DIGITAL SOVEREIGNTY REVISITED

NEW ELEMENTS FOR A SHARED AND COOPERATIVE CONCEPT

Rolf H. Weber

Rolf H. Weber, Professor, Attorney-at-Law, University of Zurich, Faculty of Law
Rämistrasse 74/38, 8001 Zürich, CH
rolf.weber@rwi.uzh.ch; https://www.ius.uzh.ch/de/staff/professorships/alphabetical/weberr/person.html

Keywords: ***Civil society, digital sovereignty, fragmentation, global cooperation, shared sovereignty***

Abstract: *The 500 years old sovereignty principle must be realigned in times of globalization. Recently, the notion of digital sovereignty was coined meaning that States claim the right to impose protective measures on infrastructures. Such kind of sovereignty causes the risk that a fragmentation of global networks occurs ("Splinternet") which is undesirable. In order to overcome this tendency, sovereignty in the digital world should be understood as a notion of shared and cooperative spaces and include civil society-based voices. Therefore, the term "digital sovereignty" needs to be developed into the direction of said concept by encompassing all relevant actors in cyberspace.*

1. Historical Foundation and Present Questions

The sovereignty principle has its roots in the 16th century. The term was originally coined by the philosopher and legal scholar Jean Bodin (1576); the historical concept goes along with the building-out of nation States.[1] The early interdisciplinary notion has been refined by Thomas Hobbes and later by Jean-Jacques Rousseau. The first political document enshrining the sovereignty thinking and prominently reflecting this concept is the Westphalian Peace Treaty of 1648. Among others, this document contains the right of each State to monopolize certain exercises of power within its territory.[2]

Over the centuries, with the globalization of data flows and business models, the cross-border infrastructures as well as some international legal instruments (for example the UN Charter and the ITU Regulations) introduced limits to national legislation. As a consequence, the traditional sovereignty concept must also address alternative values in the context of power allocation. In other words, governance is changing under conditions of interconnectedness now happening. Such a new concept realizing a cooperative sovereignty notion should lead to a shared responsibility for global resources and to the establishment of standards for transnational collaboration.[3]

As a starting point, the profound changes in social and economic patterns challenging the traditional sovereignty understanding of Nation States make it necessary to analyze the following basic questions:[4]

– Do States have a shared responsibility based on shared sovereignty to promote and encourage the development of policies?
– Do States have a shared responsibility based on shared sovereignty to ensure a fair and equitable allocation of resources?

[1] Weber, 2021a, 87.
[2] Kulesza/Weber, 2021, 3.
[3] For further details see Weber, 2021a, 87–88 with additional references.
[4] Weber, 2010, 16.

– Do States have a shared responsibility based on shared sovereignty to refrain from influencing the transnational policies related to transboundary information flows?

The following considerations assess the challenges for an appropriate digital sovereignty understanding and develop ideas for a new concept.

2. Digital Sovereignty as Promise and Threat

2.1. Notions

On a global scale, the above outlined questions have not been answered in an unanimous manner during the last few years, notwithstanding the fact that Nation States more frequently claimed a right to control the infrastructures and the data flows. But as a new term, the notion of digital (or data) sovereignty has attracted attention in the political environment. The respective notion is invoked by States as a protective or empowerment stance regarding a multitude of stakeholders.[5] The term digital sovereignty is partly also used for the vision of digital self-determination being the autonomy of individuals and their right to control the data they own or generate; this – hereinafter not to be deepened – understanding corresponds to the right of self-determination as originally coined by the German Constitutional Court in the “Census Decision” assessing the scope of privacy rights.[6]

In the Internet Governance context, digital sovereignty was mainly invoked by rather autocratically or hierarchically organized countries. Such national approaches prioritizing country-specific interests have been pursued by several governments (starting with Iran at the WCIT of 2012 in Dubai), for example by the United States mainly in the context of political assessments (Trump administration) or by China with the “Global Initiative on Data Security” of 8 September 2020[7] and with the “Wuzhen Plan” of Foreign Minister Wang Yi presented prior to the World Internet Conference (WIC, Wuzhen) of November 2020.[8] Other countries are going into a similar direction.[9]

