Digital Sovereignty in Switzerland : the laboratory of federalism

Benhamou, Yaniv; Bernard, Frédéric; Durand, Cédric

Digital Sovereignty in Switzerland: the laboratory of federalism

Yaniv Benhamou / Frédéric Bernard / Cédric Durand*

This paper analyses the issues of digital sovereignty in Switzerland, particularly from a socio-economic and legal standpoint. It aims to contribute to the general debate on digital sovereignty in Switzerland and abroad, including on a Swiss cloud. Beyond Switzerland, the specificities of the Confederation (federalism and distributed competencies) make its ecosystem an interesting laboratory for digital sovereignty. This analysis follows a complete multidisciplinary study carried out within the framework of the Latin Conference of Digital Directors (CLDN), based on desk research and interviews.

Content

* Yaniv Benhamou is associate professor of Digital law at the Faculty of Law of the University of Geneva and specialized in data protection, intellectual property, internet and media law. He is admitted to the Geneva Bar and Attorney-at-law Of Counsel in a Geneva law firm. Frédéric Bernard is professor of Public Law at the University of Geneva and is specialized in administrative law, constitutional law, human rights and the fight against terrorism. In 2010, he was a visiting scholar at the University of California, Berkeley. He is admitted to the Geneva Bar and is Of Counsel in a Geneva law firm. Cédric Durand is economist, associate professor at the University of Geneva and member of the Centre d'économie Paris Nord. Working within the tradition of Marxist and French Regulationist Political Economy, he studies globalization, financialization and contemporary mutations of capitalism. The authors would like to thank M. Ammihud Joseph (researcher at the Digital Law Center) for his help in translating and finalizing the text.

Executive Summary

Digital sovereignty can be defined as the ability of authorities to maintain their strategic autonomy, i.e. to be able to autonomously use and control the tangible and intangible assets and digital services that impact the economy, society, and democracy. Digital sovereignty has several components, mainly "technological sovereignty" and "data sovereignty". Digital technology redefines the notion of "territory" into "sovereignty on networks", which has several layers (hardware, software, and data), with the State being able to exercise exclusive sovereignty over the 1st layer (hardware) and limited sovereignty over the 2nd and 3rd layers (software and data). Finally, the degree of sovereignty is assessed according to the State's ability to control each layer, which will depend in particular on the location of the data or access to the data, and the nature and links of the service provider with the State in question. Policy and regulatory strategies may also address the different actors in the digital ecosystem (public, industry, and civil society).

From the socio-economic standpoint, the study analyses Switzerland's dependencies on the three layers (hardware, software, data) and from the point of view of the different actors (public, industry, civil society). It concludes that Switzerland has strong digital assets but that there are issues to watch out for, in particular the fact that consumer digital activity and intellectual property are concentrated in the hands of a few companies (with effects on privacy, public policy, and economic development). It also describes an autonomy-sophistication dilemma: dependencies increase in proportion to the intensity of ICT use. Consequently, measures shall be taken according to the degree of criticality. When the use is critical and complex, measures may range from data residency (or data localisation) to diversification of suppliers and shared sovereignty. The analysis also emphasises that sovereignty is not only spatial but also temporal, i.e. in terms of the ability to anticipate and react to a new situation.

From the legal standpoint, the study analyses the main components of digital sovereignty, namely data sovereignty and technological sovereignty, as well as cyberadministration and cybersecurity. Data sovereignty requires to clarify the law, including those that may have extra-territorial effects (e.g. GDPR, Cloud Act, LPD)[1] and rules on international data transfers, which may range from the free flow of data to a requirement for the localisation of data or servers. Technological sovereignty requires an innovation policy with state measures (legal, economic, and technical). This requires a careful assessment of which critical technologies (Key Enabling Technologies or KETs) can be accessed and which data protection laws apply. Cybersecurity requires coordination at different levels, depending on the area concerned (civil cybersecurity, cyberdefense, cybercrime), and requires resilient technology, adequate preparation, appropriate contracts, and compliance monitoring processes. Cyberadministration requires that the State can decide whether and how to digitise its processes and services autonomously while respecting the principles of federalism, legality, and public procurements.

[1] GDPR stands for the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016, 1-88; Cloud Act stands for Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943, 2018); LPD stands for the Swiss Data Protection Act, Loi sur la protection des données of 25 September 2020, FF 2020 7397.

On this basis, several recommendations can be made to guide public action on digital sovereignty (see II.4 and III.5)[2]. At the international level, it is also important to pursue determined diplomatic action to reduce the negative repercussions of digital sovereignty (fragmentation of the Internet, barriers to data sharing and innovation).

I. Introduction and definitions

1. Background

This paper aims to contribute to the general debate on digital sovereignty in Switzerland and abroad, including on Swiss cloud[3]. Beyond Switzerland, the specificities of the Confederation (federalism and distributed competencies) make its ecosystem an interesting laboratory for digital sovereignty[4]. This analysis follows a complete multidisciplinary study carried out within the framework of the Latin Conference of Digital Directors (CLDN), based on desk research and interviews.

Digital sovereignty presupposes that the state, the economy and society have ongoing control over their digital transformation, i.e. that they can determine whether and what information to digitize for re-use[5]. Although governments have technical expertise in this area (as shown in the rapid development of Covid applications), it is often the private sector that has control over ICT. This applies not only to market-dominant economic actors (e.g. GAFAM and BHATX)[6] who decide on the faith of data, or even replace state prerogatives

---

2 For an overview of all recommendations, see the complete report Benhamou/Bernard/Durand, 41 ff.

3 FDF/UPIC, Swiss Cloud Report; Swiss Digital Strategy 2023: These 2 reports consider the issues of Cloud and digital sovereignty as priorities and conclude that there is a need to clarify the concepts (e.g. terminology, degrees of sovereignty) and the legal framework (e.g. to reduce the risks of data access by third parties, such as foreign authorities). The purpose of this contribution is precisely to answer these questions.

4 For an analysis of the EU, see Brunessen, 15 ff; Moghior, 104, highlighting the difficulty of finding a consensus due to the decentralised nature of the institutions and the heterogeneity of the Member States. The Swiss example can be another example of decentralised institutions that neighboring countries could learn from, with its governance and consensus mechanisms.

5 Tan/Chi, 1; FDF/UPIC, Swiss Cloud Report.

6 GAFAM stands for the US tech giants, namely Google (Alphabet), Apple, Facebook (Meta), Amazon and Microsoft; BHATX stands for the Chinese tech giants, namely Baidu, Huawei, Alibaba, Tencent and Xiaomi.

(e.g. via their general terms of use, authentication techniques, or by making states dependent on their services with digital currencies or reliable authentication techniques) but also to non-market-dominant actors who create dependencies with other operators[7]. Economic actors thus acquire *de facto* normative power in cyberspace[8].

Given the emergence of new power relations, politicians frequently use the concept of digital sovereignty in their speeches with the aim of restoring the centrality of the nation-state[9]. However, this concept is not yet clarified, making achieving coherence at the decision-making and operational levels difficult. The rapid proliferation of initiatives in digital sovereignty also complicates the delimitation of the concept and the distribution of powers between the different levels of the state. The diversity of initiatives can be highlighted by models or indexes that quantify digital sovereignty based on indicators, such as the components of digital sovereignty[10]. However, these models vary according to the country and/or entity concerned, and no such model exists in Switzerland at the moment.

It is worth noting that, while it is logical for Switzerland to take a position on digital sovereignty, this debate may also have negative repercussions on society, such as the fragmentation of the Internet, barriers to data sharing for the common good and to innovation (e.g. the development of technologies such as web3)[11].

---

7 COTTIER, N 8; TÜRK and references; JÄGER et al., 189.

8 TÜRK and references; POHLE/THIEL, 6 ff; SEIFRIED/BERTSCHEK, 10 ff.

9 FALKNER et al., 3; AUFRECHTER/KLOSSA, 11, indicating that the concept of digital sovereignty is also used as a pretext for economic protectionism, referring to a US government report of 2021.

10 KALOUDIS, 8 ff; European Commission, Digital Economy and Society Index (DESI) 2022 (<https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>); PUGLIERIN/ZERKA, 5 ff; LU/MAYER, 5, regarding the Digital Dependence Index (DDI).

11 See DIPLOFOUNDATION, Balancing digital sovereignty and the splinternet (event report), Internet Governance Forum, 2022; GANNE, 101; CORY/DASCOLI, stating that data localisation requirements have doubled in 4 years worldwide; WEBER, who talks about "Splinternet", "digital sovereignism".

2. Definitions

The term "digital sovereignty" has not yet been defined in a harmonised way at the international or national level. However, several attempts to define have emerged, notably in the academic world. The concepts (a), components (b) and territories (c) at stake will be analysed to better define the outlines of this concept and to establish terminological benchmarks.

a) Concepts

An initial approach is to define the two terms that make up the concept. "Digital" refers to the infrastructure, the underlying technologies, the data and its contents and their consequences on society, culture and processes[12]. Sovereignty refers to the territory of a state, i.e. sovereign actor that is the nation (external sovereignty) and that has a monopoly on the rules of law and law enforcement (internal sovereignty)[13]. However, this classical approach is criticised because it does not take into account the new power relations exercised by non-state actors (e.g. internet users or platform operators)[14].

Digital sovereignty is also often defined from a technological standpoint, which sometimes distinguishes three degrees of sovereignty (high, medium and low) for each stage of the life cycle of a digital system and data[15]. Beyond technology and given the transversality of the issues, it is interesting to define the notion from a multidisciplinary standpoint, in particular socio-economic and legal. The latter prefers the notion of 'strategic autonomy' to that of digital sovereignty. Strategic autonomy refers to the ability of a state or organisation to decide and act autonomously and over the long term on key digital aspects of its economy, society and democracy[16]. While a state's digital sovereignty has become inseparable from technology, strategic autonomy refers to the means to achieve it, i.e. the state's ability to control ICTs and data[17]. This

---

12 Couture/Toupin, 2306.

13 See art. 2 UN Charter; Pohle/Thiel, 49; Alcaud; INTERNET SOCIETY, Navigating Digital Sovereignty and its Impact on the Internet, december 2022; Norodom, 21 ff: political and economic contexts can create divergent approaches to the same concept by state entities. A "liberal" view is traditionally opposed to a more "protectionist" view of digital sovereignty.

