The Ambiguity of Digital Sovereignty between Cybersecurity and Digital Rights

Nicola Palladino (Trinity College Dublin, palladin@tcd.ie)
Francesco Amoretti (Università degli Studi di Salerno, amoretti@unisa.it)

PAPER PRESENTED AT THE 27th IPSA-AISP WORLD CONGRESS
OF POLITICAL SCIENCE
19 JULY 2023 | BUENOS AIRES, ARGENTINA

1. Introduction

Digital sovereignty has become an increasingly popular concept in international relations and beyond. For many years the flag of sovereigntist policies and claims on information networks has been raised by China and Russia. However, in the last few years, an increasing number of western countries started to vindicate their authority on data flows and digital infrastructures affecting their territories or citizens. Brazil, after Snowden's disclosures, proposed a plan to bind US tech giants to store Brazilian data locally. Canada is working to reach so-called Canadian Network Sovereignty by improving infrastructures in order to diminish data routing through the United States. With regard to the European Union, a 2020 briefing by the European Parliament Research Service (EPRS) stresses that "'digital sovereignty' refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)." Furthermore, the European Council called for action to ensure the strategic autonomy of the EU in a post-pandemic context and stressed that investing in digital capacities, infrastructure and technologies will be a key element of the recovery effort.

The United States themselves, very often alleged to threaten other countries' digital sovereignty and not so keen to use the concept of sovereignty for geopolitical reasons, are used to carry out *de facto* sovereigntist policies as testified by the recent Chips and Science Act, or Tik Tok bans.

This paper argues that the spread of sovereigntists' claims is likely to increase geopolitical tensions and conflicts since actors employ a twofold and ambiguous notion of sovereignty applied to cyberspace. On the one hand, we have a classical conception, based on the notions of territoriality, authority, and population, according to which states claim an exclusive faculty to control the digital infrastructure of their jurisdiction and the data of their citizens. On the other hand, the transborder nature of the Internet and its distributed architecture favoured the rise of a conception that disentangles the sovereign from the territory and shifts the focus from the "recognized authority on a territory" paradigm to concepts such as autonomy, power, and self-determination. This latter conception justifies the idea of a "sovereignty of cyberspace", but paradoxically, it also constitutes the basis for States' claim to extend their jurisdiction over processes taking place outside their boundaries, or in some no physical space, if they impact their national interests or citizen rights.

Through in-depth content analysis and impact assessment of selected policies, such as the EU NIS directive, Cybersecurity Act, the US Cloud Act or the Chinese Personal Information Protection Law, the paper argues how conflicts among overlapping and competing sovereignty claims are deemed to arise, and new forms of international agreement are needed.

Then the paper also addresses the question of the ambiguous relationship between digital sovereignty, digital constitutionalism, and digital authoritarianism. It argues that while digital

sovereignty is a necessary condition for the affirmation of effective digital rights, it is not sufficient, and could easily lead to a threat to constitutional guarantees and a digital authoritarian approach.
Resorting to concrete examples the paper outlines how state actors strategically alternate between different conceptions of sovereignty to pursue their goals. The paper points out how these practices foster geopolitical conflicts and legal uncertainty, hamper cooperation to find solutions within an international law framework, and, ultimately, undermine global efforts to guarantee fundamental rights in the digital environment.
Therefore, the paper calls for the establishment of international treaties defining a transnational legal framework and dispute resolution rules, in order to ensure legal certainty and the application of the rule of law at the international level.

2. Digital Sovereignty: a twofold conceptualization.

The concept of Digital Sovereignty has become essential in policy actions worldwide.
Digital Sovereignty is primarily used by states to legitimate their power to intervene in the digital realm defining related public interests and corresponding policies, as well as duties, responsibilities and rights of digital operators citizens.
The term proves particularly valuable as it encompasses both internal and external aspects of State power. Indeed, States' digital sovereignty, could be defined as "the ability of nation states to control the digital infrastructure on their territory and the data of their citizens" (Moerel and Timmers 2021:5), and in so doing it refers both to effort to counter the growing influence of tech giants and to the competition between nations on and by the governance of digital technologies.
In many regards, the recent raise in the claims for digital sovereignty by states could be conceived as a reaction to the governance denial and US hegemony that have characterized the Internet governance field since its early stage (Drake 2004, Hoffman 2005).
Many scholars and practitioners shared the opinion according to which state sovereignty on the Internet, or the cyberspace, is both unpractical and undesirable, due to the borderless and distribute architecture of the cyberspace (Barlow 1996, Johnson, and Post 1996, Mueller 2020). On the one hand they argued that activities in the cyberspace could not be easily traced back to a specific jurisdiction. On the other hand, they depict the cyberspace as a self-governing space emerging "spontaneously, from the bottom-up, through the loosely or un-coordinated activities of technologically empowered netziens", where applying the "slow moving, bureaucratic, centralized, old paradigm, state-centric approaches would be fundamentally out of synch with and damaging to the Internet" (Drake 2004: 2). Nonetheless, such as cyber-anarchic view solidified into a self-governance regime dominated by US companies and tech-community, and in which the US government retained a special oversight role on core Internet critical infrastructures (Hofmann 2005, Palladino and Santaniello 2021).
This status quo and its underlying conceptions on sovereignty was firstly challenged during the 2003-5 World Summit on Information Society, where a 'sovereigntist' coalition led by China and Russia claiming their sovereign right to safeguard the security of networks, of their citizens and the public order, make domestic and international public policy for the internet and contested US unilateralism (Santaniello and Palladino 2022).
In the following years sovereigntist claim spread also among western democratic countries.
Following a massive cyberattack against Estonia in 2007, NATO established a Cooperative Cyber Defense Center of Excellence (CCDOE) in Tallinn, which main output, the Tallin Manual pointed out that States "may exercise control over cyber infrastructure and activities within its sovereign territory" as a crucial component of domestic and international security.

