Digitale Souveränität

Einordnung von digitalen Einflüssen auf das Territorium der Schweiz

Management Summary

Digitale Souveränität ist ein Teilaspekt von Souveränität. Viele Menschen scheinen den Begriff heute umfangreicher zu verstehen. Wie er genau zu verstehen ist – darüber gehen die Meinungen auseinander. Dieses Whitepaper richtet sich an alle, die am politischen und gesellschaftlichen Diskurs zum Begriff «digitale Souveränität» teilnehmen. Die Swiss Data Alliance tritt für ein enges Begriffsverständnis ein.

Bei digitaler Souveränität geht es um Einflüsse auf das Territorium der Schweiz. Digitale Souveränität kommt dort ins Spiel, wo (1) digitale Vorgänge (2) einen Einfluss auf das schweizerische Territorium entfalten und (3) die Schweiz als Staat institutionell betroffen ist. Zentral sind Kompetenz und Kontrolle: Wer ist zuständig, den eigenen Einflussbereich zu kontrollieren?

Digitale Souveränität ist wichtig, weil es in der Digitalisierung nicht nur um Alltagsgestaltung geht. Es gibt Ereignisse und Entwicklungen, die systemisch wirken und einen Einfluss auf den Staat «als Ganzes» haben. Dann ist der Staat in seiner Gesamtheit «als Staat» und somit als Institution betroffen. Es geht nicht mehr nur um eine einzelne Amtsstelle, ein einzelnes Unternehmen oder eine Einzelperson:

- Vor einer Volksabstimmung fluten Bots die sozialen Medien mit gezielten Desinformationen, und mit Deep Fakes wird versucht, das Vertrauen in Behördeninformationen zu unterminieren.
- Systematische Hackerangriffe legen grosse Teile der Energieversorgung oder der Kommunikationsinfrastruktur in der Schweiz lahm.
- Die E-ID ist eine Vertrauensinfrastruktur für die ganze Schweiz. Auch der neu aufgesetzte Prozess zur politischen Abstimmung dieses wichtigen Vorhabens hat Leuchtturmcharakter für die Zukunft.

Der Staat kommt dort zum Tragen, wo ein Thema für Einzelne zu gross ist und der Staat diesbezüglich Zuständigkeit beansprucht – und zwar, weil er sie beanspruchen soll und kann (Verfassung). Das Sollen orientiert sich an einer Leitvorstellung («So wollen wir den Staat haben!»). Souveränität kommt somit dort ins Spiel, wo der Staat institutionell betroffen ist (z.B. systemisch, als Ganzes oder existenziell).

Alltagsgestaltung bleibt weiterhin Aufgabe von Privaten, Unternehmen oder von Amtsstellen. Im eigenen Zuständigkeitsbereich ist man selbst zuständig, seine Situation zu kontrollieren. «Alltagsgestaltung» meint den Handlungsbereich von uns allen – was über das Institutionelle hinaus reicht. Dieses Verständnis läuft auf das Subsidiaritätsprinzip hinaus (juristisch unpräzis als das Prinzip, Verantwortlichkeiten auf die kleinstmögliche Ebene oder Einheit zu verlagern). Es ist im föderalistischen Bundesstaat der Schweiz fest verankert.

Was der Staat soll, bedarf Definitionsarbeit. Souveränität ist Resultat von gemeinsamem Wollen und Sollen. Allenfalls entstehen Gesetze, aus denen Müssen oder Ansprüche resultieren können. So verstanden schafft digitale Souveränität Klarheit und begünstigt Handlungsfähigkeit. Die Schweiz muss festlegen, in welchen Bereichen sie Handlungsfähigkeit beansprucht. Nach schweizerischer Tradition ist damit kein Appell zu Wirtschaftsförderung oder sonstigen wirtschaftspolitischen Massnahmen verknüpft.

Dieses Whitepaper erläutert die drei eingangs erwähnten Aspekte (Digitales, Territorium, Staatlichkeit) im Sinne eines Gestaltungsansatzes für digitale Souveränität und nennt Ergänzendes zur Alltagsgestaltung. Wenn digitale Souveränität nichts anderes ist als Souveränität mit Fokus auf das Digitale, braucht es keine weitere Definition. Souveränität bedeutet Gestalten. Die Schweiz muss sich, ihre Position und ihren Ansatz im Digitalen definieren. Dies ist eine grosse Aufgabe – und eine grosse Chance.

Weiterführende Dokumente

- Begriffspapier «Datensouveränität» (2022), verfügbar unter swissdataalliance.ch/datensouveränität.
- Grundlagendokument «Digitale Souveränität» mit der Herleitung wichtiger Aussagen in diesem Whitepaper, u.a. auch Aspekte des US Cloud Act, verfügbar unter swissdataalliance.ch/souveränität.

