe 2020. Available at: https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf (Accessed: 30 November 2021); C. HOBBS (ed.), *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*. 2020 Available at: https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf (Accessed: 30 November 2021); F. GUEHAM, *Digital Sovereignty – Steps Towards a New System of Internet Governance*, C. LORRIAUX, AND M. SCOTT (Trans.), Paris: *The Fondation pour l'innovation politique*, 2017; M. MĂRCUȚ, *Crystalizing the EU Digital Policy: An Exploration into the Digital Single*, Cham, 2017.

appears to fall short of the required competences to complete its security vision. The consequences for the European integration process of the Union's exercise of the competences necessary to enhance European sovereignty in relation to technology management, are potentially far-reaching. In the concluding remarks, we argue that the adoption of the proposed sets of measures and of other pieces of EU law aimed at strengthening technological sovereignty may imply an advancement of the European integration progress, should Member States decide not to challenge them before the Court of Justice.

2. A taxonomy of "European technological sovereignty" and its rationale

An analysis of the documents mentioning the term "technological sovereignty" shows that the EU institutions use it as a synonym for the Union's ability to use technology in order to make the internal market work. Thus, one of the reasons for the need to strengthen European "technological sovereignty" is that digital technology is crucial to ensure the functioning of the common market. Under this respect, the meaning of "technological sovereignty" overlap with that of "digital sovereignty". Indeed, the delivery of many essential services to society and the conduct of economic activities, in the fields of energy, health and finance depend on digital technologies. The pandemic has made dependence on them even more evident. The digital services are a priority for the Digital Single Market strategy.

The technological or digital sovereignty of the EU is reduced by the dependence on non-European digital technologies; the EU feels increasingly threatened by this situation. A case in point is that of 5G telecommunications equipment; this is supplied by Chinese companies such as Huawei that are subject to penetrating state political control. 5G telecommunications equipment, which provides connectivity, is defined as "key enablers for the delivery of digital services" and thus for the functioning of the internal market. The EU has been lagging behind in the field of telecommunications technology. The EU's technological reliance on the provision of many services via 5G networks makes it vulnerable. The new generation of digital infrastructure is crucial to achieve the objective of a digital single market. The dependence on Chinese technology also has implications for the security of the Union, since it exposes the EU member States more than in the past to cyber attacks for the purpose of industrial espionage.

The EU institutions are acutely aware of the risks connected to technological dependence. The European Parliament is concerned by allegations that 5G equipment developed by Chinese companies may have embedded backdoors that would allow manufacturers and authorities to have unauthorised access to private and personal data and telecommunications

from the EU[5]. The Commission stresses that the dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious.[6] A concerted action is advocated to increase resilience to possible disruptions carried out through digital infrastructure dominated by third countries. The Council Conclusions of 3 December 2019 supported the findings of the coordinated risk assessment and stressed "the importance of a coordinated approach and effective implementation of the Recommendation in order to avoid fragmentation in the Single Market"[7]. To this effect, the Council called upon Member States, the Commission and ENISA, to "take all necessary measures within their competences to ensure the security and integrity of electronic communication networks, in particular 5G networks and to continue to consolidate a coordinated approach to address the security challenges related to 5G technologies"[8].

Along the lines of the Council, the European Commission has emphasised that:

> "European technological sovereignty starts with ensuring the integrity and resilience of data, network and communications infrastructure and requires creating the right conditions for Europe to develop and use its own key capabilities, thereby reducing dependence on other parts of the world for key technologies. Such capabilities will strengthen Europe's ability to define its own rules and values in the digital age. European technological sovereignty is not defined in relation to others, but by focusing on the needs of European citizens and the European social model. The EU will remain open to anyone who is willing to respect its rules and comply with its norms, no matter where they are".[9]

In the afore mentioned paragraph, the idea is conveyed that should the EU be capable of ensuring the integrity of its digital infrastructure and that this will boost its ability to define its own rules and values. Such an ability is one of the core functions of a sovereign entity. The Commission more than the Council seems to stress the political dimension of enhancing the European technological sovereignty.

Recently, the EU has experienced a shortage of chips since the production of semiconductors is concentrated in a few countries (Taiwan, South Korea and the United States). The Commission has proposed to increase the production of semiconductors in the EU by 2030 to avoid disruptions in the supply chain. As the Commission put it, "Reinforcing Europe's

[5] Resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP))', par. 2.
[6] Commission Recommendation (EU) 2019/534 of 26 March 2019- Cybersecurity of 5G networks', OJ [2019] L 88/42, p. 1, para. 3.
[7] Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, cit. para. 10.
[8] Ibidem, para. 26.
[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Shaping Europe's digital future', COM (2020) 67 final, p. 3.

leadership capacities in semiconductors is a precondition for its future competitiveness, and a matter of technological sovereignty and security[10]."

