The Technological Construction of Sovereignty

Paul Timmers

Abstract For policy-makers, it has always been a struggle to do justice to a diversity of perspectives when tackling challenging issues such as market access regulation, public investment in R&D, long-term unemployment, etc. In this struggle, technology, as a force that shapes economy, society, and democracy, at best used to be considered as an exogenous factor and at worst was simply forgotten. Today, however, we live in a different world. Technology is recognized as a major driver. Digital technology is now in the veins, heart, and brains of our society. Yet, the idea that we can put technology to our hand to shape reality, rather than taking technology as a given, has still not been embraced by policy-makers. This chapter argues that we can and should give a stronger steer on technology to construct the kind of reality and in particular the kind of sovereignty we aspire.

1 Code Is Law; Law Is Code

Around the year 2000, Lawrence Lessig, a Harvard law professor, put forward his famous statement "code is law" (Lessig 2000). In brief, at that time, this was about the observation that the way the internet is technologically constructed ("code" in the sense of software code) to a large extent determines the rules of behavior in the internet. Code acts like law.

Recently, however, we would rather say: "law is code." "Law" is here understood as the requirements that governments would like to impose on the digital world. Nowadays, these requirements are evermore driven by concerns about sovereignty. Governments want more control over cybersecurity in 5G and open up access to

P. Timmers (✉)
University of Oxford, Oxford, UK

European University Cyprus, Engomi, Cyprus
e-mail: paul.timmers@iivii.eu

H. Werthner et al. (eds.), *Perspectives on Digital Humanism*,
https://doi.org/10.1007/978-3-030-86144-5_28

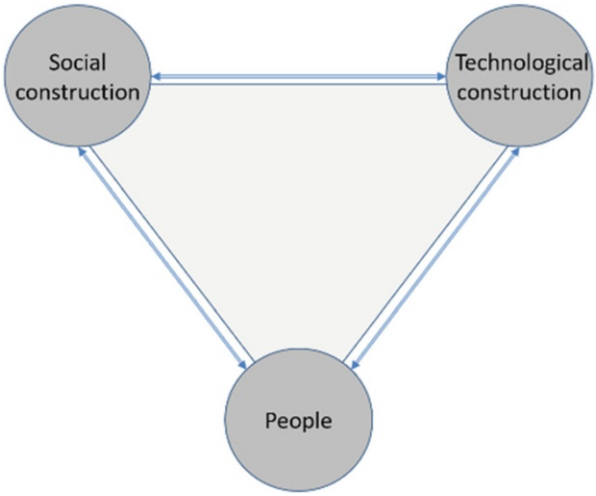

Fig. 1 Social and technological construction of reality

gatekeeper digital platforms.[1] States feel that they have to act to protect their national economic ecosystem and are worried about the erosion of society's values such as privacy. They fear that the very authority of government is being undermined. Clearly, technology as given does not safeguard sovereignty and has even become a threat. Sovereignty and strategic autonomy have become *Chefsache*.[2]

2 Social and Technological Construction of Reality

What is happening here from a conceptual point of view? I will stress two ideas, without claiming any originality in doing so.[3] The first is that technological construction of reality is as valid a notion as is the social construction of reality. The second is that there is a strong interplay between social and technological construction (Fig. 1).

The corollary is that design of social constructs such as law and design of technological constructs can and may go hand in hand. Even stronger: by ignoring that interplay, exploitative powers (dictators, populists, criminals, unscrupulous companies) will step in the void and gamble with our economies, societies, and democracy.

[1] For example, as in the EU reflected in the 5G Cybersecurity Recommendation and in the Digital Markets Act.

[2] GAIA-X, the European cloud initiative, takes (data) sovereign by design as a guiding principle for the development of software and services; see Franco-German Position on GAIA-X, 18 Feb 2020.

[3] For the origins of the underlying idea of constructivism, see Immanuel Kant, *Critique of Pure Reason* (1781).

The idea of social construction of reality rose to prominence from 1966 onward, thanks to Peter Berger and Thomas Luckmann (1967). Since that time, we accept that much of what we consider real in everyday life, such as money, values, citizens, or state, is a social construct. This holds for state sovereignty as well. Indeed, 30 years after Berger and Luckmann's *The Social Construction of Reality*, the excellent book *State Sovereignty as a Social Construct* was published (Biersteker and Weber 1996).