Inhaltsverzeichnis

MITWIRKENDE
Christian Laux, Guido Greber, Lara Burkhalter,
Tobias Abt, Jonas Bärtschi, Paula Zimmermann

Version 1.0
(13. Juni 2024)

1. Warum dieses Whitepaper?

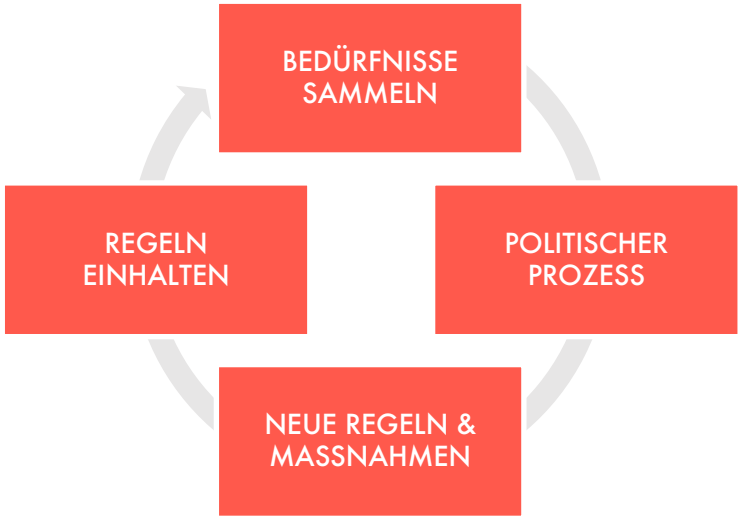
Die Reaktion auf das Aufkommen von allen Kreisen verfügbaren Maschinen mit künstlicher Intelligenz hat uns gezeigt, dass unsere Gesellschaft bereit ist, innert weniger Monate neue Technologien zu adoptieren. Dabei ist die Macht der modernen Technologien erneut spürbar geworden. Zugleich greift ein Gefühl von Ohnmacht in der Bevölkerung um sich. Die Entwicklung verläuft zunehmend exponentiell.

Uns stehen transformierende Veränderungen bevor. Und diese verlangen nach zukunftsweisender Gestaltung. Wie soll unsere Zukunft aussehen?

Wir sollten nicht vorwärts irren. Die Schweiz soll ihre digitale Zukunft selbst gestalten. Dabei sollte sie agieren. Sie sollte nicht reagieren müssen und nicht in ungewollter Weise gesteuert werden – von Kreisen, die dazu nicht berufen sind, sei es von innen oder von aussen. Es geht um Handlungsfähigkeit und Gestaltungsmacht. Gestalten heisst auch Verändern: Entwicklungen nachzuvollziehen und neue Veränderungen zu antizipieren.

Wo ist unser Nordstern? Wie behalten und benutzen wir unseren digitalen Kompass? Und wie bewahren wir im Ganzen unsere Identität? Die Verfassung gibt den Rahmen für Antworten zu diesen Fragen. Zugleich wird die Frage gestellt, was Souveränität «im Digitalen» bedeutet (z.B. Postulat Z'graggen, Motionen Juillard und Chappuis). Die Antwort scheint nicht einfach zu sein. Das Thema bewegt und ruft nach Klärung.

Die Swiss Data Alliance schlägt vor, schweizweit einen Diskurs zu führen darüber, an welchen Zielen sich die Schweiz im Digitalen orientieren soll. Sie schlägt die Methode vor, zunächst in aller Breite zu erheben, welche Bedürfnisse in der Gesellschaft, bei Unternehmen, Behörden und in der Politik geäussert werden. Dies soll das Meinungsspektrum aufzeigen. Daran anknüpfend kann der Diskurs geführt werden:



Die Swiss Data Alliance ist der Meinung, dass es für diesen Diskurs eine Klärung des zentralen Vokabulars braucht. Wichtige Begriffe sollten vorgängig geklärt sein, damit der Diskurs gelingt. So wird die Methode nutzbar. Sind wichtige Begriffe nicht geklärt, wird der Diskurs unnötig gebremst. Zentral ist dabei ein gemeinsames Verständnis darüber, wo der Begriff der digitalen Souveränität zu verorten ist. Dieses Whitepaper unterbreitet einen Vorschlag, wie man mit diesem zentralen Begriff zu greifbaren Resultaten kommt. Damit wird klar: Mit der Definition von digitaler Souveränität ist es nicht getan. Die Begriffsklärung ist notwendig, aber nicht ausreichend. Daran anknüpfend beginnt erst die eigentliche Arbeit.

2. Digitale Souveränität

Weil die Diskussion zur Souveränität für die Schweiz sehr wichtig ist und sachlich geführt werden sollte, erarbeiten wir in diesem Dokument ein Modell, das bei der Einordnung helfen soll: Geht es bei einem Thema um digitale Souveränität – und wenn ja, wer ist dafür zuständig?

2.1. BEZUG ZUM DIGITALEN

Vor einer Abstimmung in der Schweiz beeinflussen ausländische Bots die sozialen Medien.

In diesem fiktiven Beispiel geht es um digitale Souveränität. Es schält den Bezug zum Digitalen heraus, doch sind alle drei Kriterien des Modells – Digitales, Territorium, Staatlichkeit – vorhanden:

- Der digitale Bezug ist durch die Kommunikationskanäle gegeben (Social Media).
- Der Bezug zum Territorium der Schweiz besteht darin, dass es um die Beeinflussung einer hiesigen Abstimmung geht.
- Der Fall weist zudem einen institutionellen Bezug zur Staatlichkeit auf: Wenn die Schweiz ihre politische Willensbildung (Abstimmung) nicht schützen kann, ist das Staatswesen als Institution beeinträchtigt.

FAZIT

Digitale Souveränität ist dort betroffen, wo ein Bezug zum Digitalen, ein Bezug zum Territorium sowie ein institutioneller Bezug zur Staatlichkeit gegeben ist.

2.2. BEZUG ZUM TERRITORIUM

Ein Australier verübt in seiner Heimat ein Verbrechen. Belastende Informationen, deren Offenlegung in Australien zu einer Verurteilung führen würden, speichert er in einer Datei und legt sie auf einem Server in der Schweiz ab.