A further sector in which technological dependence is risky for the EU is space. Indeed, the delivery of digital services, on which many economic activities are based, is possible thanks to space services[11] and data from the Galileo, EGNOS and Copernicus programmes. The EU tried to develop independence from third countries early on in this area. The idea of European independence from American or Russian technology dates to the creation of the Copernicus programme. Galileo is the "first public infrastructure owned by the European institutions"[12] and operates independently of other existing systems; it thus contributes, among other things, to the strategic autonomy of the Union, particularly for environmental data that are essential for monitoring. The EGNOS (European Geostationary Navigation Overlay Service) programme uses and enhances the information transmitted by the signals from the satellite constellations of the American GPS and Russian GLONASS systems by means of three satellites in geostationary orbit and is linked to air navigation. It should be added that space data and technology have a dual use: they can be exploited for both civil and foreign policy purposes. Space is also crucial for defence purposes, as highlighted in the Card report[13].

Having mentioned international security leads us to the *second reason* why it is essential to strengthen the Union's technological sovereignty. Europe's technological sovereignty is invoked explicitly in debates concerning the security of the EU and its Member States for example to tackle cyber threats but also in the context of Action Plan on synergies between civil defence and space industries where it is stated that:

> [...] On the one hand, given that some essential services depend on digital technologies for their functioning, it is a matter of security to maintain their functioning. On the other hand, the Union may safeguard its security from internal or external threats only if it possesses the technology necessary to do so and is not dependent on third countries to perform this task. In this sense, technological sovereignty is the EU's ability to better address security threats (such as cyber-attacks to critical infrastructure), interferences in the domestic affairs of a Member State as well as acts of espionage[14].

[10] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions a chips act for Europe, COM (2022) 45, p. 22.

[11] European Parliament, Policy Department for External Relations, *The European space sector as an enabler of EU strategic autonomy*, 2020; J. WOUTERS AND R. HANSEN, *Strategic Autonomy in EU Space Policy: a Conceptual and Practical Exploration*, in C. AL-EKABI (ed.), *European Autonomy in Space*, Vienna, Springer, 2015, pp. 49-61; R. HANSEN, R. AND J. WOUters, *Towards a EU Industrial Policy for the Space Sector – Lessons from Galileo*, in T. HÖRBER AND P. STEPHENSON (ed.), *European Space Policy. European Integration and the Final Frontier*, London, 2015, pp. 224-238.

[12] Communication from the Commission to the European Parliament and the Council - Taking stock of the GALILEO programme, COM (2006) 272 final.

[13] EDA/EEAS, https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf, p. 7.

[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan on synergies between civil, defence and space industries, COM (2021) 70 final.

The *third reason* which is invoked to enhance technological sovereignty is well explained by the Communication on a European Industrial Strategy for 2020[15]. In this context the European Commission emphasises the need to strengthen the EU's industrial capacity in critical digital infrastructures in order to reduce technological dependence on third countries. Indeed, the EU can only protect itself from interference from third countries if it enhances its competitiveness with regard to the production of its own digital technologies. There is a link between "strategic autonomy" and "technological sovereignty"; this was made arguably most explicitly with respect to the first and third aims in the Communication on the EU industrial strategy[16] and in an Action Plan on synergies between civil, defence and space industries[17] where it is stated: "Europe's strategic autonomy is about reducing dependence on others for things we need the most: critical materials and technologies, food, infrastructure, security and other strategic areas." The EU was concerned about its dependence on foreign technology, including digital technology and is set to reducing this dependence to increase its security. It stated there: "Transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on network and information systems that are increasingly interconnected. […] Digital services and the finance sector are among the most frequent targets of cyberattacks, along with the public sector and manufacturing"[18].

The Parliament also recently underlined that "for the Union's sovereignty and strategic autonomy, an autonomous and competitive industrial base and a massive effort in research and innovation are needed to develop leadership in key enabling technologies and innovative solutions and to ensure global competitiveness"[19]. The mentioned institution emphasises that the industrial strategy should include an action plan to strengthen, shorten, make more sustainable and diversify the supply chains of European industry, in order to reduce over-dependence on a few markets and increase their resilience; a smart return strategy should also be envisaged in order to resettle companies in Europe, as well as to increase production and investment and shift industrial production to sectors of strategic importance for the Union[20]. At the same time, the Parliament calls on the Commission to "establish clear, explicit and concrete definitions of "strategic", "autonomy", "strategic autonomy", "resilience", "strategic resilience" and other related concepts, so as to ensure that actions taken with regard to these concepts are specific and targeted to EU priorities and objectives".[21]

A further advantage that is associated to the strengthening of the industrial capacity is that the

[15] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A New Industrial Strategy for Europe', COM (2020) 102.
[16] Ibidem, p. 13.
[17] COM (2021) 70, cit, pp. 7-8.
[18] European Commission/HR, Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final, pp. 1 and 3.
[19] European Parliament resolution of 25 November 2020 on a New Industrial Strategy for Europe, P9_TA(2020)0321, point O.
[20] Ibidem.
[21] European Parliament resolution of 25 November 2020, cit., pt. 13.

