SATW-Diskussionspapier

Überlegungen zu e-Society in der Schweiz

Dass die Digitalisierung unser Zusammenleben und unsere Wirtschaft nachhaltig prägt, ist unbestritten. Es ist notwendig, dass Parlament und Regierung diese Themen vorantreiben und die Rahmenbedingungen schaffen, um die Gesellschaftsordnung und den Werkplatz Schweiz auch in einer von digitalen Abläufen bestimmten Zukunft zeitgemäss, wettbewerbsfähig und erfolgreich zu halten.

Nach wie vor sind jedoch grundlegende Bausteine für die Digitalisierung in der Schweiz zu diskutieren und – dem Zeitgeist entsprechend – auch vor einer flächendeckenden Inbetriebnahme umfassend praktisch zu erproben. Fragen, wie die Gesellschaft mit den rasanten Veränderungen umgeht und wie die «e-Society» in der Schweiz aussehen soll, haben sowohl rechtliche, regulatorische, technische, als auch soziale und gesellschaftlich-politische Aspekte. Was bedeutet die Souveränität eines Landes im digitalen Raum und welches sind die Grenzen unseres Landes in Zukunft? Welche Prozesse und Dienstleistungen wollen wir in der Gesellschaft, Wirtschaft, Verwaltung und im Privatleben auch im digitalen Raum anbieten?

Wir versuchen in diesem Diskussionspapier, einzelne dieser grundlegenden Themen genauer zu betrachten und Denkanstösse zur weiteren Diskussion, Verfeinerung und Bildung eines möglichst breiten gesellschaftlichen Konsenses zu geben.

Schweizerische Akademie der Technischen Wissenschaften SATW
St. Annagasse 18 | 8001 Zürich | +41 44 226 50 11 | info@satw.ch | www.satw.ch

e-ID

Laut Bundesverfassung (Artikel 1, Absatz 1) lautet der Zweck der Schweizerischen Eidgenossenschaft wie folgt: *«Die Schweizerische Eidgenossenschaft schützt die Freiheit und die Rechte des Volkes und wahrt die Unabhängigkeit und die Sicherheit des Landes.»* Es ist davon auszugehen, dass dies zwar im Sinne der nationalstaatlichen Grenzen des 19. und frühen 20. Jahrhunderts definiert wurde, jedoch heute sinngemäss für den physischen wie auch den virtuellen Raum Anwendung finden soll.

Daher stellt sich die Frage, wie der virtuelle Raum (Cyber-Raum) und die Landesgrenzen darin definiert sind, wenn ein «digitaler Zwilling» der Schweiz mit entsprechend digital ausgestalteten Diensten, Rechten und Pflichten entsteht. Dies definiert dann auch den Raum, in dem sich Gesellschaft, Politik, Verwaltung und Wirtschaft aber auch die Sicherheitsbehörden bewegen.

Im kommerziellen Sektor ist bereits eine entsprechende Verschiebung im Gange: Firmen haben verstanden, dass weder der physische noch der Netzwerk-Perimeter im Cyber-Raum die zentralen Schutzobjekte darstellen. Die Identitäten der Mitarbeitenden und Partner und die daran geknüpften Rollen, Rechte und Fähigkeiten/Funktionen werden als neuer Perimeter angesehen.

Auf die Schweiz angewendet, bedeutet dies, dass die virtuelle Grenze des Schweizer «digitalen Zwillings» durch die Identitäten der Schweizer Bürgerinnen und Bürger sowie Einwohnerinnen und Einwohner definiert ist, da eine Kontrolle und eine Regulierung innerhalb einer physischen Grenze im virtuellen Raum weder vernünftig möglich, noch zielführend ist. Weiter ist dies in der heutigen Welt weder effektiv noch effizient umsetzbar.

Daraus lassen sich einige Kernpunkte direkt ableiten:

- Die Schweizer e-ID muss so sicher und vertrauenswürdig wie der Schweizer Pass und die Identitätskarte sein. Mit anderen Worten: Registrierung und Ausstellung erfolgen durch das (digitale) und «ex offizio» vertrauenswürdige Passbüro der Schweizer Behörden, eine Privatisierung ist ausgeschlossen. Die Produktion der digitalen Identitäten inklusive allfälliger Träger- und Speichertechnologien kann hingegen durch geeignete und entsprechend überwachte private Unternehmen erfolgen – analog Pass/Identitätskarte.
- Auch der Ausländerausweis und allfällige andere amtliche Ausweisdokumente können digital mit derselben Sorgfalt und Verbindlichkeit ausgestellt werden.
- Das Aufgabengebiet der staatlichen Hoheit wird anhand der digitalen Grenze beschrieben. Armee, Bundespolizei und Nachrichtendienst sind gemäss ihrem definierten Auftrag innerhalb dieses Identitäts-Perimeters aktiv – sinngemäss gilt dies auch für nachgelagerte subsidiäre Aufgaben.
- Die Schweizer Regulierungsbehörden erweitern ihren Geltungsbereich auf den so definierten «digitalen Zwilling» der Schweiz.
- Tieferwertige Identitäten können problemlos durch Private ausgestellt, verwaltet und geschützt werden, analog zur physischen Welt. Dies führt zu einer gewissen – durchaus gewollten – Trennung von Identitäten, allenfalls mit definierten Abbildungsfunktionen. Auch bezüglich des Datenschutzes kann dies interessant sein, indem es wünschenswert ist, dass verschiedene Profile nicht verbunden werden können.

