Digital Sovereignty and Platform Governance: A European Constitutional Laboratory

Giovanni De Gregorio

1. Introduction

Digital sovereignty has become a catch-all expression. It has extended far beyond territorial boundaries, or, more precisely, from the traditional notion of state sovereignty as the exercise of power over a certain territory while respecting sovereign powers from an external perspective (Grimm 2015). Digital sovereignty has acquired further nuances (Bratton 2016; Couture & Toupin 2019), even referring to individual autonomy in the information society (Posch 2006). However, the traditional notion of state sovereignty has not lost its relevance in the digital age. Rather, it has amplified its scope (Pohle & Thiel 2020; Mueller 2020; Gueham 2017).

This extension does not just lead to focusing on the enforcement of power on a certain territory as already shown by the Yahoo v. Licra case,[1] or limiting external interferences from other governments imposing technological standards on a global scale. The question is also about how to deal with the exercise of private powers influencing the traditional way the sovereign authority has been conceived since the rise of the Westphalian state. Sassen (1998) predicted this trend already at the end of the last century looking at the role of private actors strengthening their power and consolidating transnational regimes which would have been influenced the logic of state sovereignty. Likewise, Castells (2008) pictured this evolution underlining how the tension between the logic of state sovereignty based on territorial boundaries and the new functions which sovereignty is called to address in the information society.

While states are extending their powers on the digital environment through narratives of digital nationalism and sovereignty (Haggart, Tusikov & Scholte, 2021; Schneider 2020), even relying on network shutdowns (De Gregorio & Stremlau 2020), private powers are consolidating their role in the digital environment (Pasquale 2016; Moore & Tambini 2018; Zuboff 2019), shaping Internet governance (DeNardis & Hackl, 2015; Radu 2019). Kettemann (2020) has underlined that the normative order of the internet is "a complex of norms, values and practices that relate to the use and development of the Internet, and with which the activities of, and relationships among, states, private companies and civil society, with regard to the use and development of the Internet are legitimated".

In this case, the reference leads to looking at online platforms and their role double face role of competitors and collaborators of traditional sovereign authorities. As Daskal observed (2018), private parties mediate transnational internet governance by managing data and the flow of information. Online platforms do not only provide services which are increasingly fundamental as digital infrastructures but also contribute to defining a new geographical

[1] Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme (LICRA), 433 F.3d 1199 (9th Cir. 2006).

grammar (Grumbach 2017). This infrastructural role has been underlined during the pandemic showing the role of platforms in providing essential services to work, speak and build social relationships.

Within this framework, the Union has provided a new strategy to react against the exercise of platform power, particularly extending the scope of application of its digital policies on a global scale. Platform capitalism is not just about economic power but also the exercise of control over the flow of online information (Pasquale 2016; Srnicek 2016), raising questions for constitutional democracies about how to deal with the exercise of transnational private powers (Hindman 2018; Zuboff 2019; van Dijck et al. 2018). This situation has triggered the emergence of a new phase defined as European digital constitutionalism (De Gregorio 2021). The consolidation of online platforms as private powers has led these actors escaping not only traditional democratic circuits but also challenges the constitutional limits to regulate transnational activities.

This work aims to study the relationship between digital sovereignty and platform governance with a specific focus on the Union which is increasingly proposing a third way of digital sovereignty driven by democratic constitutional values. By looking at the policies advanced to define digital sovereignty, this research contributes to defining how far platform governance influences European digital sovereignty and how constitutional values limits the exercise of sovereign powers in the digital age. The first part of this research underlines the relationship between digital sovereignty and platform governance. The second part underlines how the translation of digital sovereignty in the extension of European digital policies is the result of the need to ensure the effective protection of rights and freedoms while, at the same time, encountering constitutional limits. The third part will underline the characteristics of the European third way regarding the extension of European digital policies on a global scale.

2. Digital Sovereignty and Platform Governance

Territory is the natural limitation of sovereign powers. Inside a certain territory, citizens are expected to comply with the applicable law in that area while, outside this framework, they would be subject to the influence of other sovereign powers. Global trends have underlined different patterns of convergence, usually named "globalization" where the State-centric model has started to lose its power (Ip, 2010). The decay of national sovereignty and territorial borders is represented by "a world in which jurisdictional borders collapse, and in which goods, services, people and information 'flow across seamless national borders'" (Hirschl & Shachar, 2019, pp. 1-2). It is not by chance whether scholars have started to refer to the rise of "Global law" (Ziccardi-Capaldo, 2008) to define a meta-legal system where different organisations and entities produce and shape norms with extraterritorial implications.

The debate is now far from the old traditional questions around the capability of states to regulate the cyberspace. At the end of the last century, Johnson and Post (1996, p. 1370) wrote that "[c]yberspace radically undermines the relationship between legally significant (online) phenomena and physical location". This statement, representing the gap between law and space, is one of the reasons for the shared critics of those scholars firmly denying the idea of

cyberspace as a new "world" outside the influence of sovereign States (Barlow 1997). Since the cyberspace is not a "lawless place", States can impose their sovereignty, especially by regulating network architecture (Reidenberg, 1997), thus, making the code as the law of the cyberspace (Lessig, 1999).