Following the revelation of mass surveillance activities conducted by the US National Security Agency (NSA) as exposed by Edward Snowden, which targeted even allied nations, along with the cyber espionage and cyber warfare operations carried out by Russia and China, and considering the growing significance of Big Tech, the concept of digital sovereignty has emerged as a focal point in European digital policy.
In 2017, French President Emmanuel Macron emphasized the significance of reclaiming control and independence in the digital domain as a fundamental policy for reshaping the European Union[1]. German Chancellor Angela Merkel, during her speech at the 2019 Internet Governance Forum, reiterated the utmost importance of digital sovereignty in the European agenda for digital policies[2]. Documents presenting the project Gaia-X published by the German Federal Ministry for Economic Affairs and Energy, identify digital sovereignty as a crucial 'aspect of general sovereignty', consisting in the 'possibility of independent self-determination by the state and by organisations' with regard to the 'use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result'[3].

However, as various stakeholders hold significant roles in the digital realm or are affected by digital technologies, the concept of digital sovereignty has been declined and re-articulated in many ways. The ongoing discourse surrounding digital sovereignty arises from inherent differences in how actors have historically approached cyberspace and defined boundaries and limitations for internet operations.
Paradoxically, the aforementioned governance denials rejected the idea of a state sovereignty on the cyberspace, to claim "that cyberspace itself was its own sovereign space" (Mueller 2020: 780). Johnson and Post put forth the concept of an "emergent law" for the Internet, envisioning it as a self-regulating system guided by networked governance practices and native institutions such as IETF and ICANN. In other words, they advocated for the idea of a *cyberspace sovereignty* completely unbounded by territoriality and States' jurisdiction.
which refers to the establishment of extensive interconnected systems, including submarine cables, data centers, and hosting farms, enabling big tech companies to operate independently and autonomously (Moore & Tambini, 2018). It also encompasses the broader objective of tech companies to maintain complete control over their value chain, either through asset ownership or by avoiding critical dependence on third parties.
Cauture and Toupin identified further declinations of digital sovereignty, such as: Indigenous Digital Sovereignty, which indicates "the aspirations rooted in the self-determination of indigenous peoples in the realm of digital data" (Cauture and Toupin 2019:2314); Social Movements Digital Sovereignty, referring to the "control of technologies and digital infrastructures by social movement and their power to develop and use tools designed by them and/or for them"(Cauture and Toupin 2019: 2315); and Personal Digital Sovereignty, which indicate to "the control of an individual over their data, device, software, hardware, and other technologies"(Cauture and Toupin 2019: 2316).

In the end, this polysemy in the concept of digital sovereignty could be reduced to two major conceptualizations.
On the one hand, we have a conception of digital sovereignty based on the classical notion of sovereignty as exercise of supreme political based on the notions of territoriality, authority, and population, which focuses on the role of states and their internal and external legitimization.

[1] https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe
[2] https://www.bundesregierung.de/breg-en/service/archive/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494
[3]

The Stanford Encyclopedia of Philosophy identifies four principles for the sovereign (Philpott 2003:3): (1) It holds authority; (2) this authority is obtained "from a mutually recognized source of legitimacy; (3) this authority is supreme; and (4) this authority extends over a defined territory. Sovereignty is often articulated in an internal and external dimension, where the former indicates that State power on a territory is exclusive and unchallenged, while the former refers to States's independence vis-à-vis other states or other external power.

When applied to the digital world, this conception of sovereignty is evoked to indicate the capability by States to control data flow, digital infrastructures and operators within their boundaries. It refers to growing geopolitical tensions between states on aspects related to digital technologies, as well as their re-appropriation of public functions and regulatory capacity left for so long in the hands of private actors.In this perspective, some relevant dimensions of digital sovereignty could be identified in cyber security and resilience; control and leadership in the digital economy and technological innovation; public trust (related to the internal recognition of sovereignty), as recently suggested by Moerel and Timmers (2021).

On the other hand, we have a heterodox conception that disentangles sovereign from the territory and shifts the focus from the "recognized authority on a territory" paradigm, to concepts such as autonomy, power, resilience and self-determination.

In so doing, digital sovereignty follows a broader trend concerning the sovereignty concept.

Cauture and Toupin (2019) have illustrated how the notion of sovereignty has been subject to critical examination through the lens of indigenous perspectives or claims made by "nations without states." Additionally, sovereignty has been reframed by employing it to assert the right to self-determination in some aspect deemed to be crucial for a subject, as in the case of 'food sovereignty' or 'body sovereignty'.

