GENERAL ARTICLE

The Treachery of Images in the Digital Sovereignty Debate

Jukka Ruohonen[1]

Abstract

This short theoretical and argumentative essay contributes to the ongoing deliberation about the so-called digitalfug sovereignty, as pursued particularly in the European Union (EU). Drawing from classical political science literature, the essay approaches the debate through paradoxes that arise from applying classical notions of sovereignty to the digital domain. With these paradoxes and a focus on the Peace of Westphalia in 1648, the essay develops a viewpoint distinct from the conventional territorial notion of sovereignty. Accordingly, the lesson from Westphalia has more to do with the capacity of a state to govern. It is also this capacity that is argued to enable the sovereignty of individuals within the digital realm. With this viewpoint, the essay further advances another, broader, and more pressing debate on politics and democracy in the digital era.

Keywords Digital democracy · Conceptual stretching · Self-sovereignty · Westphalia · Territoriality · Strategic autonomy

1 Introduction

This theoretical and argumentative essay contributes to the debate on so-called digital sovereignty. The term "digital" is used to narrow the scope; the focus is on the Internet and particularly its so-called application layer at which much of the action occurs. This layer includes the Web, electronic mail, the domain name system, cloud computing, platforms, and so forth. The alternative term "cyber" is wider, including the global positioning system and space technologies, to name a couple of examples.

The core of the debate revolves around a question on whether and how the "digital realm" aligns with the "physical realm". No particular motivation is required for an interlocutor. The question is intriguing for each and every; robots, artificial intelligence, biomedical implants, virtual reality, and whatever else comes to your mind. But as exciting as the philosophy of mind is, it will sooner

---

✉ Jukka Ruohonen
juanruo@utu.fi

[1] University of Turku, Turku, Finland

Springer

or later face the harsh realities of political philosophy. Within these realities, the question is thorny already because all classical notions of sovereignty belong to the physical realm. These notions are much older than anything digital; sovereignty as a concept traces through the whole history of Western philosophical thought, either explicitly or implicitly. Against this backdrop, it is no real surprise that digital sovereignty has recently been actively debated both in academia and in politics. In terms of academic research, a number of recent surveys and essays already exist (Christakis 2020; Couture and Toupin 2019; Floridi 2020; Timmers 2019a). Although these have done good jobs at cataloging the terminology involved, raising important arguments, and advancing the debate in general, they have often overlooked or simplified some of the nuances, historical parallels, and political underpinnings.

Regarding the political underpinnings, digital sovereignty has long been a baton in geopolitics, with some countries using the concept in their political rhetoric seeking justify increasing state control over the Internet. In a similar vein, there has been a disparity between the political stances of the EU and the United States; digital sovereignty has been advanced by the former, whereas in the United States it has been viewed in a skeptical light (Couture and Toupin 2019). Here, again, geopolitics are involved. In Europe the debate aligns with the aspirations to gain technological independence and resilience.

As the digital and physical realms increasingly intervene, not only are economic interests present but the geopolitical dimension extends toward security and defense, which, in particular, within the EU, are often debated by using a related but still distinct concept of strategic autonomy. Given that sovereignty alone is a conceptual bonanza—there are at least sixteen different notions of the concept (Christakis 2020), strategic autonomy can be reasonably excluded from the paper's scope, although—and importantly, it can be also seen as a way to achieve digital sovereignty (Timmers 2019b). Recently, for better or worse, sovereignty as a concept seems to have also lost to strategic autonomy particularly in the European security and defense debates (Rahman 2021). In other words, at the moment—and like in the past, a fully sovereign European solution does not seem plausible in this policy space without the transatlantic link. But even when excluding strategic autonomy, more restrictions are needed to distinguish the paper from the existing literature surveys and essays. What, then, to further exclude or include? For the paper's purposes, a sensible answer can be found from the following simple quotation:

> Finally, the EU is pursuing a tech industrial policy under the strategically—and morally—ambiguous heading of 'digital sovereignty.' Proponents of the concept toggle breezily between two definitions of 'sovereignty.' One is based on human-centered autonomy—each individual citizen is personally sovereign over their data, interactions with AI, etc. The other is a more Westphalian understanding of sovereignty: each state has an undisputed power monopoly within its borders. (Barker 2020)

When putting the political points aside—and also keeping in mind that the quotation supposedly reflects a sentiment held in some parts of the national security

apparatus of the United States, the quotation's value stems from its pertinence to concisely frame the two core tenets in the digital sovereignty debate. Thus, in what follows, the explicit framing contains human-centered autonomy on the one hand and autonomy of states within their territories on the other hand. Within the polemical style, there is also a further, implicit framing in the quotation. This frame is located in the claim that participants in the debate can "toggle breezily" between the two parts in the explicit frame. As will be elaborated, this alleged breeze leads to interesting theoretical paradoxes. For motivating these paradoxes, one only needs to ask: how can there be individual autonomy in the digital realm within which undisputed power exists neither within nor between states? The answer, as will be argued, has to do with authority and power to which sovereignty is unavoidably linked. Authority, in turn, requires a philosophical rather than a technological perspective, although, as the essay proceeds, some technical examples must be provided for illustrative purposes.

Even though the essay is theoretical, furthermore, some analytical tools are still required. Like the debate in politics, the academic and engineering side of the digital sovereignty debate can be read as a deliberation process. To read such a process and to further participate in the deliberation, classical yet analytical tools in political science provide a useful way forward (Steiner 2008). Thus, in what follows, a few of the main points in the debate are recapitulated by trying to reflect upon the images others have seen about digital sovereignty, and by trying to turn these reflections into new theoretical images.

But before proceeding, a few passages must be written about the analytical tools mentioned. After these methodological notes, the paper's structure is simple: the two themes—the territorial sovereignty and human-centered autonomy—are discussed in their consecutive sections. The former theme is discussed by focusing on classical definitions for state sovereignty, transborder access to digital assets and data protection laws, cyber war, and the role of large information technology companies. The Peace of Westphalia, the Holy Roman Empire, and the East India Company are used as historical parallels for elaborating the discussion. The second theme, in turn, is discussed by focusing on conflict theories and liberalism, following classical Western political philosophy. To address the paradoxes arising from the alignment of the two realms, international law, data protection, surveillance, large companies, and digital infrastructures are elaborated in conjunction with the political philosophy tenets. After these two sections, a few reflections and a concluding section follow.