Despite the relevance of these positions, these arguments neglected that, although states can exercise their sovereign powers over the digital environment within their territories, at the same time, other organisations contribute to producing their norms in turn. It is not by chance whether scholars identified a "trend toward self-regulation" (Goldsmith, 2000). More specifically, this trend in the cyberspace would derive from the code's architecture playing the role of a set of rules constituting meta-legal norms of the digital environment. The result of this approach is that state sovereignty based on the relationship between law and territory failure to capture the consolidation of the connection between norms and spaces.

The transnational dimension of platform governance leads to focusing on how states have reacted to the role of platforms expressing different strategies to extend their influence on a global scale and build their narrative of digital sovereignty.

On the western side of the Atlantic, still the First Amendment provides a shield against any public interference leading US companies to extend their powers and standards of protection beyond its territory. Despite multiple attempts and proposals to regulate platform power at the federal level (Kelly 2020), and even at the local such as in the case of Florida (Zakrzewsky 2021), nonetheless, such a liberal approach does not only foster private ordering but would also hide an indirect and omissive way to extend constitutional values beyond territorial boundaries through private ordering. Rather than intervening in the market, the US has not contributed to consolidating its role as a liberal hub of global tech giants. Failure to address platform powers in the US is not just the result of constitutional protection of free speech but also the lack of incentives. Regulating platforms could affect the smooth development of the leading tech companies in the world while also increasing the transparency of the cooperation between the governments and online platforms in certain sectors like security, thus, unveiling an invisible handshake (Birnhack & Elkin-Koren 2003). The Snowden revelations have already underlined how far public authorities rely on Internet companies to extend their surveillance programme and escape accountability (Lyon 2015). Put another way, US digital sovereignty would look at private ordering and the invisible cooperation between public and private actors as the way to move forward in the algorithmic society.

On the opposite, the cases of China and Russia are just two examples showing how states are proposing alternatives models of Internet the Internet based on their values (Broeders 2019; Claessen 2020). Particularly, China has always controlled its market from external interferences rather than adopting a liberal approach or exporting values through international economic law. China is promoting and resembling the western conception of the Internet while maintaining control over its businesses. Baidu, Alibaba and Tencent, also known as BAT, are increasingly competing with the dominant power of Google, Apple, Facebook, Amazon, or GAFA. The international success of TikTok is an example of how China aims to attract a global audience of users while supporting its business sector (Keane and Yu 2019). Besides, the adoption of the Digital Silk Road increasingly makes China a relevant player beyond territorial

boundaries (Hillman 2021). The Huawei model is based on exporting technological power supplying digital infrastructure even in peripheral areas (Wen 2020). Put another way, China is only partially opening to digital globalisation while is maintaining control over the network architecture. This twofold approach has been called the Beijing effect (Erie and Streinz 2021). This approach has resulted in multiple attempts to dismantle the western multi-stakeholder model (De Gregorio & Radu 2020) as well as extend their technological infrastructures to African countries (Gagliardone 2019).

Within this framework, the Union has already shown its ability to influence global dynamics, so that scholars have named such attitude as the "Brussel effect" (Bradford 2020). It should not surprise that the Union has also started to build its narrative about digital sovereignty based on ensuring the integrity and resilience of our data infrastructure, networks and communications aimed to mitigate dependency on other parts of the globe for the most crucial technologies (European Commission 2020). Protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies). "Now is the time for Europe to be digitally sovereign" (Merkel et al. 2021). These are the words supported by the prime ministers of Estonia, Finland, Denmark and Germany supporting the idea of a Digital Single Market which can promote innovation outside the interferences and dependences of other technological global poles. As observed by the European Council, "To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure" (European Council 2020).

This approach has also extended to the regulation of online platforms. From the first period of regulatory convergence based on neo-liberal positions at the end of the last century, the US and the Union have taken different paths. On the eastern side of the Atlantic, the Union has slowly abandoned its economic imprinting. While, at the end of the last century, the Union primarily focused on promoting the growth of the internal, this approach has been complemented (or even overturned) by a constitutional democratic strategy characterising European digital constitutionalism (De Gregorio 2021). The adoption of the General Data Protection Regulation has been a milestone in constitutionalising European data protection after the Lisbon Treaty.[2] Likewise, the Digital Services Act is another paradigmatic example,[3] showing the shift of paradigm in the Union towards more accountability of online platforms to protect European democratic values. These measures could be considered as an attempt to adatp the digital economy to the European goals (Renda 2021).

These two examples show the intention of the Union to propose a global model characterised by a sustainable democratic strategy limiting platform powers. In particular, the European framework of content and data protection is finding its path on a global scale, while raising as a model for other legislation in the world (Schwartz 2019). Even before this new phase of

[2] 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 (General Data Protection Regulation).

[3] 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.

European digital constitutionalism, the intention to overcome territorial formalities also drove the ECJ to step in and ensure the effective protection of the fundamental rights to privacy and data protection as enshrined in the European Charter (Pollicino 2020). Nonetheless, this reaction to the consolidation of platform power on a global scale is not without limits. The ECJ has contributed to defining the scope of European digital policies by extending and restricting the interpretation of constitutional rights and freedoms. If, on the one hand, the Union has showed its intention to react to the challenges raised by platform governance, being a global regulator entails dealing with the external limits of sovereign powers.

3. Interpreting Boundaries in the Digital Age

The transnational dimension of platform governance raises questions around the limits of state sovereignty. This question is particularly relevant for constitutional democracies which are not only bound by the traditional limits of sovereignty such as territory but also by substantive and procedural rules which aims to safeguard fundamental rights and democratic values.