As Werner and de Wilde a sovereignty claim could be understood as "specific form of legitimization […] a speech act to (re-)establish the claimant's position as absolute authority, and to legitimize its exercise of power" (Werner and de Wilde 2001: 287).

In this view, it could be said that "the use of sovereignty also has rhetorical performativity" (Cauture and Toupin 2019:2317) marking an opposition to different kinds of hegemonies or dependencies which pose an existential threat to a subject.

In sum, digital sovereignty could be conceived as the capability of a subject, not necessary a state, to control and decide about the digital processes in which is involved or by which is affected.

3. The ambiguity of State Digital sovereignty I: territorialization of cyberspace and extraterritorial projection of power

At first glance, it may seem that heterodox conceptions of digital sovereignty compete with and erode state digital sovereignty claims.

However, a closer analysis reveals that states commonly embrace both territory-based and de-territorialized form of sovereignty, especially if look at concrete practices.

This is well illustrated by the concept of digital strategic autonomy. According to Moerel and Timmers (2021:8), digital strategic autonomy could be considered the operationalization of states' digital sovereignty and consist of "the ability to decide and act autonomously on the essential digital aspects of our longer-term future in the economy, society, and institution".

If the goal is to ensure the ability to decide and act autonomously in the future digital aspects of a country, it is essential to acknowledge that the digital world is currently predominantly shaped by transborder processes and flows. In this context, the concept of digital strategic autonomy operates under the underlying assumption that in order to exercise digital sovereignty, states must not only maintain control over digital activities within their own territory but also strive to influence processes and entities that extend beyond their borders. In

other words, achieving digital strategic autonomy necessitates an extraterritorial projection of power and an extension of national sovereignty.

It could be said that then States operationalize digital sovereignty through two complementary processes:
1) the territorialization of cyberspace, which operationalizes the classical 'territorial' conception of sovereignty
2) the extraterritorial projection of digital power, which operationalize the heterodox de-territorialized conception of sovereignty
The territorialization of cyberspace consists in the process of bringing back aspects of physical space into the digital realm and the "extension to cyberspace of configurations of authority and power linked to territorial space" (Tsagourias 2015:21).
As said it occurs by exercising control on data flow, infrastructures and operators within a state territory, but also delimiting the boundaries of legitimated digital activities/operations.
On a more practical level, it may consists of the:
a) *Control of internet traffic*. By the means of ordinary law state may impose internet service providers to block or filter the access to determinate IP addresses, such as in the case of the Chinese Great Firewall and RuNet, or more limited shutdowns and restrictions in other countries (Chandler and Sun 2022);
b) *Nationalization of digital operators*. states can try to 'nationalize' digital operators in such a way to bound them to their jurisdiction. The first way to obtain such result is promoting the development of national digital champions by allowing industrial concentration, softening regulatory burden and responsibilities and funding research and innovation. Secondly, states may require digital operators to have a legal representatives on country territory in order to be allowed to operate within it. Finally they can raise market or regulatory barrieries in order to hinder the access of foreign companies.
c) *Data localization*. Data localization refers to the practice of storing and processing data within a specific geographic location or jurisdiction, typically within the borders of the country in which the data have been generated or collected. Data localization can take various forms, including requirements for data to be physically stored within a specific country or region, restrictions on data transfers to foreign countries, or mandatory processing of data using local infrastructure or services (Selby 2017). Having national digital champions make more likely that data are stored locally, even if provisions may be still necessary to prevent or control their transfer to other countries.
d) *Risk and Security Assessment*. By implementing mandatory risk and security assessments, states aim to ensure that ICT systems and infrastructure meet certain security standards and are aligned with their national interests. This approach involves subjecting hardware and software components, networks, and systems to comprehensive evaluations to identify vulnerabilities, assess risks, and determine the necessary security measures. The process of institutionalizing mandatory risk and security assessments allows states to exert control over cyberspace by directly influencing the design and deployment of ICT systems, also by preventing the spread of foreign technologies, firms or systems.

On the other side, even the extraterritorial extension of sovereignty may occur in different ways:
a) *International law principles.* It is worth noting that States can advance extraterritorial sovereignty claims resorting to already existing and well established international law principle, and more in detail:

i) Active nationality principle: this principle allows a country to exercise criminal jurisdiction over any of its nationals accused of criminal offenses wherever they act in the world (Gallant 2022);

ii) Passive nationality principle: The passive nationality principle allows States, in limited cases, to claim jurisdiction to try a foreign national for offenses committed abroad that affect its own citizens (Gallant 2022);

iii) Effects doctrine: According to this doctrine, States claim jurisdiction over acts committed abroad which produce harmful effects within the territory;

iv) Protective principle. Under the protective principle a state has jurisdiction to criminalise extra-territorial conduct, regardless of the nationality of the offender, where that conduct is against the security, territorial integrity or political independence of the state.