EU would become a digital leader in the global market and be able to compete with China and the US in the production of critical technology. The latter are relevant across the defence, space and related civil industries and contribute to Europe's technological sovereignty by reducing risks of overdependence on others for things we need the most. Identifying which critical technologies make a decisive contribution to key capabilities can help to decide: (i) which technologies are important for technological sovereignty (i.e. where there is a need to reduce the risk of dependence); (ii) where combined/coordinated support from different EU programmes and instruments can address such challenges. To strengthen its technological sovereignty, the EU must maintain a strong industrial competence and, where possible, seek leadership in these critical technologies. Alongside the critical technologies, the EU must also look at the value chains, including the security of supply of critical (raw) materials that are important building blocks of civil, defence and space critical technologies. And related research and testing infrastructure, which is key for standardisation and certification[22]. In many crucial areas of the economy, the EU has a low level of competitiveness. Therefore, the Commission evokes Europe's technological sovereignty with a market related meaning[23].
Indeed, it has been stated: "[W]e will need a stronger industrial and technological presence in strategic parts of the digital supply chain. Just as it became clear how important connectivity and digital technologies are, we are also reminded of the importance of security of technology. This reaffirms the need for Europe to have tech sovereignty where it matters, as well as keeping open trade and the flow of innovation going[24]." Should the EU achieve a position of world leader in this area, it would also become capable of setting global standards[25]. In its turn, this would strengthen the EU's strategic autonomy from third countries. In this case, the enhancement of technological sovereignty is invoked as a necessary process for the EU to dominate the global market thanks to the technological leadership of European companies in some key sectors of the economy.

3. Defining Digital/technological sovereignty

Technological sovereignty is used at times as a synonym for digital sovereignty by the Parliament's research service[26] and also by the Commission[27]. In other cases, digital sovereignty is considered "*a conditio sine qua non"*, that is to say, a precondition for

[22] COM (2021) 70, cit., p. 8.
[23] European Commission, (2020) 102, cit., p. 1.
[24] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Europe's moment: Repair and Prepare for the Next Generation', COM (2020) 456 final, p. 8
[25] COM (2020) 102, cit, p. 3.
[26] European Parliamentary Research Service, 2020, p. 1.
[27] European Commission, *Europe: The Keys To Sovereignty*, 11 September. Available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en (Accessed: 30 November 2021)

"technological sovereignty" to develop[28]. Yet, there are no clear borders between the concepts of digital and technological sovereignty. The authors support the view that the two concepts have different perimeters: the latter refers to the EU's ability to assert itself as leading actor in the market as far as technology is concerned. This technology may be digital and concern information and communications technologies (ICTs) or non digital (new clean technology): in the former case the concept of technology sovereignty is related to the enhancement of the security for the EU while it is not in the latter one.

In sum, there are increasingly a wide number of invocations of technological sovereignty in EU policy often with multiple aims: the first is to enable the provision of a number of essential services in a modern economy, the second is to enhance the EU's competitiveness in the global economic order and the third is to increase resilience to attacks and interferences in domestic affairs and enhance security. This multiple-purposed formulation appears increasingly and it raises many interesting questions from a legal perspective.

Digital sovereignty is described as "the ability of the EU to act independently in the digital world".[29] The concept of "digital sovereignty" has emerged since 2016 and has a particularly diverse range of meanings. From highest executive level of the EU, digital sovereignty forms a vast panoply of concepts and has a composite meaning, apparently broad enough to capture a vast legislative agenda. According to Charles Michel, President of the European Council, it relates to a vast range of policies including artificial intelligence, Internet of Things (IoT), the General Data Protection Regulation (GDPR)[30], the proposed Digital Services Act (DSA)[31] and the Digital Markets Act (DMA)[32], Competition policy, tax, EU-US tech agenda and 5G[33]. As will be outlined, this particular portfolio of topics spans a dizzying array of legal bases from the internal market and competition policy to external relations and trade policy to actorness at the international multilateral fora. According to former European Commissioner for Information Society and Media Viviane Reding technological sovereignty is crucial to the future of the EU, and immediate action is needed in order to secure digital sovereignty of the future generations[34]. According to the European Commissioner Breton, digital sovereignty is key to

[28] COM (2020) 67, cit, p. 2.
[29] T. MADIEGA, *Digital Sovereignty for Europe,* PE 651.992, European Parliamentary Research Service, 2020.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), OJ [2016] L119/1.
[31] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.
[32] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM (2020) 842 final.
[33] Digital sovereignty is central to European strategic autonomy - Speech by President Charles Michel at "Masters of digital 2021" online event, available at: https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/ (Accessed: 30 November 2021).
[34] V. REDING, *Digital Sovereignty: Europe at a Crossroads*. Available at: https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf (Accessed: 30 November 2021).

the future of EU[35]. It is difficult to see a common vision of digital sovereignty largely on account of its umbrella like terms. Its ambitions and reach are arguably its defining features rather than its practicality or utility. The notion of "digital sovereignty" appears mostly used by the EU to argue that becoming resilient to crises, increasing technological independence from others and achieving a leadership's role in the market are necessary steps to establish a "level playing field" and to protect EU's standards in the world[36].

