DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Schweizerische Bundeskanzlei
Walter Thurnherr
Bundeshaus West
3003 Bern

Per E-Mail an: evelyn.mayer@bk.admin.ch

18. August 2021

Stellungnahme zur Neuausrichtung des Versuchsbetriebs der elektronischen Stimmabgabe (Vernehmlassung 2021/61)

Sehr geehrter Herr Bundeskanzler Thurnherr, sehr geehrte Damen und Herren

Am 28. April 2021 eröffnete der Bundesrat das Vernehmlassungsverfahren zur Änderung der Verordnung über die politischen Rechte (VPR) und der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) (Neuausrichtung des Versuchsbetriebs). Für die Einladung zum Vernehmlassungsverfahren möchten wir uns bedanken.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkungen

E-Voting ist von unbestreitbaren, demokratie-politischen Mängeln betroffen, weshalb wir die in dieser Vorlage enthaltene Neuausrichtung des Versuchsbetriebs in der Schweiz gänzlich ablehnen müssen. Abweichende Regulierungen von wissenschaftlich

geforderten Empfehlungen, grundsätzliche Unvereinbarkeiten mit Schweizer Idealen und zahlreiche technische Defizite sprechen eine eindeutige Sprache: E-Voting ist mit der in der Schweiz gelebten Demokratie nicht vereinbar. Sodann von 300 erfolgreichen Versuchen zu sprechen, grenzt an Augenwäscherei. Man denke nur schon an die Ereignisse Ende 2018: Systemüberholungen des Genfer Systems zwecks Verbesserung der Sicherheit hätten mehr als zwei Millionen Franken gekostet, weshalb man dem Versuchsbetrieb überraschend den Stecker zog. Als nämlich klar wurde, dass andere Kantone keine finanzielle Unterstützung leisten würden und der Kanton Genf die Kosten der Überarbeitung des gesamten Systems alleine übernehmen müsste, wurde der Betrieb kurzerhand eingestellt.

Aktuell existiert deswegen nur noch ein ursprünglich vom spanischen Hersteller Scytl stammendes und mittlerweile von der Schweizer Post akquiriertes E-Voting-System. Anfangs Februar 2019 hat die Post den Quellcode für die neuste Version ihres Systems, das für 100 % des Elektorats zugelassen werden sollte, unter den Bedingungen eines Non-Disclosure Agreements (NDA) zugänglich gemacht. Am 25. Februar 2019 startete sie dann einen Public Intrusion Test. Auch hier ging es in der Folge schnell:

- Am 12. März 2019 veröffentlichten die drei unabhängigen Sicherheitsforscher:innen Sarah Jamie Lewis, Olivier Pereira und Vanessa Teague einen wissenschaftlichen Artikel zu einer gravierenden Sicherheitslücke. Diese betraf die sogenannte universelle Verifizierbarkeit; das Herzstück des E-Voting-Systems. Die Sicherheitslücke war Scytl und der Post bereits seit 2017 bekannt. Dennoch wurde sie weder behoben noch wurde diese Unterlassung durch die Post bemerkt. Auch KPMG, welche das System auditiert hat, scheint den Fehler nicht entdeckt zu haben. Alle beteiligten Instanzen haben versagt.
- Am 25. März 2019 wurde eine weitere gravierende Sicherheitslücke bekannt, die das bereits im Betrieb befindliche System betraf: Dieses Mal konnte die sogenannte individuelle Verifizierbarkeit kryptografisch gebrochen werden. Diese Feststellung hinsichtlich der individuellen Verifizierbarkeit belegte, dass das System bei mehreren Urnengängen im Einsatz war, ohne dass es die geforderte individuelle Verifizierbarkeit tatsächlich gewährleisteten konnte.

Beide Sicherheitspfeiler der Verifizierbarkeit konnten also gebrochen werden.

Konkret wurde die zweite Entdeckung zum entscheidenden Anlass, das System für die

Wahlen 2019 zurückzuziehen. Hätte die Post dies nicht selbst gemacht, hätte die Bundeskanzlei den Stecker gezogen.