One may object that if several States claim jurisdiction on the same cases this may led to intractable conflict making extraterritorial claim of jurisdiction unrealistic and unpractical. It useful here recall the difference between the internal and external dimension of state sovereignty. The internal dimension refer to the supreme, exclusive and comprehensive exercise of power within a State, while the external dimension refers to the "external aspect of autonomy and independence vis-à-vis other States, plenary power to regulate externalities, and power to create, implement, and enforce international law" (Tsagourias 2021: 12). In this view "external manifestations of sovereignty are coordinated and managed through consent" that should be indented as "a sovereign act of voluntary acquiescence". As a consequence potential conflicts of jurisdiction are not intractable in themselves, but they may be resolved within the traditional international law framework by the means of treaties, international courts' case law or other forms of convection and negotiation, with the same degree of opportunities and difficulties already experienced in other transnational phenomenon. In other words, by the point of view of political and legal technicality there is no Internet and digital word 'exceptionalism'.

b) *Regulation and standardization of technologies.* Regulation and standards are other means through which states can influence actors and processes beyond their boundaries.

If a state is successful in imposing the rules and standard through which a technology is s developed, deployed, and used at the international level, it could embed its own values and interests within the socio-technical architecture of such technology, and shape it accordingly, defining what is possible to do or not by whom, ensuring control points and oversight and ruling role for itself. As known the EU is supposed to exert this kind of extraterritorial effect due to the so called Brussel effect (Anu Bradford 2012), which consist in the capability to leverage and combine key factors such as market size, regulatory capacity, stringent standard and inelastic target, in order to impose de facto global standards. In this view, it should be noted that the EU is the world's largest single market, comprising over 450 million consumers, and it has a strong regulatory framework covering various sectors as well the administrative capability to enforce its regulations. When the EU sets regulations and standards in a specific area, companies around the world, to not be excluded by EU market, must comply with these regulations, even if they are not located in the EU. This creates a ripple effect, as companies adopt EU standards as a default for their global operations, since it becomes more cost-effective and efficient for them to adhere to a single set of rules rather than maintaining multiple standards for different markets.

Moreover, other countries and regions often emulate or align their regulations with those of the EU to facilitate trade and harmonize their markets. This is particularly true for countries seeking to access the EU market or establish trade agreements with the bloc.

The GDPR is often motioned as one of the most relevant illustration of the Brussels Effect inasmuch companies around the world have chosen to adopt GDPR-like standards to ensure compliance with EU regulations and facilitate cross-border data transfers and countries beyond

the EU have been influenced by the GDPR while designing or amending their own data protection laws. For instance, Brazil's Lei Geral de Proteção de Dados (LGPD) and California's California Consumer Privacy Act (CCPA) have incorporated elements resembling the GDPR, reflecting the global reach and impact of the EU's data protection standards.

c) *Tech companies as a proxy of power.* States can extend their digital sovereignty using the transnational socio-technological infrastructure of tech companies to pursue their objectives (Musiani et al . 2016, De Nardis 2014).

State can use companies' infrastructure to access user data otherwise out of their reach, often circumventing safeguard and guarantee established by constitutional norms and international treaties.

Companies could be also used to extend states' law enforcement capacities. For example Internet service providers and the DNS system could be employed to take down webpages spreading copyrighted materials even if the resource is not physically located within its borders (Schruers 2016).

States can utilize tech companies' infrastructure for surveillance purposes to gain access to real-time monitoring capabilities, enabling them to track individuals, monitor communications, and detect potential threats, as revealed by Snowden disclosure.

States may secure companies collaboration by law obligations. Companies are legal entities that can be incorporated and registered in a particular state. As such, they are subject to the laws and regulations of that state, even for their operation abroad. For example, the Foreign Corrupt Practices Act (FCPA), prohibits US companies from engaging in bribery of foreign officials. In our case, typically companies could be requested to grant access to data collected aboard to comply with national security or cybersecurity policies.

In addition, States could threat unwanted regulation concerning taxation, antitrust or other business model impacting obligations if companies do not collaborate with public authorities. They could also involve companies in mutual beneficial partnership.

4. The ambiguity of the digital sovereignty II: between digital constitutionalism and digital authoritarianism

The ambiguity of digital sovereignty is not limited to the fact it enables both territorialization of cyberspace and extraterritorial projections of sovereignty. As observed digital soveregnity could be conceived as a "double edge swords", meaning that it both enable both people protection and its control:

"While digital sovereignty may well be a geopolitical necessity in opposition to both foreign governments and foreign corporations, digital sovereignty also allows a government to assert enormous powers over its own citizens, and thus deserves exacting scrutiny." (Chander and Sun 2022:287).

In other words, it could be said that the concept of digital sovereignty enter in an ambiguous relationship with both the concept of digital constitutionalism and digital authoritarianism and the related processes of constitutionalization and securitization/weaponization of the cyberspace.

Digital constitutionalism may refer both to a political doctrine aiming "to establish and to ensure the existence of a normative framework for the protection of fundamental rights and the balancing of powers in the digital environment" (Celeste 2018: 13), and a constellation of concrete political initiative "that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet" (Berkman Center 2018:XX).

Digital constitutionalism may result in the process of constitutionalization of the cyberspace which occur when fundamental rights, intended as counter-institutions generalizing and re-specifying constitutional functions (Teubner 2011), are established in the digital environment. This process occurs at the interplay between the social process of technological design and the legal process of Internet-related law-making (Santaniello et al 2018), and it requires to embed digital constitutionalism principles into the socio-technical design of digital technologies, through a mix of regulation, standards, organizational practices, operational routines and technical solutions (Palladino 2021, 2021b, 2023, Celeste et al 2023).