2 Miscomparisons

What is a miscomparison? It is easy to say what it is not. It is not one of the fallacies commonly appearing in debates. Nor is it one of the common vices of argumentation (Aberdein 2016) to which so many weak minds are vulnerable (Laroche et al. 2018). To give a practical example: during his heyday, one famous Finnish populist pen introduced a number of brilliant comparative sayings from his Moomin pencil box. For instance: whenever "a melon and an apple each wear the same size baseball cap, everyone can see that just doesn't work" (Watts and Mamudi 2011). Although

no one still knows to whom or to what the melon (Germany?) and the apple (Finland?) exactly referred, there is a grain of wisdom in the quote, perhaps. Both melons and apples are delicious fruits. Therefore, they should be comparable. However, the method of the comparison, the baseball cap, is an awry technique for the task. Therefore, "that just doesn't work".

As it happens, this kind of a faulty reasoning is exactly what Sartori (1991) famously discussed with his miscomparison framework involving dichotomous concepts and their theoretical underpinnings. A classical example of such concepts is the notorious friend-enemy framework of the notorious Carl Schmitt, as also analyzed by Sartori (1989). Further examples are not difficult to imagine: true and false, zero and one, center and periphery, security and insecurity, war and peace, and so forth and so on. In a series of papers starting from the 1970s, Sartori also developed various means to identify miscomparisons often associated with such dichotomies. These have been frequently used to discuss different comparison problems (see, e.g., Ahram 2011; Daly 2003). Following Sartori's work (1970,1991), four such means are typically discussed in the literature.

The first is *parochialism*: typically a case study that simply ignores any categories postulated by general theories and comparative frameworks. When further accompanied with custom ad-hoc terminology and general intellectual laziness, a miscomparison often occurs in the form of a mislabel. Mislabeling is often accompanied with the second common error, *misclassification*, typically caused by conceptual orderings that are derived from a single criterion. If fruits are again classified with the baseball cap, a fruit-fruit-fruit could result from classifying a melon, an apple, and a snowberry; however, under a different classification scheme, a eatable-uneatable could result as snowberries are poisonous to humans. In other words, there are two problems here: choosing the reference baskets and putting the fruits into the right baskets. As we shall see in a moment, there are many digital sovereignty baskets, and it is not at all clear into which particular basket which particular fruit should go. Sometimes, "that just doesn't work".

The third typical error, "*degreeism*", stems from operationalization of theoretical concepts and quantitative variables. Its essence is a belief that continuous variables and continuum-based concepts are preferable over variables or concepts with a dichotomous or an ordinal scale. There are situations for which continuum-based concepts are well-suited. For instance, hybrid warfare may blur the boundaries between military and civilian and covert and overt; propaganda spread on a private platform may blur the boundary between real and unreal; and so on (cf. Chong 2014; Moskalenko and Streltsov 2017; Ruohonen 2020a, 2021). In these cases it is not necessarily meaningful to operate with strict theoretical dichotomies. However, there are problems as well. As there are seldom perfect things, all essentially dichotomous concepts become imperfect without some arbitrary threshold turning the concepts back into their dichotomous forms. Sartori (1991) asks: what is a "80 percent democracy"? The question is non-trivial. Clearly, there are no perfect democracies, but, at some point, a threshold is required to distinguish democracies from other forms of government.

The fourth error, or a problem, is *conceptual stretching*, or, depending on a situation, conceptual shrinking. In essence: whenever a concept is stretched too much,

it starts to mean everything and thus nothing (Steiner 2008). In other words, social sciences, in particular, require broad universal concepts—public, private, military, civilian, war, peace, democracy, justice, etc.—yet these frequently turn into amorphous conceptualization that are difficult to operate with and to measure (Sartori 1970). But, here, please take a note: with this simple statement, a lazy, undiscerning mind may have already committed itself to parochialism; nowhere is it stated that a difficulty would imply an impossibility (cf. WJP 2020). Likewise, it should be stressed that conceptual stretching is often necessary when a new phenomenon is initially conceptualized and theorized. From this perspective, the digital sovereignty debate can be seen as an attempt to apply a classical concept to the digital realm. Here, the risk is that the attempt goes awry; sovereignty as a concept is stretched too much, such that it starts to lose its qualifying characteristics. The consequence would be a miscomparison. Although the four concepts are simple and the coverage could be extended further, they retain their powerfulness particularly for approaching theoretical concepts—and, if anything, digital sovereignty is a still a vague and emerging theoretical concept.

3 The Peace of Westphalia as a Historical Parallel

The year 1648 haunts everyone participating in the current Internet governance and digital sovereignty debate. But why is something that happened 373 ago relevant for the debate? In 1648 the Peace of Westphalia was signed. It ended the war that for thirty years had caused misery in Europe. Later on, much later on, this peace treaty has been allegedly identified as the beginning of the contemporary international system. Therefore, it also belongs to the identity of international relations that study this system, the kernel of which is based on the concept of sovereignty, and particularly the notion that each state is sovereign within its own territory.

But sovereignty itself is a much older concept. From ancient Rome through the medieval times to the Age of Enlightenment, sovereignty was essentially framed as a question about the power of a ruler, the sovereign, over its subordinates. Bodin, Hobbes, Locke, and Rousseau; from divinity to the concept of popular sovereignty, a ruler who rules with the consent of people. Here, a dichotomous distinction between public and private is important: regardless whether the legitimacy of the rule is based on divinity or consent, a sovereign represents the public instead of the private interests (Fukuyama 2015, p. 73). But there is more: "on a given territory only one state can have sovereignty, that is, supreme authority, and that no other state has the right to perform governmental acts on its territory without its consent" (Morgenthau 1949, p. 245). But with respect to the digital sovereignty debate, is there a paradox, a treachery in this image and where is it?