Furthermore, a certain risk exists that State power is undermined by private actors (such as big social media or telecom operators).[10] The main examples for data- and market-dominant companies are the GAFAM group in the United States (Google, Apple, Facebook, Amazon and Microsoft) and the BAT group in China (Baidu, Alibaba, Tencent).[11] But national and home business-oriented initiatives contradict the inherent value of Internet governance that touches upon aspects which have a “common interest” character being a well-known concept in transnational law.[12]

2.2. Examples for Digital Sovereignty Phenomena

Cross-border data flows should be legal, free and secure. Obviously, data flows do have an impact on the digital sovereignty since the delivery of information across borders is directly confronting State power with the “import” of data. Therefore, many States are elaborating on the development of a digital foreign policy strategy. The main regulatory issues in this context are privacy, cybersecurity and data localization measures.

[5] Internet & Jurisdiction Policy Network, 2021, 39.

[6] BVerfGE 65, 1 (1983).

[7] For the Chinese original initiative see https://www.mfa.gov.cn.; for an English discussion of its contents see https://digichina.stanford.edu/work/knowldge-base-chinas-global-data-security-initiative/ (both accessed on September 15, 2022).

[8] See https://www.wuzhenwic.org (accessed on September 15, 2022).

[9] For the European Union see Bendiek/Stürzer, 2022, 3–4.

[10] Cartwright, 2020.

[11] Sahin, 2022, 2.

[12] See also Kettemann, 2020, passim.

Privacy

Privacy concerns gained major importance during the last ten years; a majority of countries around the world now know data protection laws and specifically regulate cross-border data flows. Intensively discussed as model for many other laws is the General Data Protection Regulation (GDPR) of the European Union. In most national statutes, various conditions for cross-border data transfers are applicable, in particular the principle of the equivalent level of data protection. However, no general international consensus exists on the best means to achieve online privacy. The core problem lies in the fact that the socio-cultural environment on privacy across countries is different; partly, the protection of the personal integrity is at the forefront, partly the aspect of information security prevails; even consumer rights can play a role.[13]

In international (trade) law agreements, some rules are contained, particularly in regional agreements having introduced a number of generally observable standards that try to achieve a minimum harmonization.[14] The General Agreement on Trade in Services (GATS) is acknowledging the importance of privacy protection as part of its exception clauses; according to article XIV(c)(ii) national restrictions are acceptable to the extent of being necessary to secure compliance with laws or regulations addressing the "protection of privacy of individuals in relation to the processing and dissemination of personal data and protection of confidentiality of individual records and accounts". But this exception clause appears to be insufficient as it pressurizes regulators to adjudicate on sensitive privacy issues being particularly difficult given that "data-source countries" are "unlikely to accept one-sided limits on their right to protect privacy".[15]

In order to deal with the given uncertainty and distrust in privacy matters, increasingly more countries seek for data protection rules enabling cross-border data flows while ensuring privacy protection as an important societal objective. Therefore, reconciliation models mapping data flows and data protection interests must be developed based on a better understanding and contextualization of their complex interfaces. The chances and challenges of available legal solutions need to be adequately balanced;[16] in addition, internationally recognized standards and guidelines provide a basis for aligning privacy laws across countries.[17] Thereby, an undesirable fragmentation of Internet communications should be avoided.

Cybersecurity

Cybersecurity recently became a more debated topic since security threats have increased and international efforts to reach a mutual agreement on the UN level were not successful.[18] Divergent cybersecurity laws and technical standards around the globe make cross-border data flows more difficult. At least international (trade) law contains exception clauses, similarly to the privacy situation: cybersecurity measures could be necessary to maintain public order or be required to prevent deceptive and fraudulent practices or protect safety (article XIV GATS). Furthermore, article XIV^{bis} GATS stipulates three general security exceptions, namely the information supply contrary to essential security interests, trade restrictions which are aimed at the protection of essential national security interests, and measures adopted in war time or in other emergency situations concerning international relations.