The ECJ has contributed to explaining the need to extend European rules to ensure the effective protection of fundamental rights in the digital age. The GDPR territorial scope of application has codified the doctrine of establishment developed by the ECJ in *Weltimmo* and *Google Spain*.[4] In *Weltimmo*, the ECJ adopted a broad interpretation of the concept of 'establishment' avoiding any formalistic approach linked to the place of companies' registration. Likewise, in *Google Spain*, the ECJ underlined this flexible interpretation '[i]n the light of the objective pursued by Directive 95/46, consisting in ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data'.[5] The consequence of such a rule is twofold. On the one hand, this provision involves jurisdiction. The GDPR's territorial scope of application overcomes the doctrine of establishment developed by ECJ's case-law, since even those entities that are not established in the EU will be subject to the GDPR. On the other hand, the primary consequence of such an extension of territoriality is to extend European constitutional values to the global context.

The intention to overcome territorial formalities also drove the ECJ in the *Schrems* case,[6] by invalidating the Commission's adequacy decision,[7] known as the 'safe harbour agreement', concerning the transfer of personal data from the EU to the US. In this case, it is possible to observe another manipulation of data protection law extending its boundaries across the Atlantic. Although the Data Protection Directive required US data protection law to ensure an 'adequate' level of protection, the ECJ went beyond this boundary by stating that the safeguards

[4] C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság (2015); C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014).

[5] C-131/12, 53.

[6] Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015).

[7] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000) OJ L 215/7.

should be 'equivalent' to those granted by EU law to ensure the effective protection of the fundamental rights to privacy and data protection as enshrined in the Charter.

However, this decision did not exhaust the concerns about the safeguards in the transfer of personal data across the Atlantic. The ECJ invalidated the new adequacy decisions (i.e. Privacy Shield),[8] in light of the protection of fundamental rights as also translated into the new framework for personal data transfer introduced by the GDPR.[9] The ECJ went even further assessing the Standard Contractual Clauses ('SCCs') framework. Even without invalidating the Commission Decision on the use of these clauses,[10] the ECJ underlined that the equivalent level of protection applies even to this legal instrument. The Court expressly underlined the limits of EU law in relation to third countries since SSCs are not capable of binding the authorities of that third country.[11] Therefore, the ECJ recognised the role of the controller established in the Union and the recipient of personal data to check and monitor whether the third country involved ensures an essentially equivalent degree of protection.[12] When this is not the case, the ECJ did not preclude the transfer but underlined the need to set additional safeguards to ensure that degree of protection.[13]

This system has recognised the freedom of business actors to define the standard of protection of personal data across the Atlantic. Besides, Daskal underlined the limits of the entire system since 'there is no guarantee that the companies will win such challenges; they are, after all, ultimately bound by US legal obligations to disclose. And even more importantly, there is absolutely nothing that companies can do to provide the kind of back-end judicial review that the Court demands' (Daskal 2020).

These cases provide an example of the extension of constitutional values beyond the European territory, showing how litigating data privacy has also been an instrument for expressing digital sovereignty (Woods 2018). At the same time, the ECJ has also contributed to defining the limits of this approach which are based on the balancing between the same constiutitonal values whose protection has triggered the extension of the European model.

3.1 Global Delisting

The ECJ has recently highlighted these challenges in the decision *Google v CNIL* where the core of the preliminary questions raised by the French judge aimed to clarify the boundaries of the right to be forgotten online, especially its global scope.[14] Within this framework, the ECJ

[8] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016) OJ L 207/1.

[9] C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (2020).

[10] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010) OJ L 39/5.

[11] C-311/18, 136.

[12] ibid, 135, 137, 142.

[13] ibid, 133.

[14] Case C-507/17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (2019).

ruled on a preliminary reference concerning the territorial scope of the right to be forgotten online. The Court observed that the scope of the Data Protection Directive and the GDPR is to guarantee a high level of protection of personal data within the Union and, therefore, a de-referencing covering all the domains of a search engine (i.e. global delisting) would meet this objective. This is because the role of search engines in disseminating information is relevant on a global scale since users can access links to information 'regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself'.[15]

Nevertheless, the ECJ underlined the limits of this global approach. Firstly, States around the world do not recognise the right to delist or provide different rules concerning the right to be forgotten online.[16] Even more importantly, since the right to privacy and data protection are not absolute rights, they need to be balanced with other fundamental rights,[17] among which the right to freedom of expression.[18] The protection of these fundamental rights (and, therefore, their balance) is not homogenous around the world. The GDPR does not aim to strike a fair balance between fundamental rights outside the territory of the Union.[19] Before this crossroads, rather than extending the boundaries of data protection law to the global scale, the ECJ followed the opinion of the AG Szpunar,[20] thus, observing that neither the Data Protection Directive nor the GDPR recognises the right of data subjects to require a search engine like Google to delist content worldwide.[21]

Therefore, although Google falls under the scope of European data protection law, it is not required to delist information outside the territory of Member States. Nonetheless, Member States still maintain the possibility to issue global delisting order according to their legal framework. The ECJ specified that, if, on the one hand, EU law does not require search engines to remove links and information globally, on the other hand, it does not ban this practice. It is for Member States to decide whether extending the territorial scope of judicial and administrative order according to their constitutional framework of protection of privacy and personal data balanced with the right to freedom of expression.[22]

The ECJ also explained that the impossibility to require search engines to delist information on a global scale is the result of the lack of cooperation instruments and mechanisms in the field of data protection. The GDPR only provides the supervisory authorities of the Member States with internal instruments of cooperation to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data against the interest of the

---

[15] Ibid, 57.