Clearly, another keyword here is territory. Actually, it can be argued that territory, whether real or (and) imagined by its occupants—a non-trivial distinction, is the only solid yet continuously moving boundary line for sovereignty; without it there would not be a sovereign according to many classical theorists (Lombardo 2015, pp. 71–74; for the imaged part cf. also Anderson 1991). This argument opens the door for conventional criticism about digital sovereignty: because the digital realm does

not follow geographic borders, there cannot be a supreme authority over the realm (cf. Mueller 2019). While not fool-proof, this criticism has its philosophical merits. But it is not where the image's treachery is located. Do you see it already? Correct: it is in the quotation's second sentence claiming that no other state can, without a consent, exert power in a territory of another sovereign state.

The late 2010s digital ping pong across the Atlantic provides one of the means with which the definition quoted can be criticized. The game played is also good drama. Particularly jolly are the frequent episodes depicting the players swinging in slow motion even though the ball has been taken away from them; namely, by Schrems (I) in 2015 and Schrems (II) in 2020. The latter case annulled the so-called Privacy Shield arrangement on transatlantic digital data transfers, which had been established to replace the so-called Safe Harbor arrangement that the former case had destroyed. In terms of sovereignty, the former case is particularly relevant as the corresponding court decision emphasized the supreme authority of national data protection authorities with respect to the European Commission on one hand and with respect to the states outside of the supranational union on the other. Thus, in essence, both the legal and institutional bases were questionable for the Commission to use its power to make the two decisions over transatlantic data flows (for a thorough treatment of the current situation see Christakis and Terpan 2021). But there is more.

With respect to ping, extraterritorial power—the ability of a sovereign to exert governmental actions in another sovereign's realm without its consent—has long been a part of ping's data protection legislation. Already before the General Data Protection Regulation (GDPR), the extraterritorial reach was specified in Directive 95/46/EC, and contested in the famous Google Spain case (Kindt 2016). It was also the GDPR's sharpened extraterritoriality provisions that provoked many critical comments from pong. That said, the same year the GDPR came into force, pong passed its Clarifying Lawful Overseas Use of Data Act (CLOUD Act). It provides pong's authorities access to data stored in cloud services without the cumbersome mutual assistance treaty, effectively deprecating ping's people constitutional protections provided by a jurisdiction where the data is stored (see Siry 2019; and Osula 2015 for an international law perspective). The same goes for the spicier cases; the mass surveillance programs with which a country bypasses another country's laws due to the borderless nature of the Internet. Snowden was merely a case; the show must go on, for both justifiable and unjustifiable reasons (cf. BBC 2021). From a theoretical point of view, these examples exemplify how supreme authorities are trying to align themselves and their jurisdictions with technology by using conceptual stretching, and bypassing international norms and laws along the way—as there is no way to conduct allegedly nearly global mass surveillance otherwise. As noted, however, every coin has two sides; transborder access to digital assets is also an important tool in criminal investigations.

Sovereignty as a concept is "plastic and evolving" (Mueller 2020) to all directions; as it has always done, sovereignty transforms and expands. However, the transformations through the stretching have clearly led to paradoxes. Besides (a) the misplaced authority of the Commission over the decisions, which, in retrospect, can be interpreted as a theoretical miscomparison regarding sovereign power, (b)

the CLOUD Act demonstrates that the EU's complete territorial sovereignty over its citizens' personal data has been legally challenged by the United States even without the two Schrems decisions. Nor is the analogy of a ping-pong game by accident; (c) the ongoing sequence of events in the transatlantic data protection game demonstrates also the strategic element present in the digital sovereignty affair. When one state stretches sovereignty, other states respond with their own stretching, shrinking, or something else. The data protection example further (d) illustrates how the paper's two themes—territorial sovereignty and human autonomy—are theoretically connected. From this perspective, the EU's data protection strategy ever since the 1990s can be also interpreted as an attempt to provide autonomy for Europeans over their own data. If strategy as a concept carries cynical connotations, as it often does in politics, a rephrasing is easily available: the attempt can be seen as a milestone in the efforts to establish human rights in the digital realm. But reaching such a milestone seems to imply theoretically difficult and practically contested conceptual stretching of territorial sovereignty.

After this detour, it is worth returning to 1648 in which the Thirty Years' War ended. Three points are relevant for the digital sovereignty debate. First, there is a debate about whether the peace treaty established the system of international relations we know today. There are both proponents (Philpott 1999) and opponents (Osiander 2001; Sen 2012). The debate has also been seized to argue that there cannot be sovereignty in the digital realm (Mueller 2019). But are we seeing the same historical image? It was not the only war. At the same time, the Eighty Years' War raged, having started from Spain's attempt in the 1560s to crush the revolts in the Netherlands. The longevity of these conflicts is astonishing for a today's reader. Indeed, alongside military *innovations*, the perhaps most striking element in the conflicts was the *capacity* of the states to engage in active warfare, year after year and decade after decade, and to bear the burdens of the wars, including the extreme human losses and financial costs. What the Westphalian settlement brought was at least some religious and political *balance* across the Holy Roman Empire whose imperial power was limited but not entirely eliminated. (Kennedy 1989, pp. 40–93.) Although the settlement's relation to territorial sovereignty may be disputed, state capacity and balance of power are still key concepts in international relations. So is what threatens sovereignty, war.

Second, innovations and capacity, but not balance, characterize also today's digital conflicts between states (Ruohonen 2020b). Even though different states have different stances on these conflicts just as they have different positions on digital sovereignty (Chong 2014; Couture and Toupin 2019; Mueller 2019), what seems clear is that the line between war and peace is becoming foggy in the digital realm, or that it has already become blurry. Warfare in the digital realm may be a myth (Gartzke 2013), or it may be that obscurity prevents seeing the treachery of the image. But we can read, and by reading we can learn that while a "policy of ambiguity and silence" has been common, at least some states have agreed that sovereignty applies in the digital realm together with Article 51 of the Charter of the United Nations (Moynihan 2019). This article defines a right to self-defense for a state or a collective of states in case of an armed attack. An armed attack is a direct violation of a state's sovereignty in a territory. But it has

already been noted that the digital realm is not bound to territories, and, hence, in theoretical terms, there cannot be armed conflicts in the realm. The theoretical paradox is thus clear. For addressing this quagmire, recent discussion has contemplated about thresholds for attacks in the digital realm (Assaf et al. 2020; Pawlak et al. 2020). Against this backdrop, it is possible to continue with another miscomparison involving the apparent presence of degreeism. What is a "90 percent peace" or a "10 percent war"? Is parochialism further present? Maybe it is not war *or* peace but war *and* peace?