Notwithstanding the fact that cybersecurity was not an issue at the time of the WTO inception (1995) and that the security exceptions were not designed in a way that would easily match the cybersecurity challenges, the WTO Panel in the case "Russia – Measures Concerning Traffic in Transit" has asserted that interests relating to the quintessential functions of the State, namely the protection of its territory and its population from external threats, and the maintenance of the internal law and public policy order would be relevant if taken in

[13] Kuner, 2013, 33–34.
[14] Burri, 2021a, 20–33.
[15] Mattoo/Melzer, 2018, 789.
[16] For a detailed analysis of the available reconciliation models see Burri, 2021b, 129 et seq.
[17] Mitchell/Mishra, 2021, 105 with further references.
[18] Weber, 2021d, nos. 8 et seqq. with further references.

good faith.[19] In legal doctrine, some reluctance can be seen in respect of qualifying cybersecurity as national security in trade agreements since cybersecurity-related laws do often not draw a rational distinction between military and social/economic security and since a lack of international consensus on cybersecurity governance would be given.[20] Indeed, complex cybersecurity measures cause the risk to burden governmental bodies with the adjudication of technical and political questions; the legal developments on this issue remain to be seen.

Data Restrictive Measures (Data Localization)

The imposition of data restrictive measures is often driven by competitive considerations between governments in order to achieve more intelligence by controlling data flows.[21] Different governments have adopted measures to increase regulatory control by implementing data localization laws.[22] Around the globe, such requirements are designed in a variety of forms. Information and communication technology companies may be obligated to host all subscriber and consumer data locally within the country. However, data localization reduces access to data and digital technologies and may also be counterproductive; the risk of fragmentation of the global infrastructures increases and deprives civil society from taking advantage of global communications channels.

2.3. Risk of Fragmentation

As shown, an extensive notion of digital sovereignty causes the risk that international governance principles will become re-nationalized and that the global Internet evolves into a so-called “Splinternet”,[23] particularly since some countries think of creating an independent national Internet.[24] Such a development that leads to fragmentation is undesirable; any kind of fragmentation would not be future-oriented and have a negative impact on global infrastructures.[25] Indeed, as Floridi observed, the “risk, when supporting national sovereignty, is to end up supporting digital sovereignism or digital statism”.[26]

In view of this (doubtful) development towards fragmentation it does not come as a surprise that in an attempt of avoiding political discussions ICANN introduced the notion of “Technical Internet Governance” (TIG) being a more neutral language for its activities. As far as the “lower” technical layer, namely the (i) design or structure of the TIG layer is concerned, the Internet could remain without major fragmentation. In contrast, on the “upper” layer, namely the (ii) “use” of Internet services, a politically-driven fragmentation would be subject to the chosen (governmental) policies.[27]

The fragmentation risk equally threatens an appropriate platform governance in the online business context. Transnational actors should not be precluded from communications and transactions activities as long as not the intention prevails to escape generally accepted rules by hiding responsibility behind territorial formalities and as long as constitutional public values are complied with in an appropriate manner.[28] In order to avoid a problematic fragmentation, standard-setting and governance of standards must be conducted in an open and objective-oriented way.[29] Such global processes are able to enhance digital cooperation in the age of cyber-interdepence.

[19] WTO Panel Report, Russia – Measures Concerning Traffic in Transit, WT/D512/7, 29 April 2019, no. 7.130 and no. 7.133.

[20] Mishra, 2020, p. 576 et seq.

[21] Selby, 2017, p. 231/32.

[22] Mitchell/Mishra, 2021, p. 99.

[23] See Kleinwächter, 2021, 1 et seq. and European Parliamentary Research Service, 2022, passim.

[24] Weber, 2021a, 88–89.

[25] Mueller, 2017, 131; to the different policy options with benefits and drawbacks see European Parliamentary Research Service, 2022, 47–58.

[26] Floridi, 2020, 374.

[27] Kleinwächter, 2021, 6, and Weber, 2021a, 89.

[28] Tiedeke, 2021, 626; Floridi, 2020, 372.

[29] For further details see Cohen, 2020, 60 et seq.