Dass man nach fast 20 Jahren gescheiterter E-Voting-Projekte deren Hauptstecker noch immer nicht ziehen mag, kann nur erstaunen. Teure Systemüberholungen und vermeintliche Verbesserungen der Sicherheit vermochten die schwerwiegenden Defizite der zahlreichen Versuche nicht auszubügeln, und trotz offensichtlichen Gefahren für das wohl teuerste Gut der Schweizer Bevölkerung, scheint man das Thema E-Voting noch immer nicht abschreiben zu wollen.

Unmöglicher Spagat zwischen Sicherheit und demokratischer Legitimation

Um nur schon in der Theorie denkbar zu sein, müssen E-Voting-Systeme die folgenden drei Kriterien zwingend und kumulativ erfüllen: Es muss klar sein, wer überhaupt abstimmen darf, es muss ein kontrollierbares Abstimmungsresultat geben und das Stimmgeheimnis muss stets gewährleistet werden. Die Erfüllung der letzten beiden Konditionen zusammen ist auch genau die Krux, an der das Genfer Konsortium scheiterte: Nachzählungen durchführen zu können, ohne dabei das Stimmgeheimnis zu verletzen, ist ein kaum zu bewerkstelligendes Unterfangen, dass es klar von der korrekten Stimmabgabe selbst abzugrenzen gilt.

E-Voting-Systeme müssen zudem vor Manipulationen geschützt sein (Ghielmini et al., 2021, S. 62-63), da solche bei elektronischen Wahlen und Abstimmungen im Vergleich zur Urnen- oder Briefwahl viel grossflächiger möglich sind (statt vieler: Lauer, 2020, S. 183). Manipulationen können selbstverständlich auch in konventionellen Wahl- und Abstimmungsverfahren vorkommen. Aufgrund der dezentralisierten, kleinteiligen Organisation sind diese aber weitaus weniger anfällig, da sie nur mit sehr vielen Absprachen überhaupt möglich sind und dadurch auch viel eher entdeckt werden. Manipulationen innerhalb eines E-Voting-Systems sind im Vergleich dazu viel einfacher auf einen gesamten Kanton oder gar auf den gesamten Wahlkörper skalierbar.

Oftmals wird innerhalb der E-Voting-Debatte auf die Addition der Brief- zur Urnenwahl verwiesen. Auch wenn die Briefwahl selbst über Verbesserungspotential verfügt (Killer / Stiller, 2019), kann diese jedoch kaum mit der aktuellen Ergänzung verglichen werden, denn diese beiden Wahlkanäle unterscheiden sich in der Schweiz (ausser offensichtlich bei der Übermittlung des Stimmzettels selbst) nicht wesentlich. Die Briefwahl erlaubt es bereits, zeitlich flexibel abzustimmen. Nachdem das

Stimmzettelcouvert in der Urne angekommen ist, sorgen das Wahlbüro und gewählte Stimmenzähler:innen für den korrekten Ablauf der Auszählung. Sie überwachen die Meldung des ermittelten Resultats sowie die Versiegelung der Stimmzettel und Stimmrechtsausweise für eine allfällige Nachzählung. Für eine Manipulation müssten sich alle beteiligten Personen verbünden. Die paritätische Zusammensetzung dieser Gruppe, die die Vielfalt des Politspektrums widerspiegelt, verhindert einen solchen Betrug. Durch die dezentralen Auszählungen in den Gemeinden blieben die verfälschenden Auswirkungen zudem beschränkt. Bei E-Voting hingegen geschieht der Auszählungsvorgang zentral.

Der also umso bedeutendere Schutz vor grossflächigen Manipulationen ist nur möglich mit sogenannten durchgängig verifizierbaren Systemen (z. T. auch unter dem Begriff «vollständige Verifizierbarkeit» bekannt), jedoch sind diese Vorkehrungen informationstechnisch äusserst komplex. Schliesslich muss nicht nur sichergestellt werden, dass eine Stimme im System richtig angekommen ist, sondern auch ob sie korrekt ausgezählt wurde.