Welche Rechtsordnung bestimmt in diesem fiktiven Beispiel die Strafverfolgung – die schweizerische oder die australische? Während in der physischen Welt die rechtlichen Zuständigkeiten weitgehend geklärt sind, ist der digitale Sachverhalt komplexer. So lassen sich die Daten des Australiers aus drei Gesichtspunkten betrachten: Mit Fokus auf ihren Inhalt («Content Layer»), mit Fokus auf ihre Codierung in einer Datei («Code Layer») oder mit Fokus auf ihren physischen Speicherort («Physical Layer»).

Physical Layer
z.B. Standort des Servers

Code Layer
z.B. Art der Verschlüsselung

Content Layer
«Inhalt» der Daten

Im Beispiel wirkt die Datenspeicherung in der Schweiz eher zufällig. Obwohl es mit der Speicherung der Daten einen Bezug zum Territorium der Schweiz gibt (das Gehäuse des Servers ist auf schweizerischem Boden verschraubt), ist es viel naheliegender, dass der Fall unter die australische Rechtsordnung fällt.

FAZIT

Bei Fällen mit einem digitalen Bezug ist die sachliche Nähe besonders zu beachten. Es ist verleitend, den physischen Standort der Datenhaltung (Physical Layer) besonders stark zu gewichten. Oftmals ist ein Fokus auf den inhaltlichen Bezug (Content Layer) angemessener.

2.3. BEZUG ZUR STAATLICHKEIT

Die Schweiz ist digital souverän, wenn sie im digitalen Bereich handlungsfähig ist. Ausschlaggebend ist dabei die Handlungsfähigkeit der Eidgenossenschaft als Institution.

Die Eidgenössische Finanzmarktaufsicht FINMA gibt in einem Rundschreiben Vorgaben zu Auslagerungen (Outsourcing) ins Ausland.[1] Die «Sanierbarkeit» bzw. «Abwickelbarkeit» einer Bank in der Schweiz muss gewährleistet bleiben. Die FINMA schreibt ausdrücklich, dass der «Zugriff auf die dafür notwendigen Informationen … jederzeit in der Schweiz möglich sein» muss.

Das Beispiel schält heraus, welche Art von Staatlichkeit die Abgrenzung zwischen digitaler Souveränität und Alltagsgestaltung erlaubt. Im Anschluss werden wiederum alle Kriterien – Digitales, Territorium, Staatlichkeit – geprüft).

- Im Beispiel besteht ein digitaler Bezug (Datenzugriff).
- Der Bezug zum Territorium der Schweiz ist ebenfalls gegeben.
- Die Handlungsfähigkeit der Eidgenossenschaft als Ganzes ist bei diesem Thema kaum je beeinträchtigt.

Die FINMA hat eine öffentliche Aufgabe. Diese Aufgabe ist für die schweizerische Volkswirtschaft wichtig. Könnte die FINMA die zur Abwicklung einer Bank erforderlichen Informationen nicht lesen, wäre sie in der Ausübung ihrer öffentlichen Aufgabe beeinträchtigt. Braucht es dazu Datenhaltung in der Schweiz?

Die Frage ist nicht abschliessend geklärt. Wie auch immer die Antwort ausfällt: Sofern die Schweiz nicht systemisch betroffen ist (es geht nicht um eine systemkritische Bank, der Vorfall ist auf eine einzelne Bank beschränkt), bleibt der schweizerische Staat selbst dann funktionstüchtig, wenn die FINMA im Zugriff auf Daten beeinträchtigt wäre.[2] Der Staat ist nicht institutionell betroffen. Es handelt sich also nicht um eine Frage der digitalen Souveränität.

FAZIT

Die digitale Souveränität der Schweiz wird dort tangiert, wo die Funktionstüchtigkeit des schweizerischen Staates gefährdet ist. Sie ist nicht gefährdet, wenn im digitalen Alltag einer einzelnen Amtsstelle Schwierigkeiten auftauchen – es sei denn, es handle sich um ein Systemereignis[3] (grosse Tragweite, institutionelle Auswirkung).

[1] Rundschreiben 2018/3 Outsourcing, Rz. 31, abrufbar unter finma.ch/de/dokumentation/rundschreiben.

[2] Natürlich wird die FINMA dem Vorfall nachgehen und allfällige Rechtsverletzungen sanktionieren. All dies beeinträchtigt aber nicht die Handlungsfähigkeit der Schweiz als Gesamtes.

[3] Art. 23 Abs. 1 lit. a StPO (Anwendungsfall: Erpressung einer Magistratsperson) ist ein Beispiel für «deklarierte» institutionelle Betroffenheit: Das Ereignis braucht keine systemische Wirkung zu haben, muss den Staat nicht existenziell bedrohen oder die Funktionsfähigkeit des Staats als Institution nicht beeinträchtigen, und dennoch deklariert die Eidgenossenschaft in einem solchen Fall, dass die Bundesanwaltschaft tätig werden soll (mit Blick auf die institutionelle Betroffenheit).