3. Towards the Concept of a Shared and Cooperative Sovereignty

3.1. Society-based Multistakeholderism

In order to increase a cooperative communications network and to avoid fragmentation, the governance functions should remain embedded in horizontal structures creating a multistakeholder environment.[30] In addition, a political force is needed to stand up for the value of global connectivity and for the right of people everywhere to self-govern their online transactions.[31] The respective substantive foundation of the interrelations can be built on the basis of international legal concepts. Several theoretical models have been developed so far; as the most important inter-national legal concepts, the notions (i) of global public goods, (ii) of shared spaces and (iii) of due diligence / State responsibility are available.[32]

Numerous multistakeholder and interdisciplinary projects and initiatives have been launched during the last few years, for example the Contract for the Web (Tim Berners-Lee), the Paris Call for Trust and Security, the Global Commission on the Stability of Cyberspace, the Internet & Jurisdiction Initiative (Paris), the Tech Accord (Microsoft), the Global Forum on Cyber Expertise, etc.[33] These groups should attempt at joining forces with their valuable activities in order to overcome national approaches that cause a substantial risk of an Internet fragmentation.

Consequently, traditional national sovereignty over cross-border communications flows should be replaced by a transnational "popular" (i.e. civil society-based) sovereignty. The respective political concept needs to be strong enough to remove legitimacy and authority over critical aspects of the infrastructure from established governments to non-governmental actors.[34] In addition, the vague term "digital sovereignty" needs to be reconsidered in order to reflect the requirements of modern societies around the globe.

3.2. Non-discrimination and Non-appropriation

In order to combat the growing undesirable fragmentation, it appears obvious that the traditional notion of States' sovereignty must be revisited and turned into a concept of shared and cooperative sovereignty being an understanding generally accepted by the global legal community. Otherwise, the newly invented "digital sovereignty" will be confronted with the same "fate" as earlier forms of sovereignism that have introduced "walls" at the State borders.

Transnational data flows around the globe are only possible in a regime of shared and cooperative sovereignty; such an approach has already been realized for example by the Outer Space Treaty of the United Nations which was adopted more than 40 years ago.[35] The main purpose of this Treaty consists (i) in the submission of all outer space activities to international law, as well, as (ii) in the implementation of the principles of non-discrimination and of non-appropriation by any claim of (national) sovereignty.[36] The law of outer space appears to be the most prominent example for the implementation for the shared and cooperative spaces concept and can also be a model for cyberspace regulations. The application of the non-discrimination and non-appropriation principle means that national measures should not be imposed on the global community and should not restrict the cross-border exchange of opinions and communications.

[30] Radu, 2019, 194.

[31] Weber, 2021a, 88–89, and Mueller, 2017, 131–132.

[32] For more details see Weber, 2021c, 610–619.

[33] See Weber, 2021a, 100–101.

[34] Mueller, 2017, 131.

[35] 610 UNTS 205.

[36] Weber, 2021c, 612–616; Kulesza, 2012, 145–146.

The concrete design of the shared and cooperative spaces still needs to be further developed; thereby, the involvement of civil-society based participants cannot and should not be avoided in order to make the future digital governance successful. Efforts must be undertaken by joint multilateral and multistakeholder initiatives into the direction of a collaborative normative environment that is reflected in a common understanding of generally accepted legal standards. Such movements can be partly seen in the context of harmonization efforts for privacy/data protection instruments and cyberstability measures.[37]

3.3. Relevance of Commons

In addition, the new ecosystem should be built on the foundation of a strong presence of commons, public institutions and civil society participations.[38] The inclusion of the commons principles helps to appropriately develop a more focused analysis in respect of a harmonized and stable framework designing global policies. In particular, governments should closely cooperate in continuing efforts to arrive at an operable consensus that avoids an inappropriate exercise of power and authority causing harm in cross-border relations[39] and that takes into consideration global interoperability, network stability, reliable access, and cybersecurity due diligence.[40]

As mentioned, digital spaces are to be managed as commons through collaborative, equitable and proportionate governance measures. Thereby, data commons are suitable to realize a new form of knowledge commons with the sharing of varied types of information. In other words, digital cooperatism must be related to the commons model of shared and cooperative ownership, democratic governance and solidarity.[41] Thereby, the duty of cooperation needs becoming a part of the cyberspace framework.[42] In addition, sustainable and accessible infrastructures not being dependent from a few (public or private) actors are of utmost importance.[43]

