Why Digital Sovereignty is more than mere Legal Compliance

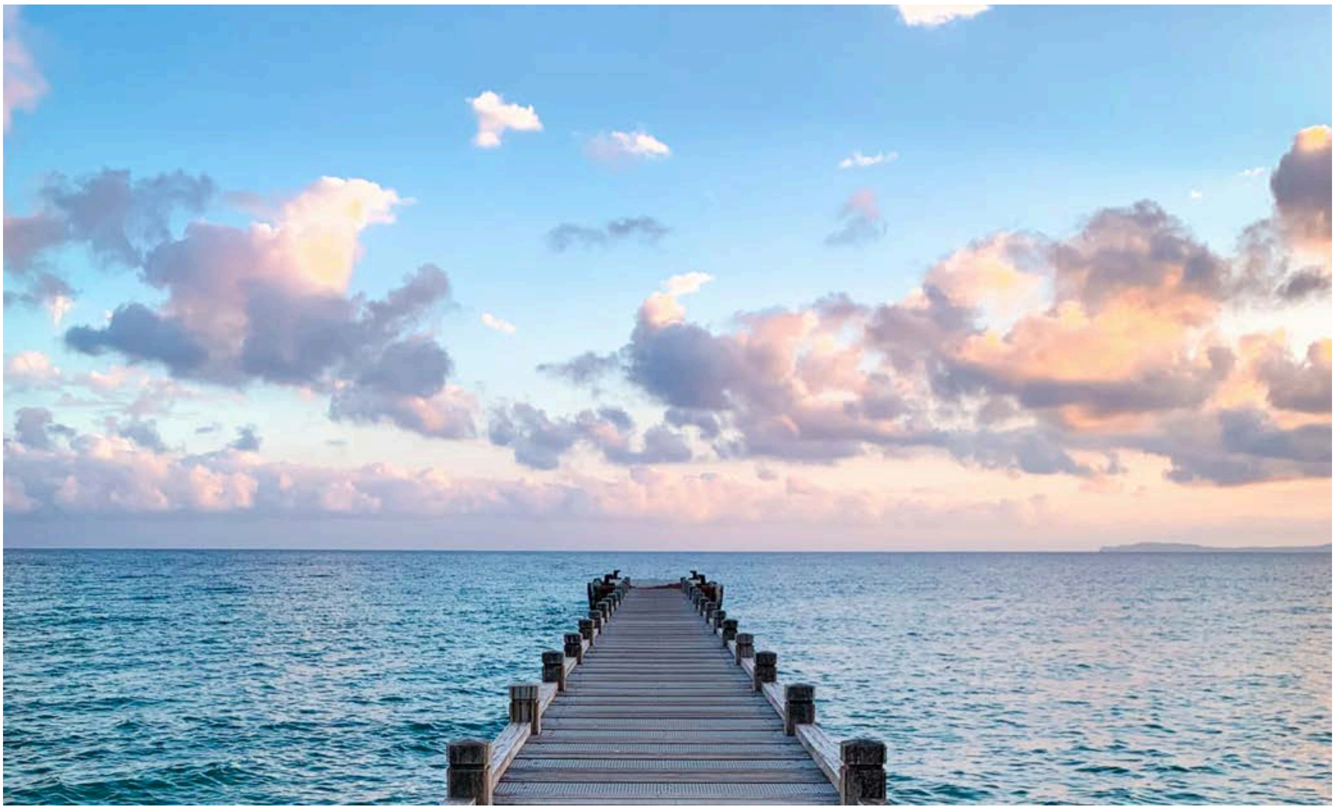
Hardly any other term has been redefined and re-framed so frequently in last year's digital political discourse as "digital sovereignty". This article is intended to help demystify the term "digital sovereignty" by exploring the different dimensions of digital independence and is a first approach to create a well-defined taxonomy that allows an evaluation of digital offerings far away from buzzwords and hypes.

Hardly any other term has been redefined and re-framed so frequently in last year's digital political discourse as "digital sovereignty". The common interpretations range from the use of Open Source Software down to local franchise agreements with tech companies whose commercial success relies on the lock-in effect achieved by having proprietary software in a few stack's key places. This interpretive diversity of "digital sovereignty" not only allows these companies to use the term as a fig leaf, but also makes it difficult for governments, institutions, companies, and individuals to rationally evaluate the available offerings in order to make a strategically reasonable decision in the end.