Digital authoritarianism instead could be defined as a way of governing by asserting power, order and control through digital tools and the Internet, regardless of people freedom and international law. At a more practical level it may result in processes of securitization/weaponization of the cyberspace, consisting in surveillance and censoriship, activities, as well as in interferences in other countries to achieve political and security objectives.
As shown in Table 1, the same digital sovereignty practices may serve both digital constitutionalism and digital authoritarianism purposes, resulting in processes of constitutionalization, rather than securitarzation/weaponization of the cyberspace. Control over digital infrastructures and data flow within a country is crucial for effectively safeguarding fundamental rights and ensuring the rule of law, but it can also lead to mass surveillance and censorship policies. Similarly, de-territorialized digital sovereignty claims may serve to promote forms of 'personal digital sovereignty', or extend the reach of fundamental rights protection norms at the transnational level, as seen in the case of GDPR. However, it can also be used as a projection of states' power using tech companies as a proxy to extend the scope of mass surveillance and censorship programs, or to conduct cyber warfare operations.

Table 1: Digital Sovereignty, Constitutionalism and Authoritarianism

	Digital Constitutionalism	Digital Authoritarianism
Territorialization of Cyberspace	Effective Constitutional Right Safeguard	Surveillance
Extraterritorial Projection of Power	Transborder fundamental rights (personal digital sovereignty)	Undue Interferences, espionage, cyber warfare

In short, digital sovereignty could be considered as a necessary even if not sufficient condition for digital constitutionalism but it could also easily reverse in digital authoritarian practices. This is not true only for authoritarian countries. Even within democratic societies where already existing constitutional safeguard could be applied to the digital environment, the opaqueness of digital technologies and the necessity to transpose constitutional principles within digital socio-technical architectures to be effective may lead to systematic abuses.
Furthermore, human rights or citizen protection rhetoric may be used to justify or hidden surveillance and projection of power activities.

The above suggests that digital soveregnity should be limited by a system of check and balance…

5. Ambiguity in Practices: Territorialization of cyberspace and extraterritorial projection of power in EU, US and Chinese data sovereignty

This section aims at illustrating how states resort strategically to different digital sovereignty conceptions and practices, in such a way that give rise to conflicts and legal uncertainty, which impede cooperation to find solutions within an international legal framework, and ultimately undermine global efforts to guarantee fundamental rights in the digital environment.
To this purpose, the analysis focuses on 'data sovregnity' issue, inasmuch it appears to be the component of digital sovereignty upon which there has been an intense policy activities in the last decades and best show the processes described in the previous paragraph.
Thus we scrutinized policy initiatives on the matter from the three major geopolitical actor in the digital ecosystem US, China and European Union case, as reported in Table 2:

Table 2: Policy Initiatives Analysed

	China	USA	EU
DATA SOVEREIGNTY POLICIES	Cybersecurity Law Personal Information Protection Law Data Security Law National Intelligence Law	Stored Communication Act, Executive order 12333 Executive Order 14034 Executive Order 13971, No TikTok on Government Devices Act Cloud Act Foreign Intelligence Surveillance Act Prism and Tempora programs	NIS I e NIS II, Cybersecurity Act GDPR, DSA GAIA-X

Qualitative coding, combining deductive and inductive approaches, has been utilized to analyze the aforementioned documents. This methodological approach, as described by Saldaña (2013), allows researchers to blend predetermined coding categories with emerging themes that arise during the analysis. By employing both deductive and inductive coding, a comprehensive understanding of the data can be achieved.
To facilitate this coding process, we utilized Nvivo software (Mayring, 2019; Kaefer et al., 2015). Nvivo is a powerful qualitative data analysis tool that enables researchers to manage, organize, and analyze qualitative data efficiently. By leveraging the capabilities of Nvivo, researchers can easily code, categorize, and extract meaningful insights from the documents under study.
Deductive coding involves applying pre-existing concepts or theories to the data. In this case, we started with a set of predetermined coding categories derived from the discussion in section 2 and then they have been integrated or respecified with themes or concepts emerging from texts.

Table 3: Territorialization of cyberspace and extraterritorial projection of power in EU, US and Chinese data sovereignty

		China	USA	EU
Territorialization of Cyberspace	Data localization	Cybersecurity Law (art.37) Personal Information Protection Law (art.36, 40) Data Security Law	De facto market condition	Secondary Effect of GDPR (art. 44-50) Gaia-X
	Data Transfer Privacy Standards		Cloud Act	GDPR (Art.44-50)
	Data Transfer Security Assessment	Cybersecurity Law Personal Information Protection Law (art.36)		
	Obligation for private companies to collaborate with intelligence	National Intelligence Law (Art.7)	Stored Communication Act, Executive order 12333	
	Security assessment of foreign hardware and software	Cybersecurity Law (art.35)	Executive Order 14034	NIS I e NIS II, Cybersecurity Act
	Ban of foreign technologies	2009 Ban of Facebook, Google and Twitter	Executive Order 13971, No TikTok on Government Devices Act	EU Tik Tok ban
	Establish a legal representative in the country	Personal Information Protection Law		GDPR, DSA
Extraterritorial expansion of sovereignty	Explicit legal claim of extraterritoriality	National Intelligence Law (Art.10)	Cloud Act	GDPR (Art.3)
	Companies used as proxies (obligation to grant access to data collected abroad)	National Intelligence Law (Art.10)	Foreign Intelligence Surveillance Act (sec. 702, 704) (Prism and Tempora program) Cloud Act, Executive Order 12333	
	Data Transfer Privacy Standards		Cloud Act	GDPR
	Data Erasure/Filtering			GDPR