Global governance means that the concerned persons and institutions of the public and private spaces are enabled to identify, understand, and address potential transnational problems; this means that more engagement in capacity-building efforts and confidence-building measures are needed.[44] Such an approach is followed by the UN Secretary-General with the "Roadmap for Digital Cooperation" of June 2020;[45] this Roadmap contains elements of improved digital cooperation. Furthermore, the UN Secretary-General has appointed a new IGF Leadership Panel in August 2022; it remains to be seen how the eminent members of this Panel are able to embed the multilateralism in a multistakeholder environment.[46]

A shared and cooperative sovereignty principle could also contribute to the improvement of an appropriate Internet integrity understanding based on a cooperative and collaborative model of multilateral and multistakeholder forces. The so far (incoherent) patchwork of rules does not really correspond to the political and societal requirements. In the current "Internet in Everything" being a "World with No Switch Off", as recently framed by DeNardis,[47] it is essential to establish generally acknowledged concepts and standards of international law. Furthermore, the normative framework should also enshrine the obligation to comply with the core

[37] A good example is the Final Report of the Global Commission on the Stability of Cyberspace, Advancing Cyberstability, published in 2019, and updated in the meantime.

[38] NGI Forward, 2022, 20 et seq.

[39] See Haggart/Tusikov/Scholte, 2021, passim.

[40] Weber, 2021c, 615–616.

[41] NGI Forward, 2022, 21–22.

[42] See Weber, 2021b, nos. 1 et seq,

[43] Sahin, 2022, 2.

[44] Weber, 2021c, 624.

[45] See https://www.un.org/en/content/digital-cooperation-roadmap/.

[46] Kleinwächter, 2022, 2–3.

[47] DeNardis, 2020; the text cites a part of the title of the book.

elements of human rights and of human development;[48] relevant aspects of such compliance are due diligence standards, good behavioral practice, exchange of information and international cooperation.[49]

4. Outlook

Digital sovereignty has become a buzzword during the last few years. But the reference to digital sovereignty is frequently used to justify extended State control about cyberspace. Such an approach contradicts the global nature of transnational networks.

In contrast, the development should go into the direction of a "common" interest model; widely accepted norms must become the foundation for responsible behavior and activities. As a consequence, enhanced co-operation should be implemented in order to reflect the interconnectedness of the world. Initiatives supporting cross-border connectivity and digital inclusion have the chance to lead to a convincing global architecture for cyberspace.[50]

In line with such a model, sovereignty cannot be national but its character and design should be combined with cooperative elements of multilateralism and multistakeholderism. Therewith, the social, technical, cultural, economic and legal spheres can be guided to an appropriate equilibrium.

5. References

Bendiek, Annagret/Stürzer, Isabella, Die digitale Souveranität der EU ist umstritten, SWP-Aktuell Nr. 30, Berlin 30. April 2022.

Burri, Mira, Data Flows and Global Trade Law, in: Burri, Mira (ed.), Big Data and Global Trade Law, Cambridge 2021, 11–41 (Burri, 2021a).

Burri, Mira, Data Flows versus Data Protection: Mapping Existing Reconciliation Models, in: Mathis, Klaus/Tor, Avishalom (eds.), Law and Economics of Regulation, Cham 2021, p. 129–158 (Burri, 2021b).

Cartwright, Madison, Internationalising state power through the internet: Google, Huawei and geopolitical struggle, *Internet Policy Review* 9 (3), 2020, https://doi.org/10.14763/2020.3.1494 (accessed on September, 15, 2022).

Cohen, Julie E., Networks, Standards and Network-and-Standard-Based Governance, in: Werbach, Kevin (ed.), After the Digital Tornado – Networks, Algorithms, Humanity, Cambridge 2020, 57–80.

DeNardis, Laura, The Internet in Everything – Freedom and Security in a World with No Switch Off, New Haven/London 2020.

European Parliamentary Research Service, 'Splinternets': Addressing the renewed debate on internet fragmentation, Brussels, July 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf (accessed on September 15, 2022).