Durchgängig verifizierbare Systeme, durch die alle Stimmenden sowohl kontrollieren können, ob ihre Stimme angekommen ist, als auch, dass alle Stimmen korrekt ausgezählt wurden, sind prinzipiell nur mittels öffentlicher Listen aller Verifizierungscodes (sog. «Public Voting Boards») möglich: Unter Zuhilfenahme von Quantencomputern bestünde jedoch in (vermutlich nicht allzu ferner Zukunft) die Möglichkeit, auf Basis dieser Listen zurückrechnen zu können, wer wie abgestimmt oder gewählt hat. Diese öffentlichen Listen wären also nur gerade pseudonym und würden stets eine latente Verletzung des Stimmgeheimnis' bedeuten. Deshalb hat man sich in der Vorlage dafür entschieden, diese Codes nicht der Öffentlichkeit zu Verfügung zu stellen, sondern die allumfassende Kontrolle von Wahlen und Abstimmungen dem Gremium der Prüfer:innen zu überlassen.

Das bedeutet jedoch auch, dass die Stimmenden nur gerade nachprüfen können, ob ihre eigene Stimme richtig abgegeben wurde, nicht aber, ob die Gesamtheit aller Stimmen richtig abgegeben, geschweige denn ausgezählt wurde. Dass dieses Manko nicht zu überwinden ist, gesteht auch der erläuternde Bericht in den Erläuterungen zu **Artikel 5 VEleS** (S. 15, Erläuterungen zu Art. 5 Abs. 2 & 3 VEleS) ein: Dort wird erklärt, dass die individuelle Verifizierbarkeit nur gerade ermöglicht, die missbräuchliche Verwendung des eigenen Stimmrechts festzustellen. Die universelle Verifizierbarkeit ermöglicht es demgegenüber, Manipulationen in der Infrastruktur zu entdecken. Diese

Möglichkeit zur universellen Verifikation soll im Gegensatz zur individuellen Verifizierbarkeit jedoch nicht zwingend den Stimmberechtigten angeboten werden, weshalb sie in der zugrundeliegenden Vorlage den Prüfer:innen vorbehalten wurde.

Abhilfe schaffen auch die A**bsätze 2 und 3 des Artikel 5 VEleS** nicht, nach denen der Prozess der Überprüfung für die Bevölkerung zwar beobachtbar sein muss, jedoch sollen nur die Prüfer:innen die Bedeutung und die Ergebnisse der einzelnen Handlungsschritte möglichst gut nachvollziehen. Dazu müssen sie die Möglichkeit haben, die korrekte Durchführung der Handlungsschritte sowie die Prüfergebnisse bezeugen zu können, beispielsweise indem sie sich an den Ort der Durchführung begeben. Ob eine physische Deplatzierung dieses Gremiums vertrauensfördernd sein wird, scheint umso fraglicher, da selbst in den Erläuterungen zu **Artikel 27m VPR** eingestanden wird, dass auch die vollständige Verifizierbarkeit nur dann glaubwürdig wirken kann, wenn ihr Nutzen im Kern verstanden wird (Art. 27m VPR Abs. 3). Hierfür sollen Informationen über das System und den Betrieb von E-Voting auch für Personen ohne Fachkenntnisse nachvollziehbar aufbereitet werden, und zwar mittels Offenlegung des Quellcodes (Erläuternden Bericht, S. 11 Erläuterungen zu Art. 27m Abs. 2 VPR). Eine technisch kaum versierte Person soll also durch diese «zentrale Transparenzmassnahme» mehr Vertrauen in E-Voting-Systeme haben, obwohl sie wahrscheinlich noch nie einen Code gesehen haben mag.

Die fehlende Nachvollziehbarkeit wird auch mit den anderen, neuen Transparenzbestimmungen nicht besser. Die Ergänzung der bestehenden Bestimmung von **Artikel 3 VEleS** bezüglich öffentlichen Zugangs zu Informationen verdeutliche gemäss erläuterndem Bericht (S. 14 Erläuterungen zu Art. 3 VEleS Bst. D) die Wichtigkeit der Transparenz. Wenige Bestimmungen später wird jedoch im **Artikel 12 VEleS** eingeräumt, dass der Systeminhaber verlangen kann, dass mit Informationen zu vermuteten Mängeln verantwortungsvoll umgegangen wird. Unter anderem sollen sich abzeichnende Entdeckungen von Sicherheitslücken nicht unnötig bekanntgemacht werden. Informationen dazu werden nur mit Personen geteilt und diskutiert, die zur Behandlung der Fragestellung vermutungsweise fähig und gewillt sind und die ebenfalls verantwortungsvoll damit umgehen (Erläuternder Bericht, S. 18, Erläuterungen zu Art. 12 Abs. 4 VEleS). Auch im Dialog mit der Wissenschaft wurde angemerkt, dass qualitativ mangelhafte Prüfberichte zu Vertrauenverlusten innerhalb der Bevölkerung führen könnten (S. 3). Ob die richtige Abhilfe hierfür die Verheimlichung von Systemmängeln ist, scheint fragwürdig.