As shown in Table 3 all the considered cases put in place both territorialization of the cyberspace and extraterritorial expansion of sovereignty.
In particular, all of them reached some form of data localization even if through different means. Chinese resorted to legal obligations, which have been reiterated in several pieces of

legislations such as the Cybersecurity Law (art.37), the Personal Information Protection Law (art.36, 40) and the recent Data Security Law.
In the case of the European Union data localization could be considered more as a secondary effect of privacy requirements for data transfer that make for companies more convenient to store EU data locally. Indeed, GDPR's art.44-50 discipline the conditions and requirements to transfer generated in the EU territory to a third country. Data transfer could be allowed as a consequence of an 'adequacy decision' by the European Commission stating that the target country shows adequate level of data protection comparable with EU standards. Otherwise, data transfer could be permitted if data controller provides for 'appropriate safeguards' established by the Commission through 'standard data protection clauses' or 'binding corporate rules'. Only under specific conditions GDPR allow for transfers derogating from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country. The commission has recognized until now just 16 countries as providing adequate data protection. In particular, two agreement on data transfer between the EU and US, namely the Safe Harbour and Privacy Shield have been rejected by the European Court of Justice. The high level of legal uncertainty due to the complexity of the normative framework in absence of a 'adequacy decision' make for the major (US and Chinese) tech companies more attractive to keep personal data locally in the EU (Gstrein and Zwitter 2021).
In the case of US, data localization did not require any legislative intervention, but it a de facto situation due to market conditions. As observed: "The fact that the largest internet companies are based in the United States also means that data about Americans are typically stored in the United States" (Chandler and Sun 2022: 302). In its turn, this situation could be considered the result of Clinton administration's neoliberal agenda in the early nineties, which through initiatives such as the Telecommunication Act or the Digital Millennium Act, High Performance Computing Act, supported innovation and fostered inter-sectorial acquisitions and merges allowing the rise of giant companies in the information sector (Palladino 2021a). It is worth noting that as soon as a foreign platform such as TikTok gains significant traction in the domestic market, the US government has imposed a ban on its operations.

However, ban of foreign technologies and security assessment of foreign hardware and software are common practices in all the three cases.
The US government in the last few years has released an impressive amount of act in order to limit the penetration of a single foreign application. The Trump presidency signed three different executive orders (Executive Order 13942, Executive Order 13943, and Executive Order 13971) specifically targeting Tik Tok or related companies. These have been replaced by the Biden Administration Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries" to conduct an extensive evaluation of foreign-owned applications on an ongoing basis, providing regular updates to the President regarding the potential risks these applications pose to personal data and national security. On December 30, 2022, the president signed the No TikTok on Government Devices Act into law. This legislation prohibits the usage of the TikTok app on devices owned by the federal government. In the subsequent year, 34 states also implemented similar restrictions on the app.
At the beginning of the 2023 other piece of legislation was introduced at the Congress, the RESTRICT Act, which would grants the Secretary of Commerce the power to assess business transactions conducted by IT service and product vendors associated with designated "foreign adversaries" when there is a potential undue risk to national security.
Also European institutions recently adopted similar measures. In a European Parliament statement we can read: "In view of cybersecurity concerns, in particular regarding data protection and collection of data by third parties, the European Parliament has decided, in

alignment with other institutions, to suspend as from 20 March 2023, the use of the TikTok mobile application on corporate devices".
Furthermore, NIS I (Directive on Security of Network and Information Systems) and NIS II (proposed update) directives aim to enhance the overall level of cybersecurity in the EU by establishing a common framework for the protection of network and information systems. These directives primarily focus on operators of essential services (OES) and digital service providers (DSPs) and set out specific security and incident reporting obligations.
Regarding foreign hardware and software, the NIS I and NIS II directives do not explicitly address the issue in detail. However, they do emphasize the importance of risk management and security measures, which would include considering the security implications of using foreign technology components. The responsibility lies with the OES and DSPs to ensure that appropriate security measures are in place to protect their networks and systems.
The Cybersecurity Act, which came into effect in June 2019, is a regulation aimed at strengthening the EU's cybersecurity capabilities and fostering a more coordinated approach. introducing a framework for European cybersecurity certification. The certification schemes can evaluate the compliance of products with defined security requirements and standards, taking into account potential risks associated with foreign components. This helps organizations and users make informed decisions regarding the security of the technology they use.
In its turn, the Chinese government already banned major tech companies such as Google, Facebook and Twitter since 2009-2010, replacing them with national digital champions such as WeChat and Weibo, which are heavily monitored and regulated by the Chinese authorities. Although Chinese government never provided clear explanation for those bans, the 2017 Cybersecurity law offer more formal reasons to control and limit foreign technologies or to push operators to adopt domestic alternatives. Article 35 focuses on the procurement of foreign software or hardware by government agencies and "critical information infrastructure operators." It mandates that any purchased hardware or software undergoes a review by the State cybersecurity and informatization departments and relevant departments of the State Council.