3. Gestaltung des digitalen Alltags

Digitale Souveränität steht auf dem Spiel, wenn es um den Staat als Institution geht. Alles andere ist Alltagsgestaltung. Welche Software eine Behörde für sich auswählt, ist z.B. eine Frage der Alltagsgestaltung:

Eine Schweizer Behörde baut in der Cloud-Umgebung eines grösseren Hyperscale-Anbieters Applikationen. Sie nutzt dafür Container-Technologien, die auf einem Open-Source-Standard beruhen. Dadurch ist es möglich, dass die Behörde ihre Applikationen in kürzester Zeit auf die Container-Umgebung eines anderen Anbieters migriert, bevor sie ihren Vertrag mit dem Hyperscaler kündigt.[4]

Open Source Software kann hilfreich sein, um in der Gestaltung des digitalen Alltags Abhängigkeiten zu reduzieren und mehr Handlungsoptionen zu eröffnen – zumindest, wenn genügend Fachpersonen vorhanden sind, die die Software pflegen und weiterentwickeln können. Doch geht es dabei um eine Frage der digitalen Souveränität? Nein. Doch wie ist es, wenn es um Software für eine Amtsstelle geht?

- Der Bezug zum Digitalen ist gegeben.
- Ein Bezug zum Territorium der Schweiz ist etwas schwieriger zu bejahen.
- Ein Bezug zur Staatlichkeit mit institutioneller Wirkung liegt mit grosser Wahrscheinlichkeit nicht vor.

Würde eine Amtsstelle statt Open-Source-Software eine proprietäre Software einsetzen, käme der schweizerische Staat kaum in Bedrängnis. Souveränität betrifft die Staatlichkeit. Diese kann neben der Beziehung zu anderen Staaten (Gestaltung nach aussen) auch die Gestaltungsfähigkeit nach innen betreffen. Doch muss der Staat institutionell beeinträchtigt sein (z.B. systemisch, in seiner Gesamtheit), wenn man von Souveränität sprechen möchte. Dies ist bei Open Source Software nicht der Fall. Im Vordergrund steht vielmehr der Wunsch nach einer Gestaltung des digitalen Alltags in der Schweiz. Das ist ein grundlegend anderes Anliegen, als die Staatlichkeit der Schweiz zu sichern.

FAZIT

Es ist richtig und wichtig, bei Ausschreibungen potenzielle geschäftliche Abhängigkeiten und Risiken im Hinblick auf den Datenzugriff zu berücksichtigen. Dabei geht es aber selten um die digitale Souveränität des Staats, sondern vielmehr um die Gestaltung des digitalen Alltags. Dies gilt es zu unterscheiden.

Wenn der Staat frühzeitig erkennt, dass eine kritische Mehrheit von Amtsstellen einem Risiko mit erheblicher systemischer Tragweite ausgesetzt ist, können bestimmte Massnahmen gerechtfertigt sein. Diese müssen aber verfassungsrechtlich im Rahmen des Zulässigen bleiben, was beispielsweise die Wirtschaftsfreiheit angeht (z.B. Beobachten und Informieren, anstatt auf der Nachfrageseite wettbewerbswidrig zu koordinieren).

[4] Ein Hyperscaler ist ein Anbieter von IT-Ressourcen auf Basis des Cloud Computing, dessen Ressourcen in hohem Mass skalieren, damit viele Kunden auf denselben Ressourcen ein individuelles Nutzungserlebnis geniessen. Container: Anwendungssoftware benutzt jeweils Ressourcen der gesamten Systemumgebung (z.B. Betriebssystem etc.). Diese Systemumgebung kann als Behälter (Container) aufgesetzt werden. Der Container enthält alle Elemente, die zur Ausführung von Programmen in beliebigen Umgebungen erforderlich sind. Der Container kann dann auf unterschiedlichen Cloud-Plattformen eingerichtet werden (und somit auch die Anwendungssoftware, die eigentlich interessiert).

4. Wer ist zuständig? Wofür?

In der Schweiz sind Zuständigkeitsfragen weitgehend vom Leitgedanken des Subsidiaritätsprinzips geprägt. Dies gilt auch im Hinblick auf die Digitalisierung. Somit sind Individuen, Unternehmen und Amtsstellen in erster Linie selbst zuständig für die Gestaltung ihres digitalen Alltags und für die Abwehr negativer digitaler Einwirkungen.

Wenn ein Unternehmen wegen Fehlern im digitalen Alltag strauchelt (z.B. als Folge ungenügender Schutzmassnahmen gegen Cyberangriffe), steht dies in der Regel nicht im Konflikt mit der digitalen Souveränität der Schweiz.[5]

Entsprechendes gilt prinzipiell auch für Amtsstellen: Sie müssen das Recht einhalten und haben in einem gewissen Bereich einen Ermessensspielraum, was die Alltagsgestaltung angeht. Ein weiteres, in welcher Art auch immer dem Recht vorgelagertes «Souveränitätsziel» müssen sie nicht erreichen.

Im Souveränitätsbereich soll der Staat als Institution aktiv sein. Hier hat der Staat Garantieverantwortung. Für einzelne Individuen, Unternehmen und Amtsstellen ist dieser Bereich «zu gross». Verfassung und Gesetze fassen diesen Bereich in Worte, und es resultieren daraus Vorgaben, Pflichten und Ansprüche. Amtsstellen wenden auch in diesem Bereich das Gesetz an. Für das «Ob» gibt es hier kein Ermessen. Für das «Wie» gibt es auch hier Ermessen.

FAZIT

Individuen und Unternehmen sind für die Gestaltung ihres digitalen Alltags und die Abwehr negativer Einflüsse primär selbst zuständig. Darüber hinaus gibt es Bereiche, wo der Staat Garantieverantwortung trägt und wirken muss. Sollte eine Anpassung dieser staatlichen Zuständigkeit (Garantieverantwortung) nötig sein, so muss dies über den regulären demokratischen Prozess geschehen

5. Praktische Anwendung

Auf Basis der vorstehenden Ausführungen können nun Massnahmen zur Definition der Politik zur Souveränität entworfen werden. Nachdem die Frage von Digitalität und Territorium beantwortet ist, kann der Bezug zur Staatlichkeit geprüft werden.