[16] Ibid, 58.

[17] Ibid, 59.

[18] See Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (2010), 48; Opinion 1/15 EU-Canada PNR Agreement (2017), 136.

[19] GDPR, Art 17(3)(a).

[20] Opinion of Advocate General in C-507/17, 63.

[21] C-507/17, 64.

[22] Case C-617/10, Åklagaren v Hans Åkerberg Fransson (2013), 29; C-399/11, Stefano Melloni v Ministerio Fiscal (2013), 60.

public in various Member States in having access to information.[23] Therefore, such instruments of cooperation cannot be applied outside the territory of the Union.

Regarding the second question concerning the territorial scope of delisting within the territory of the Union, the ECJ observed that the adoption of the GDPR aims to ensure a consistent and high level of protection of personal data in all the territory of the Union and, therefore, delisting should be carried out in respect of the domain names of all Member States.[24] Nonetheless, the ECJ acknowledged that, even within the Union, the interest of accessing information could change between Member States as also shown the degree of freedom Member States enjoy in defining the boundaries of processing in the field of freedom of expression and information pursuant to Article 85 of the GDPR.[25] In other words, the ECJ underlined not only that freedom of expression does not enjoy the same degree of protection at the international level but also, in Europe, it can vary from one Member State to another. Therefore, it is not possible to provide a general obligation to delist links and information applying to all Member States.

To answer this issue, the Court left this decision to national supervisory authorities which through the system of cooperation established by the GDRP should, *inter alia*, reach 'a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union'.[26] Likewise, even concerning geo-blocking techniques, the ECJ did not interfere with Member States' assessment about these measures just recalling by analogy that 'these measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name'.[27] By distancing itself from the AG Szpunar's view on this point,[28] the ECJ decided not to recognise a general removal obligation at the European level but relied on the mechanism of cooperation of national authorities as well as to the discretion of Member States concerning preventing measures.

3.2 Global Removal

Just one week later, in *Glawischnig-Piesczek v Facebook*,[29] the Court addressed the territorial extension of national injunctions concerning the removal of content. The ECJ observed that Article 18 of the e-Commerce Directive does not provide for any limitation to the territorial scope of the measures that Member States can adopt and, consequently, EU law does not

[23] GDPR, Arts 56, 60-66.
[24] C-507/17*,* 66.
[25] Ibid, 67.
[26] Ibid, 68.
[27] Ibid, 70. See, *inter alia,* Case C-484/14, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (2016), 96.
[28] Opinion of Advocate General in C-507/17, 78.
[29] Case C-18/18, *Eva Glawischnig-Piesczek* v Facebook (2019).

prevent a national order to extend the scope application of their measures globally. As a general limit, the ECJ specified that Member States should take into consideration their international obligations given the global dimension of the circulation of content, without either specifying which rules of international law would apply in this case.

With regard to the territorial extension of national order, the ECJ did not clarify to which rules of international law the Member States should refer to assess the territorial scope of removal orders. Some perspectives on this point can be found in the decision *Google v CNIL*. In this case, the ECJ expressly refers to the potential contrast of a global delisting order with the protection of rights at an international level. Therefore, national competent authorities can indeed strike a fair balance between individuals' right to privacy and data protection with the right to freedom of information. However, the different protection of freedom of expression at a global level would limit the application of the balancing results. The AG Szpunar reaches the same conclusion in the Facebook case, explaining that, although EU law leaves Member States free to extend the territorial scope of their injunctions outside the territory of the Union, national courts should limit their powers to comply with the principle of international comity.[30]

This trend towards local removal is based not only on the *status quo* of EU law at the time of the decisions but also on the effects that a general extension of global removal can produce in the field of content and data. As observed by the AG Szpunar, a worldwide de-referencing obligation could initiate a 'race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale'.[31] In other words, the ECJ's legitimacy could start a process of cross-fertilisation, thus, leading other countries to extend their removal order on a global scale. This could be particularly problematic when looking at authoritarian countries which could exploit this decision to extend their orders.

Moreover, in *Google v CNIL*, the ECJ explained that the limit for global removal also comes from the lack of intention to confer an extraterritorial scope to right to erasure established by the GDPR.[32] The lack of cooperation mechanisms between competent authorities extending outside the territory of the Union would confirm this argument. Nevertheless, by supporting this position, the ECJ did not consider that, more generally, the GDPR establishes a broad territorial of application covering processing activities related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.[33]

Nonetheless, it is worth underlining that the Union has not closed the doors to the possibility of extending the territorial scope of removal orders beyond EU borders. At first glance, ECJ seems to express at an opposite view in the two cases regarding the territorial scope of national orders. On the one hand, in *Google v CNIL*, the ECJ stated that EU law does not require search engines to carry out the delisting of information and links on a global scale. In *Glawischnig-*

[30] Opinion of Advocate General in C-18/18, 100.
[31] Ibid, 61.
[32] C-507/17, 62.
[33] GDPR, Art 3(2).

Piesczek v Facebook, on the other hand, the ECJ explained that there are no obstacles to global removal, but also it leaves the evaluation to the Member States.