Third, the peace of Westphalia is important for understanding the historical developments behind the notion of a modern state in Germany and elsewhere. Before the peace, during the long and rancorous politico-religious war, which was partially fueled by the invention of the printing press that led to the invention of modern propaganda, there were hundreds of sovereigns in Germany, nominally united by the transnational Holy Roman Empire. None of the sovereigns possessed the capacity of a state. They had no monopoly of force in their territories. Their administrations were weak; they were even unable to raise professional armies through systematic taxing of their territories. Instead, their wars, were fought by mercenaries hired with borrowed money, and when money ran short, the mercenaries turned to raiding and looting. The Peace of Westphalia brought the impetus for a change. In a course of about hundred years, the independent militias were disbanded, financial control was established through a common bureaucracy, and military authority was centralized. Army and bureaucracy were the innovations. (Fukuyama 2015, pp. 67–70; Graham 2011.) In terms of balance of power, the reduction in the number of European players eventually followed (Morgenthau 1949, p. 270), as did the principle of non-intervention into states' territorial sovereignty (Philpott 1999). In addition to the relevance for the history of international relations, the Holy Roman Empire provides a useful historical parallel; in some parts and to some extent, it can be used to reflect the state of the European Union as well as the state of the Internet (for the latter see Gurri and Roberts 2020). For the present purposes, however, the lesson from Westphalia has more to do with the capacity of a state to rule than with the territorial notion of sovereignty. It is this lesson that the criticism of digital sovereignty tends to miss—or, intentionally or unintentionally, obscure due to parochialism of thinking.

There is also another lesson closely related to Westphalia. When fast-forwarding in time, it is possible to find another kind of a sovereign via conceptual stretching. That is, a private company raging private or quasi-private wars to advance commercial goals; and, again, military innovation and the capacity to exert power, but not balance, were present just as sovereignty was (Robins 2002; Sen 2012). While the East India Company was eventually dissolved, certain parallels are present with our times. In someone else's words:

> Sadder still to think that if this is a new realm of national sovereignty then our existing nation-state world order is just simply not able to engage with the new IT corporate nation-states in any manner that can curb their overarching power to defend their chosen borders. The 1648 Peace of Westphalia has much to teach us, and not all of the lesson is pleasant. (Huston 2020)

As is often the case with history, a sense of irony is present: states and international organizations greatly contributed to the expansion of the digital realm throughout the 20th century (Cortada 2012, pp. 571–599), but they, willingly or unwillingly, lost their control during the early 21th century. Again via conceptual stretching, it is possible to argue that a new form of sovereignty emerged in the realm, a "de facto digital corporate sovereignty" (Floridi 2020). Unlike the East India Company, the new digital corporate sovereignty is not geographically bound, which is again paradoxical because states and the legitimacy for their power are still largely dependent on territories. But now, in 2021, it seems undisputed that states are nevertheless determined to fight back, partially due to the many unforeseen consequences from the loss of control, and partially due to other states who retained their control. The task is easier said than done. But before briefly contemplating about obstacles, the other side in the debate, the human-centered autonomy, should be tackled. As the task is formidable, in what follows, the broader digital sovereignty debate again frames the discussion and deliberation.

4 Toward Human Autonomy in the Digital Realm

For lack of a better term, let "digital self-sovereignty" describe the autonomy of individuals in the digital realm. Think of it as a superset to which different sovereignty-related subsets belong. The most important subset is the autonomy of individuals vis-à-vis a sovereign, the supreme authority—or authorities if one adopts the viewpoint that there are no territorial sovereignties in the digital realm.

Here, again, we are confronted with centuries of thought. For Hobbes, writing three years after the Peace of Westphalia, during the English Civil War, an absolute sovereign was needed because otherwise everyone would be in a war against each other. For later theoretical extremists such as Schmitt, in particular, it was precisely this state of anarchy, where everyone is a *lupus*, a wolf, to one another, that revealed the true essence of politics, which, according to Schmitt, cannot be tamed by liberalism (Sartori 1989). This philosophical anarchy was also later hijacked to describe the international relations between states, and, by extension, state actors in the digital realm, although the pirating was not entirely accurate because for Hobbes the anarchy was between individuals and not states (Christov 2017; Ruohonen 2020b). For this reason and other reasons, we must look elsewhere to attach our thought. To do so, we again fast-forward in time.

In the early 19th century, Constant, during the Napoleonic Wars and their terror, published a set of principles for "all governments". By attacking Hobbes directly, he advocated popular sovereignty but was eager to limit its power against individuals—as power is evil and dangerous, it was to be constrained by institutions and individual freedoms, among them the freedom of thought, as it was also language through which despotism triumphed (Garsten 2012; Rosenblatt 2018, pp. 65–67). From this, we can crystallize the first subset of the superset as the rule of law, which, among other things, limits politics and power by law. Then, individuals can pool "their self-sovereignties (sovereignty on themselves) through deliberation, negotiation, and voting, to create popular sovereignty, which then legitimises national sovereignty,

which then controls individuals' legal exercise of their self-sovereignties" (Floridi 2020, p. 375). But as beautiful as this idea is, and despite the optimism expressed by some (Noveck and Cerf 2020), the deliberation required for digital self-sovereignty can hardly be argued to work properly. Hence, also the creation of a popular sovereignty remains incomplete, which then transforms into a partial delegitimization of a national sovereignty, which then transforms to a partial deprecation of individuals' self-sovereignties.