Aus unserer Sicht sollten diese Konzepte weiterverfolgt und detailliert ausgearbeitet werden, und die gesetzlichen Anpassungen sowie ggf. notwendigen internationalen Diskussionen sollten von diesen Ideen geleitet sein.

In der Sicherheits-Technologie werden momentan grosse Fortschritte im Bereich der dezentralen Identitäten auf Basis der Blockchain-Technologie erzielt. Diese Ideen und Ansätze müssen zwingend in die Überlegungen zu einem modernen Identitäts-Perimeter miteinbezogen werden, da gegebenenfalls eine moderne und auch relativ risikoarme Umgebung geschaffen werden kann, welche gleichzeitig zu einem signifikanten Fortschritt im Bereich des Datenschutzes führt.

e-Voting

e-Voting ist in der Schweiz ein sehr öffentlichkeits- und medienwirksames e-Government-Projekt. Es versucht, den wichtigsten demokratischen Prozess der Schweiz zu digitalisieren. Aus unserer Sicht erreichen heute weder die verfolgten Ansätze noch die öffentliche Diskussion einen Reifegrad, der es zulassen würde, die wichtigste Säule der direkten Demokratie darauf aufzubauen. Allerdings widerspricht ein Moratorium und damit ein Innovationsstop oder «Denkverbot» dem Selbstverständnis der Schweiz, weshalb es nicht zielführend ist.

Versuche zum e-Voting sollen hierzulande zulässig sein, die Risiken jedoch in vernünftigen und abschätzbaren Grenzen gehalten werden. Wir schlagen vor, dass wir als Gesellschaft an begrenzten praktischen Beispielen lernen sollen, wie wir mit e-Voting umgehen, welche Einflüsse e-Voting auf unsere demokratischen Prozesse hat und ob wir es überhaupt wollen. Fragen der Stimmbeteiligung aber auch der politischen Debatte sollen geklärt werden. Ein Wählen durch einfaches «Wischen nach links und rechts» (à la Tinder) mag der Effizienz dienen, dürfte aber kaum der Qualität, Nachvollziehbarkeit und Verbindlichkeit des demokratischen Prozesses zuträglich sein.

Daher schlagen wir ein risiko- und nutzen-basiertes Vorgehen vor:

- Die Gruppe mit dem höchsten unmittelbaren Nutzen von e-Voting sind die Auslandschweizerinnen und -schweizer, vor allem diejenigen die in Ländern leben, welche die etablierten Mechanismen der brieflichen Stimmabgabe nicht zulassen oder nur unzureichend unterstützen (z.B. durch unzuverlässige oder verspätete Postdienste). Auslandschweizerinnen und -schweizer sollen daher eine zentrale Zielgruppe durchzuführender Pilotversuche mit flankierenden Massnahmen wie statistischen Auswertungen, der Erkennung von Stimm-Anomalien gegenüber definierten Kontrollgruppen, usw. sein. Die entsprechenden Details sind noch genauer zu definieren und auszuarbeiten, damit Pilotversuche über einen ausreichend langen Zeitraum stattfinden können.
- Einzelne Abstimmungssonntage sollen als limitierter Test gelten können, wenn wichtige Kriterien erfüllt sind:
  - Die Anzahl Bürgerinnen und Bürger, welche e-Voting einsetzen, ist limitiert und statistische Ausreisser können erkannt werden. Zusätzlich zu den Auslandschweizerinnen und -schweizern können einzelne Kantone – wie heute – mit einer limitierten Anzahl Stimmen Pilotprojekte durchführen.
  - Es werden entweder nur kommunale Vorlagen verwendet oder kantonale und eidgenössische Vorlagen mit limitierter öffentlicher und internationaler Ausstrahlung, um die Risiken einer externen Einflussnahme zu limitieren.

- Die Abstimmungen wie auch die dafür eingesetzten technischen Systeme und organisatorischen Abläufe werden technisch eng überwacht und es wird transparent über die Ergebnisse und allfällige Auffälligkeiten kommuniziert.
- Eine Risiko-Übersicht des heutigen Abstimmungs-Prozesses wie auch eines möglichen e-Votings soll erstellt und kritisch analysiert werden. Die Analyse soll in einer Art und Weise bereitgestellt werden, welche eine öffentliche Debatte erlaubt und nicht nur in Expertenkreisen verständlich ist. Gegebenenfalls könnten die Hochschulen für diese Aufgabe beigezogen werden.