Nach dem Gesagten wird eine Tatsache klar: Durch das Abstimmungsgeheimnis ist eine öffentliche Prüfung von E-Voting-Resultaten nicht möglich. Auch wenn gewisse Experten versuchen, diese Kontrolle elektronisch nachzuvollziehen, so entgeht sie doch in jedem Fall einer demokratischen Kontrolle durch die Öffentlichkeit. Die Funktion einer Wahlkommission findet in der ursprünglich vorgesehenen Form nicht mehr statt. Würde man simplere Systeme anwenden, wäre zwar Anonymität gegeben, da eine Stimme von einer Person getrennt wäre, aber man würde dadurch auch keine Nachzählungen durchführen können. Unter Anwendung der derzeitigen Vorlage kann man Wahlergebnisse zwar nachzählen, aber nicht mehr nachvollziehen. Die demokratische Legitimation der Wahl- und Abstimmungsresultate kann also nicht mehr durch die Gesellschaft entstehen, sondern nur gerade bei diesem Gremium der Prüfer:innen, denen die Stimmenden der Schweiz notgedrungen vertrauen müssen. Ob man diesem Gremium Glauben schenkt oder nicht, und ob sie selbst dieses enorm komplizierte IT-Projekt überhaupt verstehen oder nicht, können Stimmende schlicht nicht beurteilen, geschweige denn selbst nachvollziehen. Selbst wenn die Gesellschaft als Ganzes (potenziell) Vertrauen in die Prüfer:innen hat, ist die Nachvollziehbarkeit der Ergebnisse für einzelne Stimmende trotzdem nicht mehr gegeben.

In der Tat wurde in der Schweiz – nota bene obschon vor allem die Lehre seit geraumer Zeit verfassungsrechtliche Bedenken diesbezüglich äussert – die Verfassungsmässigkeit von E-Voting im Vergleich zu anderen Staaten Europas noch nie materiell untersucht (Markić, 2019). In Deutschland hingegen schob das Bundesverfassungsgericht bereits vor mehr als zehn Jahren E-Voting den Riegel vor, da es selbst weit weniger komplexe Wahlcomputer als verfassungswidrig bezeichnete. Das Gericht ergänzte die politischen Rechte um den Grundsatz der Öffentlichkeit der Wahl, wodurch alle wesentlichen Schritte öffentlicher Überprüfbarkeit unterliegen müssen. Nur eine solch öffentliche Wahl kann demokratischer Willensbildung entsprechen, da das begründete Vertrauen der Stimmenden nur durch Nachvollziehbarkeit der Vorgänge erreicht werden kann.

Im Detail führte das Deutsche Bundesverfassungsgericht aus, dass der Einsatz von Wahlgeräten, die die Stimmen der Wähler:innen elektronisch erfassen und das Wahlergebnis elektronisch ermitteln, nur dann den verfassungsrechtlichen Anforderungen genügt, wenn die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können. Der Wähler selbst müsse ohne nähere computertechnische Kenntnisse nachvollziehen können, ob seine abgegebene Stimme als Grundlage für die

Auszählung oder jedenfalls als Grundlage einer späteren Nachzählung unverfälscht erfasst wird. Auch eine umfangreiche Gesamtheit sonstiger technischer und organisatorischer Sicherungsmassnahmen sei allein nicht geeignet, fehlende Kontrollierbarkeit der wesentlichen Schritte des Wahlverfahrens durch die Bürger zu kompensieren. Denn die Kontrollierbarkeit der wesentlichen Schritte der Wahl fördert begründetes Vertrauen in die Ordnungsmässigkeit der Wahl erst dadurch, dass die Bürger selbst den Wahlvorgang zuverlässig nachvollziehen können (Pressemitteilung BVGER).