Moving on the extraterritorial expansion of sovereignty we can note that both US, EU and China while vindicate digital sovereignty in their own territories, at the same time they advance explicit extraterritorial claims, recalling implicitly or explicitly to one of the international law principles we mentioned before.
So art.3 of the GDPR states that "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union".
With regard to US, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is a piece of legislation amending the Stored Communication Act (SCA), a law that while extending the protection of the Forth Amendment to online communication, establishes procedures permitting the US government to seek data from service providers for law enforcement purposes. The Cloud Act clarify that mandatory disclosure provisions under the SCA to apply extraterritorially, because the SCA reached all records in the recipient's custody or control, no matter where the materials are located. In addition to the CLOUD Act, also the Foreign Intelligence Surveillance Act (FISA) entails extraterritorial claims allowing the U.S. government to target non-U.S. persons reasonably believed to be located outside the United States for foreign intelligence purposes.
Extraterritoriality is also evoked in the art.10 of Chinese National Intelligence Law, where it says: "As necessary for their work, national intelligence work institutions are to use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad".

However, it should be considered that these extraterritorial claims of sovereignty appear to serve very different purposes. In the case of USA and China they constitute the legal basis to ensure that their national digital champions act as a proxy in enforcement, intelligence and security operations. Notably, the CLOUD Act was introduced in response to the challenges faced by the FBI when attempting to access emails belonging to U.S. citizens that were stored on a Microsoft server located in Ireland, which Microsoft declined to disclose. FISA provisions instead had been the legal basis for the "Planning Tool for Resource Integration, Synchronization, and Management" (PRISM) program a system through which the US National Security Agency (NSA) reportedly accessed data from several major technology companies, including Microsoft, Google, Apple, Facebook, and others including emails, photos, videos, and documents.

Similarly to the CLOUD Act that should be interpreted as a extraterritorial extension of a previous obligation for Internet service provider to collaborate with government authorities established in the Stored Communication Act, even the Chinese National Intelligence Law's Article 10 should be understood in conjunction with Article 7 of the same law, which states that "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law and shall protect national intelligence work secrets they are aware of." This implies that Chinese telecommunications companies operating abroad are obligated to provide data to Chinese national intelligence institutions.

On the contrary European Union extraterritorial claims of sovereignty aims to ensuring a full safeguard of European citizens rights against abuses that may be conducted by third countries' entities.

Overall speaking, as it has been noted, in the EU case "that the framework of digital sovereignty is positioned in continuity, and as a completion, of the framework of digital constitutionalism, providing the latter with a series of tools - and powers - that enable effective protection of rights" (Santaniello 2022: 50). Instead, US and China, in different ways, use digital sovereignty to conduct surveillance and intelligence operations, being closer to a digital authoritarianism model.

However this difference should not be exaggerated considering that some European Union's feature prevent European institutions from the possibility to use digital sovereignty in a mere exercise of state powers. First, EU lacks digital champions that could be used as a proxy of power to collect data, conduct intelligence operation or enforce law beyond its borders. Second, the Union has no jurisdiction in matters of intelligence and defence, as this responsibilities are instead bestowed upon individual member states, which are more likely to conduct surveillance and cyber espionage operations.

6. Conclusions: The effect of ambiguity: raising conflicts and jeopardized human rights

From the above analysis we can observe that the current landscape is animated by overlapping digital sovereignty claims that feed geopolitical conflicts and tensions.

For example, we can say that the GDPR has been in part motivated by the US mass surveillance activities against foreign countries performed by the NSA with the collaboration of American tech companies. In its turn, the US CLOUD Act, where it establishes an obligation for US firms to grant access to data stored abroad for US law enforcement authorities, may be regarded as an attempt to reassert their control over data flows.

Not by chance, the European Data Protection Supervisor has highlighted potential conflicts between GDPR and the Cloud Act suddenly after its approval (especially for art.48-49 GDPR).

Similarly, the Chinese National Intelligence Law that requires companies incorporated in China to collaborate with Chinese intelligence authorities and disclose data that may have been collected and stored abroad, has sparked concerns about the potential for Chinese intelligence agencies to conduct surveillance and espionage activities abroad, potentially infringing on the sovereignty and security of other countries, raising suspicions around Chinese technologies.
Beyond the various Tik Tok ban mentioned above, this has also been reflected for example in the withdrawal or slowdown in the adoption of Huawei 5G technologies, or in the CCTV sector.
Chinese government strongly reacted to the ban, that has been defined by the Chinese Foreign Ministry spokesperson as an abuse of power and an attack to the principles of market economy and fair competition. It is worth noting that the Chinese government has been banning Facebook, Google and Twitter since 2009 for similar reasons.