This article is intended to help demystify the term "digital sovereignty" by exploring the different dimensions of digital independence and is a first approach to create a well-defined taxonomy that allows an evaluation of digital offerings far away from buzzwords and hypes. So, what is this digital sovereignty and if so, how much? Let's find out together!

Sovereignty in general sense

The ambiguity of this conception already begins with the notion of sovereignty. Not without reason the German jurist Lassa Oppenheim writes:



"There exists perhaps no conception the meaning of which is more controversial than that of sovereignty. It is an indisputable fact that this conception, from the moment when it was introduced into political science until the present day, has never had a meaning which was universally agreed upon." - (Oppenheim and McNair 1926)

Although the meaning of sovereignty has varied throughout history and across scientific disciplines, its core meaning can be condensed to "supreme authority within a territory" (Philpott 2020).

As Stéphane Couture and Sophie Toupin outline in their work "What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty?", the notion of territory does not need to be restricted to the landmass, "but also - and this is important for our later analysis - to resources lying on the territory such as human infrastructures …" (Couture and Toupin 2019).

For instance, in this same article, Couture and Toupin point out various notions of sovereignty, be it food sovereignty, energy sovereignty, or body sovereignty. While the former both terms address the sovereignty over the means of production, the latter term describes the self-determination over one's own body.

But what exactly does sovereignty in the digital realm refer to? Does it conceptualize the state authority in the digital space, does it relate to the means of production, or ultimately, to self-determination over technology?

Many attempts have already been made to fundamentally define this term. For Instance, the focus group "Digitale Souveränität in einer vernetzten Gesellschaft" postulated at the German "Digital Gipfel" 2018:

"Today, digital sovereignty is an important aspect of general sovereignty, which refers to the ability to use and design digital systems, self-determination over aggregated and stored data, as well as over the related processes."

How can we foster this self-determination over technology, aggregated data and digital processes?

To answer this question, we will now take a closer look at the various dimensions of digital sovereignty.

Legal dimension

From a legal perspective, digital sovereignty would encompass the ability of a society to define the rules for digital solutions and to also enforce these rules. An important rule that the European Union has put in place is the General Data Protection Regulation (GDPR), which aims to govern the collection, processing and deletion of personally identifiable data in order to protect the freedom of individuals by giving them some level of transparency and control over their own data.

Current discussions around digital sovereignty usually arise from the use of (cloud) offerings that transfer or process personal data outside of the EU and thus are in conflict with the recent Schrems II judgment.[1]

For example, a variety of data protection authorities have raised concerns over the use of Microsoft 365 offerings as several violations of the GDPR have been identified:

"Third, EU institutions faced a number of linked issues concerning data location, international transfers and the risk of unlawful disclosure of data. They were unable to control the location of a large portion of the data processed by Microsoft. Nor did they properly control what was transferred out of the EU/EEA and how. There was also a lack of proper safeguards to protect data that left the EU/EEA. EU institutions also had few guarantees at their disposal to defend their privileges and immunities and ensure that Microsoft would only disclose personal data insofar as permitted by EU law." - (European Data Protection Supervisor 2020)

A possible remedy is to create franchise agreements with local trustees who operate the software in their respective jurisdiction.[2] While this approach addresses the aforementioned conflict, neither self-determination nor sovereignty over the means of production are given.

Only the freedom to inspect, adapt, use and share the underlying technology grants sovereignty in the sense of self-determination

Even if local security institutions audit every single modification coming from the outside software provider, these offerings still need a high presumption of trust between software vendor, local franchise partner and customer. Are security updates provided to the trustees in a timely manner? Is operational knowledge around the technology (which may originally not have been designed to be operated by third parties) sufficiently shared and documentation appropriately maintained? Isn't there still a complete dependence on the single technology provider and operator?

These and more questions arise as soon as considering more than just the legal dimension of these offerings.

Freedom of choice

When building digital services on top of infrastructure, the services will leverage the interfaces, automation capabilities, and higher-level services from the infrastructure in order to work well and to be efficient in development and operations. This invariably makes the thus developed services dependent on the infrastructure.

The dependence makes it hard to move these services to different infrastructure. The switching cost can easily become prohibitive and create a lock-in effect that makes it extremely hard to ever redeploy the services elsewhere.

This can be mitigated in several ways. In the best case, all the interfaces, automation capabilities and higher-level services are standardized well and can be implemented independently by a variety of software solutions and infra-

[1] In its July 2020 Schrems II judgment, the Court of Justice of the European Union (CJEU) declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. See "The CJEU judgment in the Schrems II case" by the European Parliamentary Research Service.