14 See footnote 5.

15 Couture/Toupin, 2313; Pohle/Thiel, 6 ff; Kaloudis, 16.

16 Moerel/Timmers, 8 and references; Tan et al., 4 and references; Danet/Desforges, 179 ff; Schmitz Seidl, 12.

17 Chrétien/Drouard, 15 ff; Danet/Desforges, 184; Moerel/Timmers, 8.

definition seems more precise and better delimited than the notion of "digital sovereignty", in particular because it would avoid the legal controversies linked to the recognition of the "sovereignty" of non-state or supranational actors[18].

b) Components

Digital sovereignty includes several components, mainly "technological sovereignty" and "data sovereignty"[19]. Technological sovereignty refers to the ability of a State and its economic operators to control the layers (hardware, software, data)[20]. Data sovereignty refers to the capacity of the different actors (administration, industry, civil society) to control and use data in a self-determined way[21]. It therefore implies control over the personal and non-personal data stored and processed, including access rights (on a contractual or technological basis)[22].

Data sovereignty (control over data) has become central in an ultra-connected society given the security and privacy issues at stake[23]. As data are strategic assets, states also seek to minimise foreign interference with state or private, sensitive or strategic data (e.g. through espionage methods). In order to protect against intelligence activities and to protect the Swiss economy, the concept of the "*Swiss cloud*" emerged in political circles[24], which evolved into the notion of "*sovereign cloud*".

Sovereign cloud can be defined as a *cloud computing* environment controlled, deployed and/or managed locally within a single jurisdiction. The idea is that the user organisation retains control over the data, systems and applications. The requirements vary according to the degree of control: for some, the provider, data, systems and/or applications must be managed locally; for

---

18 See MOEREL/TIMMERS, 8 and DANET/DESFORGES, 180; SCHMITZ/SEIDL, 31.

19 Other dimensions of sovereignty can also be considered, such as "network sovereignty", "information sovereignty", "platform and infrastructure sovereignty", "economic sovereignty", "energy sovereignty". See KAGERMAN ET AL., 13; POHLE/THIEL, 6 ff; SEIFRIED/BERTSCHEK, 6 ff; TAN ET AL., 4; SWISS DATA ALLIANCE, 2, indicating that "data sovereignty" is central for digital sovereignty.

20 See. *below* III.3; FABIANO, 272; BERTANI ET AL., 7; COUTURE/TOUPIN, 2317; KAGERMAN ET AL., 10.

21 See. *below* III.2; GOLLIEZ, 83; CELESTE, 211 ff; KALOUDIS, 6.

22 GOLLIEZ, 83: distinguishing three axes of data sovereignty: the use of non-personal data by as many actors as possible ("*open data*"), the use of personal data by the persons concerned ("*my data*") and the sharing of sensitive data between companies and administrations under strict conditions ("*shared data*").

23 See *below* III.1; TAN ET AL., 2.

24 FDF/UPIC, Swiss Cloud Report, 22 ff.

others, it is sufficient that the data is inaccessible from abroad. There are thus different degrees of cloud sovereignty according to the following 3 components: (*i*) data sovereignty (controlling who owns and accesses the data) regardless of the data localisation a single territory (data residency), (*ii*) operational sovereignty (controlling operations on services, including business continuity and regulatory compliance), (*iii*) technical sovereignty (performing operations oneself without relying on a provider)[25].

c) Territories

Technologies evolve in a context of interconnected global communications networks without well-defined spatial territories. We are therefore shifting from an approach of "territorial sovereignty" to a notion of "sovereignty over networks"[26].

These networks (new forms of territories) are composed of several layers over which the State can exercise its authority: (*i*) physical layer (ICT components and technical capacities located on a spatial territory) (*ii*) logical layer (codes and standards governing the ICT components, making it possible to exchange information between them) and (*iii*) data layer (data circulating on the networks)[27]. The degree of sovereignty will depend on the State's ability to control each layer. The State can exercise exclusive sovereignty over the 1st layer (physical) and limited sovereignty over the 2nd and 3rd layer (logical and data) which have no spatial limits[28].

d) Actors

Digital sovereignty requires political and regulatory strategies, which may involve various actors in the digital ecosystem (the State through public and semi-public entities, industry, civil society), each of which plays different roles and can be described as "governance and regulatory levers"[29]. The State is the

---

25 CAPGEMINI, referring to a sovereign cloud *continuum* and distinguishing several categories of cloud (from least to most sovereign): (i) Public Cloud (without local providers and without restriction as to the jurisdictions from which services are deployed), (*ii*) Hybrid Cloud (without local providers but with pre-approved data centres), (*iii*) *Open source Cloud* (for software and/or components of foreign origin), (*iv*) Private Cloud (i. e. local providers, and only local data) (*v*) *Full in-house private cloud* (i.e. local providers, data and components).

26 VATANPARAST, 1; CHAPDELAINE/MCLEOD, 66; COTTIER Cyberespace, 205 ff; ROGUSKI, 5.

27 ROGUSKI, 5; DUCHEINE, 458 ff; GOLDMAN, 17-1; SHEIKH, 6.

28 This is subject to a nationalisation of cyberspace (e.g. China and Russia). ROGUSKI, 10 ff.

29 COUTURE/TOUPIN, 2317; TÜRK and references; POHLE, 14; GUEHAM, 12; POHLE/THIEL, 8.

first actor concerned. Through its regalian and regulatory functions, the state plays a key role in protecting state or critical infrastructures, the population and industry[30]. Industry also has a decisive role as technology companies influence innovation and generate skills. Civil society is an essential lever of governance and regulation within a democratic system. The term 'weak sovereignty' is used when these issues are driven by the private sector (e.g. in the form of self-regulation) and 'strong sovereignty' when they are driven by the state (e.g. in the form of strict regulation and safeguarding national security)[31]. The term 'internal sovereignty' is also used when rules and policy are focused on internal processes and 'external sovereignty' when they are internationally oriented[32].

This report defines digital sovereignty as the development of strategic digital autonomy. It is the right and ability of political entities to autonomously (independently and/or self-determinedly) use and control tangible and intangible assets and digital services that significantly impact democracy, the economy and society.

3. Digital sovereignty initiatives

Digital sovereignty is subject to numerous initiatives, both internationally, abroad and in Switzerland.

At the international level, it should be recalled, without going into detail, that digital sovereignty has become a major issue, it being recalled that the debate on digital sovereignty may also have negative consequences and that some people are calling for increased international collaboration to reduce these risks[33].

Abroad, digital sovereignty initiatives vary by region and state. Three approaches to digital sovereignty can be identified: the first one focused on entrepreneurial freedom (e.g. in the US), the second one on the state (e.g. in

30 FABIANO, 270; TAN ET AL., 5.

31 COUTURE/TOUPIN, 2313; POHLE/THIEL, 6 ff; CELESTE, 6; POHLE, 6; KALOUDIS, 7.

32 BENDIEK/STÜRZER, N 20; SWISS DATA ALLIANCE, 3, looking at "digital sovereignty" from an international perspective and asking how Switzerland can promote its objectives (positive approach) and protect itself from interventions by other actors (negative approach).

33 DIPLOFOUNDATION (op.cit.).

China), the third one on the individual (e.g. in the EU)[34]. In the EU, digital sovereignty is mainly envisaged in the strengthening of local European capabilities, in particular in its dimensions of infrastructure and *cloud* platforms (also called "*sovereign cloud*") and cybersecurity[35]. At the strategic level, it focuses on artificial intelligence on the one hand and on data on the other hand[36]. At the regulatory level, it aims to create norms allowing the emergence of global standards (e.g. RGPD with extra-territorial effects) and to limit access to the European market for non-European companies (e.g. by controlling access to data)[37]. At the national level, several Member States (e.g. Germany, France) follow the same approach centred on European values (freedom, tolerance and solidarity), some having a real policy of digital sovereignty[38]. Finally, it is generally observed that the EU is pushing to emancipate itself from foreign technology by creating European "champions", while smaller or more liberal countries want to benefit from the best technologies available.

---

34 DETEC / DFAE, Création d'espaces de données fiables, sur la base de l'autodétermination numérique, 30 March 2022, 35; BENDIEK/STÜRZER; BAISCHEW ET AL., 63 ff; CELESTE, 8 ff; BARRINHA/CHRISTOU, 362: reminding that the concept of digital sovereignty in the EU has appeared for the first time explicitly in the field of cyber security, in particular in the December 2020 EU Cyber Security Strategy. For other jurisdictions, see ERGAS/BRANIGAN, 75 ff (Australia), YEN, 105 ff (Taiwan); YUGUCHI, 75 ff (Japan).

35 As an European sovereign cloud project, mention should be made of the Gaïa-X project launched in 2020. As cybersecurity projects, the "cloud (EUCS)" certification issued by ENISA or "SecNumCloud" issued by the French National Agency for the Security of Information Systems (ANSSI), guarantees a level of cybersecurity, the location and processing of data in the EU, as well as immunity to the extraterritoriality of foreign laws. For critics of the Gaia-X project (notably because of the possible participation of non-European private actors in its board of directors and because of extra-territorial laws), see LUZEAUX, 14 ff.

36 Among many documents, see BURWELL/PROPP, 11: defining data and AI as the Lifeblood of Digital Sovereignty.

37 BURWELL/PROPP, 15.

38 For example, Germany and France are keen to develop indigenous skills in relevant technology areas to counterbalance non-European suppliers and are investing in certain strategic areas (hardware (infrastructure and hardware), software (applications and software), artificial intelligence, cyber security, digital platforms and data). For Germany, see BMWK, Shaping the Digital Transition: SEIFRIED/BERTSCHEK, 6 ff; LAMBACH/OPPERMANN, 7; WEBER H., 15 ff; BURGFRIED/RECKERT-LODDE, 611 ff. For France, WOOD ET AL., 11; BAISCHEW ET AL., 63 ff; AUFRECHTER/KLOSSA, 11, reminding that already in 2006 President Chirac called on Europeans to develop an indigenous information search capacity to respond to the "global challenge posed by Google and Yahoo" and that already in 2010 the French government was alerting about the loss of sovereignty to foreign technology companies.