5.1. VORFRAGE: ANALYSE DER HANDLUNGSFÄHIGKEIT

Jene, die den Alltag gestalten müssen (Private, Unternehmen, Amtsstellen), sind zunächst selbst verantwortlich, für Kontrolle zu sorgen:

- **Kontrollieren kann nur, wer versteht**: Amtsstellen, Private und Unternehmen müssen verstehen, welche Daten sie auf welcher Schicht einer Infrastruktur speichern und inwiefern Drittzugriffe drohen bzw. inwiefern auf andere Weise ihre Zielsetzungen gefährdet sind (z.B. Aufrechterhaltung des Betriebs, Änderungsfähigkeit, Reaktionsfähigkeit). Es kann sich dabei um Ziele handeln, die sie sich setzen oder die sie erfüllen müssen, z.B. wegen zwingender gesetzlicher Regelung.
- **Dritteinfluss identifizieren**: Genereller gesprochen müssen diese Stellen in Erfahrung bringen, inwiefern z.B. die Wahl einer technischen Lösung zu einem «Dritteinfluss» führt, dem sie sich nicht entziehen können. Wenn dadurch Abhängigkeiten entstehen, sind diese zu identifizieren.
- **Gegenmassnahmen planen und umsetzen**: Mit konkreten Gegenmassnahmen sollte man solchen Dritteinflüssen begegnen. Diese Massnahmen können technischer, organisatorischer oder vertraglicher Natur sein. Die Art der Massnahmen hängt vom Nutzungskontext ab.

[5] Generell zum Konzept systemkritischer Daten in der Schweiz: «Welches sind die wichtigsten Daten der Schweiz und wie gehen wir mit ihnen um?» von André Golliez, netzwoche.ch/news/2024-03-13/welches-sind-die-wichtigsten-daten-der-schweiz-und-wie-gehen-wir-mit-ihnen-um (abgerufen am 14.03.2024).

An dieser Stelle fragt sich, ob es eine Lösung gibt für die Kontrolle: Können die Handelnden die Situation ausreichend unter Kontrolle bringen, schon ohne Hilfe des Staats?
- Wenn ja, gibt es von vornherein kein Problem (es gibt ja eine Lösung).
- Wenn nein (d.h. jene, die den Alltag gestalten müssen, können die Situation nicht selbst lösen), könnten sie sich an den Staat wenden: «Bitte hilf mir, ich kann es nicht selbst lösen.»

5.2. ANALYSE DER STAATLICHKEIT

Der so angegangene Staat (z.B. die Eidgenossenschaft) muss nun eine Position entwickeln. Zunächst, ob sich der Staat als zuständig ansieht, das an ihn herangetragene Problem zu lösen, das auf der Ebene der Eigenverantwortung nicht lösbar ist. Diese Antwort wird abhängen von der verfassungsrechtlichen Ordnung, d.h. ob der Staat überhaupt helfen muss (Bereich mit Garantieverantwortung des Staats) oder nicht.

5.3. ANALYSE DER DIGITALEN SOUVERÄNITÄT

Wenn der Staat hilft (in einem Bereich, in dem er muss) und wenn so eine Lösung zustande kommt, ist der Staat digital souverän (da der Staat «alles kann», wo er handeln muss). Gelingt ihm dies nicht aufgrund von Kräften, die er nicht kontrolliert (z.B. aus dem Ausland), ist der Staat nicht digital souverän; er kann sich offensichtlich nicht gegen die stärker bestimmenden Kräfte durchsetzen, obwohl er erfolgreich sein müsste.

Dabei sollte man berücksichtigen, dass Souveränität ein Gestaltungsprinzip ist. Es wäre verfehlt, darin eine Messgrösse zu sehen, die nur entweder «Ja» oder «Nein» als Antworten zulässt. Die Analyse resultiert in einem «mehr» oder «weniger» an Souveränität. Solche Abstufungen müssen möglich sein; denn Souveränität ist ein Spektrum.

6. Zum Diskurs über digitale Souveränität

6.1. FRAGESTELLUNGEN FÜR DEN DISKURS

Welche Massnahmen zu ergreifen sind, hängt von den Erwartungshaltungen an die Schweiz ab. Ein Inventar der Erwartungen an die Schweiz fehlt derzeit. Die Swiss Data Alliance setzt sich dafür ein, den dafür notwendigen pluralistischen Prozess zu unterstützen. Für den in Kapitel 2 umrissenen Zukunftsprozess werden die folgenden Fragen wichtig sein:

- Die Frage nach dem Bezug zum Digitalen grenzt das Thema ein (es geht um die digitale Souveränität).
- Die Frage nach dem territorialen Bezug bringt zum Ausdruck, in welchen Fällen die Schweiz Interesse haben soll. Dies sollte eher der Fall sein, wenn es ums IKRK, unsere Amtsstellen und unsere Bevölkerung geht, als wenn es um ausländische Themen und Personen geht. Die Tatsache, dass ein Server mit dem Boden der Schweiz verschraubt ist, sollte uns hier nicht fehlleiten.
- Die Frage nach der Handlungsfähigkeit ist eine Vorfrage, um zu verstehen, ob es denn überhaupt ein Problem gibt, das man sich genauer ansehen muss. Wo kein Problem ist, muss man nicht optimieren. Es kann aber Themen geben, die «zu gross» sind für jene, die den Alltag gestalten müssen. Hier könnte Staatlichkeit betroffen sein.
- Die Frage nach der Staatlichkeit entscheidet darüber, ob der Staat sich einem bestehenden Problem annehmen muss. Hier ist gestaltungsrelevant, ob der Staat institutionell betroffen ist. Wenn ja, stellt sich die Souveränitätsfrage.
- Jetzt erst geht es um die Frage nach der digitalen Souveränität. Wo sie nicht gegeben ist, will man dies erkennen (retrospektiv) und etwas dagegen unternehmen (prospektiv).