Can reality also be technologically constructed?[4] Pretty obviously "yes" when we just consider the many technological physical artifacts around us. These are the tangible technological reality "as we know it."

Such technological reality can even shape artifacts in our mind such as our perception of reality. Jean Baudrillard, a French sociologist and philosopher, argued in his provocative set of essays "The Gulf War Did Not Take Place" that this war was presented to us through technology with a specific imagery (Baudrillard 1991). Remember the cockpit images of bombing targets in the cross-hairs? These became for many the reality of the Gulf War (as long as you were not on the ground. . .). Technology-generated perception becomes evermore part of reality. Some young people have an unhealthy obsession with their image on social media (McCrory et al. 2020).

But can social reality, social artifacts, also be technologically constructed? The answer is affirmative here too. Consider Lessig's "code is law" as mentioned before. Lessig focused on the interplay of technology and law. Law is of course a social construct *par excellence*. Julie Cohen, in her 2017 book *Between Truth and Power*, built on Lessig and the 1970s governmentality concept of Michel Foucault (Cohen 2019). She analyzed the interplay of technological and social construction in the governance of law development by governments and tech companies. One conclusion: technology may be malleable, but such social constructs are malleable as well.

3 Technological Construction of Sovereignty

What then is technological construction of sovereignty? Sovereignty is loosely speaking about territory and borders, people, "our" values, and resources that "belong to us." Sovereignty requires internal legitimacy of the authority toward the people. Sovereignty also requires external legitimacy, that is, recognition by other states (Biersteker 2012; Timmers 2019).

Firstly, sovereignty includes assets that "belong to us." These are not only land or rivers but increasingly also technologically constructed assets, notably digital ones such as our health data or the country's internet domain name.

[4] That is, the reality of technological artifacts, technology mediating reality, and technology shaping or conditioning social reality.

Secondly, technology can redefine core privileges of the state such as the identification of citizens (the French call it *une fonction régalienne*). Electronic identity or eID raises the question of control. Can only a government-issued identity be an official eID? Could it also be a self-sovereign identity? Or even an identity owned by a platform like Facebook or Google? Should the *fonction régalienne* loose its state anchor? The technological choice, in combination with social constructs such as law and market power, can redefine a core aspect of sovereignty.

Thirdly, technology, in its Baudrillard's sense of intermediator to reality, unlocks cultural heritage which is clearly a sovereign asset. Technology, properly designed, protects and strengthens our values. Privacy by design is an illustration.

What then about digital technologies shaping internal and external legitimacy, those core qualities of sovereignty? Internal legitimacy implies accountability and transparency of the legitimate authority. As citizen we may wonder: is my court case treated fairly? Why have I been singled out for income tax scrutiny? Which civil servant is looking at my personal data?

On the one hand, transparency can be enabled by an appropriate technology architecture. Estonia has chosen to base its e-government platform on blockchain—which cannot be tampered with—for that purpose. On the other hand, internal legitimacy can also be undermined by technology that intentionally or unwittingly does not respect fundamental and human rights. In the Netherlands, recently "smart" but discriminatory technology for detecting misuse of child support in combination with strict bureaucracy and blind politics led to serious injustice for thousands of citizens. The Dutch government fell over the case. It lost its internal legitimacy.

The counterpart of technology-defined control of government is technology-defined control of citizens. Already today, even in free societies, ever-smarter cameras are ubiquitous. COVID-19 apps have raised concerns about surveillance creep (Harari 2020). Democratic processes everywhere are heavily shaped by social media, which stimulate by their very design the formation of echo chambers and thereby give raise to polarization. Hostile states seek to undermine the very legitimacy of incumbent governments by making use of the architecture of social media platforms to spread misinformation. Alternatively, social media are put under government control in order to suppress any citizen movement that may contest the state. This is a main motivation of online censorship in China (King et al. 2014).

External legitimacy can equally be shaped by technology. Kings and castles have fallen at the hand of new technologies such as trebuchet and cannon balls. The nuclear bomb prompted France to develop its own atomic capacity to safeguard its sovereignty. Asserting legitimacy in cyberspace has become a technological war where the power of one nation vis-à-vis others is increasingly being defined by militarizing artificial intelligence. One may wonder, though, what the nature is of such AI. How will it interpret aggression, and will it counterstrike autonomously or not? AI is a technology that can take over agency from the state, shaping external and internal legitimacy and thereby redefining sovereignty in the digital age.