In Switzerland, public digital policies have already been considered, without defining digital sovereignty or strategic autonomy[39]. As Switzerland is a federal state, reflections on digital sovereignty are conducted at all levels of the state (federal, cantonal, communal and intercantonal)[40] as well as in the academic world[41] and civil society[42]. The difficulty of solving the challenges of digital sovereignty can be illustrated by several concrete cases, such as the electronic patient record or cybersecurity.

II. Socio-economic issues

Digital sovereignty is a concept used in many ways. However, they all refer to a central meaning: to what extent is a political entity able to control the 3 layers (physical, logical and data)[43]. This question of control of the layers arises from the point of view of the various actors, in particular national security, economic development and the capacity of the authorities to preserve the rights of individuals and their autonomy of individual and collective action. These three dimensions of digital sovereignty (regalian, economic and civic) depend on the more or less important capacities to supervise and standardise the design and use of technologies and data[44]. These capacities are themselves a direct function of Swiss ICT capacities (1), and of their material (2) and intellectual (3) dependence.

---

39 MAYER/LU, 5.

40 At the federal level: FDF/UPIC, Swiss Cloud Report. At the cantonal and communal level: for example, in Geneva, the Geneva Digital Policy, 37 ff and in Vaud, the Digital Strategy, 35 ff. At the intercantonal level: see PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, 4.; CLDN.

41 For example, in spring 2022, the University of Geneva set up a "UNIGE Digital Sovereignty" think tank, which is working on drafting a Charter of Good Practice.

42 See SWISS DATA ALLIANCE, which brings together companies, professional associations, civil society organisations, research institutions and individuals to establish a future-oriented data policy in Switzerland.

43 See *above* I.2.c); CHANDER/SUN, 283; FLORIDI, 369 ff; FALKNER ET AL., 3.

44 See *above* I.3.

1. Swiss ICT capacities

Switzerland consistently ranks high in the indexes assessing digital development and ICT usage[45]. This assessment is based on nationally developed infrastructure, services and skills that play a favourable role for innovation. But it is also a potential source of social, economic and political vulnerability. This is the case in the field of cybersecurity, where Switzerland is considered to be lagging behind due to poorly developed legislation and insufficient preparation of public authorities for major incidents[46]. It is also the case of the omnipresence of foreign technological devices, i.e. devices produced, developed and/or controlled outside the country. Thus, the notion of digital sovereignty implies taking into account the degree of dependence of a country on the rest of the world in general and on certain countries in particular with regard to ICTs. This dependence cannot be reduced to a single metric and must be understood in its material and intellectual dimensions[47]. Rather than seeking a state of unattainable and undesirable autarky, it is a question of pointing out the vulnerabilities and potential problems that they pose.

2. Material dependence

The degree of Switzerland's material dependence in the digital domain can be assessed on the one hand through usage data from internet browsing and on the other hand through trade. With regard to usage data (i.e. data from devices such as computers, smartphones and tablets used from Switzerland), the studies show a total dependence on foreign hardware infrastructure (e.g. Apple and Samsung accounting for 85% of the equipment used in Switzerland)[48]. With regard to trade, the studies also show a dependence on certain

---

45 Switzerland was 3rd in 2017, International Telecommunication Union (ITU), ICT Development Index 2017 (website); World Economic Forum (WEF), Global Competitiveness Index 2017-2018 (website); Portulans Institute, Network Readiness Index, Switzerland (<https://networkreadinessindex.org/country/switzerland/>).

46 Switzerland was 23rd in the 2021 edition of the National Cyber Security Index of the Estonian e-Governance Academy. eGovernance Academy, National Cybersecurity Index (website). It should be noted that the Confederation is currently making numerous efforts to improve cybersecurity, in particular with the transformation of the NCSC into the Federal Office for Cybersecurity.

47 See Lu/Mayer, 5 ff.

48 Statcounter GlobalStats, Browser Market Share Worldwide (<https://gs.statcounter.com/vendor-market-share/mobile/switzerland/2022>).

countries (e.g. around 85% of consumer hardware, computers, telephones and components are imported, 95% of which come from China)[49].

3. Intellectual dependence

Dependencies are not limited to hardware, but also refer to intellectual aspects (e.g. computer services and softwares)[50]. This is particularly sensitive for government services, including in their regalian functions, when they have to call on foreign service providers for office suites, specialised software or specific audits, including in the field of technological security.

With regard to usage data, the studies show total dependence on foreign software infrastructure, whether for browsers or platforms, with American companies dominating (e.g. Microsoft, Apple and Google account for 90% of operating systems)[51]. Trade in digital services (e.g. computer services, software and telecommunications) is less unbalanced. At the global level, imports of digital services account for 56% of trade (compared with 76% for ICT goods) and are more geographically diversified. A country's intellectual dependence requires a global view of intellectual property[52]. The concentration of intellectual property in the digital fields on a global scale is a source of vulnerability for Switzerland as for most countries. The United States has the most digital patents in the world (42%), followed by Japan (23%) and South Korea (8%), accounting for three quarters of digital IP. China and Germany account for 8% and 3% respectively, leaving only 15% for the rest of the world. Among the main digital fields (e.g. semiconductors, audiovisual technologies, telecommunications, coding/decoding), Switzerland relies on foreign intellectual property with only 0.9% of Swiss patents.

The development of learning and adaptive algorithms has major implications for human-machine relations, economic competition, and military-police control capabilities[53]. Despite having one of the highest densities of artificial intelligence researchers in the world, this development is a concern for

---

49 DFAE, Strategy China 2021-2024, 28-29.

50 Haskel/Westlake, 153.

51 Statcounter GlobalStats, Browser Market Share Worldwide (<https://gs.statcounter.com/os-market-share/all/switzerland/2022>).

52 Pagano, 1413.

53 Durand/Rikap, emphasising that the dynamics of intellectual monopolisation in the digital age cannot be reduced to patent issues, but also include specific logic relating to returns to scale associated with massive data and the modalities of innovation.

Switzerland's digital sovereignty, as it is for other European countries[54] and most other countries except China and the United States, which are in exclusive rivalry in this area[55].

This duopoly is mostly a success of consumer platform firms in these two countries. Conversely, the lack of consumer platforms comparable to *Big Tech* in Europe and in Switzerland[56] has negative effects. Since user data is one of the main fuel for innovation in this field, without the huge pools of user data generated by consumer platforms it is very difficult to be at the frontier of the evolution of artificial intelligence[57]. Countries such as Switzerland are exposed to the consequences of external developments of these powerful technologies, but over which they have almost no control.

4. Recommendations

As an outcome, Switzerland has strong strengths in the digital field, in particular thanks to the quality of its infrastructure and skills that are reflected in the dynamic and balanced foreign trade in digital services. Such trade is however unbalanced on the hardware side, particularly in terms of the terminals used, but this is part of a more general context of international fragmentation of production processes and is not a concern, at least as long as there are various supply options.

However, a first worrying concern relates to the consumer digital activity on the Internet which is almost entirely in the hands of American companies (Apple, Microsoft, Alphabet, Meta). There is a threefold issue of sovereignty here. Firstly, in terms of control of personal data and respect for privacy. Secondly, in terms of public action, the data controlled by *Big Techs* not only makes it possible to better understand individual behaviour but also to influence it[58]. Thirdly, in terms of long-term economic development. The rise of artificial intelligence is largely driven by the mass harvesting of data by consumer platforms and has implications for the security of individuals, organisations and political institutions based in Switzerland as well as for future economic development.

---

54 GROTH/STRAUBE, 7.

55 LUNDVALL/RIKAP, 2 ff.

56 See *above* II.2.

57 GROTH/STRAUBE, 7.

58 A recent example is the impact of social networking platforms on the health of young and old.

A second important concern relates to intellectual property in digital fields which is concentrated on a global scale in American and Asian companies (Japan, Korea, China). This limits the ability of Swiss-based entities to act, with cumulative effects on innovation, as in the case of data.

	General capabilities	*Physical infrastructure*	*Massive data*	*Intellectual property*
Vulnerability	***low***	***moderate***	***strong***	***strong***
Highlights	– *good quality of infrastructure* – *high competence* – *cybersecurity to be strengthened*	– *unbalanced trade in consumer goods and equipment* – *balanced trade in components (core industrial competencies)*	– *uses of consumer data monopolised by US platforms* – *development of artificial intelligence*	– *concentration of intellectual property* – *limits to innovation capacity* – *economic cost*

Table 1. Summary assessment of sovereignty issues in the field of ICT

These vulnerabilities exposed on the material and intellectual levels result in the existence of an autonomy-sophistication dilemma (Figure 1). Authorities must be aware that being at the forefront of digital uses may result in a loss of autonomy, both in terms of public action and data control by individuals and industry. Indeed, since the State cannot control ICT in all its dimensions given the dependencies exposed, the vulnerability of the various domains grows in proportion to the intensity of ICT use.

This difficulty is unavoidable, but it must be the subject of an assessment of the degree of criticality of the various uses of digital technology within and outside administrations, in order to guide public action in terms of digital sovereignty. This cannot be done *a priori* and requires a multi-criteria assessment of what is critical from a digital sovereignty standpoint, in the regalian, economic and social fields. On the basis of such an assessment by

domain, four configurations can be identified, involving distinct measures depending on the complexity of the systems mobilised and the degree of criticality[59].

1. When the uses are not critical and simple, it is *desirable* to maintain openness (blue zone). This ensures dissemination of the most effective solutions to local actors and allows for learning effects.
2. When the uses are critical and simple (green zone), it is *necessary* to develop local solutions guaranteeing maximum sovereignty, especially as relatively inexpensive solutions allow this.
3. When the uses are critical and complex (red zone), it is *desirable but difficult* to develop local solutions ensuring full sovereignty. When the issues at stake are essential for the community, it is important to preserve a capacity for action that is not hindered by dependence on actors beyond the reach of public action. These solutions can be very costly. In the event that they are completely out of reach, because it is not possible to exercise genuine sovereignty, public action must seek ways of limiting the risks incurred, either through protective measures, or in the selection of the entities with which it contracts, or by seeking cooperation enabling it to exercise shared sovereignty.
4. When the uses are both uncritical and complex (orange zone), the development of autonomous solutions is either out of reach or extremely costly while the issues are not essential. Openness is then *necessary*.