Ein Diskurs über Digitale Souveränität könnte in Schritten somit wie folgt verlaufen:

6.2. PERSPEKTIVEN IM DISKURS

Es geht beim Diskurs über digitale Souveränität um Kontrolle in der digitalen Dimension. Das «Digitale» wirkt unabhängig von nationalen Grenzen. Kontrolle muss hier ungeachtet der nationalen Landesgrenzen gedacht werden und durchsetzbar sein. Was zu klären ist: Wer ist zuständig? Wofür? Wer soll in einer hochgradig vernetzten Welt in Bezug auf welche Aspekte und mit welchen Instrumenten Kontrolle ausüben oder dafür Instrumente bereitstellen? Netzwerkeffekte sind zu berücksichtigen. Führen sie einseitig zu wirtschaftlichen oder anderen Vorteilen? Oder bestehen sogar Machtasymmetrien?[6]

Die Schweiz als stark vernetztes Land muss festlegen, wie sie sich einbringen kann, um ihre Stärken auszuspielen und ihre Souveränität zu stärken. Aus Sicht des Staates sind Massnahmen zu planen, damit er seine Ziele für die Souveränität realisieren kann. Welche Ziele dies sind, ist eine politische Frage. Man sollte diese Frage nun klären. Die Analyse kann man aus zwei zeitlichen Perspektiven beleuchten: aus einer aktuellen «Konfliktsituation» heraus oder mit Blick auf die Zukunft. Für die Massnahmenplanung ist der Blick nach vorn gefragt.

6.3. DISKUSSIONSPUNKTE IM DISKURS

Business Continuity: Die Aufrechterhaltung des Betriebs von Infrastrukturen ist abhängig davon, welche Technologie beschafft wird und davon, wie sie verwaltet wird. Beides – Beschaffung und Betrieb – gehört zur Alltagsgestaltung. Wenn beim Fedpol ein Server aussteigt, ist nicht immer gleich die Eidgenossenschaft als Institution betroffen, obwohl ein Incident auf dem Server einer Blaulichtorganisation überaus schmerzlich sein kann. Essenzielle Funktionen werden im Rahmen des Informationssicherheitsgesetzes (ISG) unter Umständen eine andere Betrachtung erfahren (enger Begriff der «kritischen Infrastrukturen»).

Swiss Government Cloud: Gemeint ist ein Angebot, das der Bund für seine Amtsstellen und evt. weitere Nutzende bereitstellt. Eine Amtsstelle, die ihre Daten speichern muss, wählt ihre IT-Infrastruktur im Rahmen der Alltagsgestaltung. Die Amtsstelle muss dabei das Recht einhalten. Aus heutiger Sicht kann man sagen: Die Amtsstelle ist frei, welche IT-Infrastruktur sie wählt, solange sie das geltende Recht einhält. Sie kann das Angebot des Bundes nutzen, aber sie könnte im Rahmen des Zulässigen auch ein anderes Angebot wählen. Derzeit wird diskutiert, wie z.B. geopolitische Aspekte ein grösseres Mass an Koordination erfordern.[7]

[6] Die Arbeiten z.B. von Henry Farrell and Abraham L. Newman betonen, dass Bezüge in Netzwerken auch zu Asymmetrien führen können und dass kritische Analyse notwendig ist, um den aus eigener Perspektive richtigen Weg festzulegen. Vgl. dazu doi.org/10.1017/S0043887114000057 Domestic Institutions beyond the Nation-State: Charting the New Interdependence Approach (S. 331-363), sowie doi.org/10.1162/isec_a_00351 Weaponized Interdependence: How Global Economic Networks Shape State Coercion (S. 42-79).

[7] Die geopolitische Grosswetterlage wird zu gewichten sein, ebenso der Bezug zur Neutralität oder das Ziel, Abhängigkeiten zu reduzieren, um aussenpolitisch handlungsfähig zu bleiben.

E-Embassy: Sollte die Schweiz eine E-Embassy nach dem Vorbild von Luxemburg[8] einrichten? Es geht um eine Frage des Business Case. Wenn der Bund andere Länder als Kunden gewinnen kann, dann kann der Bund mit seiner IT-Infrastruktur den Business Case verbessern. Wenn sich das Bundesparlament für die Swiss Government Cloud entscheidet, sollte der Bund auch das Angebot einer E-Embassy prüfen.