Dies wird es erlauben, die richtigen Diskussionen innerhalb der Schweiz mit ausreichender Sorgfalt und auf Basis praktischer Erfahrungen ohne unnötigen Zeitdruck zu führen. Fragen der einfachen Verifizierbarkeit des Prozesses durch die Bürgerinnen und Bürger müssen mit besonderer Sorgfalt adressiert werden. Weiter müssen Überlegungen angestellt werden, was geschieht, wenn am Tag nach einer Abstimmung auch nur der Verdacht einer Manipulation geäussert wird und eine Flut von Stimmrechtsbeschwerden eingeht. Sind die entsprechenden Prozesse dafür nicht definiert oder nicht leistungsfähig genug ausgelegt, könnte dies das Ende von e-Voting in der Schweiz sein – zumindest vorläufig.

Diese Fragen müssen umfassend angegangen und in der Öffentlichkeit diskutiert werden, nicht nur in ausgewählten Expertenkreisen.

Zu guter Letzt ist es ist unrealistisch zu glauben, dass jedes Land seinen eigenen Weg gehen soll. «e-Voting made in Switzerland» ist eine Illusion, wenn die heutige, global agierende IT-Industrie betrachtet wird: es kann also sein, dass die e-Voting Software in der Schweiz entwickelt wird, dass aber Betriebssystem, Hardware, grundlegende Komponenten usw. von ausländischen Anbietern bezogen werden. Daher ist der Gewinn eines eidgenössischen Vorgehens und eines «swiss-made» Labels marginal, sofern überhaupt vorhanden. Es wäre zielführendender, günstiger, effizienter und nicht zuletzt sicherer, sich im befreundeten Ausland nach adäquaten, in Aufbau, Betrieb und Wartung prüfbaren Lösungen umzuschauen und dort Partnerschaften einzugehen, wo sich Synergien ergeben und ggf. vorhandene Nutzungserfahrungen die Umsetzung in der Schweiz erleichtern können.

Partnerschaften

Aufbauend auf diesen Überlegungen zu e-Voting als aktuellem Beispiel für e-Government-Angebote müssen sich Politik und Gesellschaft die Frage stellen, welche Aufgaben zwingend lokal im Schweizer Cyberraum gelöst werden müssen und wo nur internationale Partnerschaften zum Erfolg führen können. In diesem Umfeld muss disruptives Denken zugelassen sein und es müssen gegebenenfalls neue Wege beschritten werden. Partnerschaften sollen also nicht nur zwischen Regierungen und Nachrichtendiensten gepflegt werden, auch geeignete, überprüfbare Public Private Partnerships mit vertrauenswürdigen Gegenparteien sind ein wichtiges Mittel, die vorhandenen Ressourcen zielführend und effizient einzusetzen. Grosse kommerzielle Cloud-Anbieter besitzen und verarbeiten heute mehr und rascher Signale betreffend der allgemeinen Bedrohungslage wie auch sehr spezifischer Angriffsmuster und –wellen, als die meisten Regierungen je entsprechende Informationen haben werden. Der nötige Informationsaustausch bis hin zu Handlungsempfehlungen und koordinierten Massnahmen muss also mit einem partnerschaftlichen Ansatz gelöst werden,

bei dem alle Seiten im Rahmen ihrer rechtlichen, regulatorischen, politischen und wirtschaftlichen Vorgaben profitieren. Hierbei muss aber jederzeit klar und nachweisbar sein, welche Aufgaben zwingend und nicht delegierbar durch den Staat erfüllt werden müssen und welche Aufgaben mit vertretbaren Risiken und klar definiertem und kontrollierbarem Umfang Dritte übernehmen können und sollen.

Die Schweizer Regierung und Verwaltung können und sollen sich auf die Wahrnehmung ihrer hoheitlichen Aufgaben im Cyber-Raum konzentrieren. Sie dürfen sich allerdings nicht von vornherein scheuen, mit internationalen Konzernen zusammenzuarbeiten, insbesondere um Bedrohungslagen für den «digitalen Zwillling» der Schweiz zu erstellen, zu bewerten und zu bewältigen – auch dies wieder in Zusammenarbeit mit etablierten nationalen Kompetenzzentren, bestehende Vertrauensnetzwerken und privaten Organisationen, die hier bereits erhebliche Anstrengungen unternehmen.

satw it's all about technology

Impressum

Schweizerische Akademie der Technischen Wissenschaften SATW

Autoren und Autorinnen: Karl Aberer (EPFL) | Umberto Annino (ISSS) | Alain Beuchat (UBS) | Adolf Doerig (Doerig & Partner) | Roger Halbheer (Microsoft) | Martin Leuthold (Switch) | Hannes Lubich (FHNW) | Adrian Perrig (ETHZ) | Bernhard Tellenbach (ZHAW) | Daniel Walther (Swatch Group Services) | Andreas Wespi (IBM Research Lab)

Redaktion: Adrian Sulzer | Nicole Wettstein

30. April 2019