Why is the digital self-sovereignty not working? To answer to the question, we need to look for other subsets, for other freedoms Constant and his later followers put forward. From the Universal Declaration of Human Rights we can find many of the necessities for digital self-sovereignty, among them the rule of law provisions, the freedom of thought, and the right to privacy and honor. These can be further extended, as the EU has done with its right to data protection, the basis of the GDPR, for instance. Thus, all the ingredients are there—international law, human rights, and so forth; yet it is not working. To seek for a partial explanation, the Thirty Years' War again provides a useful historical parallel; there were bandits pillaging, wars that seemed eternal, and sovereigns who were not states. Thus, the analogy with the current digital realm is clear, whether the context is cyber warfare or the ongoing online information disorder (cf. Ruohonen 2020b, 2021). Earlier, we also noted the rivalry between ping and pong. The same rivalry applies to privacy legislations, although their positions are not necessarily too far apart (Büyüksagis 2019; Christakis and Terpan 2021). From ping's experience we can also learn how difficult it is to enforce the rule of law in the digital realm, at least at short notice, as the GDPR's early enforcement problems demonstrate (Ruohonen and Hjerppe 2020). From the lesson of Westphalia we learned that it took almost a hundred years or so for a change to occur. Indeed, not all of the lesson is pleasant. Maybe it is Hobbes instead of Constant after all; conflicts and anarchy instead of liberalism and rights?

Are there more paradoxes? The functioning of the Internet is often described with the so-called Open Systems Interconnection (OSI) model (see, e.g., Kurose and Ross 2008). Although it has never entirely accurately described the reality, it is a useful analytical framework akin to the concept of ideal types in social sciences. The model has seven layers; the lower a layer is located, the more low-level the technical details. As said, much of the action visible to end-users occurs at the seventh layer, at the application layer. It is also this layer through which individuals express their digital self-sovereignties. But it is the third layer, the network layer, that is fundamental to the functioning of the Internet. Regarding this layer, some have recently expressed fears that changes, such as regulation, at the application layer will spill over to the network layer, or that new protocols will be rolled out for this layer, potentially causing unintended changes and fragmentation (O'Hara and Hall 2020; Mueller 2020). While such fears—rational or irrational as they may be—reflect the critical side in the digital sovereignty debate, there should be no reason to shy away from also acknowledging the current problems, such as well-known issues with routing (Hesselman et al. 2020; Testart et al. 2019). To some degree, conceptual shrinking is present; the debate is directed toward narrow technical topics.

In the big picture, in contrast—and besides the mass surveillance programs supposedly operating already at the network layer or below, it is increasingly difficult

to separate different layers due to the East India Companies who provide everything from fiber to applications. Centralization follows (cf. Moura et al. 2020). By implication, it is not clear whether the OSI model is applicable for the digital sovereignty debate. In addition to companies' technical strong-arm over sovereignty, they also control and govern, without the rule of law, the rights and freedoms, and, thus, individuals' self-sovereignties, which provide the popular sovereignties, which transform to national (territorial) sovereignties.

Data is a further subset in the superset. Ever since the 1983 decision of the German constitutional court, the European perspective has relied on information self-determination; personal data belongs to a person from whom it was extracted. Yet, in terms of self-sovereignty in the digital realm, the bargain has long been about "selling your soul while negotiating the conditions" (Belli et al. 2017), a phrasing that refers to the dubiousness of consenting to the conditions of digital services and applications. For this reason, the GDPR, like other emerging legislations (Tunney 2020), have moved, or at least have tried to move, away from consent as a single mechanism for the rule of law in this context. At the same time, in Europe, there has been a trend toward strengthening self-sovereignty through voluntary data-sharing that benefits also the economy.

Here, too, the image suffers from a paradox; do they understand, when they sell their souls for voluntary data sharing? A thorough literature search of empirical studies is not necessary to put forward an answer that most of them do not understand what they are consenting to (for the background of this privacy paradox see, e.g., Norberg et al. 2007). There are no reasons to suspect that this claim would be different for altruistic data-sharing. While the goals are noble, masquerading as empowerment and agency, there has thus been a tension between those who portray self-sovereignty through consumerism and those who value citizenship and rights (Lehtiniemi and Haapoja 2020). Further issues are easy to pinpoint. Particularly in the industrial setting, data sovereignty has been understood to mean that you own and can control your own data; you own and can control the data that your machinery in your factory continuously produces (Jarke 2020). But there are also employees in your factory who increasingly generate data on their own when working with your machinery in your factory. Who owns such data related to the means of production? Answers to the question remain open.

There is also a red flag in the digital sovereignty debate, data localization. While it lingered in European policy circles throughout the 2010s, often in disguise (Celeste and Fabbrini 2020), recent large-scale projects, such GAIA-X, the pan-European cloud computing framework, have poured gasoline to the fires kept by those critical to data localization. In general, the technical details (cf. Hesselman et al. 2020) are still too vague to make any definite conclusions; therefore, it suffices to merely point out the critical arguments that data localization in itself does not guarantee self-sovereignty in terms of security and privacy of personal data (Komaitis 2017). Regardless whichever side one takes in this debate, the theoretical underpinning is essentially again about the intervening and alignment of the two realms. Finally, it is worth noting a point that national and transnational digital infrastructure projects can also be portrayed as an attempt to build imagined national (European) digital identities in the new digital era (Möllers 2021). Here, again, the

Holy Roman Empire, the peace of Westphalia, the later age of great powers, and the East India Company provide good historical parallels because nationalism and national identities emerged much later in many European countries. By and large, although not everywhere, the modern nation-states and their supranational unions were also forged on anvils of war.

5 Reflections

This short theoretical essay asked us to think and participate in the debate on digital sovereignty. It urged us to reflect upon the treacheries of images, including the implicit political dogmas and academic miscomparisons. We did so. But what did we see? Together, hopefully, we saw some important reflections, and beyond. To briefly summarize the paradoxes arising from different miscomparisons, it is clear that classical definitions of state sovereignty, such as the one provided by Morgenthau (1949), align only poorly with the digital realm. The GDPR and the CLOUD Act together provide a good example in this regard; theoretically, these can be seen to stretch and shrink, respectively, the territorial notion of sovereignty. Stretching of the concept seems also necessary in order to achieve digital sovereignty for the subordinates of a democratic state sovereign. But such stretching is difficult even among democracies due to international relations that are still largely based on Westphalian and later ideas about territorial boundaries. Given these reasons and the paradoxes elaborated, strategic autonomy seems a better concept theoretically.