Datenräume: Ein Datenraum ist ein rechtlicher, organisatorischer und technischer Rahmen für die gemeinsame Nutzung und Weiterverwendung von Daten durch mehrere Akteure.[9] Im Rahmen eines Datenraumes nehmen die Daten-Akteure eine oder mehrere der folgenden fünf Rollen wahr: Datennutzer («data user»), Datenproduzenten/-lieferanten («data provider»), Datenvermittler («intermediaries»), betroffene Personen («data subjects» oder auch «concerned persons») und Nutzniesser («beneficiaries»).[10]

Zum Konzept «Datenraum»
Wer IT-Infrastrukturen (technische Komponenten für Datenpublikation, Datenaufbereitung und Datennutzung) betreibt, die dem Konzept des jeweiligen Datenraums entsprechen, ermöglicht, dass Datennutzende Zugang erhalten zu denjenigen Daten, die sie für ihre Anwendungen (datenbasierte Dienstleistungen) benötigen, und zu deren Nutzung sie gemäss Vereinbarung mit den Datenlieferanten berechtigt sind. Sofern sich die Daten auf Dritte beziehen (natürliche oder juristische Personen), haben diese je nach Ausprägung des Regelwerkes des Datenraumes die Kontrolle über die Weitergabe ihrer Daten (durch die Datenlieferanten) sowie deren Nutzung (durch die Datennutzenden) und partizipieren an den Ergebnissen der Datennutzung. Datenräume dienen somit dem Zweck, Austausche über Daten zu ermöglichen, unter Aufrechterhaltung eines grösstmöglichen Masses an Kontrolle für mehrere Interessengruppen.

Mit Blick auf diese Aspekte (Kontrolle, Nutzen für den Staat) stellt sich die Frage, ob Datenräume ein Thema der digitalen Souveränität sind. Die Antwort ist Nein. Das Potential von Datenräumen zur Optimierung von Use Cases der Datennutzung, z.B. um Fragen der Verkehrsführung besser zu lösen, ist gross. Dies ist Alltagsgestaltung. Der Nutzen entsteht ausserhalb der digitalen Souveränität, denn Datenräume stützen nicht den Staat als Institution.
Es haben sich Standards setzende Organisationen herausgebildet, die Austauschplattformen für Daten konzeptionell unterstützen. Dazu gehören die International Data Spaces Association[11] (IDSA) ebenso wie z.B. Gaia-X[12]. Die Bereitstellungen von IDSA und Gaia-X unterstützen Individuen, Unternehmen und Amtsstellen dabei, ihren Alltag zielgerichteter regeln zu können. Somit betreffen diese Initiativen den Bereich der Alltagsgestaltung und nicht die digitale Souveränität.[13]

Fake News: Der Umgang mit Fake News stellt die Gesellschaft vor Herausforderungen. Wahrheit lässt sich nicht verordnen. Welche Rolle hat der Staat, Referenzwerte (z.B. Statistik), -systeme (z.B. E-ID) und -konzepte (Einbindung breiter Kreise ins Policy Making) bereitzustellen, damit Bezugspunkte entstehen, auf die man im Rahmen des (weiterhin freien) Diskurses und Wirtschaftslebens referenzieren kann?

[8] Ein Staat kann einem anderen Staat versprechen, dessen digitale Güter (Daten, Server) zu schützen (gegen Zugriffe eigener Behörden sowie gegen solche von Dritten). Das Konzept ist nicht gefestigt. Es kann in Anlehnung an den etablierten Schutz von Botschaftsgebäuden auf fremdem Staatsgebiet definiert werden: Der Gastgeberstaat schützt Rechenzentren des Gaststaats, die auf dem Territorium des Gastgeberstaats stehen. Der Gastgeberstaat kann darüber hinausgehen und diese Rechenzentren gleich selbst betreiben, so dass der Schutzanspruch des Gaststaats sich auf Daten bezieht.

[9] Ein Datenraum ist keine IT-Infrastruktur, was oft missverstanden wird. Die Swiss Government Cloud ist z.B. kein Datenraum.

[10] Definition gemäss Swiss Data Alliance, abrufbar unter swissdataalliance.ch/glossar/datenraum.

[11] internationaldataspaces.org

[12] gaia-x.eu

[13] Obwohl Gaia-X die von ihr gesetzten Austauschstandards wie folgt bewirbt: «Gaia-X strives for innovation through digital sovereignty. Our goal is to establish an ecosystem, whereby data is shared and made available in a trustworthy environment. Our intention is that we give the control back to the users by retaining sovereignty over their data.»
So sieht es auch die deutsche Regierung: «Gaia-X Ökosystem – Souveräne Dateninfrastruktur für Europa. Mit Gaia-X entwickeln Vertreterinnen und Vertreter aus Wirtschaft, Wissenschaft und Politik auf internationaler Ebene einen nachhaltigen Beitrag zur Gestaltung der nächsten Generation einer europäischen Dateninfrastruktur. Ziel ist ein sicheres föderiertes Datenökosystem, das für digitale Souveränität der Dateninhaber, Interoperabilität sowie den Open-Source-Gedanken steht und die föderale Idee Europas umsetzt. Auf dieser Basis können Daten und Dienste zur Verfügung gestellt, vernetzt sowie vertrauensvoll geteilt und genutzt werden, um Innovationen zu fördern und die Mehrwerte der Datenökonomie für alle Datengeber nutzbar zu machen.» bmwk.de/Redaktion/DE/Dossier/gaia-x.html

Zum Begriff der «Unabhängigkeit»
Die Reduktion von Abhängigkeiten kann ein wichtiges Ziel der Alltagsgestaltung sein. Im Praktikermodell zur Planung von Technologie («CIA» für Confidentiality, Integrality, Availability, zu deutsch: Vertraulichkeit, Integrität und Verfügbarkeit) kommt Unabhängigkeit im Sinne der Sicherung von Business Continuity im Prüfpunkt «Availability» (Verfügbarkeit von Systemen und Daten) zum Tragen.