Although the two judgments may seem opposite, they lead to the same result, namely that EU law does not either impose or preclude national measures whose scope extends worldwide. This is a decision which rests with Member States which are competent to assess their compliance with international obligations. Art. 18 of the e-Commerce Directive does not provide a specific territorial scope of application and the ECJ has not gone further. Besides, the reasons for this different approach can be attributed to the different degree of harmonisation of the protection of personal data and defamation as observed by the AG Szpunar.[34] Therefore, it is not just an issue concerning public international law but also private international law contributes to influencing the territorial scope of removal orders (Cavaliere 2019).

Despite the relevance of this point, leaving Member States free to determine when a national order should be applied globally could lead to different national approaches which would fragment harmonisation goals. This is particularly relevant in the framework of the GDPR since it provides a new common framework for Member States in the field of data. Indeed, while the content framework still relies on the e-Commerce Directive leaving margins of discretion to Member States, this approach in the field of data is more problematic. On the one hand, the GDPR extends its scope of application to ensure a high degree of protection of fundamental rights of the data subjects. On the other hand, such a framework can be questioned by the autonomy of Member States to decide the reach of the right to be forgotten online. As Zalnieriute (2020) explains, '[b]y creating the potential for national data protection authorities to apply stronger protections than those afforded by the GDPR, this decision could be seen as another brick in the "data privacy wall" which the ECJ has built to protect EU citizens'.

Furthermore, even in this case, the ECJ has not focused on the peculiarities of platform activities and the consequences of these decisions on the governance of freedom of expression in the digital space. In *Glawischnig-Piesczek v Facebook*, a local removal order would not eliminate the possibility of accessing the same content – identical or equivalent – through the use of other technological systems or outside the geographical boundaries envisaged by the removal order. This problem is particularly relevant in *Google v CNIL* since it is possible to access different Google domain names around the world easily. The interest in the protection of reputation could also require an extension beyond the borders of the Union to avoid relying just on partial or ineffective remedies. The ECJ recognised that access to the referencing of a link referring to information regarding a person in the Union is likely to have 'immediate and substantial effects on the person'.[35] Therefore, even if this statement is just one side of the balancing activity with the protection of international law on the other side, it leads to contradictory results frustrating data subjects' right to be forgotten due to the potential access to search engines' domain names. Furthermore, to comply with geographical limits, geo-blocking and other technical measures would require an additional effort for platforms, thus,

[34] Opinion Advocate General in C-18/18, 79.
[35] C-507/17, 57.

increasing the risk of censorship on a global scale and create a technological barrier for small-medium platforms.

4. The European Third Way

The concrete extension of digital sovereignty on a global scale to face the transnational challenges of platform governance has showed the tensions between the territorial characteristics of state sovereignty and the transnational dimension of platform governance. Still, this approach is likely to extend their influence on other fields in the next years with the consolidation of the Union as a global regulator (Bradford 2020).

The European policy is orienting towards extending its measures. The GDPR provides a scope of application which would extend beyond the European territory. Precisely, even though the data controller is established outside the Union, European data protection law is nevertheless applicable if the activities of which the processing of personal data implies the provision of products or services to data subjects who are in the Union and the processing activities are related either to the offering of goods and services in the EU; or the monitoring of the behaviour of data subjects in the EU.[36] In these years, the long arm of European data protection law has been already highlighted in the framework of the Data Protection Directive (Moerel 2011), defining the 'global reach of EU law' (Kuner 2019). The European framework of data protection is finding its path on a global scale (Schwartz 2019), while raising as a model for other legislation in the world (Greenleaf 2019).

Likewise, the Digital Services Act will cover intermediary services provided to recipients of the service that have their place of establishment or residence in the Union, irrespective of the place of establishment of the providers of those services.[37] Even, the proposal for the regulation of artificial intelligence is an example of this European approach. The scope of the proposal would extend to 'providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country',[38] thus, providing a broader territorial coverage which aims to ensure that European standards are taken seriously on a global scale.

The consequences of this constitutional architecture, and political choice, is to increase the regulatory burdens for those entities which, although not established in the Union territory, offer of goods and services or monitor the behaviour of data subjects in the Union. Indeed, it cannot be excluded that this over-reaching scope could impact on free speech and financial interests of other countries and their citizens and decrease the degree of legal certainty leading to a binary approach which is not scalable (Svantesson, 2013; Kuner, 2015). Although other scholars do not share the same concerns, they have observed that "when a law is applicable extraterritorially, the individual risks being caught in a network of different, sometimes conflicting legal rules requiring simultaneous adherence. The result – conflicts of jurisdiction

[36] GDPR, Art 3(2).

[37] Digital Services Act, Art. 1(3).

[38] Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Art. 2(1).

– may put an excessive burden on the individual, confuse him or her, and undermine the individual's respect for judicial proceedings and create a loss of confidence in the validity of law" (De Hert & Czerniawski, 2016, p. 240). The GDPR has also been criticised for its 'privacy universalism' (Arora 2014). Proposing the GDPR as a global model entails exporting a western conception of privacy and data protection that could clash with the values of other areas of the world, especially, in peripheral areas of the world, thus, opening a new phase of (digital) colonialism (Kwet 2019; Coleman 2019; Pinto 2018).