Reding explains that sovereignty contains the EU's capacity of determining own actions and norms, but also using this sovereignty to shape the world, setting "gold standards of the digital age".[37] Moreover, according to Competition Commissioner Margrethe Vestager the EU's competences need enhancement in order to be fit for the task.[38] The Internal Market Commissioner Thierry Breton framed digital sovereignty in September 2020 -and thus during the last US administration as a form of "war": "Faced with the 'technological war' being waged by the United States and China, Europe must now lay the foundations of its sovereignty for the next 20 years", stating that "[o]ur digital sovereignty rests on 3 inseparable pillars: computing power, control over our data and secure connectivity".[39]

It is commonly understood that the notion of digital sovereignty has emerged as a means of promoting European leadership and strategic autonomy in the digital field[40]. Some define digital sovereignty as Europe's ability to act independently in the digital world, in terms of protective mechanism and offensive tools to foster digital innovation including in cooperation with non-EU companies[41]. Digital policy is one of the key policy priorities of the Von der Leyen Commission, pledging that Europe must achieve technological sovereignty in critical areas[42]. The wording thereof continues to evolve but remains also a constant of the highest level of EU policy-making in contemporary times.

4. The available legal bases to enhance technological sovereignty

It is necessary to verify what legal bases in the Treaty support the EU's competence to enhance the "European technological sovereignty". There are scholars who have questioned whether the EU is fully equipped to achieve such an objective in the area of cyber security[43].

[35] European Commission, *Europe: The Keys To Sovereignty*, cit; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - 2030 Digital Compass: the European way for the Digital Decade', COM (2021) 118 final.
[36] *Digital sovereignty is central to European strategic autonomy* - Speech by President Charles Michel, cit
[37] REDING, *Digital Sovereignty: Europe at a Crossroads*, cit.
[38] M. Vestager, *Assessing the EU's Capacity to Act*, Speech at European Union in International Affairs (EUIA) Conference, Brussels, 26-28 May 2021 (notes on file with the authors).
[39] European Commission, *Europe: The Keys To Sovereignty*, cit.
[40] T. MADIEGA, *Digital Sovereignty for Europe*, cit.
[41] T. MADIEGA, *Digital Sovereignty for Europe*, cit; European Political Strategy Centre, *Rethinking Strategic Autonomy in the Digital Age*, EPSC Strategic Notes Issue 30, 21.11.2019. Available at: https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en (Accessed: 30 November 2021).
[42] U. VON DER LEYEN, *A Union That Strives For More*, cit.
[43] R. WESSEL, *Towards EU Cybersecurity Law: Regulating a New Policy Field*, in N. TSAGOURIAS AND R. BUCHAN (ed.), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015, p. 403, p. 491.

The first and most commonly used in this domain and the most important legal foundation to harmonise national rules governing the provision of the digital services is represented by art. 114 TFEU. The latter allows the adoption of measures relating to the approximation of the laws, regulations and administrative provisions of the Member States which have as their object the establishment and functioning of the internal market. As De Witte states, Article 114 "is the most powerful tool for the expansion of the EU legislative activity".[44] But the need to decrease technological dependence on foreign countries requires an action in areas in which the Union has supporting, coordination or complementary competences. However, exclusive national competences in the field of national security, i.e. art. 4(2) TEU, are also touched upon by EU measures. For example, in order to intervene on the technological dependence of 5G devices, the EU must exercise its competences in a matter of shared competence (trans-European networks) but given the reflections of 5G on the broader security of the EU, Member States' competences are also affected.

The EU sets out ambitious goals in its Communication on a European industrial policy; yet, the EU has a coordinating and supporting competence (art. 6 b) in the field of industry. In order to be able to compete on a global level as well as the protect itself from external security threats, the EU may need to exercise its powers in areas of shared (i.e. internal market, trans-European network) and "*sui generis*" shared competences (technological development and space). With regard to the latter, the exercise of EU competences does not prevent Member States from exercising theirs (Art. 4(3) TFEU); moreover, EU measures in this area do not have the effect of harmonising national laws and regulations. Space technology and services are crucial both for civilian and defensive objectives. The EU has limited competences in the area of space and even after the organisation exercises those competences, this shall not result in Member States being prevented from exercising theirs (art. 4(3) TFEU). As it was argued by some scholars, art. 189 TFEU seems to be a provision "that protects the status quo of European space governance by expressly endorsing the member states' cooperation through European Space Agency".[45] The Commission has recently emphasised that: "Although some space capabilities have to remain under exclusive national and/or military control, in a number of areas synergies between civilian and defence can reduce costs, increase resilience and improve efficiency. The EU needs to better exploit these synergies"[46]. Therefore, there seems to be an interest in cooperating at EU more than at intergovernamental level.

[44] B. DE WITTE, *Exclusive Member State Competences-Is There Such a Thing?*, in I. GOVAERE AND S. GARBEN (ed.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford, Hart Publishing, p. 69 ff.
[45] F. MAZURELLE, J. WOUTERS, W. THIEBAUT, *The evolution of European space governance: policy, legal and institutional implications* in *International Organizations Law Review*, 2009, p. 27.
[46] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Space Strategy for Europe, COM (2016) 705 final, p. 10.

Exercising competence in fields of national competence may also be necessary in order to achieve the objective of a digital/technological sovereignty. Greater EU integration in fields affecting national security could also advance the European integration process and strengthen the powers of the EU with respect to those of the Member States. This is somewhat paradoxical since Member States are jealous of their prerogatives in the field of AFSJ/CFSP but at the same time it is so crucial to rely on critical infrastructures both for civil and defensive purposes that Member States may prefer to give up their sovereignty in areas of exclusive national competence instead of being dependent on third countries.