[59] See Luzeaux, 16, who speaks of 3 levels of sovereignty, namely (1) weak with limited control over vital infrastructure, (2) partial with limited control over critical infrastructure and (3) complete with extensive control.

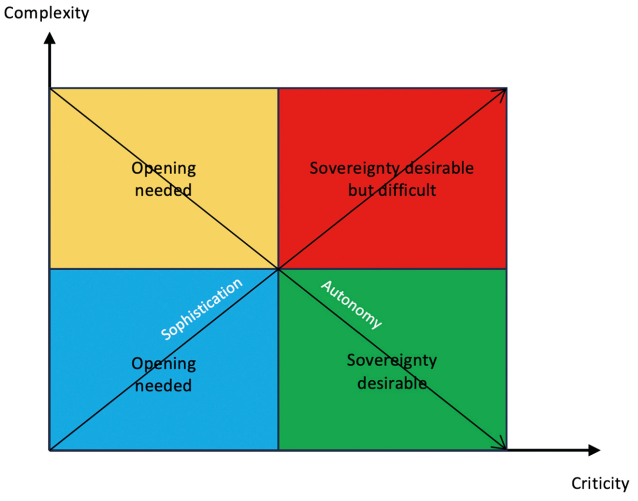

Figure 1. The autonomy-sophistication dilemma in data processing

In sum, with regard to dependencies, it is *recommended* to adapt the measures according to the degree of criticality of the various digital uses within and outside administrations (e.g. critical and simple uses; complex but not very critical; critical but simple; critical and complex). In the latter case (critical and complex uses), measures may range from data residency to diversification of suppliers or the search for cooperation for shared sovereignty[60].

Finally, temporality should be taken into account. Indeed, the question of criticality evolves over time. While some issues are crucial at all times (control of administrative and tax data, confidentiality in military and diplomatic matters), other applications that are *a priori* less sensitive (e.g. in the field of education, transport or health infrastructures) may suddenly become so in a geopolitical crisis. In particular, it should be borne in mind that legal guarantees of data access abroad are not equivalent to political and material control over data on national territory. Only the latter is a real guarantee of sovereignty in the event of a major geopolitical crisis, as the Covid-19 crisis and the war in Ukraine have reminded us.

[60] For the concept of shared and cooperative sovereignty, see Weber, Digital Sovereignty revisited, 77.

Sovereignty is thus not only spatial but also has a temporal dimension[61], i.e. in terms of the ability to anticipate and the time an authority has to react to a new situation. In a field where innovation is very dynamic, it is difficult for public authorities to anticipate relevant problems upstream through regulation alone. Indeed, territorial location requirements are not necessarily a sufficient guarantee, as an entity resident in Switzerland and controlled from abroad could be subject to decisions contrary to the country's interests by the parent company. This is all the more true as the very question of nationality is not self-evident when it comes to effective economic control: is it the address of the head office, the majority of the shareholding, the nationality of the *management*? Based on these uncertainties, public authorities could be led to take shareholdings in the resident entities on which they depend for critical services, so as to have an internal view of the issues that directly concern their sovereignty[62].

III. Legal issues

The legal challenges are numerous, starting with the variety of legal regimes that apply depending on the components, layers and actors involved[63]. Among the main legal regimes, one thinks of personal data protection laws[64] and intellectual property, unfair competition and contractual rights[65]. There are also fundamental rights[66], cybersecurity and secrecy issues (e.g. art. 320 CP;

---

61 JESSOP, 41-61.

62 This would mean going further than the Swiss Cloud Report recommends. See FDF/UPIC, Swiss Cloud Report.

63 For the components, layers and actors, see *above* I.2.

64 The monitoring of compliance with data protection laws by companies and federal bodies is the responsibility of the Federal Commissioner, while the monitoring of compliance with cantonal laws by the cantonal administration is the responsibility of the Cantonal Commissioner, which may lead to divergent interpretations of the legal framework.

65 Beyond personal data, data in general (e.g. industrial and technical data) are at the heart of technologies, which explains why they are subject to several legislative developments in Switzerland and abroad. See DE WERRA, RSDA, 365 ff and the references; BENHAMOU Y., RSDA, 393.

66 At the international level, one thinks first of the general instruments protecting human rights (ECHR; UN Covenant II; Convention 108). At the national level, one thinks of the Cst./CH, in particular the right to personal freedom (art. 10 para. 2 Cst./CH), the rights to privacy, informational self-determination and protection against the misuse of personal data (art. 13 Cst./CH) and the right to freedom of information (art. 13 Cst./) and to freedom of information (art. 16 Cst./CH). One also thinks of the cantonal constitutions, including those revised and containing a catalogue of fundamental rights (e.g. in Geneva art. 14-43 Cst./GE, and Vaud art. 9-38 Cst./VD).

art. 47 LB and 321 CP)[67]. The analysis of legal issues will focus on the two components of data sovereignty (1) and technological sovereignty (2), as well as on cyberadministration (3) and cybersecurity (4) as prerequisites for digital sovereignty.

1. Data Sovereignty

a) Extra-territoriality of laws

The concept of territorial sovereignty has been undermined over the last decade by the extraterritoriality of certain laws that apply to events occurring abroad (e.g. GDPR and *Cloud Act*). This generally serves strategic and economic objectives[68]. For example, the GDPR protection extends to all data subjects who are in the European Union, regardless of the actual location of the data[69]. The *Cloud Act* gives authorities a right of access to data located outside the US but managed by US companies[70]. Swiss law also provides for laws with extra-territorial effect, such as the DPA (art. 3 DPA)[71].

This extraterritoriality of laws leads to a certain decline in territorial sovereignty, or even to a deterritorialisation of law, it being specified that it creates

---

67 CP stands for the Swiss criminal code, code pénal suisse RS 311.0; LB stands for the Swiss banking act, loi sur les banques, RS 952.0. FDF/UPIC, Swiss Cloud Report, 27; FEDERAL COUNCIL, Federal IT Strategy 2020-2023, 6.

68 THELISSON, 524 ff; BRADFORD, who speaks of the "*Brussels effect*" of the GDPR in imposing data protection standards on a global scale consisting of the EU promoting its standards and leading to a Europeanisation of the European legal framework abroad.

69 THELISSON, 524 ff, indicating that the GDPR also serves strategic and economic purposes and influences digital sovereignty as it subjects the data of European individuals to European protection regardless of their location. On the Trans-Atlantic Data Privacy Framework see INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP), Is data localization coming to Europe?, 23 August 2022.

70 THELISSON, 521, stating that the *Cloud Act* is seen as a US response to the extraterritoriality of the RGPD and complements and gives extra-territorial scope to the SCA (for *Stored Communications Act*); CASSART, 41; US DEPARTMENT OF JUSTICE, USA DoJ, White Paper, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *Cloud Act*, April 2019.

71 With the DPA, the Federal Court extended the scope of application of the former DPA by making certain data processing operations that take place abroad subject to it (see in particular ATF 138 II 346, ATF 138 II 346), before the legislator codified this theory of effects in the law, by providing that "this Act applies to facts that have effects in Switzerland, even if they occurred abroad" (art. 3 para. 1 DPA).

competition between jurisdictions[72] and that it must in any case respect international law[73].

b) Data transfer abroad

Given the strategic importance of data, states adopt rules on the transfer of data abroad. These rules can be liberal with free flow of data or restrictive with localisation requirements for data, servers and/or data controllers. These localisation requirements characterise the debate on digital sovereignty. Thus, they pursue both a legal objective (to control compliance with these rules abroad) and a political objective (to strengthen data sovereignty).

Under Swiss law, the rules on data transfer abroad provide for the free flow of data to countries with an adequate level of protection and, in the absence of such a level of protection, for the data transfer abroad subject to additional safeguards (e.g. standard contractual clauses or bilateral agreement)[74]. Thus, where there is a risk that data will be transferred to a country without an adequate level of protection, a risk assessment should be carried out and the contractual relationship should be adapted accordingly. The assessment will take into account the nature of data (e.g. ordinary, sensitive data, secret data) and the existence of a right of access to the data by foreign authorities under foreign law[75].

---

72 See THELISSON, 525, indicating that competing jurisdictions should be resolved according to the conflict of laws rules that determine the applicable law (subject to regional solutions for resolving possible conflicts through governance, such as the designation of a lead authority); PRETELLI, 22.

73 THELISSON, 513-517: *in* Swiss law, the Constitution establishes the principle of respect for international law by the Confederation and the cantons (Art. 5); MAYER, 9 ff; VAN HECKE, 309.

74 FF 2017 6594, stressing that the free flow of data is a cardinal principle of the Swiss Data Protection Act (LPD).

75 E.g. if the data is hosted by a US provider or a Swiss provider under the control of a US group, the US Stored Communications Act respectively the *Cloud Act* may give access to the authorities from US soil. See PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, 4; SCHWARZENEGGER ET AL., 83 ff. Also see FISCHER/PITTET, who distinguishes between a one-off and a general legal right of access and points out that the risk analysis must still assess the likelihood that the authority will assert this right and achieve its ends. It should be noted that the *Cloud Act is not the* only foreign regulation providing for a right of access to foreign authorities. One example is the current debate concerning the TikTok application, whose parent company ByteDance, based in China, could be required to provide access to Chinese authorities from Chinese territory, regardless of the location of the data, on the basis of Chinese law.

In European law, the rules are similar and provide for the free flow of data, even if authorities and courts sometimes limit the possibilities of transferring data abroad through a strict interpretation of the rules (e.g. the Schrems II judgment)[76] and localisation requirements for certain personal data and infrastructures (e.g. the DGA providing for data localisation requirements respectively cybersecurity certification requirements for cloud services)[77].