The same applies to state power, which, too, at least thus far, is ultimately territorial with respect to both other states and the subordinates within states. Here lies the crux of the paper's contribution to the digital sovereignty debate. For the early utopian theorists, such as Barlow (1996), the cyber space was a sovereign space by itself, but since there was no authority, no Leviathan, which is required for sovereignty as a theoretical construct without losing its qualifying characteristics, the discourse was later hijacked by "realists" who perceived the cyber space as an anarchy akin to Hobbes, Schmitt, and other conflict theorists (cf. Mueller 2019). The fundamental theoretical paradox is that much of Western philosophical thought has been either intentionally or inexpertly skipped with this utopian-realist parochialism. Among these omissions is liberalism together with international law and norms. If there is only a sovereign space without a sovereign authority, can there be freedom, liberty, human rights, democracy, etc., and can these even survive in such a space? The peace of Westphalia has three painful lessons for a deliberation about this question.

The first is administration—and not "governance". To rule—to move from the "code is law" idiom to a "law is code" notion (Timmers 2019a), is to have a well-functioning administration, a bureaucracy that ultimately enforces the Weber's definition for the monopoly of force. (To avoid dogmas, it should be added that no one participating in the debate has advocated anything like Weber's iron cage of bureaucracy.) In addition, the collective decisions made must be legitimate and overrule all other decisions, and they cannot provide an exit in a sense that they would not cover a whole territory and its population. These are lessons from the Peace of Westphalia.

With these lessons the concept of sovereignty, as well as the concept of politics, is expanded to something different than what territory and morality can provide. When taken to the theoretical extreme, the concept of sovereignty transforms into a sovereign as an exception (Sartori 1989), and it has always been the rule of law that constraints sovereignty as an exception, as well as the Hobbesian anarchy. If anything, the lessons from Westphalia are also lessons about warfare. Therefore, territorial sovereignty cannot be ignored. Unfortunately, there are no easy answers to a question about how the digital realm, law, and territory could be combined; one option would be to extend sovereignty to cover administration, such that interference with a state's core decision-making processes would violate law (Midson 2014). But what is a core decision-making process? In a democracy digital deliberation is, and must be, open and public, and, therefore, it is also vulnerable to new threats such as disinformation. Even though there are again no easy answers on the horizon, our reflection pointed toward digital self-sovereignties of individuals, which, in a democracy, are directly related to popular sovereignty, which is related to administration, which is related to other things. In this difficult puzzle the different pieces reinforce each other.

But the fundamental problem is that the pieces are not reinforced together in the puzzle. In the big picture, there are three problems. None of these have easy answers. First, the technical Internet community, including standardization organizations, committees, and talkshops, is unlikely to be able to solve the problems alone (O'Hara and Hall 2020). Nor is it clear whether the community's views reflect the views of the self-sovereigns in the Internet. Aligning the community with the global civil society community might be an option, but the latter seems to too fragmented, lacking sufficient political legitimacy and thus power. Further alignment is required. But this alignment brings the second problem: the international relations, power politics, and, more or less, anarchy. In this context it seems again appropriate to quote someone else:

> International law is a decentralized legal order in a dual sense. In the first place, its rules are, as a matter of principle, binding only upon those states which have consented to them. In the second place, many of the rules that are binding by virtue of the consent given are so vague and ambiguous and so qualified by conditions and reservations as to allow the individual states a very great degree of freedom of action whenever they are called upon to comply with a rule of international law. (Morgenthau 1949, p. 244)

This quotation summarizes many points in our reflection. There is again the concept of consent. Not everyone consents, whether they are states or self-sovereign individuals and East India Companies. Then there are the leeway and ambiguity so typical to international arrangements, whether laws or norms. Particularly in the digital realm, the international arrangements are often a bizarre "*shadow theater*" carefully constructed by those states who benefit from the *status quo* (Tikk and Kerttunen 2018), or want to benefit from it, or simply do not care. When stretched a little, the quotation can be read also as a statement about enforcing laws in the digital realm. If the word international is replaced with the word regional, the quotation could also describe some laws enacted in the European Union. Despite rigorous

legal safeguards and frameworks established in Europe, including the GDPR and associated laws, state surveillance has continued alongside commercial surveillance. While controlling the latter through the power granted by the EU's internal market is difficult but still possible, the former seems to be generally beyond the power of the EU and its institutions. Irrespective of several high-profile cases fought and won in the highest European courts, national security concerns have kept surveillance capabilities firmly on the table. A good example would be data localization and its relation to data retention laws enacted—and systematically violated—throughout Europe (for the background see Albrecht 2020; Grabowska-Moroz 2020). Thus, to some extent, a miscomparison is present; the degree of freedom for states to comply with international law applies also to the EU and its member states. Not all laws are equal and not all laws are enforced with the same vigor; here we have the eternal lesson about law-making—laws that are not laws are mere norms.

The third and final problem is the most important. It is about functioning of political systems. Without functioning systems, whether democratic or something else, it is impossible to solve the previous two problems, provided that there is political will to solve them. At minimum, a functioning democratic political system requires a well-functioning tripod: the state, the rule of law, and political accountability, each reinforcing each other (Fukuyama 2015, pp. 532–534). Today, technology should be perhaps added to the rack as a fourth item, a well-functioning technology, that is. By implication, the urge, if not pressure, for the world's tripods to work with technology-makers is increasing day by day (Schneier 2020). But there is more. Political accountability implies that the output from a political system is legitimate. For an output to be legitimate, there must be also input to a democratic political system. The input cannot be from technology-makers alone. Nor cannot it occur only through elections. Deliberation is required by informed citizens. For deliberation to work, the voice of everyone affected by a particular policy should be heard; however, the input only qualifies as valid input when it is backed by qualified reason rather than pure self-interest, force, or manipulation (Gaus et al. 2020). Deliberation further requires public channels in order to deliver inputs to sovereigns who represent the public interests. Disinformation and related information warfare tactics can effectively destroy such delivery channels. For these and related reasons, the self-sovereignty umbrella concept sketched should not be taken lightly—even if further theorization is required to sharpen the concept.