Nun sind aber die Abläufe beim E-Voting nochmals deutlich komplexer als die Verwendung von Wahlcomputern. Vollständig verifizierbare E-Voting-Systeme bedingen umfangreiche technische und anderweitig begleitende Massnahmen. Die Verifikation setzt insbesondere weitreichendes Fachwissen – speziell auch bei den abstimmenden Personen – voraus. Dabei geht es nicht im Detail darum, die eingesetzten kryptografischen Verfahren zu verstehen. Ein Verständnis davon zu haben, wie die Resultatermittlung fälschungssicher zustande kommt, ist für die Verifikation und Anerkennung des Resultats jedoch wichtig. Die technische Umsetzung des Entscheidungsverfahrens muss für alle Bürger:innen verständlich bleiben, sonst kann das Verfahren gar nicht demokratisch sein.

Man erkennt schnell, dass beide Seiten des Spektrums schwerwiegende Schwächen für die Demokratie bedeuten: Entweder E-Voting-Systeme sind verständlich und nachvollziehbar, verletzen jedoch das Stimmgeheimnis, oder aber sie schützen Letzteres und entschwinden gerade deswegen jeglicher demokratischer Legitimation. Vollständig verifizierbare Systeme sind also (zumindest theoretisch) die Lösung für die drohende Verletzung des Stimmgeheimnis', schaffen jedoch ein mindestens gleich grosses Problem auf ebenso heiklem Terrain, da sie sich aufgrund fehlender Nachvollziehbarkeit der in der Schweiz so wichtigen direktdemokratischen Legitimation entziehen.

Historische Bedeutung der Schweizer Demokratie

Im Gegensatz zu vielen anderen Staaten ist die direkte Demokratie und das daraus entstehende Mitspracherecht das zentrale Identitätsmerkmal der Schweizer Bevölkerung und sorgt für eine gelebte Volkssouveränität (Cottier & Liechti, 2008, S. 41). Selbst Rousseau, wohl der prägendste Philosoph und Polittheoretiker des vergangenen Jahrtausends, sieht die Konstitution eines Volkes zeitgleich mit der

Gesetzesentstehung, ohne die sie per se niemals zu einem Volk erwachsen kann (Tanner, 2015, S. 31). Das Schweizer Volk als solches gäbe es nach dieser Notion ohne Gesetze gar nicht; sie sind ebenso Teil unseres Selbstverständnisses wie der den Schweizer:innen automatisch zustehende Anspruch, an der hier herrschenden direkten Demokratie nicht nur teilnehmen, sondern ihr auch vertrauen zu können.

Daher stammt auch die immense Bedeutung des aktuellen **Artikels 34 der Bundesverfassung**, der nicht nur die demokratische Grundordnung der Schweiz, sondern neben den politischen Rechten im weiteren Sinne auch die freie Willensbildung sowie die unverfälschte Stimmabgabe gewährleistet (BGE 139 I 195 E. 2; BGE 131 I 442 E. 3.1; BGE 141 II 297 E. 5.2). Artikel 34 Absatz 2 der Bundesverfassung verankert die Wahl- und Abstimmungsfreiheit, die die für den demokratischen Prozess und die Legitimität direktdemokratischer Entscheidungen erforderliche Offenheit der Auseinandersetzung gewährleistet (BGE 136 I 364, E. 2.1). Damit soll garantiert werden, dass die Stimmberechtigten ihre Entscheidungen gestützt auf einen möglichst freien und umfassenden Prozess der Meinungsbildung treffen und entsprechend mit ihren Stimmen zum Ausdruck bringen können. Insbesondere beinhaltet die Abstimmungsfreiheit die zentralen Garantien der Gewährleistung des Stimmgeheimnisses und die korrekte Ermittlung der abgegebenen Stimmen zum Schlussergebnis (Tschannen, BSK-Kommentar, Art. 34 BV; Hangartner/Kley, 2000). Die damit einhergehende staatliche Schutzpflicht zugunsten der Abstimmungsfreiheit enthält den Anspruch der Stimmberechtigten, dass das sicherste und am besten geeignete Abstimmungssystem zur Verfügung gestellt wird.