It should be noted that, even when data is hosted in Switzerland but with a provider controlled by a foreign group (e.g. Swiss Microsoft), some legislations have extra-territorial effects and give access to authorities regardless of the localisation of the data (e.g. *Cloud Act*)[78]. On this basis, in case of data storage and processing in Switzerland, the risk of access by foreign authorities can only be avoided when the Swiss-based data controller has no relationship or contact with foreign companies (e.g. with a US affiliate) or, if it does, when the foreign companies do not have possession, custody, control or responsibility of the Swiss entity. This kind of immunity of the Swiss-based data controller presupposes, in organisational terms, that its registered office and central administration are established in Switzerland and that its share capital and voting rights are not individually or collectively held above a certain threshold (e.g. 24% individually, 39% collectively) by third parties with their registered office, central administration or principal place of business based abroad[79].

For this reason, the use by the public administration of service providers located abroad or belonging to an American group is currently under debate. The Federal Data Protection Commissioner (FDPIC) considers that the use of M365 *cloud* (*Outlook* and *Teams* services) by the Swiss Accident Insurance Fund (SUVA) is contrary to the DPA, even if the data is hosted in Europe, on the grounds that there is a residual risk of access by foreign authorities (zero-risk approach)[80], whereas the Federal and Zurich Cantonal Administrations

---

76 European Court of Justice, 16 July 2020, C-311/18 (Schrems II).

77 See Joint Opinion 03/2021 of the EDPB and the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), adopted on 10 June 2021 (<https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en>); EDPS, Opinion of 28 February 2023 on the adequacy decision on the EU-US Data Privacy Framework.

78 See III.1.a).

79 RAMOS ET AL.

80 See FDPIC, Guide June 2021: contrary to SUVA's assessment of the risk as very unlikely (*höchst unwahrscheinlich*).

consider that such recourse for the administration is permissible provided that certain additional protective measures are taken to limit the risk of access by foreign authorities (risk-based approach)[81].

In both cases, there is a question of risk analysis, in that the lawfulness of the *cloud* is analysed according to whether or not the additional protection measures make it possible to limit the risk of access by foreign authorities[82]. The reluctance of the FDPIC is certainly due to the tightening of the practice of the European authorities regarding transfers to the United States and pending an agreement replacing the *Privacy Shield*[83]. This being said, the risk of access by foreign authorities is reduced, since a data transfer by a Swiss entity to foreign authorities would be a violation of Article 271 of the Swiss Criminal Code, which prohibits activities on behalf of a foreign state (except mutual assistance)[84].

c) Digital self-determination

Digital self-determination is a new approach to strengthening data sovereignty, in particular the control of individuals, businesses and society over their own data. It could be enshrined through the interpretation of fundamental rights[85] or through the recognition of a new right, such as the "right to digital integrity", which has been recently proposed in French-speaking cantons[86].

---

81 Federal Council, La Confédération passe à Microsoft 365, Communiqué de presse, 15 February 2023.

82 The Swiss Lawyers Bar (FSA), follows the risk-based approach but recommends caution (local solutions), at least on tax and ILL issues and if foreign legislation makes it difficult to enforce contracts. Schwarzenegger et al., 30 ff.

83 See Fischer/Pittet, citing the strict decisions in the *Google Analytics* cases.

84 See Fischer/Pittet, recalling other issues that are just as important as the access risk in the case of data outsourcing, such as data security and the need to ensure *business continuity in the event of* the provider's failure.

85 E.g. right to life and personal freedom (Art. 10 Cst./CH), from which personality rights (Art. 27 ff CC) are derived; protection of the private sphere (Art. 13 Cst./CH), from which informational self-determination is derived ATF 148 I 233).

86 Draft constitutional amendments have recently emerged in Geneva, Jura, Neuchâtel, Valais and Vaud, so as to fil the gaps of existing laws (e.g. for a right to offline life and a better cybersecurity). At federal level, the initiative 22.479 "Introduce the right to digital integrity into the Constitution" is currently under consideration, so that one can speak of the "laboratory of federalism".

2. Technological sovereignty

Technological sovereignty requires an innovation policy that includes state measures (legal, economic and technical) and international cooperation[87]. Protectionist measures (e.g. investment controls, repatriation of the value chain) should be avoided, as total independence from exclusively indigenous ICTs is unlikely, given the extreme interweaving of the Swiss digital ecosystem with the infrastructures and services deployed worldwide[88]. An innovation policy aimed at technological sovereignty requires an analysis of which technologies are critical ("*key enabling technologies*", KETs) and what measures are needed to maintain control over these KETs (in the short or medium term)[89]. It will also be necessary to improve the decision-making and operational skills of public and private users in order to strengthen freedom of choice and avoid a concentration of supply (e.g. advanced training to make up for the lack of personnel in the production and/or use of KETs)[90]. The digital transformation of government activities (e.g. e-ID identification and electronic signature) should also be reclaimed[91].

Intellectual property regulation is a key element in strengthening innovation, data protection and trade secrets (e.g. algorithms and data analysis techniques)[92]. However, regulation alone is insufficient, as only an understanding of the technologies and an *ex ante* analysis of the regulation can strike the right balance between protection and free use[93]. It is in this spirit of balance that data flow is at the heart of the development of innovation policy, including

---

87 See CHRÉTIEN/DROUARD, 24 ff; COMCO, Annual Report 2020 of the Competition Commission (COMCO), DPC 2021/1 23 ff, 42, categorising innovation policies according to 3 approaches: the "competition" approach consisting of creating European champions in order to compete with dominant players (1t approach); the "competition" approach consisting of industrial alliances with existing European players (2nd approach); the "cooperation" approach aiming at data openness and interoperability of technologies (e.g. GAIA-X) (3rd approach).

88 ILLGNER, 8 ff; SEIFRIED/BERTSCHEK, 6 ff.

89 EDLER ET AL., 19 ff; WESTPHAL, 7; CHRÉTIEN/DROUARD, 23 ff; MAURER ET AL., 53 ff; ILLGNER, 8; KALOUDIS, Action Plan, 7 ff, pointing out that access to the necessary raw materials and knowledge must also be taken into account.

90 Decision-making skills are understood as the ability to understand, evaluate and verify the reliability of solutions in the market, operational skills as the effective use of technologies to increase one's own competitiveness and innovative capacity. See SEIFRIED/BERTSCHEK, 6 ff and references.

91 TÜRK and references.

92 See MARCH/SCHIEFERDECKER.

93 PAGANO, 1413.

artificial intelligence (AI), which explains why it is the subject of numerous legislative developments in Switzerland and abroad.[94] In addition, complementary support measures (e.g. standard contracts, certification, awareness raising and training) could be used to promote data flows rather than major legislative measures[95].

3. Cyberadministration

a) Federalism and the distribution of powers

Digital sovereignty presupposes that the state can freely decide whether and how to digitise its internal processes and services to the population (*cyberadministration*) under the right conditions and independently[96]. Digital sovereignty can also mean not digitising certain services (e.g. for cybersecurity and/or digital sobriety reasons).

Digital sovereignty is a cross-cutting issue, which requires a common public policy for the Confederation, the cantons and the municipalities[97]. The main constraints stem from the federal nature of the state (federalism). The cantons are sovereign as long as their sovereignty is not limited by the Federal Constitution and their rights are not delegated to the Confederation (art. 3 Cst/CH[98]). Thus, if digital transformation (in the broad sense including administration and society) is considered a new task of the state, it is by default a cantonal task[99]. Consequently, there is a certain tension between

---

94 In European law, one thinks of sectoral or horizontal regulations, such as the GDPR, the Regulation on the free flow of non-personal data, the Open Data Directive, the Data Governance Act, the Digital Services Act, the Digital Market Act, the Data Act proposal. In Swiss law, there are several initiatives that aim to promote access to personal and non-personal data, see INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE (IPI), Rapport concernant l'accès aux données non personnelles dans le secteur privé, 1er March 2021, 4 ff; DE WERRA, RSDA, 365 ff and the numerous references cited.

95 The European certification mechanisms for a sovereign cloud are good examples that Switzerland could learn from, especially given the similar considerations that led the EU to turn to certification mechanisms, see n. 35.

96 The term "cyberadministration" is used here in a broad sense to refer both to the transformation processes of the administration and to the digitised processes themselves providing administrative services. MONTAVON, 25 ff.

97 MONTAVON, 25 ff; FDF, Digital Administration (website); FEDERAL COUNCIL, Swiss Digital Strategy 2020, 12.

98 Cst/CH stands for the Federal Constitution, RS 101.

99 MONTAVON, 53 ff.

power decentralization (which is guided by the cantonal autonomy, Art. 47 Cst/CH) and power centralization (which is guided by the efficiency principle, Art. 170 Cst/CH). This raises the question of how far the Confederation can restrict cantonal competences for the sake of efficiency.

In this context, many voices advocate the introduction of common norms and standards at all levels of the state, while others see the diversity of technical solutions adopted in the various communities that make up the federal state as an asset in terms of cyber security[100]. The cantons will also be better able to take account of their specific characteristics (e.g. large cross-border population)[101]. On the other hand, when a competence has been entrusted to the Confederation by means of a federal constitutional amendment and the Confederation has made use of its competence, the cantons are no longer competent to make certain choices (e.g. in the area of digital transformation) (Art. 49 Cst/CH; primacy of federal law)[102].

b) Principle of rule of law

Digital transformation must comply with the principle of rule of law (Art. 5 para. 1 Cst/CH), which requires that any state action be based on a legal basis (legal basis requirement) and that the latter be sufficiently precise (normative

---

100 This is illustrated by the electronic patient file (EPR) project, for which it was decided to introduce the EPR in a decentralised manner through officially certified regional "communities". See Swiss Confederation and Conference of Cantonal Health Directors, Electronic Patient Record: The introduction phase is underway, 16 August 2022. The EPR is provided for and framed by the LDEP, which was adopted in 2015 and entered into force in 2017. This is also illustrated by the LMETA, a federal law for the digital transformation, for which the federal National council wanted to give the federal government the power to issue federal technical standards, while it finally gave up upon opposition of States Council and Cantons and left the technical standards to cantonal autonomy. See Parliamentary Press Release, 18 October 2022, The elimination of divergences on the LMETA. See Montavon, 53 ff.

101 To take account of these constraints, more flexible modes of collaboration can be used (e.g. Framework Agreement on eGovernment Collaboration in Switzerland).