These brief considerations highlight how, on the basis of the Treaty, there are certain limits, linked to the operation of the principle of attribution powers, which the EU faces when it adopts measures aimed at strengthening European technological sovereignty. In this context, the question arises as to what legal instruments have been used to date to implement the objective of strengthening European technological sovereignty. It is necessary to examine how the problem of EU's limited competences has been addressed in the practice so far.

5. Legal instruments: on powers and competences

We move then in this paper to the specifics of implementing this taxonomy that we have attempted to present in outline form. It is certainly possible to identify a series of EU measures that aim, on the one hand, to prevent a further weakening of European technological sovereignty and on the other to react to the situation of technological dependence on third countries. As to the former, the most important one is the framework for controlling foreign direct investment[47], which has its legal basis in the common commercial policy, an area of exclusive competence. The concerned act is a screening instrument enabling Member States to assess whether foreign direct investment in their territories affect public order and security by taking into account their effects on critical infrastructure and technology. The Commission is involved in the monitoring of the foreign investment and where it considers that the investment in question is likely to affect the public order or security of more than one Member State, it may issue an opinion which the Member State concerned by the investment will take into due consideration when taking their final decision. Yet, this instrument does not reinforce European technological sovereignty; at most it can limit a further worsening of the technological dependence on third parties, but it is not likely to remedy it.

Let us now turn to the latter, that is to say, measures having a reactive character. They are the most interesting ones since they are problematic as far as the appropriateness of the legal basis is concerned. In the next sub-section, measures affecting areas where the EU has so to speak "weak" competences under the Treaty will be identified. In the following sub-section,

[47] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ [2019] L79I/1.

some measures based on Article 114 TFEU will be discussed.

5.1 Reinforcing technological sovereignty by relying on supporting, coordination and complementary competences and sui generis shared competences

Measures to strengthen technological sovereignty may also include the establishment of the European Centre of Competence for Cyber Security in Industry, Technology and Research ("Competence Centre") and the network of national coordination centres ("network")[48], as well as the European Institute of Innovation and Technology[49]. In these cases, the legal bases used are Articles 173(3) and 188(1) TFEU. The mission of the Centre and the Network is to develop the Union's technological, industrial and research capabilities in cybersecurity and to increase the competitiveness of the Union's cybersecurity industry.

The Commission has also proposed the adoption of a Regulation, based on Articles 185 and 187, setting up joint undertakings, including the Smart Networks and Services Joint Undertaking. This partnership will support technology sovereignty for smart grids and services in line with the new Industrial Strategy for Europe and the 5G cyber security toolkit. It aims to help solve societal challenges and enable the digital and green transition. In relation to the COVID-19 crisis, it will support technologies that respond to both the health crisis and economic recovery. This partnership will enable European operators to develop technological capabilities for 6G systems as a basis for future digital services towards 2030.

The establishment and management of the EU space programme is a further noteworthy legislative development in the context of this overview. Indeed, space technology is central not only for the functioning of the internal market but also for other essential services of modern economies as well as the EU internal and external security, which in principle falls within Member States' exclusive competence.

The mentioned programme has been established together with the European Union Space Programme Agency ("Agency") in 2021[50]. The Commission is responsible for the programme, without prejudice to the prerogatives of Member States in the field of national security. One of the objectives of the Programme shall be "to provide or contribute to the provision of up-to-date, high-quality and, where appropriate, secure space services, information and data, seamlessly and where possible on a global basis, meeting current and future needs and supporting the Union's political priorities and related independent and evidence-based

[48] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, OJ [2021], L 202/1.

[49] Regulation (EU) 2021/819, Regulation (EU) 2021/819 of the European Parliament and of the Council of 20 May 2021 on the European Institute of Innovation and Technology (recast), OJ [2021], L 189/61.

[50] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, OJ [2021], L 170/69.

decision-making, inter alia, in relation to climate change, transport and security issues". Other objectives are: (b) to strengthen the intrinsic and extrinsic security of the Union and its Member States and to enhance the Union's autonomy, in particular in terms of technology. Finally, it is announced that the measure intends to promote the role of the Union as a global player in space[51].

It should be emphasised that through a CFSP decision the Council has established its responsibilities and those of the High Representative for the prevention of threats arising from the deployment, operation and use of space systems and services, or in the event of a threat to such systems or services. It is even provided that, in an emergency, the High Representative may issue the necessary provisional instructions to the Agency or to the relevant structure designated for security monitoring[52]. As a result, it can be said that the Union is assuming increasing functions/tasks as far as the management of the space security is concerned.

The piece next moves to considering the place of the internal market in recent technological sovereignty measures.

5.2 Strengthening technological sovereignty through art. 114 TFEU: what are the limits?

Chief amongst the measures aimed at directly or indirectly strengthening European technological sovereignty are those based on Article 114 TFEU. This provision enables the EU to adopt measures for the approximation of domestic legislation with the object of the establishment and functioning of the internal market. Therefore, the mentioned Treaty basis is a key legal tool to reinforce the EU's technological sovereignty. For example, the proposed EU Chip Act is rooted, amongst others, on the internal market harmonization provision of TFEU since, as the Commission convincingly argues, it aims at creating a harmonised legal framework for increasing the Union's resilience and security of supply in the area of semiconductors.[53] At the same, the proposed act is also based on other multiple legal bases[54] related to EU's complementary competences. Indeed, the EU measure aims at supporting actions taken by Member States to foster innovation and adjustment of the industry of semiconductors to structural changes and to accelerate the production of these products. All this is intended to reinforce sovereignty in the semiconductor supply chain[55].