[2] Examples include SAP and Arvato in cooperation with Microsoft (see https://news.sap.com/2022/02/sap-arvato-systems-partnership/) , T-Systems in cooperation with Google (see https://www.telekom.com/en/media/media-information/archive/joint-innovation-from-t-systems-and-google-cloud-632222) in Germany, as well as Orange and Capgemini in cooperation with Microsoft (see https://www.orange.com/en/newsroom/press-releases/2021/capgemini-and-orange-announce-plan-create-bleu-company-provide-cloud) in France.

structure operators. This is the case with Open Standards and Open Source Software.

In somewhat less ideal scenarios, the interfaces and solutions are not standardized across vendors, but at least the software is easily available and can be and is operated independently by many providers, so all these providers can offer compatible solutions. The consumer of these services could also opt to deploy the software himself and operate the infrastructure in house if no external provider meets his needs.

In the absence of open standards and available open source implementations, even with enough choice of providers, there remains a full dependence on the software provider, though.

Technological dimension

With regard to sovereignty over the means of production, it is thus mandatory that we also analyze the technological self-determination of digital offerings.

For the time being, we will ignore the area of hardware and focus entirely on software. This also corresponds to the observation of Kagermann et al:

"In traditional contexts such as data centers, hardware is a readily available, standardized commodity. The users of enterprise software and other similar types of software can freely choose which hardware (e. g. PCs and notebooks) they use and are thus able to avoid dependence on individual manufacturers. As long as hardware and software are decoupled, it doesn´t matter that there are no German hardware suppliers of note in the private and commercial markets." - (Kagermann, Streibich, and Suder 2021)

However, in the scope of software, on the other hand, proprietary licenses and vendor lock-in effects can create dependencies that ultimately contradict a self-determined usage of this technology.

The answer is a global movement that originated in the late 1980s:

"The open source movement has brought the world a new way of developing software", as Dirk Riehle points out correctly in his plea "The Unstoppable Rise of Open Source". Open source is a "development method for software that harnesses the power of distributed peer review and transparency of process. The promise of open source is better quality, higher reliability, more flexibility, lower cost, and an end to predatory vendor lock-in." - (Riehle 2013)

This is exactly where the importance of Open Source Software for achieving sovereignty and self-determination becomes evident. While we had to assume a high level of trust in the previously mentioned local franchise example, Open Source Software can be transparently peer-reviewed at any time. Simultaneously, we are not dependent on a single technology provider and e.g. security updates can be provided by either an established community or a suitable contractor.

Only the freedom to inspect, adapt, use and share the underlying technology grants sovereignty in the sense of self-determination. From a strategic perspective in the sense of digital sovereignty, however, securing these freedoms requires much more than just the corresponding licenses.

On one hand, strategically important building blocks should also be sustained by a sufficiently active and open community that develops software according to the principles of the Four Opens.[3]

The flip side is: it requires skills and knowledge to actually be able to practice this self-determination at all. While open source makes the skill building possible, the required amount of knowledge can become prohibitive to actually exercising these possibilities. This will be the main subject of our next dimension.

The answer to this must be the collectivization of operational knowledge, just as it is being practiced for many years with software code.

Dimension of competence

The greatest software is useless if it cannot be operated confidently. But for this to happen, skills and knowledge must be built up, fostered and retained. In an increasingly competitive market for skilled people and increasingly complex IT systems, this is becoming an ever-greater challenge for governments, institutions, and companies. How can we operate digital offerings in a self-determined, secure and qualitatively excellent manner?

While software as a means of production has been and is being increasingly collectivized thanks to the open source movement, organizations continue to protect op-

[3] The Four Opens are a set of principles guidelines that were created by the OpenStack community as a way to guarantee that the users get all the benefits associated with open source software, including the ability to engage with the community and influence future evolution of the software. See https://openinfra.dev/four-opens.

erational knowledge like a holy grail. How sovereign can an organization act, if precisely this important knowledge only adds to the lottery factor?[4]

The answer to this must be the collectivization of operational knowledge, just as it is being practiced for many years with software code. So, we need to build communities who collaborate on exchanging and recording this experience and the tooling built to simplify the automation of operational processes. We create a climate in which operations is not supposed to never make any mistakes – instead we create infrastructure that is robust against mistakes and a culture where openly talking about mistakes – even beyond organizational boundaries – and learning from them is appreciated and considered a strength. We learn more from our mistakes than from our successes – usually because we analyze them much more intensely.