To conclude we would to point out how the ambiguous strategic use of digital sovereignty conceptions and practices by states may jeopardise fundamental rights protection in the digital ecosystem.
A first risk concerns the weaponization of privacy and data protection. This is particular evident in the case of the Chinese Personal Information Protection Law. This law indeed recall a series of very advanced privacy and data protection principle from the GDPR, but they are mostly used to constrain the operation of domestic and foreign tech companies and to prevent data transmission abroad, rather than to safeguard Chinese rights, which are still being constantly violated, also due to the many exceptions provided for public authorities in the law.
But even if we consider a more genuine attempt to protect fundamental rights such as the GDPR, we should consider that it could be successful at ensuring a full privacy safeguard only to the extent in which it is able to exert influence on transnational private tech companies. Therefore, the success of European Union depends on power relations and resources as described in the Brussels effect theory.
However, this should be considered a risk because at the international level, it replaces international law with power resources, which are an unstable terrain on which to ground human rights protection.
Nothing prevent that in the next future the Brussel effect could be replaced by a Beijing effect and tech company will forced to adapt to Chinese rules and standards, as it is already happening to some extent.
Furthermore, the climate of reciprocal allegations and retaliations caused by overlapping sovereignty claims undermine the possibility to insert privacy and data protection principles in some international treaty.
Instead, the best way for states to solidify digital sovereignty without escalating geopolitical tensions would be to use their sovereignty to engage international cooperation to reach international agreements setting basic rules to solve disputes and regulate the functioning of digital technologies.
The discussion that are currently taking place for the Global Digital Compact could be considered a good starting point to reach this goal.
But if, due to the already existing geopolitical tensions, reaching and meaningful global agreement turn out to be too ambitious, another path that could be taken into account is a deal between Western democracy (such as the Coe's Convention 108) that could also be a chance to create a truly democratic and human rights based Internet at least in one relevant region of the world.

7. Acknowledgement

Nicola Palladino has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the HUMAN+ COFUND Marie Skłodowska-Curie grant agreement No. 945447, to carry out this research.

8. References

Celeste, E., Palladino, N., Redeker, D., & Yilma, K. (2023) The Content Governance Dilemma Digital Constitutionalism, Social Media and the Search for a Global Standard. Palgrave McMillan

Celeste E. (2019): Digital constitutionalism: a new systematic theorisation, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2019.1562604

Celeste, E. (2021). Digital sovereignty in the EU: challenges and future perspectives. Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty, 211-228.

Chander, A.,and Sun, H. (2022). Sovereignty 2.0. Vanderbilt Journal of Transnational Law, 55(2), 283-324.

David R Johnson and David G Post, 'Law and borders: The rise of law in cyberspace' (1996) 48 Stanford L Rev 1367.

Gallant, Kenneth S., 'The Nationality Principle', International Criminal Jurisdiction: Whose Law Must We Obey? (New York, 2022

Gstrein, O. J. & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: promoting European values or power?. Internet Policy Review, 10(3). https://doi.org/ 10.14763/2021.3.1576

Gunter Teubner (2004) Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory? In Joerges Christian, Sand Inger-Johanne and Teubner Gunther (eds.), 2004, Transnational Governance and Constitutionalism, Hart Publishing, Oxford, p.3-28.

John P Barlow, 'A Declaration of Independence for Cyberspace' (Davos, 1996) <https:// projects.eff.org/~barlow/Declaration-Final.html> accessed 22 July 2014.

Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. EU Cyber Direct, Research in Focus series.

Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance* (pp. 268-p). New York: Palgrave Macmillan.

Palladino, N. (2021a). The role of epistemic communities in the "constitutionalization" of internet governance: The example of the European Commission High-Level Expert Group on Artificial Intelligence. *Telecommunications policy*, *45*(6), 1-15.

Palladino, N. (2021b). Imbrigliare i giganti digitali nella rete del costituzionalismo ibrido. Spunti dall'approccio europeo alla governance dell'Intelligenza artificiale. *Comunicazionepuntodoc*, (25), pp. 123-140.

Palladino, N. (2023). A 'biased'emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*, *47*(5), 102479.

Palladino, N., & Santaniello, M. (2020). Legitimacy, power, and inequalities in the multistakeholder Internet governance: Analyzing IANA transition. Springer Nature.

Redeker, D., Gill, L., & Gasser, U. (2018). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazette*, *80*(4), 302-319.

Santaniello, M. (2022). Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance. *Rivista italiana di informatica e diritto*, *4*(1), 47-51

Santaniello, M., Palladino, N., Catone, M. C., & Diana, P. (2018). The language of digital constitutionalism and the role of national parliaments. *International Communication Gazette*, *80*(4), 320-336.

Santaniello M., Palladino N. (2022) "Discourse Coalitions in Internet Governance: Shaping Global Policy by Narratives and Definitions". In: Meryem Marzouki, Andrea Calderaro. Internet Diplomacy: Shaping the Global Politics of Cyberspace. Rowman & Littlefield, 2022, ISBN: 978-1-5381-6117-3.

Schruers, M. (2016). Copyright, Information Intermediaries, and Internet Architecture. *The Turn to Infrastructure in Internet Governance*, 107-124.

Selby J., 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25 International Journal of Law and Information Technology 213;

Stephen D Krasner, Sovereignty: Organized Hypocrisy (Princeton University Press 1999) 1–42.

Teubner G (2011) Transnational fundamental rights: Horizontal effect? Netherlands Journal of Legal Philosophy 40(3): 191–215

Tsagourias N. 2015, The legal status of cyberspace, in Nicholas Tsagourias and Russell Buchan Research Handbook on International Law and Cyberspace Elgar Publishing