While there is a clear basis for the Union to use art. 114 TFEU and the other mentioned Treaty provisions for the EU chip Act, this is not the case for other Commission's proposals. As is well known, the choice of legal basis is based "on objective elements, such as to be capable

[51] Art. 1 a, c and d.
[52] Art. 4 c. 1.
[53] Proposal for a Regulation of the European parliament and of the council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), COM (2022) 46, p. 9-10.
[54] These are 173(3), industry, 182(1) and 183 (research).
[55] COM (2022) 46, cit., p. 9.

of being the subject of judicial review, including, in particular, the purpose and content of the act"[56]. Given the close links between the smooth functioning of the internal market of digital services and the security of communication networks, there is a trend to stretch the use of art. 114 TFEU beyond the limits allowed by the principle of conferral:[57] the EU institutions make wide use of internal market provision of the TFEU to act in areas that affect Member State's security. This will likely lead to what we term the "marketisation of the EU's security" which may imply a loss of Member States' powers/competence in the field of security.

A legal instrument can pursue twofold objectives – a leading objective and another - "a decisive factor in the choices to be made" i.e. the second objective could be related to another field[58]. However, there is a vast jurisprudence and matching literature on the use of this provision, which mostly has been deferential to the EU legislator[59]. Most of the key caselaw has largely related to the dual usage or boundaries between the internal market, a strong EU competence, and lesser competences of the EU as to heath, environment or labour. Security is a national competence and not an EU competence, pursuant to Article 4(2) TEU. There is a wealth of jurisprudence where the Court has been asked to adjudicate upon systems and bodies being established in frameworks developed pursuant to Article 114 TFEU. Data protection rights most likely triumph security. The Court of Justice in *Digital Rights Ireland*[60] annulled the Data Retention Directive,[61] striking down the Directive for its indiscriminate surveillance reach despite its legal basis in Article 114 TFEU. However, there is little by way of precise caselaw on the use of Article 114 TFEU for security measures. There, in *Digital Rights Ireland*, the place of the internal market was raised by a referring Court in one of two sets of proceedings merged where ultimately the CJEU struck down the Data Retention Directive in Digital Rights Ireland on fundamental rights grounds as to the Charter.

There is an urgent need to clarify whether the EU institutions can continue to use Article 114 TFEU or not; this is to avoid possible actions for annulment brought by Member States against future acts that the EU might want to adopt to reinforce its technological sovereignty. At the moment, there are at least two Commission proposals that are based on Article 114 TFEU, outlined next. It is therefore appropriate to question the limits of this provision with respect to EU actions that are intended, albeit indirectly, to strengthen technological sovereignty.

Among the technological sovereignty measures based on Article 114 TFEU the following ones

[56] Case C-376/98, *Germany v. Council*, ECLI:EU:C:2000:544.
[57] For a study on this issue see S. WEATHERILL, *The competence to harmonise and its limits* in P. KOUTRAKOS AND J. SNELL, *Research Handbook on the Law of the EU's Internal Market*, Chelthenam/Northampton, 2017, p. 82 ff.
[58] Case C-58/08, *Vodafone Ltd and Others v. Secretary of State for Business, Enterprise and Regulatory Reform*' (2010) ECLI:EU:C:2010:321, para. 36.
[59] B. DE WITTE, *Exclusive Member State Competences-Is There Such a Thing?*, cit.,
[60] Case C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238
[61] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ [2006] L 105/54.

can be listed, derived from the most comprehensive sampling of legal measures on technological sovereignty, as set out by the European Parliament Research Service, numbering 24 possible initiatives[62]. We select four of the most topical and salient Regulations or Directives, including proposals of amendment of three Directives, concerning cybersecurity of network and information systems and other critical infrastructures *beyond* this sampling also using Article 114 TFEU. These measures show that their predominant objective is to enhance the EU security.

a) Among the measures based on this provision is *the Regulation establishing the European Union Agency for Cyber Security (ENISA)*[63], which also regulates cybersecurity certification for information and communication technologies. Even though the Court of Justice has justified the use of the mentioned provision as a legal basis for other agencies such as the European Securities and Markets Authority (ESMA)[64], ENISA's activity seems to focus on enhancing cybersecurity and the effective implementation of Directive (EU) 2016/1148[65] and other relevant legal instruments with cybersecurity aspects. The agency's mandate is primarily to achieve a high common level of cybersecurity throughout the Union[66]. ENISA serves as a point of reference for advice and expertise in this field for Union institutions, bodies, offices and agencies, as well as other relevant Union stakeholders. The last paragraph of Article 1(1) of the above-mentioned Regulation states: "By carrying out the tasks assigned to it under this Regulation, ENISA shall contribute to reducing fragmentation in the internal market." This implies that the Agency contributes only in an ancillary manner to the achievement of the objectives of Article 114 TFEU.