We are still at the beginning of a new movement, which is becoming increasingly important as the overall complexity of software stacks increases. For true self-determination in the ever-growing digital realm, we urgently need to build skills and share the gained knowledge freely and in unlimited ways also in the realm of operational knowledge — exactly the way we started with software code almost 40 years ago.

Let's start closing the gap to have open source style collaboration not just for the Dev piece in DevOps. And this is just another urgently needed piece to enhance and grow the overall digital capabilities for achieving sovereignty in the digital realm.

Sources

- Couture, Stephane, and Sophie Toupin. 2019. "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?" New Media & Society 21 (10): 2305–22. https://doi.org/10.1177/1461444819865984.
- Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen des Digital Gipfel 2018
- European Data Protection Supervisor. 2020. EDPS Public Paper on Outcome of Own-Initiative Investigation into Eu Institutions' Use of Microsoft Products and Services. Publications Office. https://doi.org/doi/10.2804/14519.
- Kagermann, Henning, Karl-Heinz Streibich, and Katrin Suder. 2021. Digital Sovereignty: Status Quo and Perspectives. Acatech Impuls. acatech - Deutsche Akademie der Technikwissenschaften. https://www.acatech.de/publikation/digitalesouveraenitaet-status-quo-und-handlungsfelder/.
- Oppenheim, L., and McNair Arnold Duncan McNair. 1926. International Law / a Treatise by L.oppenheim. 4th Ed. Ed. By A.d.mcnair. Book. 4th ed. Longmans Lond.
- Philpott, Daniel. 2020. "Sovereignty." In The Stanford Encyclopedia of Philosophy, edited by Edward N. Zalta, Fall 2020. https://plato.stanford.edu/archives/fall2020/entries/sovereignty/; Metaphysics Research Lab, Stanford University.
- Riehle, Dirk. 2013. "The Unstoppable Rise of Open Source / Der Siegeszug von Open Source." It - Information Technology 55 (5): 171–72. https://doi.org/doi:10.1515/itit.2013.9005.

Eduard Itrich

Eduard Itrich is an open source and infrastructure evangelist currently empowering the Sovereign Cloud Stack community at the OSB Alliance (Open Source Business Alliance). After graduating from university, he was part of a software development team and responsible for the release management of a Linux enterprise distribution. Following up his two-year parental leave, during which he orchestrated his twin daughters rather than continuous deployment pipelines, he became the head of digitization and IT of a medium-sized town in southwestern Germany. In his spare time, he hangs around at Section77 e.V. — a local CCC affiliated Hackspace in Offenburg — and enjoys playing around with electronics.
Contact details: https://scs.community/itrich

Kurt Garloff

Kurt Garloff has spent his professional life with open source projects. Educated as physicist (in Dortmund and Eindhoven), he has a desire to fundamentally understand things. Applying this to computers made choosing open source a natural consequence. Leading the growth of SUSE Labs, he had the opportunity to forge successful teams from brilliant individuals. Since 2011, his focus is on cloud technology and is an active participant of the Open Infrastructure Community. As VP Engineering at Deutsche Telekom and later as chief architect of the Open Telekom Cloud, he has been involved with building quite some open source cloud infrastructure. Since early 2020, he is working with an increasing number of co-workers on defining and assembling a standardized, open, modular technology stack that enables a large number of operators to jointly provide a large, federated, open cloud. This is the Sovereign Cloud Stack (SCS) project of the Open Source Business Alliance, is part of Gaia-X, has received a significant grant and has released R1 in September 2021.
Contact details: https://scs.community/garloff

Felix Kronlage-Dammers

Felix Kronlage-Dammers has been building (open source) IT Infrastructure since the late 90s. Between then and now Felix was part of various open source development communities (from DarwinPorts, OpenDarwin to OpenBSD and nowadays the Sovereign Cloud Stack). His interests range from monitoring and observability over infrastructure-as-code to building and scaling communities and companies. He has been part of the extended board of the OSBA for the last six years and describes himself as an unix/open source nerd. If not working, he is usually found on a road bike.
Contact details: https://scs.community/kronlage-dammers

[4] The lottery factor, also referred to as bus factor, is a measurement of the risk loosing key technical experts that kept information and knowledge unavailable to the rest of the organization.