102 This is illustrated by the debate on the deployment of 5G technology, in respect of which the Constitutional Chamber of the Geneva Court of Justice annulled the Geneva law on buildings and various installations (LCI/GE) on the grounds that both telecommunications (Art. 92 Cst/CH) and the protection of human beings and their natural environment against harmful interference (art. 74 Cst/CH) were federal competences that had been duly implemented (in particular in the LTC, the LPE and more specifically the ORNI with regard to mobile telephone antennas). ACST/11/2012 of 15 April 2021, recitals 6 and 7.

density requirement)[103]. In our view, the digital transformation must be based on formal legal foundations (legal basis requirement), given its importance beyond the organisational measures of the administration[104]. Much of the debate surrounding digital transformation currently focuses on the requirement for a legal basis, as in the case of the LMETA[105], and the awarding of *cloud* contracts to private service providers[106]. However, the requirement for normative density must be equally analysed and well used. The technical complexity of the field and its development make it difficult to regulate exhaustively in law. To a certain extent, therefore, it seems legitimate to allow for clauses delegating powers to the executive[107], as well as references to technical standards[108].

Finally, one could consider experimental legislation, that is to say legislation that is limited in time and to specific sectors, which can be then evaluated and, if necessary, made permanent and extended to other sectors (e.g. the LLExp in Geneva)[109]. This solution would be well suited to the digital transformation of the administration and society, which is currently in the midst of a "learning phase" and characterised by legal uncertainties[110]. This solution would allow time to learn and to develop the elements necessary for the adoption of a final regulation at a later stage[111]. It should also be added that innovations may be

---

103 MALINVERNI ET AL., 683 ff; OFK-BIAGGINI, BV 36 N 13 and BV 164 N 3-4, recalling that the degree of requirement depends on the norm in question (see Art. 36 para. 1 and 164 para. 1 Cst./CH requiring that serious restrictions of fundamental rights be imposed).

104 MONTAVON, 350 ff.

105 Loi fédérale du 4 mars 2022 sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités, FF 2022 804, 2.

106 Federal Supreme Court, Decision 1C_216/2022 of 28 July 2022.

107 MONTAVON, 323: The author also identifies a phenomenon of 'legislative inversion', which reverses the traditional model of elaboration and hierarchy of norms. On this phenomenon, FLÜCKIGER, Légistique, 244.

108 ZUFFEREY, 61 ff.

109 Loi genevoise du 14 décembre 1995 concernant la législation expérimentale (RS/GE A 2 35).

110 MONTAVON, 431 ff. On experimental legislation and the precautions that must accompany its use in a rule of law, FLÜCKIGER, Légistique, 660 ff; FLÜCKIGER, Droit expérimental, 142; COTTIER, Cyberspace, 247 ff.

111 See FOJ, Guide to Legislation, 269, which sets out the principles that must be observed when creating and applying legislation of an experimental nature.

proposed at the cantonal level before being considered at the federal level, which can be called the "laboratory of federalism"[112].

c) Three steps of the implementation of public policy

In the implementation of public policy, it is useful to distinguish between different steps (each of which takes place at the three levels of the state, Confederation, canton, municipalities).

As a first step, a planning phase should be carried out to examine existing technical solutions and the risks they pose to the values and principles of the Swiss rule of law (e.g. massive data collection, concentration of a few *hyperscalers*, extraterritoriality of foreign laws, threat to secrecy), in order to identify strategic choices, such as legislative initiatives at the international or national level[113]. This implies clarifying the division of competences between the different levels of government, the role to be played by public authorities (e.g. service providers and/or issuers of an appropriate legal framework or self-regulation)[114] and the need for dedicated infrastructures (e.g. National infrastructure of network for mobility data, NaDIM in the field of national mobility data infrastructure), cooperation bodies (e.g. Swiss Digital Administration ANS in the field of cyberadministration) and the authority(ies) in charge to support or promote digital transformation within each public authority (e.g. at federal level, the Federal Statistical Office (FSO) for networking AI skills)[115]. In a second phase, the implementation phase begins, which consists of the adaptation of existing legal texts (e.g. LMETA), the creation of new bodies or

---

112 For a recent example, one can think of the draft constitutional amendment in GE for the recognition of a "right to digital integrity" (Cst.-GE) (For a strong protection of the individual in the digital space) (PL 12945), published on 30th September 2022. See above III.1.c).

113 Federal Council, Message of 4 March 2022 on the Federal Act on the Use of Electronic Means for the Execution of the Tasks of the Authorities, FF 2022 804; DETEC/DFAE, Report on the Creation of Trusted Data Spaces, 3; see also FDF/UPIC, Swiss Cloud Report, 7; FDFA, Digital Foreign Policy 2021-2024, 14; FDF/UPIC, 27; Federal Council, Federal IT Strategy 2020-2023, 6.

114 DETEC/DFAE, Report on the Creation of Trusted Data Spaces, 40.

115 At the cantonal and communal level, for example, the digital delegates who meet in the Assembly of Delegates of the Swiss Digital Administration. See Federal Chancellery, Digital Transformation and IT Governance, DTT Sector (website); FSO, New Statistical Information, Artificial Intelligence Competence Network, 25 August 2021 (<https://www.bfs.admin.ch/bfs/en/home/dscc/blog/2022-02-ecosystem.assetdetail.18164964.html>).

the selection of companies to provide the desired services[116]. In a third phase, the measures adopted, and their implementation are **monitored.** This control is carried out by judicial or supervisory bodies and may lead to changes in the adopted legislation in order to comply with the set requirements.

d) Public procurement law

Digital transformation of the administration must also take into account public procurement law, as the procurement of ICT by administrative entities from private companies is in principle subject to public procurement law[117]. This requires an analysis of the scope of application of public procurement law (e.g. which IT services are subject to the Public Procurement Agreement with their classification code).

The application of public procurement law makes the wording of tenders and the requirements set by contracting entities crucial. For example, the tender "*Public Clouds Confederation*" in 2020 for the provision of *cloud* services for a period of five years required that "*[t]he bidder must have data centres on at least 3 continents (including within the European Economic Area*"[118]. This meant that Swiss companies were excluded from the procedure and the award decision selected foreign companies. This being said, public procurement law allows a certain amount of leeway for the use of direct agreement procedures, particularly in the case of an *in-house* solution or the presence of a single company capable of supplying the required goods or services. It should also be noted that the European States are interested in the American procedures for awarding public contracts (e.g. the *Small Business Act*), which have enabled the

116 At the communal level, the Municipal Council of the City of Geneva voted on 28 June 2022, on the proposal of the Administrative Council, a credit of CHF 2,000,000 for the implementation of the Office 365 suite from Microsoft in the City of Geneva.

117 Public procurement law includes the agreements ratified by Switzerland in the field of public procurement, i.e. the WTO Agreement on Government Procurement revised in 2012 ("GPA 2012", RS/CH 0.632.231.422) and the Agreement between the Swiss Confederation and the European Community on certain aspects of government procurement concluded in 1999 (RS/CH 0.172.052.68).

118 See simap.ch, project no. 204859 (call for tender of 7 December 2020).

development of technological giants, by putting in place instruments enabling small and medium-sized enterprises (SMEs) to use public contracts to develop[119].

4. Cybersecurity

Cybersecurity is a key element in a digital society, especially in view of the risks of unauthorised access to data, manipulation of information or other forms of cybercrime, which are amplified in a technology-dependent digital society[120]. Cybersecurity is a cross-cutting issue that concerns all levels of government, especially in Switzerland, where the division of tasks is governed by federalism. However, cybersecurity has several dimensions for which the responsibility lies at different levels: civil cybersecurity requires consultation at different levels, cyberdefence is primarily a matter for the Confederation and the military, and cybercrime for the criminal prosecution authorities[121].

Cybersecurity implies the use of resilient ICT, i.e. technological means to ensure the security, confidentiality and availability of data. The sovereign *cloud* or, more generally, the storage of data in a single territory (*data residency*) is often mentioned for this purpose[122]. However, this approach may be counterproductive, as the more concentrated the data, the more vulnerable it is[123]. Instead, a diversification of hardware and software solution providers

---

119 E.g. the *Small Business Act* has directed a share of public procurement to small businesses, which has allowed innovative companies to rely on creditworthy customers to improve their products and services. For French experts, this type of instrument could be deployed at French level for innovative public procurement without contravening European law. See BENHAMOU B., Souveraineté numérique.

120 FEDERAL COUNCIL, Security Report, 7. See DURAND, 91; National Cyberstrategy, 13 April 2023, 9.

121 National Cyberstrategy, 13 April 2023, 9.

122 TIPPER/KRISHNAMURTHY, 2 ff, distinguish 4 approaches to resilience: isolationist consisting of using domestic components and local labour for a state's digital infrastructure (e.g. Russia's creation of Mir to replace Visa and Mastercard) (1st approach); cooperative consisting of entering into international treaties, agreements and standards to regulate ICT (e.g. GAIA-X within the EU) (2nd approach); competitive consisting of strategic partnerships between domestic industry and government (e.g. China's *Digital Silk Road Initiative*) (3rd approach); military consisting of mobilising military resources to protect the physical and cyber digital infrastructure (4th approach).

123 BAUER/ERIXON, 26 ff.

is needed to reduce dependencies[124], taking into account that imported technologies may contain *backdoors*[125].

Cybersecurity also requires adequate preparedness in case of a cyber incident[126], which implies the development of (production, decision-making and/or operational) skills, the establishment of contracts to maintain (legal and de facto) control over data[127] and of monitoring and *compliance* processes with regard to potential breaches of applicable regulations[128]. Cybersecurity also requires a clear legal framework, possibly by strengthening legal instruments (e.g. criminal offences, obligations to report cyber attacks)[129], by National Cybersecurity Center's (NCSC) recommendations and incentives or constraints to ensure compliance[130].

Internationally, it would be interesting to look for global solutions to protect civilians in case of state cyber attacks[131], to sanction government cyber

---

124 FEDERAL COUNCIL, Product Security and Supply Chain Risk Management in Cyber Security and Cyber Defence, 7; BAUER/ERIXON, 26: Cyber espionage, however, remains undetectable in most cases.