b) We have mentioned that ENISA has to ensure the effective implementation of the Directive (EU) 2016/1148 of 6 July 2016, known as the "NIS Directive." The latter is also based on Article 114 TFEU. The objective of this act is to achieve a "high level of network and information system security within the national context, contributing to an increased common level of security within the European Union." This is to improve the functioning of the internal market as networks and information systems allow operators of essential services or providers of digital services to carry out their activities in secure conditions and play an essential role in facilitating the cross-border movement of goods, services and persons and thus in ensuring the functioning of the internal market. The directive is aimed at strengthening the cyber resilience of networks and information systems that are exposed to cyber incidents and crises;

[62] T. MADIEGA, *Digital Sovereignty for Europe*, cit., pp. 9-10.
[63] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ 2019, L 151/15.
[64] Case C-270/12, *United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council*, ECLI:EU:C:2013:562.
[65] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ [2016], L 194/1.
[66] Art. 1 c. 1.

therefore, the centre of gravity of this measure does not seem to be the internal market but the desire to harmonise, albeit minimally, the security rules that network and information system operators must comply with at national level. The sectors affected by the directive are: energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution and digital infrastructure and three digital services (online marketplaces, online search engines and cloud computing services). However, the 2016 Directive was not challenged on legal grounds.

The first proposal for a Directive on the resilience of critical entities is set to revise the NIS Directive[67]*.* The aim of the proposed act is to extend the number of sectors covered by the 2016 Directive as in the assessment of the Commission there would currently be more digitised sectors providing key services to the economy than in 2016. Furthermore, it is underlined that the Directive in its original version granted Member States a wide discretion in setting security and incident reporting requirements for operators of essential services; however, this has resulted in a great inconsistency of rules at national level and has caused additional costs and has created difficulties for companies offering cross-border goods or services. The Commission considers the choice of Article 114 TFEU to be compatible with the position taken by the Court of Justice in this regard in its judgment of 8 June 2010, Case C-58/08, *Vodafone*[68]*.* It held that recourse to Article 114 TFEU is justified in the event of divergences between national rules where these directly affect the functioning of the internal market[69]. According to the Commission, "The proposed legal act would facilitate and improve the establishment and functioning of the internal market for essential and important actors in the following ways: by establishing clear and generally applicable rules relating to the scope of the NIS Directive and by harmonising the applicable rules in the area of cybersecurity risk management and incident reporting"[70]. Again, the Commission underlines that regulatory fragmentation at national level in this area constitute obstacles to the internal market. However, the main objective pursued by the proposal appears to be the enhancement of cybersecurity in the Member States, which are required to set up national cyber crisis management frameworks. The question arises, however, whether this is sufficient to use Article 114 TFEU as the sole legal basis for the measure. In the judgment under review, the question was whether the cited provision could be used as a legal basis for a regulation on roaming services. On the contrary, in this case the proposal for a directive seems more aimed at strengthening the cyber security crisis management framework under ENISA than at improving the functioning of the internal market by eliminating regulatory disparities that

[67] European Commission, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM (2020) 829.
[68] European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823, p. 3.
[69] C-58/08, cit, para. 32.
[70] European Commission, COM (2020) 823, cit, p. 3.

directly affect this process. Certainly, the Court of Justice has favoured the wide use of this provision, going so far as to allow it to be used for measures aimed at preventing the emergence of obstacles to the functioning of the internal market, stating that the institutions may use "the most appropriate harmonisation technique where the approximation envisaged necessitates highly technical and specialised analyses and the taking into account of developments in a particular sector",[71] and also to create bodies, such as the European Securities and Markets Authority (ESMA), which acts in the face of serious threats to the orderly functioning and integrity of financial markets or the stability of the financial system in the Union and which, in certain well-defined circumstances, may adopt measures applicable throughout the Union, which may possibly take the form of decisions addressed to private operators[72]. However, the new Directive seems to aim at increasing the level of harmonisation as regards the security conditions under which companies operate. Without prejudice to the possibility for Member States to take the necessary measures to ensure the protection of their essential safety interests, it is clear that the proposal aims to extend the scope of European rules in areas that fall within national competence.

The second proposal put forward by the Commission is *to amend Directive 2008/114 laying down a procedure for the designation of European critical energy and transport infrastructures* ("European Critical Infrastructure" or "ECI")[73] whose disruption would have cross-border effects. The 2008 directive aims to protect those infrastructures that enable the provision of essential services or functions for society or economic activities. The 2020 proposal is based on Article 114 TFEU instead of Article 352 TFEU, which was the legal basis of the original Directive that applied to energy and transport infrastructures only. It was a first step to identify and designate ECIs whose disruption caused by attacks had significant cross-border impacts (on at least two Member States). At a later stage, the need to improve and extend the protection to other sectors, inter alia, the information and communication technology ("ICT") sector was to be explored. The objective of the Directive was to increase the critical infrastructure protection capability in Europe which could be the object of man-made and technological threats such as terrorist and cyber attacks and also natural disasters. The EU institutions recognised that "the primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures." However, the Directive defined a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. About 94 ECI located mostly in Central and Central Eastern Europe were identified as a result of the application of the Directive.