Technological construction starts to reshape social constructs such as sovereignty. The writing is on the wall. The rise of cryptocurrencies challenges central banks as a sovereign institution. The rise of interoperable data spaces worries some

data holders who fear that their autonomy is threatened. Data hoarding by digital platforms makes governments realize that their presumed sovereignty is evermore in the hands of a few global corporates and foreign governments. Technology is re-allocating legitimacy between the extremes of massive decentralization—such as with blockchain or personal data pods—and massive centralization in the hands of a few actors that escape democratic control.

4 Conclusions

The reader, having come all the way until here to read about something she or he already knew or at least intuited, may be left with the question: "so what?" The answer is that technology fundamentally shapes sovereignty and it is us who can influence the shaping of such technology.

Policy-makers who are concerned about strategic autonomy do not need to accept technology "as is." Technology is neither a force of nature nor to just be left to the market nor to be taken for granted, as an exogenous factor. Policy-makers can insist that (digital) technology is designed in such a way that internal and external legitimacies are strengthened. Digital technology can be required to be designed such as to grow assets "that belong to us" and protect our values, human rights, and humanism (TU Wien 2019).

Sure, we then sacrifice one holy cow as we must conclude that technology is not neutral. Fine. But there is a more radical proposition here, namely, that during the design of law policy-makers would sit together with technology designers. They would engage in a dialogue about technology requirements such as sovereignty safeguards. They would not be satisfied until there is mutual re-assurance of the compatibility of technology and law (or policy).

There is also no need to take the law and organization of government and administration for a given. Sure, we want stability with law. But if technology can do a better job, law-as-is should not stand in the way. This then leads to a second radical proposition: to consider in the design of any law whether promotion of technological disruption should be included in that same law. The intent would be to enable replacement of the social constructs in that law by technological constructs. Of course, only provided the end result is better.

An example would be to include in future laws that seek to safeguard sovereignty (such as on data or AI or cloud) a chapter on R&D for sovereignty-respecting technology, with corresponding budget and objectives. That same law should then foresee to scale back human oversight following proper and successful assessment of the resulting technology.

Co-design of law and technology in the way proposed here is not yet found anywhere, as far as the author is aware of. It would likely be seen as a radical change. But hopefully this chapter convinced the reader that this change is thinkable, enlightening, and, above all, necessary today in order to construct the sovereignty that we aspire. We have a choice.

References

Baudrillard, J. (1991) *La Guerre du Golfe n'a pas eu lieu*. Paris: Galilée.
Berger, P. and Luckmann, T. (1967) *The Social Construction of Reality*. Anchor.
Biersteker, T. J. (2012) 'State, Sovereignty and Territory', in Carlsnaes, W. (et al.) (ed.) *Handbook of International Relations*. SAGE Publications Ltd.
Biersteker, T. J. and Weber, C. (1996) *State Sovereignty as Social Construct*, *Cambridge Studies in International Relations*. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511598685.
Cohen J. (2019) *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.
Harari Y. (2020) 'The world after coronavirus', *Financial Times*. Available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.
King, G., Pan, J. and Roberts, M. E. (2014) 'Reverse-engineering censorship in China: Randomized experimentation and participant observation', *Science*, 345(6199), p. 1251722. doi: https://doi.org/10.1126/science.1251722.
Lessig L. (2000) 'Code Is Law', *Harvard Magazine*, (1 Jan 2000). Available at: https://www.harvardmagazine.com/2000/01/code-is-law-html.
McCrory, A., Best, P. and Maddock, A. (2020) 'The relationship between highly visual social media and young people's mental health: A scoping review', *Children and Youth Services Review*, 115, p. 105053. doi: https://doi.org/10.1016/j.childyouth.2020.105053.
Timmers, P. (2019) 'Strategic Autonomy and Cybersecurity', *EU Cyber Direct*, (September 2017), pp. 1–10.
TU Wien (2019) *Vienna Manifesto on Digital Humanism*. Available at: https://dighum.ec.tuwien.ac.at/dighum-manifesto/.