At first glance, this approach would suggest that the Union is adopting a form of constitutional imperialism by imposing its own legal standard of protection on a global scale. Nonetheless, while European digital policy is increasingly emerging as a global model, it is not driven by a mere goal of extraterritoriality. Rather, it provides an example of how constitutional democracies struggle to ensure that formal territorial limitations would not undermine the protection of fundamental rights and democratic values. The extraterritorial reach of European data protection law and, in general of the GDPR can be considered an 'anti-circumvention mechanism' (Yakovleva & Irion 2020). In other words, the Union is trying to ensure that formal geography could not constitute a shield to avoid compliance with any regulation. Rather than a 'European data privacy imperialism' (Svantesson 2013), this approach would aim to protect users' fundamental rights, while avoiding businesses escape from complying with EU law just by virtue of a formal criterion of establishment. Otherwise, the primary risk is to encourage a disproportionate unbalance between businesses operating physically in the territory of a State, and other entities which, by processing data and offering other digital services, would avoid complying with the law of the States in which perform their business.

Therefore, the scope of European digital sovereignty would not express a form of constitutional imperialism or protectionism. The need to ensure the protection of fundamental rights in a globalised world leads the Union to exercise a global influence which, at first glance, would be the opposite of constitutional protectionism. At the same time, the Union is aware of the consequences of the extension of constitutional values on the global scale which, according to the ECJ case law, seems to appear an exceptional resort based on Member States' assessment.

The Union is increasingly aware of its ability to extend its 'regulatory soft power', influencing the policy of other areas of the world in the field of digital technologies. It should not surprise that the Union has also started to build its narrative about digital sovereignty. As underlined by the Commission (2020), 'European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks and communications' aimed to mitigate 'dependency on other parts of the globe for the most crucial technologies'. This does not entail closing European boundaries towards a form of constitutional protectionism but to ensure the Europe's ability to define its rules and values in the digital age. Indeed, 'European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model', and, as a result, 'the EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based' (European Commission 2020). Rather than focusing just on promoting the European industry, the Union approach is oriented towards rising as a global

standard maker. Its narrative is not adversarial but cooperative toward external actors while, at the internal level, it is not possible to foresee how digital sovereignty will be articulated at the supranational level or driven by Member States single actions. This is also why the fight for digital sovereignty is particularly relevant on the external and internal level, especially for the Union.

In this way, the Union is rising as global regulator proposing a political model to transnationally to limit interferences from models of governance based on wide liberal approach or oppressive public control. In other words, rather than adopting an extraterritorial or protectionist approach, the Union seems to have chosen a third way once again. Like in the case of values and governance, the Union has shown its intent to take a third way proposing its role as a global regulator rather than a liberal or authoritarian hub for tech giants.

Such a third way is the result of the role of European digital constitutionalism which, in these years, has shown how rights and freedoms cannot be frustrated just by formal doctrines based on territory and establishment. At the same time, this approach does not express imperialist or protectionist goals but rather proposes a different political and normative model to protect fundamental rights and democratic values on a global scale. This is almost a mandatory step for the Union to avoid constitutional annilhation driven by approaches based on neoliberal or technodeterministic approaches. Besides, this constitutional framework leads to wonder about a uniform set of rules which can build a uniform approach to platform governance rather than the sum of different measures picturing a dangerous path for the rule of law in the digital age.

Fragmentation and hybridisation of standards are the primary threats for the Union in the algorithmic society. This challenge does not only concern the supranational level but even the national strategies. Member States have showed to propose their narrative of digital sovereignty in different ways, particularly looking at Germany and France. This is a critical point to understand whether Member States speaking about digital sovereignty look at the local or at the supranational level. As observed by Floridi (2020), “the risk, when supporting national digital sovereignty, is to end up supporting digital sovereignism or digital statism”. And this situation is even more problematic when looking at the emerging Internet fragmentation, or splinternet, showing the multiple expressions of digital sovereignty (O’Hara and Hall 2021).

The fight for digital sovereignty has seen even constitutional democracies restricting the use of social media such as in the case of TikTok (Gertz 2020), or even trying to limit the reach of Huawei in extending digital infrastructures in different countries (Kharpal 2020). This tech clash shows the double face of digital sovereignty which can support political narrative to censor online speech or the freedom of businesses to operate in different markets. In the case of the ban of TikTok in the US, courts reacted to the dark side of digital sovereignty blocking the ban (Shu 2020), thus, showing the relevance of constitutional values in the field of platform governance.

Besides, this is a particular moment for the Union which has captured the attention of global policy makers. As underlined by Kaye (2019), the Union could play a relevant role in order to propose a regulatory architecture oriented to the protection of fundamental rights and democratic values. At the same, the Union can also provide a justification to other governments

to regulate digital technologies based on public interests. For authoritarian regimes, the conceptual vagueness of digital sovereignty is an opportunity to support the introduction of rules and standards which are only apparently based on the protection of rights and freedoms. Indeed, digital sovereignty is not only a concept used for promoting the autonomy of state against technological interferences but also as a political narrative justifying protectionist measures opposing the global idea of an open Internet. This situation is particularly relevant when looking at processes of surveillance, reterritorialisation of internet governance, and Internet shutdowns.

5. Conclusions

Digital sovereignty does not lead any longer to wondering about the effectiveness of state powers but the different strategies to express authority in the digital environment. The question of digital sovereignty is still traditional in this sense, even if this notion is no longer referred to state actors but extends to the multiple ways actors such as transnational corporations or individuals can express their governance in the digital age. Put another way, the question is not just around the capabilities of states to regulate the digital environment but how different models arise and compete as expressions of powers in the digital age.