[71] Case C-270/12, cit, para. 103.
[72] Case C-270/12, cit, para. 108.
[73] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM (2020) 829.

In December 2020, the Commission put forward an amendment to the ECI Directive, which is complementary to the proposal to replace Directive 2016/1148 (the so called "NIS2" Directive)[74]. The proposed new rules are aimed at increasing resilience of "critical entities". The scope of the Directive is not limited to energy and transport, but it extends to banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space. The proposed rules seek to "enhance the resilience of entities in the Member States which are critical for the provision of services which are essential for the maintenance of vital societal functions or economic activities in the internal market in a number of sectors underpinning the functioning of many other sectors of the economy of the Union"[75]. The idea behind the Commission's proposal is that considering the increased interdependency between services provided using critical infrastructure in the sectors mentioned above, a disruption in one Member State may have implications in other Member States or the whole EU. The divergence of regulations at national level is a factor that obstructs the functioning of the internal market and makes the Union more vulnerable in terms of security. Harmonising the security requirements which should be respected by critical entities providing essential services is necessary. The proposed directive sets up a procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment and sets out obligations on Member States. It is interesting that the legal basis of this piece is now art. 114 TFEU as if the new rules were needed to improve the functioning of the internal market. The change in legal basis from art. 352 of the TFEU to art. 114 TFEU is justified with the "need to establish a more level playing field for critical entities"[76]. It is doubtful that the mention provision supports the new measure. The proposal aims to strengthen the resilience of critical actors (entities operating critical infrastructure) to incidents. Given the divergence of national legislation governing the security requirements of these infrastructures, harmonised minimum standards should be established to ensure the provision of essential services in the internal market and to increase the resilience of critical actors. Here again, the use of Article 114 TFEU seems to exceed the limits allowed by the case law of the Court of Justice, since it is not actually and objectively apparent from the legal act that its purpose is to improve the conditions of the establishment and functioning of the internal market[77].

There is an urgent need to clarify whether the EU institutions can continue to use this legal basis or not; this is to avoid possible actions for annulment brought by Member States against future acts that the EU might want to adopt to reinforce its technological sovereignty. At the moment, there are at least two Commission proposals that are based on Article 114, and it is

[74] COM (2020) 823 final.
[75] Ibidem, p. 4.
[76] Ibidem, p. 4.
[77] Case C-270/12, *UK v. Parliament/Council*, ECLI:EU:C:2014:18, par. 113 and case C-66/04, *UK v. Parliament and Council*, ECLI:EU:C:2005:743, par. 44.

therefore appropriate to question the limits of this provision with respect to EU actions that are intended, albeit indirectly, to strengthen technological sovereignty. Legal scholars argue that certain decisions that could be adopted to reduce technological dependence on third countries would be incompatible with the internal market harmonization legal basis[78]. For example, according to one author, the exclusion of "'*high risks' technology suppliers*", such as 5G equipment suppliers or the reduction of the non-European presence of 5G infrastructure, cannot be approved on the basis of an act rooted in this legal basis[79]. It was no coincidence that in 2019 the European Commission had recognised in its recommendation on cybersecurity that the competence to exclude certain suppliers from their markets on national security grounds lay with the Member States[80].

6. Conclusions

It is necessary to draw some conclusions on the measures adopted (or proposed) with the explicit and implicit aim of strengthening European technological sovereignty. It seems that the EU has used all the competences at its disposal to increase the cyber security of essential digital services, to have its own digital technologies and to protect Member States' critical infrastructures. The trend of making an extensive use of Article 114 TFEU is justified if this is to strengthen the production of chips in the EU; however, this practice is criticisable in order to increase the security of network and information services since the concerned legal basis is stretched to cover security-related measures. At the moment, there seems to be a broad convergence between the Commission, the Council and the Parliament on enhancing the European technological sovereignty. As to the Member States, two scenarios can be envisaged. On the one hand, should they continue not to challenge security-related measures proposed by the Commission on the basis of art. 114 TFEU, we could say that an erosion of state sovereignty (and conversely a strengthening of European technological sovereignty) is occurring. This will advance the European integration process. On the other hand, there may be countries interested in seeking the annulment of the future measures designed to enhance the European technological sovereignty. The UK has been one of the countries that in the past has unsuccessfully challenged measures based on art. 114 TFEU.[81] However, there may be other countries (i.e. Hungary and Poland) who could put at risk the rules that the Union will adopt in the coming years to achieve the mentioned objective. We will see which of the two scenarios comes true.

[78] M. VARJU, *5G networks, (cyber)security harmonisation and the internal market: the limits of Article 114 TFEU*, in *European Law Review*, 2020, pp. 471-486, p. 485.
[79] Ibidem.
[80] Commission Recommendation 2019/544, cit, recital n. 26.
[81] Case C-270/12, cit and C-66/04, cit.

The City Law School
City, University of London
Northampton Square
London EC1V 0HB

T:+44(0)20 7040 3309
E: law@city.ac.uk

Email enquiries:
law@city.ac.uk

Telephone enquiries
+44 (0) 2 7040 5787

Find out more, visit
www.city.ac.uk/law

www.city.ac.uk/law