Das E-Voting birgt das technische Risiko der Ergebnismanipulation durch Missbräuche. Diese müssen gemäss Artikel 34 Absatz 2 der Bundesverfassung und auch durch Artikel 8a Absatz 2 des Bundesgesetzes über die politischen Rechte ausgeschlossen sein. Genau hier liegt auch der klare Widerspruch zur elektronischen Stimmabgabe, da ein Laie nicht einmal ansatzweise die zur Wahrung des Stimmgeheimnis‘ notwendigen komplexen IT-Systeme verstehen kann. Selbst wenn er dann die Abgabe der eigenen Stimme mittels individueller Verifizierbarkeit nachvollziehen könnte, ist es der stimmenden Person auch dann nicht möglich, eine Wahl als Ganzes beurteilen zu können. Somit muss das Vertrauen in die korrekte Stimmabgabe anderer zur blossen Hoffnung verkommen, dass diese ihre Pflicht zur individuellen Verifizierbarkeit ebenfalls wahrnehmen. **In Ziffer 13 des Anhangs** wird nämlich auch verlangt, dass die Stimmenden die sogenannten Beweise auch prüfen (Erläuternder Bericht, S. 28, Erläuterungen zum Anhang Ziff. 13.12 VEleS). Schliesslich können nur sie feststellen,

ob ein Beweis nicht doch missbräuchlich zur Abgabe einer systemkonformen Stimme verwendet wurde – die Prüfer:innen können dies gemäss **Ziffer 2 des Anhangs** nämlich nicht (Erläuternder Bericht, S. 25, Erläuterungen zum Anhang Ziff. 2.6 VEleS). Ob eine solche bevölkerungsübergreifende Pflicht zur Mithilfe und Kontrolle innerhalb des politischen Teilhaberechts überhaupt verfassungskonform ist oder nicht, kann an dieser Stelle aufgrund grundsätzlicherer Mängel dahingestellt bleiben.

Zudem erstaunt auch, dass der Umfang dieser Beweisprüfung noch unklar scheint und deswegen Gegenstand der Forschung bilden könnte (Erläuternder Bericht, S. 24, Erläuterungen zum Anhang Ziff. 2.5 VEleS). Die Beweise werden ihre Wirkung auch nur entfalten können, wenn die Stimmenden diese auch tatsächlich prüfen und sich im Zweifelsfall an die Behörden wenden. Welche Massnahmen hierzu beitragen werden (oder überhaupt können), soll ebenfalls mittels wissenschaftlicher Begleitung zu einem späteren Zeitpunkt eruiert werden. Wie genau diese Information den Stimmenden also dargereicht werden soll, bleibt unklar, dennoch hielt man in den Erläuterungen zu **Artikel 27m Absatz 3 VPR** fest, dass man den Stimmberechtigten das Grundkonzept der Verifizierbarkeit näherbringen muss, da Unregelmässigkeiten ja auch nur dank derer Nutzung der individuellen Verifizierbarkeit entdeckt werden können.

Die Spitze des Eisbergs bleibt die Tatsache, dass nach **Art. 17 Absatz 2 VEles** bei Wahlen nach Majorzverfahren (Mehrheitswahlsystem) von der individuellen Verifizierbarkeit gänzlich abgesehen werden kann, wenn die Stimme durch die Eingabe eines Namens in ein Freitextfeld abgegeben wird (Erläuternder Bericht, S. 21, Erläuterungen zu Art. 17 Abs. 2 VEleS). Dies führt entweder zu einem Eingriff in Schweizer Gegebenheiten, indem sogenannte «Write-Ins» durch Voranmeldung von Kandidat:innen ersetzt werden, oder aber, dass die Regulierung beiläufig in Kauf nimmt, dass das wesentliche Sicherheitsmerkmal der elektronischen Stimmabgabe gar nicht für alle Wahlen gelten soll. Da wird also gross eine Garantie verkündet und dann nebenher gleichsam stillschweigend wieder zurückgenommen, ohne dass die Stimmenden konkret auch nur im Ansatz verstünden, was nun wo wie gilt und warum da plötzlich die Codes als Sicherheitsmerkmal fehlen.