125 And the risk of leakage of critical data or cyber attacks on critical systems. See BERCHTOLD Carina, Have you thought about all the backdoors? *in* ICTJournal, 22 August 2022; The market is mainly dominated by US, Chinese companies and a few isolated players from Korea (Samsung), Russia (Kaspersky) and Germany (SAP). See SATW, Cybersecurity Map, Sovereignty (<https://www.satw.ch/en/cybersecurity/cybersecurity-map>).

126 Adequate cybersecurity preparedness traditionally involves the following 5 phases: identify, protect, detect, respond, recover (*NIST Core Framework*). DEFR/OFAE, IT Resilience, 14 ff.

127 Contractual commitments include the commitment to technical and organisational measures (e.g. data encryption), the absence of liability in the event of a breach of confidentiality, the obligation to inform about the precise location of the servers as well as about possible data requests by foreign authorities (*lawful access*).

128 TAN ET AL., 3; TIPPER/KRISHNAMURTHY, 2 ff.

129 These obligations are provided for in various laws and reinforce the identification of threats, in particular in the NISP (Art. 24 NISP) and in the ISL (Art. 74a ff ISL). See FF 2023 84.

130 See CHAVANNE Yannick / ZÜLLIG Yannick, Cybersecurity: the Confederation launches a prevention campaign, *in* ICTJournal, 5 September 2022; KOLLER Rodolphe, Mobilising employees to report phishing emails: it works, according to a Swiss study, *in* ICTJournal, 14 January 2022.

131 E.g. Digital Geneva Convention was envisaged to protect cyberspace. See Digital Geneva Task Force, A white paper to make Switzerland the core of digital governance in a secure digital world, 9.

attacks[132] and to subject technology companies to humanitarian law rules[133]. It would also be interesting to develop political-legal measures, such as virtual embassies (i.e. *data* storage with immunity/inviolability status like diplomatic missions)[134].

5. Recommendations

On this basis, several recommendations can be made to guide public action on digital sovereignty. With regard to data sovereignty, it is *recommended* that, when foreign laws apply in Switzerland, the courts analyse their compatibility with Swiss sovereignty before admitting their extra-territorial effects in Switzerland. When transferring data abroad (whether personal or non personal), it is also recommended that the contractual relationship be adapted to the risk of access to the data by foreign authorities, and that a local solution be preferred if critical data or infrastructures are involved.

With regard to technological sovereignty, it is *recommended* to favour European and international cooperation (instead of protectionist measures). With regard to state measures, it is recommended to favour complementary support measures (e.g. standard contracts, certification, awareness raising and training) over major legislative measures. It is also recommended to improve the skills of public and private users and to keep full control (e.g. in-sourcing) for the digital transformation of regalian activities (e.g. e-ID identification and electronic signature).

With regard to cyberadministration, it is *recommended* that the digital transformation be planned on an ongoing basis, carefully analysing the need to adapt or enact the necessary legal bases and public procurement law (e.g., wording of calls for tender or competitive bidding procedures). It is also recommended to clarify which cantonal autonomy remains and, in case of doubt, to consider that there is cantonal autonomy by default in the name of the principle of primacy of federal law and subsidiarity.

---

132 BREITENFELDT/JORDAN, 959 ff.

133 E.g. based on the Montreux Document. See DFAE Montreux Document (website) and ICRC, The Montreux Document (website).

134 The Estonian state stores a duplicate of critical data "in a friendly country", in order to ensure system continuity in case of a serious cybercriminal attack on the national state infrastructure. MONTAVON/SCHWAB, 16; ROBINSON ET AL., 391 ff; WGS/OECD, 42 ff.

With regard to cybersecurity, it is *recommended* that contracts with ICT providers that include TOMs be put in place. It is also recommended to ensure a clear legal framework, which calls for the follow-up of the NCSC recommendations and incentives or binding measures to ensure compliance. Internationally, it would be interesting to look for solutions to protect civilians in the event of state cyber attacks, to subject technology companies to the rules of humanitarian law and to develop solutions such as data *embassies*.

Bibliography

Alcaud David, Souveraineté, *in* Encyclopædia Universalis <https://www.universalis-edu.com/encyclopedie/souverainete/> (12 October 2022).

Aufrechter Fabien / Klossa Guillaume, Pour une souveraineté numérique européenne, Concilier indépendance et attractivité, Paris 2022.

Baischew Dajan / Kroon Peter / Lucidi Stefano / Märkel Christian / Sörries Bernd, Digital Sovereignty in Europe – a first benchmark, Bad Honnef 2020 (cited: Baischew et al.).

Barrinha André / Christou George, Speaking sovereignty: the EU in the cyber domain, *in* European Security, 2022, vol. 31, no. 3, 356 ff.

Bauer Matthias / Erixon Fredrik, Europe's quest for technology sovereignty: Opportunities and pitfalls, *in* European Centre for International Political Economy (ECIPE) Occasional Paper, No. 02/2020.

Baur Andreas, European Dreams of the Cloud Imagining Innovation and Political Control, *in* Geopolitics, 2023.

Belli Luca, Structural Power as a Critical Element of Digital Platforms Private Sovereignty (non-final draft), *in* Edoardo Celeste / Heldt Amélie / Iglesias Keller Clara (Ed.), Constitutionalising Social Media, 2022.

Bendiek Annegret / Stürzer Isabella, Advancing European internal and external digital sovereignty: The Brussels effect and the EU-US Trade and Technology Council, *in* Stiftung Wissenschaft und Politik (SWP) Comment, 2022, no. 20.

Benhamou Bernard, Souveraineté numérique: quelles stratégies pour la France et l'Europe? <https://www.vie-publique.fr/parole-dexpert/276126-souverainete-numerique-quelles-strategies-pour-la-france-et-leurope> (cited: Benhamou B., Souveraineté numérique).

Benhamou Yaniv, Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property-like rights, their exceptions and licensing practices, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, no. 4, 393 ff <https://archive-ouverte.unige.ch/unige:145046> (cited: Benhamou Y., RSDA).

Benhamou YAniv / Bernard Frédéric / Durand Cédric, Souveraineté numérique : étude pluridisciplinaire pour la Suisse, 2023, <https://archive-ouverte.unige.ch/unige:168718>.

Bertani Sebastiano / Caccia Andrea / Massimo Fabio / Allard Jean-Luc / Tumietto Daniele, White Paper on Digital Sovereignty, Bruxelles 2021 (cited: Bertani et al.).

Bradford Anu, The Brussels effect: how the European Union rules the world, New York 2020.

Breitenfeldt Friedo / Jordan Sylvain, Atteinte à l'indépendance de la Confédération, *in* AJP/PJA 2022, vol. 9, 959 ff.

Brunessen Bertrand (Ed.), La politique européenne du numérique, Bruxelles 2023.

Büchel Jan / Engels Barbara, The Importance of the Data Economy for Europe's Digital Strategic Autonomy, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 13-18.

Burgfried Andreas / Reckert-Lodde Andreas, Die Deutsche Verwaltungscloud-Strategie, Auf dem Weg zur Digitalen Souveränität, *in* Datenschutz und Datensichercheit (DuD), 2022, vol. 46, no. 10, 611 ff.

Burwell Frances G. / Propp Kenneth, Issue brief – The European Union and the Search for Digital Sovereignty – Building "Fortress Europe" or Preparing for a New World?, *in* Atlantic Council, 22 June 2020.

Cassart Alexandre, Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD, *in* Revue du droit des technologies de l'information, 2018, vol. 73, 41 ff.

Celeste Edoardo, Digital Sovereignty in the EU: Challenges and Future Perspectives, *in* Fabbrini Federico / Celeste Edoardo / Quinn John (Ed.), Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Oxford 2021, 211-228.

Chander Anupam / Sun Haochen, Sovereignty 2.0, *in* Vanderbilt Journal of Transnational Law, 2022, vol. 55, no. 2, 283 ff.

Chapdelaine Pascale / McLeod Rogers Jaqueline, Contested Sovereignties: States, Media Platforms, Peoples, and the Regulation of Media Content and Big Data in the Networked Society, *in* Laws, 2021, vol. 10, no. 66.

Chrétien Jennyfer / Drouard Étienne, European technological sovereignty, Paris 2022, <https://www.renaissancenumerique.org/wp-content/uploads/2022/01/renaissancenumerique_note_souverainetetechnologique.pdf>.

Cory Nigel / Dascoli Luke, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, *in* Information Technology & Innovation Foundation (ITIF), 19 July 2021 <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

Cottier Bertil, La privatisation de la fonction législative ou la face sombre de la révolution numérique, *in* LeGes, 2019, vol. 30, no. 3 (cited: Cottier, Privatisation).

Cottier Bertil, Le droit "suisse" du cyberespace ou le retour en force de l'insécurité juridique et de l'illégitimité, *in* ZSR/RDS 2015, vol. 134, no. 2, 205 ff (cited: Cottier, Cyberespace).

Couture Stéphane / Toupin Sophie, What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?, *in* New Media & Society, 2019, vol. 21, no. 10, 2305 ff.

Danet Didier / Desforges Alix, Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques, *in* Hérodote, 2020, vol. 177-178, no 2-3 (2020), 179 ff.

Département fédéral des finances (DFF) / Unité de pilotage informatique de la Confédération (UPIC), Rapport sur l'évaluation des besoins d'un nuage informatique suisse ("Swiss Cloud"), Berne, December 2020 (cited: DFF/UPIC, Swiss Cloud Report).

DE WERRA JACQUES, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non personnelles (par des licences obligatoires ou des licences "FRAND")?, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, vol. 92, no. 4, 365 ff. (cited: DE WERRA, RSDA).

DUCHEINE PAUL A. L., Military Cyber Operations, *in* DIETER Fleck / GILL Terry D. (Ed.), The Handbook of the International Law of Military Operations, 2nd edition, Oxford 2015, 458-475.

DURAND CÉDRIC / RIKAP CECILIA, Intellectual monopoly capitalism – challenge of our times, 5 October 2021 <https://socialeurope.eu/intellectual-monopoly-capitalism-challenge-of-our-times>.

EDLER JAKOB / BLIND KNUT / KROLL HENNING / SCHUBERT TORBEN, Technology Sovereignty as an Emerging Frame for Innovation Policy – Defining Rationales, Ends and Means, Fraunhofer ISI Discussion Papers Innovation Systems and Policy Analysis No. 70, July 2021 (cited: EDLER ET AL.).