Nevertheless, the extensive scope of digital sovereignty does not mean that the notion of state sovereignty has lost relevance in the digital age. Particularly, the transnational dimension of platform governance raises questions about how states deal with transnational private powers on a global scale while respecting the rule of the game of sovereign states. While the US neoliberal approach would export sovereign powers through the unaccountable cooperation with the private sector and China relies on a centralised model governing technological companies, the Union is proposing a third way raising as a global regulator driven by the need to ensure the respect of fundamental rights and democratic values in the evolution of the digital environment. These examples show how the narratives around digital sovereignty have led states to express models of digital sovereignty that are deeply related to different institutional and political frameworks.

The Union approach to digital sovereignty is characterised by the extension of constitutional values on a global scale. The need to ensure the effective protection of fundamental rights and freedom beyond territorial boundaries has driven European digital policies to preclude transnational actors, primarily online platforms, from escaping European rules by hiding responsibility behind territorial formalities. Particularly, the invalidation of two adequacy decisions in the Schrems saga has underlined how the Union is proposing a model overcoming territorial boundaries depowering the effectiveness of constitutional values in the digital age. At the same time, European digital sovereignty has encountered constitutional limits. The ECJ has played a critical role not only in enlarging the extension of European digital policies but also to define how far this strategy could extend on a global scale.

The rise of the third way of the Union is providing an alternative model of digital sovereignty and platform governance which put at the forefront the protection of fundamental rights and democratic values. However, the path of European digital sovereignty is still at the beginning.

The limits to extend digital policies beyond European boundaries and the challenges relating to the exportation of a model which can be exploited by illiberal regimes seems to constitute the price to pay to advance a model which does not follow neoliberal or illiberal narratives.

References

Arora P. (2014). "GDPR – A Global Standard? Privacy Futures, Digital Activism and Surveillance Cultures in the Global South". Surveillance & Society, 17, 5, 717;

Barlow J.P. (1997). "The Declaration of Independence of Cyberspace" https://www.eff.org/cyberspace-independence;

Birnhack M. D. and Elkin-Koren N. (2003). "The Invisible Handshake: The Reemergence of the State in the Digital Environment". Virginia Journal of Law & Technology, 8, 1;

Bradford A. (2020). *The Brussels Effect. How the European Union Rules the World.* Oxford University Press;

Bratton B. (2016), *The Stack: on Software and Sovereignty*. MIT Press;

Broeders D. et al. (November 2019). "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace". The Hague Program for Cyber Norms Policy Brief. https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace;

Castells M. (2008). "The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance". Annals of the American Academy of Political and Social Science 616, 1, 78;

Cavaliere P. (2019). "Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations". European Data Protection Law, 4, 573;

Chander A. and Sun, H (2021). "Sovereignty 2.0". *Georgetown Law Faculty Publications and Other Works*. 2404;

Claessen E. (2020). "Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU" Journal of Cyber Policy, 5, 1, 140;

Coleman D. (2019). “Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws”. Michigan Journal of Race & Law, 24, 417;

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;

Couture S. and Toupin S. (2019). “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?”. New Media & Society, 21, 10, 2305;

Daskal J. (2018). “Borders and Bits”. Vanderbilt Law Review, 71, 179;

Daskal J.C. (17 July 2020). “What Comes Next: The Aftermath of European Court’s Blow to Transatlantic Data Transfers”. Just Security. https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/;

De Gregorio G. (2021). “The Rise of Digital Constitutionalism in the European Union”. International Journal of Constitutional Law, 19, 1, 41;

De Gregorio G. & Radu R. (July 14, 2020), Fragmenting Internet Governance: Digital Sovereignty and Global Constitutionalism. MediaLaws https://www.medialaws.eu/fragmenting-internet-governance-digital-sovereignty-and-global-constitutionalism/;

De Gregorio G. & Stremlau N. (2020). “Internet Shutdowns and the Limits of Law”. International Journal of Communication, 14, 4224;

De Hert P. & Czerniawski M. (2016), “Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context”. International Data Privacy Law, 6, 3, 230;

DeNardis L. & Hackl A.M. (2015). “Internet Governance by Social Media Platforms”. Telecommunications Policy, 39, 9, 761;

Erie M.S. & Streinz T. (2021). “The Beijing Effect: China's ‘Digital Silk Road’ as Transnational Data Governance”. SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256;

European Council (2020). “Special meeting of the European Council (1 and 2 October 2020) – Conclusions”, https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf;

Floridi L. (2020). “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU”. Philosophy and Technology, 33, 369;

Gagliardone I. (2019). *Africa, and the Future of the Internet*. ZED;

Gertz G. (7 August 2020). “Why is the Trump Administration Banning TikTok and WeChat?” Brookings. https://www.brookings.edu/blog/up-front/2020/08/07/why-is-the-trump-administration-banning-tiktok-and-wechat/;

Goldsmith, J. L. (2000). “Unilateral Regulation of the Internet: A Modest Defence”. European Journal of International Law, 11, 1, 105;

Greenleaf G. (2019). “Global Data Privacy Laws 2019: 132 National Laws & Many Bills”. Privacy Laws & Business International Report, 157, 14;

Grimm, D. (2015). *Sovereignty: The Origin and Future of a Political and Legal Concept*. Columbia University Press;

Grumbach S. (2017). “Digital Platforms: A New Grammar for Territories”. Ethics in Progress, 8, 101;

Gueham F. (February 2017). Digital Sovereignty - Steps towards a new System of Internet Governance. Fondapol, https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/;