Floridi, Luciano, The Fight for Digital Sovereignty: What It Matters, Especially for the EU, Philosophy & Technology 33, 2020, p. 369–378.

Global Commission on the Stability of Cyberspace, Advancing Cyberstability, Final Report, Berlin, November 2019.

Haggart, Blayne/Tusikov, Natasha/Scholte, Jan Aart, Power and Authority in Internet Governance, London 2021.

Internet & Jurisdiction Policy Network. We Need to Talk About Data – Framing the Debate Around the Free Flow of Data and Data Sovereignty, Paris 2021, https://www.internetjurisdiction.net/news/aboutdata-report (accessed on September 15, 2022).

Kettemann, Matthias C., *The Normative Order of the Internet*, Oxford 2020.

[48] For further details see Kettemann, 2020, 36 et seq.

[49] Kulesza/Weber, 2021, 12; Weber, 2021c, 626.

[50] Weber, 2021a, 103.

KLEINWÄCHTER, WOLFGANG, Internet Governance Outlook 2021: Digital Cacaphony in a Splintering Cyberspace, CircleID of 8 January 2021, https://circleid.com/posts/20210108-internet-governance-outlook-2021-digital-cacaphony/ (accessed on September, 15 2022), 2021.

KLEINWÄCHTER, WOLFGANG, Amplifying the Internet Governance Forum: Will the New IGF Leadership Panel Make the Difference?, CircleID of 1 September 2022, https://circleid.com/posts/20220901-amplifying-the-internet-governance-forum-will-the-new-igf-leadership-panel-make-the-difference (accessed on September 15, 2022).

KULESZA, JOANNA, *International Internet Law*, London/New York 2012.

KULESZA, JOANNA/WEBER, ROLF H., Protecting the Internet with International Law, *Computer Law & Security Review* 40, 2021, 105531, p. 1–12.

KUNER, CHRISTOPHER, Transborder Data Flows and Data Privacy Law, Oxford 2013.

MATTOO, AADITYA/MELZER, JOSHUA P., International Data Flows and Privacy: The Conflict and its Resolution, Journal of International Economic Law 9, 2018, p. 769–789.

MISHRA, NEHA, The Trade: (Cyber)Security Dilemma and Its Impact on Global Security Governance, Journal of World Trade 54, 2020, p. 567–590.

MITCHELL, ANDREW D./MISHRA NEHA, WTO law and cross-border data flows, an unfinished agenda, in: Burri, Mira (ed.), Big Data and Global Trade Law, Cambridge 2021, p. 83–112.

MUELLER, MILTON L., *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Oxford 2017.

Next Generation Internet (NGI) Forward (ed.), Generative Interoperability – Building Online Public and Civil Spaces, Brussels, March 2022, https://openfuture.eu/publication/generative-interoperability/ (accessed on September 15, 2022).

RADU, ROXANA, *Negotiating Internet Governance*, Oxford 2019.

SAHIN, KAAN, Aussenpolitische Digitalstrategien, SWP-Aktuell Nr. 27, Berlin 27. März 2022.

SELBY, JOHN, Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks or Both?, International Journal of Law and Information Technology 25, 2017, p. 213–232.

TIEDEKE, SOPHIA, Die (notwendige) Relativität digitaler Souveränität, *Multimedia und Recht* 2021, p. 624–628.

WEBER, ROLF H. New Sovereignty Concepts in the Age of Internet? *Journal of Internet Law*, August 2010, p. 12–20.

WEBER, ROLF H., Internet Governance at the Point of No Return, Zurich 2021 (WEBER, 2021a).

WEBER, ROLF H., Duty of Co-operation as New Cybergovernance Concept, Weblaw IT-Jusletter 25 February 2021 (WEBER, 2021b).

WEBER, ROLF H., Integrity in the 'Infinite Space' – New Frontiers for International Law, *ZaöRV/HJIL* 81, 2021, p. 601–626 (WEBER 2021c).

WEBER, ROLF H., Cybersecurity Governance – international law as policy driver, Weblaw IT-Jusletter 27 May 2021 (WEBER, 2021d).