Am Beispiel Open Source: Open Source kann nützlich sein, um die Verfügbarkeit von Systemen zu sichern, wie das Beispiel in Kapitel 3 zeigt (der Einsatz von Open-Source Container-Technologien erlaubt unter Umständen die rasche Migration von Systemen von einer Basistechnologie auf jene eines anderen Anbieters). Unzutreffend wäre aber der Schluss, dass nur Open Source die Business Continuity sichert, ebenso wie die Behauptung, dass es mit Open Source nicht zu Abhängigkeiten kommen kann. Ob die Reduktion von Abhängigkeiten notwendigerweise oder besser mit Open Source gelingt (und ob es im Beispiel nicht eher um die Architekturfrage als um die Lizenzfrage geht), muss man im Einzelfall ansehen.

Statt «Unabhängigkeit» müsste man wenn schon den Gegenbegriff (d.h. Abhängigkeit) verwenden. Totale Abhängigkeit von aussen kann handlungsunfähig machen. Dagegen macht «ein bisschen» Abhängigkeit kaum je handlungsunfähig. Das heisst nicht, dass man Abhängigkeiten nicht angehen soll. Man sollte seine Abhängigkeiten im Griff haben, denn Abhängigkeit kann ein Risiko darstellen, das man mit geeigneten Massnahmen abfedern muss. Dabei gilt Methodenvielfalt.

Am Beispiel öffentliches Beschaffungswesen: Abhängigkeiten sollten im Rahmen von Ausschreibungen berücksichtigt werden. Zu viel Abhängigkeit kann ein Qualitätsfehler sein, der im Rahmen von Zuschlagskriterien bewertet werden kann. Abhängigkeit ist aber kein Ausschlusskriterium, denn jeder Entscheid begründet Abhängigkeiten. Zu bewerten und zu gewichten ist somit das Mehr-oder-Weniger der Abhängigkeit, sofern Abhängigkeit mit Blick auf den Beschaffungsgegenstand eine Bedeutung hat. Ob es diese Bedeutung gibt, ist aus der Brille der Alltagsgestaltung zu beantworten.

Dass sich aus Abhängigkeiten eine institutionell nachteilige Wirkung entwickeln kann, kann hier nicht rundweg ausgeschlossen werden (siehe den Hinweis am Ende von Kapitel 3). Aber man sollte sachlich bleiben. Mit nur potenziell denkbaren Befürchtungen sollte man anders umgehen als mit konkret drohenden Risiken.

FAZIT
«Unabhängigkeit» ist kein justiziabler Gradmesser. Man sollte in der Diskussion über Souveränität nicht mit dem Begriff «Unabhängigkeit» operieren.

7. Ausblick: Neudefinition des territorialen Bezugs

Die Digitalisierung bringt viele Chancen und Herausforderungen. In welchen Anwendungsfällen besteht ein Bezug zum Territorium der Schweiz, der wichtig genug ist, dass die staatliche Zuständigkeit beansprucht werden sollte? Nicht dieses Whitepaper soll die Antwort geben. Es steht Definitionsarbeit an, die pluralistisch und in einem breit abgestützten politischen Prozess entwickelt werden muss. Es braucht eine aktive Definition der eigenen Werte und einen Fokus auf das, was die Schweiz ausmacht. Die in Kapitel 1 vorgeschlagene Methode soll die Grundlage hierfür bieten. Wir haben es in der Hand, die digitalisierte Zukunft aktiv mitzugestalten.

Es ist nicht so, dass Digitalisierung bislang in der Schweiz nicht diskutiert worden wäre. Es gibt bereits mannigfaltige Grundlagen. Mit der anstehenden Definitionsarbeit können die bestehenden Grundlagen auf eine neue Stufe angehoben werden. Insofern ist die Diskussion zur Souveränität eine grosse Chance.

Wenn digitale Souveränität nichts anderes ist als Souveränität mit Fokus auf das Digitale, braucht es an sich keine weitere Definition für «digitale Souveränität». Aber es ist nützlich, für den Fokus auf das Digitale in der Diskussion über Souveränität gemeinsame Worte zu finden. In diesem Sinne schlägt die Swiss Data Alliance die folgende Formel für digitale Souveränität vor:

DEFINITION

Digitale Souveränität ist die Fähigkeit eines Staates im digitalen Raum, seine Zuständigkeit international zu definieren (unter Berücksichtigung der anerkannten Souveränität anderer Staaten), seine inneren Angelegenheiten zu gestalten und beides zu verteidigen.

Wie wird diese Formel mit Inhalt gefüllt? Nicht einige Wenige sollen dies tun. Es braucht einen integrativen und pluralistisch geführten Diskurs. Die Swiss Data Alliance schlägt vor, in einer nächsten Phase an einem runden Tisch Positionen und Bedürfnisse aus der ganzen Schweiz zusammenzutragen. Die Meinungsvielfalt muss zur Geltung kommen, bevor der Blick durch das Kaleidoskop ein gemeinsames Zielbild offenbart. Der nächste Schritt soll allen Gehör verschaffen – auch jenen, die bislang wenig wahrgenommen wurden. Die eigentliche Arbeit steht somit noch bevor. Aber es liegt das Potenzial vor uns, als Schweiz den Weg in die Zukunft selbständig zu gestalten. Diese Chance sollten wir jetzt ergreifen.