6 Conclusion

This theoretical essay addressed digital sovereignty by focusing on its territorial and human-centered aspects. The primary conclusion is clear and simple: as a theoretical concept, sovereignty aligns poorly with the digital realm, including the Internet. The main reason is the concept's close ties to territoriality and geographic boundaries of states, their supranational unions, and their alliances. In many respects, international law and related aspects rely on the same boundaries. This reliance on geography makes it also difficult to achieve human-centered autonomy in the digital

realm; because there is no supreme authority in the realm, it is difficult to enact and particularly enforce laws in the realm.

Attempts to overcome the difficulty has resulted different theoretical paradoxes, whether in terms of surveillance, transborder access to digital assets, or recent data protection laws, which all tend to contradict the classical territorial notion of state sovereignty. Several historical parallels can be used to illustrate these paradoxes. Among these are the famous peace of Westphalia and the Holy Roman Empire. In addition, the equally famous East India Company provides an interesting albeit not perfect historical parallel for the concept of digital corporate sovereignty. Further paradoxes emerge with the human-centered autonomy: the famous privacy paradox, the ownership of data, the vagueness of consent for data protection and privacy, surveillance, and the complex relation between data localization, data retention, and digital self-sovereignty. Through the historical parallels, the argument put forward is simple: to move forward, to at least partially address the paradoxes and their practical political ramifications, efficient administration is necessary alongside finding and theorizing new openings that go beyond the simplification of realism and utopianism. Pioneering new ideas is arguably also necessary to advance democracy in the new digital era.

References

Aberdein, A. (2016). The vices of argument. *Topoi*, *35*, 413–422.

Ahram, A. I. (2011). Concepts and measurement in multimethod research. *Political Research Quarterly*, *66*(2), 280–291.

Albrecht, H. (2020). Data, data banks and security. *European Journal for Security Research*, *5*, 6–23.

Anderson, B. (1991). *Imagined communities: Reflections on the origin and spread of nationalism*. London: Verso.

Assaf, A., Moshnikov, D., et al. (2020). Contesting sovereignty in cyberspace. *International Cybersecurity Law Review*, *1*, 115–124.

Barker, T. (2020). Europe can't win the tech war it just started: The European Union is running in circles in pursuit of "Digital Sovereignty". Foreign Policy. https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/. Accessed December 2020.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*, https://www.eff.org/cyberspace-independence. Accessed June 2021.

BBC (2021). NSA Spying Row: Denmark accused of helping US spy on European officials. https://www.bbc.com/news/world-europe-57302806. Accessed June 2021

Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: From notice and consent to data control by design. *Health and Technology*, *7*, 453–467.

Büyüksagis, E. (2019). Towards a transatlantic concept of data privacy. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *30*(1), 139–222.

Celeste, E., & Fabbrini, F. (2020). Competing jurisdictions: Data privacy across the borders. In T. Lynn, J. G. Mooney, L. van der Werff, & G. Fox (Eds.), *Data privacy and trust in cloud computing: Building trust in the cloud through assurance and accountability* (pp. 43–58). Cham: Palgrave Macmillan.

Chong, A. (2014). Information warfare? The case for an Asian perspective on information operations. *Armed Forces & Society*, *40*(4), 599–624.

Christakis, T. (2020). 'European digital sovereignty': Successfully navigating between the 'Brussels Effect' and Europe's quest for strategic autonomy. archived manuscript. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098. Accessed March 2020.

Christakis, T., & Terpan, F. (2021). EU–US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options. *International Data Privacy Law*, *2*, 1–26.

Christov, T. (2017). The invention of Hobbesian Anarchy. *Journal of International Political Theory*, *13*(3), 296–310.

Cortada, J. W. (2012). *The digital flood: The diffusion of information technology across the U.S., Europe, and Asia*. Oxford University Press.

Couture, S., & Toupin, S. (2019). What does the notion of "Sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2522.

Daly, S. (2003). The ladder of abstraction: A framework for the systematic classification of democratic regime types. *Politics*, *23*(2), 96–108.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*, 369–378.

Fukuyama, F. (2015). *Political order and political decay: From the industrial revolution to the globalisation of democracy*. Profile Books.

Garsten, B. (2012). Liberalism and the rhetorical vision of politics. *Journal of the History of Ideas*, *73*(1), 83–93.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41–73.

Gaus, D., Landwehr, C., & Schmalz-Bruns, R. (2020). Defending democracy against technocracy and populism: Deliberative democracy's strengths and challenges. *Constellations*, *27*, 335–347.

Grabowska-Moroz, B. (2020). Data retention in the European Union. In M. Zubik, J. Podkowik, & R. Rybski (Eds.), *European constitutional courts towards data retention laws* (pp. 3–17). Springer.

Graham, S. E. (2011). Reflections on the thirty years war and the origins of propaganda. USC Center on Public Diplomacy (CPD) blog, available online in April 2021: https://uscpublicdiplomacy.org/blog/reflections-thirty-years-war-and-origins-propaganda.

Gurri, M., & Roberts, R. (2020). Martin Gurri on the revolt of the public. EconTalk, the library of economics and liberty. https://www.econtalk.org/martin-gurri-on-the-revolt-of-the-public/. Accessed April 2021.

Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J. H., Jonker, M., et al. (2020). A responsible internet to increase trust in the digital world. *Journal of Network and Systems Management*, *28*, 882–922.

Huston, G. (2020). DNS Wars. Potaroo, https://www.potaroo.net/ispcol/2019-11/dnswars.html. Accessed November 2020.

Jarke, M. (2020). Data sovereignty and the internet of production. In S. Dustdar, E. Yu, C. Salinesi, & Pant, D. R. V. (Ed.), *Proceedings of the 32nd international conference on advanced information systems engineering (CAiSE 2020), Lecture notes in computer science (Volume 12127)* (pp. 549–558). Springer.

Kennedy, P. (1989). *The rise and fall of great powers: economic change and military conflict from 1500 to 2000*. Fontana Press.

Kindt, E. J. (2016). Why research may no longer be the same: About the territorial scope of the new data protection regulation. *Computer Law & Security Review*, *32*, 729–748.

Komaitis, K. (2017). The 'Wicked Problem' of data localisation. *Journal of Cyber Policy*, *2*(3), 355–365.