ERGAS HENRY / BRANIGAN JOE, Digital Strategic Autonomy: An Australian Perspective, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 75-84.

European Commission, Digital Economy and Society Index (DESI) 2022 (<https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 >).

FABIANO NICOLA, Digital Sovereignty Between "Accountability" and the Value of Personal Data, *in* Advances in Science, Technology and Engineering Systems Journal, 2020, vol. 5, no. 3, 270 ff.

FALKNER GERDA / HEIDEBRECHT SEBASTIAN / OBENDIEK ANKE / SEIDL TIMO, Digital Sovereignty-Rhetoric and Reality, Framework Paper, 2022 (cited: FALKNER ET AL.).

FISCHER PHILIPP / PITTET SÉBASTIEN, Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?, 16 août 2022 in <www.swissprivacy.law/165>.

FLORIDI LUCIANO, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *in* Philosophy & Technology, September 2020, vol. 33, no. 3., 369 ff.

FLÜCKIGER ALEXANDRE, Le droit expérimental : Potentiel et limites en situation épidémiologique extraordinaire, *in* Sécurité et droit, 2020, vol. 3, 142 ff (cited: FLÜCKIGER, Droit expérimental).

FLÜCKIGER ALEXANDRE, (Re)faire la loi : Traité de légistique à l'ère du droit souple, Berne 2019, 244 (cited: FLÜCKIGER, Légistique).

GANNE EMMANUELLE, Can Blockchain revolutionize international trade?, Geneva 2018.

GOLDMAN JAMES E., Network Concepts, *in* WHITAKER Jerry C. (Ed.), Systems Maintenance Handbook, 2nd edition, Boca Raton / London / New York / Washington D.C. 2002.

GOLLIEZ ANDRÉ, Souveraineté des données, in SCHÄRER Claudia (Ed.), Technology Outlook 2021, Zurich / Lausanne (Schweizerische Akademie der Technischen Wissenschaften), April 2021.

GROTH OLAF / STRAUBE TOBIAS, Analysis of current global AI developments with a focus on Europe, Berlin (Konrad-Adenauer-Stiftung), 2020.

GUEHAM FARID, Vers la souveraineté numérique, Paris 2017.

HASKEL JONATHAN / WESTLAKE STIAN, Capitalism without capital: the rise of the intangible economy, Princeton / Oxford 2018.

Illgner Klaus (Ed.), Technological Sovereignty: Methodology and Recommendations, Frankfurt am Main 2020.

Jäger Wilfried / Nentwich Michael / Embacher-Köhle Gerhard / Krieger-Lamina Jaro, Digitale Souveränität und politische Prozesse, *in* Bogner Alexander / Decker Michael / Nentwich Michael / Scherz Constanze (Ed.), Digitalisierung und die Zukunft der Demokratie Beiträge aus der Technikfolgenabschätzung, Baden-Baden (Nomos) 2022, 189-204 (cited: Jäger et al.).

Jessop Bob, Redesigning the state, reorienting state power and rethinking the state, *in* Jenkins Craig / Leicht Kevin (Ed.), Handbook of politics, New York 2010, pp. 41-61.

Kagerman Henning / Streibich Karl-Heinz / Suder Katrin, Souveraineté numérique, Statu quo et champs d'action, Munich 2021 (cited: Kagerman et al.).

Kaloudis Martin, Digital Sovereignty–European Union's Action Plan Needs a Common Understanding to Succeed, *in* History Compass, 2021, vol. 19, no. 12 (cited: Kaloudis, Action plan).

Kaloudis Martin, Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan?, *in* New Global Studies, 25 October 2021 (cited: Kaloudis, Index).

Lambach Daniel / Oppermann Kai, Narratives of digital sovereignty in German political discourse, *in* Governance Journal (early view), 2022, 1 ff.

Lu Yen-Chi / Mayer Maximilian, Illusions of Autonomy? Global Digital Dependence Structures, Bonn 2022.

Lundvall Bengt-Åke / Rikap Cecilia, China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems, *in* Research Policy, 2022, vol. 51, no. 1.

Luzeaux Dominique, *Cloud* souverain: souveraineté et résilience, ou confiance ?, *in* Revue Défense Nationale, 2022, vol. 855, no. 10, 14 ff.

Malinverni Giorgio / Hottelier Michel / Hertig Randall Maya / Flückiger Alexandre, Droit constitutionnel suisse, vol. I : L'Etat, 4th éd., Berne 2021 (cited: Malinverni et al.).

March Christoph / Schieferdecker Ina, Technological Sovereigntyas Ability, Not Autarky, Center for Economic Studies and IfoInstitute (CESifo) Working Paper, 2021, no. 9139.

Maurer Tim / Skierka Isabel / Morgus Robert / Hohmann Mirko, Technological Sovereignty: Missing the Point?, *in* 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, p. 53 ff (cited: Maurer et al.).

Mayer Pierre, Le phénomène de la coordination des ordres juridiques étatiques en droit privé : cours général de droit international privé, *in* RCADI, 2007, vol. 327, 9 ff.

Montavon Michael, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Zurich 2021.

Montavon Michael / Schwab Stéphane, eGovernment : quelques comparaisons et réflexions à partir de l'exemple estonien (1/2), Revue fribourgeoise de jurisprudence (RFJ), 2019.

O'Neil Cathy, Algorithmes, la bombe à retardement, Paris 2018.

Pagano Ugo, The crisis of intellectual monopoly capitalism, *in* Cambridge Journal of Economics, 2014, vol. 38, no. 6, 1409 ff.

Pohle Julia, Digital Sovereignty, A New Key Concept of Digital Policy in Germany and Europe, Berlin 2020.

Pohle Julia / Thiel Thorsten, Digital Sovereignty, *in* Herlo Bianca / Irrgang Daniel / Joost Gesche / Unteidig Andreas (Ed.), Practicing Sovereignty, Digital Involvement in Times of Crises, Bielefeld 2021, 47-67.

Pretelli Ilaria, Conflict of Laws in the Maze of Digital Platforms/Le droit international privé dans le labyrinthe des plate-formes digitales, Zurich 2019.

Puglierin Jana / Zerka Pawel (Ed.), European Sovereignty index, ECFR/451, June 2022 <https://ecfr.eu/wp-content/uploads/2022/06/European-Sovereignty-Index.pdf>.

Ramos Gretchen / Maciejewski Andrea / Jongen Herald (Greenberg Traurig LLP), Application of the CLOUD Act to EU Entities, Memorandum to the Dutch Ministry of Justice and Security, 26th July 2022 <https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo> (cited: Ramos et al.).

Robinson Nick / Kask Laura / Krimmer Robert, The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis, *in* ICEGOV2019, Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, 2019, 391 ff (cited: Robinson et al.).

Roguski Przemysław, Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment, *in* 11th International Conference on Cyber Conflict (CyCon), 2019, 1 ff.

Schmitz Luuk / Seidl Timo, As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy, *in* Journal of Common Market Studies (JCMS), 2022, 1 ff.

Schwarzenegger Christian / Thouvenin Florent / Stiller Burkhard, Avis de droit concernant l'utilisation des services de cloud par les avocates et avocats, 2019 <https://digital.sav-fsa.ch/documents/1060627/1169162/gutachten_sav-franzoesisch.pdf/81740267-8cf0-36b1-6918-c3ddb9c71ee4?t=1618228137307> (cited: Schwarzenegger et al.).

Seifried Mareike / Bertschek Irene, Schwerpunktstudie Digitale Souveränität, Berlin 2021.

Sheikh Haroon, European Digital Sovereignty: A Layered Approach, *in* Digital Society (DISO), 2022, vol. 1, no. 25.

Tan Kheng-Leong / Chi Chi-Hung / Lam Kwok-Yan, Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization, 2022 (cited: Tan et al.).

Thelisson Eva, La portée du caractère extraterritorial du Règlement général sur la protection des données, *in* Revue internationale de droit économique 2019/4, 501 ff.

Tipper David / Krishnamurthy Prashant, Digital Sovereignty and Resilience, 1 August 2022.

Türk Pauline, Définition et enjeux de la souveraineté numérique, 14 September 2020 <https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique>.

Van Hecke George A., Le droit anti-trust : aspects comparatifs et internationaux, *in* Recueil des cours de l'Académie de droit international de La Haye, 1962, vol. 106, 309 ff.

Vatanparast Roxana, Data Governance and the Elasticity of Sovereignty, *in* Brooklyn Journal of International Law (Brook. J. Int'l L), 2020, vol. 46, no. 1, 1 ff.

Weber Herbert, Digitale Souveränität, *in* Informatik Spektrum, 2022, vol. 45, 152 ff (cited: Weber H.).

Weber Rolf H., Digital Sovereignty revisited, new elements for a shared and cooperative concept, jusletter 2023, 73 (cited: Weber R., Digital Sovereignty revisited).

Weber Rolf H., Elements of a Legal Framework for Cyberspace, *in* Swiss Review of International and European Law, 2016, vol. 26, no. 2, 195 ff (cited: Weber R.).

Westphal Kirsten, Strategic sovereignty in energy affairs: reflections on Germany and the EU's ability to act, SWP Comment 7/2021, Berlin 2021.

Wood Sam / Hoffmann Stacie / McFadden Mark / Kaur Akhiljeet / Wongsaroj Sarongrat / Schoentgen Aude / Forsyth Grant / Wilkinson Laura, Digital Sovereignty: the overlap and conflict between states, enterprises and citizens, London 2020, p. 11 (cited: Wood et al.).

Yen Huai-Shing, Digital Autonomy and Taiwan–EU Partnership, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 105-110.

Yuguchi Kiyotaka, Japan: Digital Sovereignty as an Element of the Economic Security, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 75-84.

Zufferey Jean-Baptiste, Le traitement de l'énergie en droit de la construction : Une belle illustration des problèmes du renvoi aux normes techniques, *in* Hottelier M. / Foëx B. (Ed.), La propriété immobilière face aux défis énergétiques : Du statut juridique de l'énergie au contrôle des loyers, Genève 2016.