Haggart B., Tusikov N., Scholte J.A. (2021). *Power and Authority in Internet Governance. Return of the State?*. Routledge;

Hillman J. (2021). *The Digital Silk Road: China's Quest to Wire the World and Win the Future*. Oxford University Press;

Hindman, M. (2018). The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy. Princeton University Press;

Hirschl R. & Shachar A. (2019). “Spatial Statism”. International Journal of Constitutional Law, 17, 2, 387;

Ip E.C. (2010). “Globalization and the Future of the Law of the Sovereign State”. International Journal of Constitutional Law, 8, 3, 636;

Johnson, D. R., & Post, D. (1996). “Law and Borders: The Rise of Law in Cyberspace”. Stanford Law Review, 48, 5, 1367;

Kaye D. (2019). *Speech Police: The Global Struggle to Govern the Internet*. Columbia Global Reports;

Keane M. & Yu H. (2019). “A Digital Empire in the Making: China’s Outbound Digital Platforms”. International Journal of Communication, 13, 4624;

Kelly M. (3 March 2020). “All the Ways Congress is Taking on the Tech Industry. Every Bill, Every Plan, Every Threat”. The Verge, https://www.theverge.com/2020/3/3/21153117/congress-tech-regulation-privacy-bill-coppa-ads-laws-legislators;

Kettemann M. (2020). *The Normative Order of the Internet*. Oxford University Press;

Kharpal A. (21 October 2020). “U.S. tries to get Huawei Blocked from Brazil’s 5G Networks with $1 Billion Financing Pledge”. CNBC. https://www.cnbc.com/2020/10/21/us-tries-to-get-huawei-blocked-from-brazils-5g-networks.html;

Kuner C. (2019). “The Internet and the Global Reach of EU Law”, in Marise Cremona & Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law.* Oxford University Press;

Kuner C. (2015). “Extraterritoriality and regulation of international data transfers in EU data protection law”. International Data Privacy Law, 5, 4, 235;

Kwet M. (2019). “Digital Colonialism: US Empire and the New Imperialism in the Global South”. Race & Class, 60, 4, 3;

Lessig L. (1999). *Code: And Other Laws of Cyberspace*. Basic Books;

Lyon D. (2015). *Surveillance after Snowden*. Polity Press;

Merkel A. et al. (1 March 2021). “Joint Letter”. https://valitsus.ee/uudised/saksamaa-taani-eesti-ja-soome-valitsusjuhid-euroopa-digitaalne-suveraansus-tagab-meile;

Moerel L. (2011). “The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?”. International Data Privacy Law, 1, 1, 28;

Moore M. & Tambini D. (eds.) (2018), *Digital dominance: The Power of Google, Amazon, Facebook and Apple*. Oxford University Press;

Mueller M. L. (2020). “Against Sovereignty in Cyberspace”. International Studies Review, 22, 4, 779;

O'Hara K. & Hall W. (2021). *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. Oxford University Press;

Pasquale F. (2016). “Two Narratives of Platform Capitalism”. Yale Law & Policy Review, 35, 1, 309;

Pinto R.A. (2018). “Digital Sovereignty or Digital Colonialism?” SUR, 27 https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/;

Pohle J. & Thiel T. (2020). “Digital Sovereignty”. Internet Policy Review, 9, 4, https://policyreview.info/pdf/policyreview-2020-4-1532.pdf;

Pollicino O. (2020). Judicial Protection of Fundamental Rights Online: A Road Towards Digital Constitutionalism?. Hart;

Radu R. (2019). *Negotiating Internet Governance*. Oxford University Press;

Reidenberg J.R. (1997) *Lex Informatica: The Formulation of Information Policy Rules through Technology*. Texas Law Review, 76, 553;

Renda A. (2021). Making the Digital Economy “fit for Europe”. European Law Journal. In Press;

Sassen S. (1998). “On the Internet and Sovereignty”. Indiana Journal of Global Legal Studies, 5, 545;

Schneider F. (2020). *China's Digital Nationalism*. Oxford University Press;

Schwartz P. (2019). “Global Data Privacy: The EU Way”. NYU Law Review, 94, 771;

Srnicek N. (2016). *Platform Capitalism*. Polity Press;

Svanteson D.B.J. (2013). “A ‘layered approach’ to the Extraterritoriality of Data Privacy Laws”. *International Data Privacy Law*, 3, 4, 278;

Wen Y. (2020). *The Huawei Model. The Rise of China's Technology Giant.* Illinois University Press;

Woods A.K. (2018). “Litigating Data Sovereignty” Yale Law Journal, 128, 328;

Yakovleva S. & Irion K. (2020). “Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation”. AJIL Unbound, 114, 10;

Zakrzewski C. (25 May 2021). The Technology 202: Tech Groups Criticize Florida's Social Media Law as Unconstitutional, Setting the Stage for Legal Action. The Washington Post, https://www.washingtonpost.com/politics/2021/05/25/technology-202-tech-groups-criticize-florida-social-media-law-unconstitutional-setting-stage-legal-action/;

Zalnieriute M. (2020). “Google LLC v. Commission Nationale de l’Informatique et des Libertés (CNIL)”. American Journal of International Law, 114, 2, 261;

Ziccardi-Capaldo G. (2008). *The Pillars of Global Law*. Routledge;

Zuboff S. (2019). *The Age of Surveillance Capitalism*. Profile Books.