Kurose, J. F., & Ross, K. W. (2008). *Computer networking: A top-down approach* (4th ed.). Addison-Wesley.

Laroche, H., Steyer, V., & Théron, C. (2018). How could you be so gullible? Scams and over-trust in organizations. *Journal of Business Ethics*, *160*, 641–656.

Lehtiniemi, T., & Haapoja, J. (2020). Data agency at stake: MyData activism and alternative frames of equal participation. *New Media & Society*, *22*(1), 87–104.

Lombardo, M. (2015). *Critique of sovereignty: Book I: Contemporary theories of sovereignty*. Punctum Books.

Midson, D. (2014). Geography, territory and sovereignty in cyber warfare. In H. Nasu & R. McLaughlin (Eds.), *New technologies and the law of armed conflict* (pp. 75–93). Asser Press.

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology & Human Values*, *46*(1), 112–138.

Morgenthau, H. J. (1949). *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.

Moskalenko, O., & Streltsov, V. (2017). Shaping a 'Hybrid' CFSP to face 'Hybrid' security challenges. *European Foreign Affairs Review*, *22*(4), 513–532.

Moura, G. C. M., Castro, S., Hardaker, W., Wullink, M., and Hesselman, C. (2020). Clouding up the internet: How centralized is DNS traffic becoming. In *Proceedings of the Internet Measurement Conference (IMC 2020)* (pp. 42–49), Virtual. ACM.

Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention. Chatham House, The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf. Accessed December 2020.

Mueller, M. L. (2019). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801.

Mueller, M. L. (2020). Hague keynote: Sovereignty in cyberspace. internet governance project. https://www.internetgovernance.org/2020/11/13/hague-keynote-sovereignty-in-cyberspace/. Accessed November 2020.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). the privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126.

Noveck, B. S., & Cerf, V. G. (2020). Digital democracy: Past, present, future. *Digital Government: Research and Practice*, *1*(1), 2:1–2:10.

O'Hara, K., & Hall, W. (2020). Four internets. *Communications of the ACM*, *63*(3), 28–30.

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian Myth. *International Organization*, *55*(2), 251–287.

Osula, A.-M. (2015). Transborder access and territorial sovereignty. *Computer Law & Security Review*, *31*, 719–735.

Pawlak, P., Tikk, E., & Kerttunen, M. (2020). Cyber conflict uncoded: The EU and conflict prevention in cyberspace. Policy brief, the European Union Institute for Security Studies (EUISS). https://www.iss.europa.eu/content/cyber-conflict-uncoded. Accessed November 2020.

Philpott, D. (1999). Westphalia, authority, and international society. *Political Studies*, *47*(3), 566–589.

Rahman, M. (2021). European sovereignty has lost its biggest champion: French president Emmanuel Macron has been quietly redefining the terms of the debate. politico. https://www.politico.eu/article/european-sovereignty-has-lost-its-biggest-champion-emmanuel-macron/. Accessed April 2021.

Robins, N. (2002). Loot: In search of the East India company, the world's first transnational corporation. *Environment and Urbanization*, *14*(1), 79–88.

Rosenblatt, H. (2018). *The lost history of liberalism: From ancient Rome to the twenty-first century*. Princeton University Press.

Ruohonen, J. (2020a). An acid test for Europeanization: Public cyber security procurement in the European Union. *European Journal for Security Research*, *5*(2), 349–377.

Ruohonen, J. (2020b). Do cyber capabilities and cyber power incentivize international cooperation? Archived manuscript. https://arxiv.org/abs/2011.07212. Accessed December 2020.

Ruohonen, J. (2021). A few observations about state-centric online propaganda. Archived manuscript. http://arxiv.org/abs/2104.04389.

Ruohonen, J., & Hjerppe, K. (2020). The GDPR enforcement fines at glance. Archived manuscript. https://arxiv.org/abs/2011.00946. Accessed December 2020.

Sartori, G. (1970). Concept misformation in comparative politics. *The American Political Science Review*, *64*(4), 1033–1053.

Sartori, G. (1989). The essence of the political in Carl Schmitt. *Journal of Theoretical Politics*, *1*(1), 63–75.

Sartori, G. (1991). Comparing and miscomparing. *Journal of Theoretical Politics*, *3*(3), 243–257.

Schneier, B. (2020). Technologists vs. policy makers. *IEEE Security & Privacy*, *18*(1), 71–72.

Sen, S. (2012). unfinished conquest: Residual sovereignty and the legal foundations of the British empire in India. *Law, Culture and the Humanities*, *9*(2), 227–242.

Siry, L. (2019). Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens. *New Journal of European Criminal Law*, *19*(10), 227–250.

Steiner, J. (2008). Concept stretching: the case of deliberation. *European Political Science*, *7*, 186–190.

Testart, C., Richter, P., King, A., Dainotti, A., and Clark, D. (2019). Profiling BGP serial hijackers: Capturing persistent misbehavior in the global routing table. In *Proceedings of the Internet Measurement Conference (IMC 2019)* (pp. 420–434), ACM.

Tikk, E., & Kerttunen, M. (2018). International cybersecurity: Orchestral manoeuvres in the dark. Policy brief, Norwegian Institute for International Affairs (NUPI). https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2566138/NUPI_Policy_Brief_11_2018_Tikk_Kerttunen+FINAL.pdf. Accessed December 2020.

Timmers, P. (2019a). Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines*, *29*, 635–645.

Timmers, P. (2019b). Strategic autonomy and cybersecurity. EU cyber direct: Supporting EU cyber diplomacy. https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf. Accessed June 2021.

Tunney, C. (2020). Companies could face hefty fines under new canadian privacy law. CBC. https://www.cbc.ca/news/politics/privacy-bill-bains-fines-1.5804779. Accessed November 2020.

Watts, W. L., & Mamudi, S. (2011). Finnish election results may spark Euro Jitters. MarketWatch https://www.marketwatch.com/story/finnish-election-results-may-spark-euro-jitters-2011-04-17. Accessed November 2020.

WJP. (2020). Rule of law index. World justice project (WJP). https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2020-Online_0.pdf. Accessed September 2020.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.