Vor dem Hintergrund der (nicht zuletzt im Laufe der Coronapandemie befeuerten) Radikalisierung und Skepsis grösserer Bevölkerungsteile gegenüber dem Staat als solches erscheint es fragwürdig, die demokratische Legitimation von Wahlen und Abstimmungen derart leichtsinnig und zu Gunsten kaum überzeugender Vorteile (siehe nächster Abschnitt) aufs Spiel setzen zu wollen. Bestünde nur der kleinste

Verdacht auf potenzielle Stimmgeheimnisverletzungen, würden wegen des Chilling- oder Abschreckungseffektes wohl noch weniger Menschen wählen und abstimmen gehen. Ausserdem sind viele Resultate knapp und würden mit erhöhter Skepsis der allgemeinen Bevölkerung wohl noch weniger akzeptiert.

Vor allen Dingen der Gründungsmythos der Schweiz versinnbildlicht auch die Entschärfung politischer Gegensätze, ermöglichte er doch auch Anhängern gegengesetzter Lager eine Verständigungsbasis zu finden. Er suggerierte Konsens selbst dort, wo tatsächlich Dissens herrschte, und liess politischen Kommunikationsraum entstehen, wo sonst politische Differenzen dominiert hätten (Tschopp, 2012, S.62). Eine zweifelsfrei nachvollziehbare direkte Demokratie entspricht viel eher dem politischen System, dass allen voran die Schweizer Bevölkerung aktuell braucht, um erneut anständigen politischen Diskurs aufnehmen zu können. Stattdessen erneut auf das tote Pferd namens E-Voting zu setzen, dessen zahlreiche Gefahren bereits mehrfach öffentlich wurden, grenzt an Wahnsinn.

Kaum Vorteile – zahlreiche Risiken

Dass die Digitale Gesellschaft dem E-Voting dermassen kritisch gegenübersteht darf keinesfalls dahingehend gedeutet werden, dass wir als Organisation grundsätzlich gegen Vorstösse im Bereich E-Government und E-Democracy sind – im Gegenteil: Wir begrüssen jegliche sinnvolle Vereinfachung von Behördentätigkeiten, wie beispielsweise den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EmbaG). So stehen wir auch einer Verbesserung der Schweizer Demokratie durch Technologie grundsätzlich positiv gegenüber, weil sie das Potenzial hat, die Möglichkeiten zur Mitbestimmung zu vervielfältigen und noch mehr Menschen zu integrieren. Themen wie E-Collecting oder eine Weiterentwicklung und Öffnung des Vernehmlassungsverfahrens bieten viel mehr Chancen für unsere Demokratie bei kleinerem Aufwand für die Sicherheit der technischen Prozesse, die es dafür braucht.

E-Voting hingegen bringt schlicht kaum Vorteile, die die potenziell massiven Gefahren für unsere erwiesenermassen wichtige Demokratie aufwiegen könnten.

Erstens ist E-Voting schlicht teurer. Gemäss Schätzungen werden sich die zusätzlichen Gesamtkosten für alle Kantone auf ungefähr eine Million Schweizer Franken pro Jahr belaufen (Erläuternder Bericht, S. 8, Abschnitt Auswirkungen).

Zweitens wird mit E-Voting auch keine erhöhte Stimmbeteiligung (mehr) angestrebt. Zu oft wurde der Nachweis des Fehlens eines diesbezüglichen Effektes erbracht.

Bereits die Evaluation der E-Voting-Testphase im Kanton Zürich von 2008 bis 2011 kam zum Schluss, dass sich die Stimmbeteiligung durch das E-Voting-Angebot nicht erhöht hat. Zum selben Ergebnis kommt das Zentrum für Demokratie Aarau (ZDA) in einer Untersuchung für Genfer und Zürcher E-Voting-Gemeinden: «Es zeigten sich keinerlei Effekte hinsichtlich der Stimmbeteiligung, auch nicht für die unter 25-Jährigen». Zudem ist davon auszugehen, dass sich die Akzeptanz von E-Voting beim Einsatz der neuen, individuell verzierbaren Systemen verringern wird, da diese deutlich komplizierter zu benutzen.

Drittens gilt soeben Gesagtes auch für Auslandschweizer:innen, denen im Übrigen auch nur bedingt geholfen wird: Um fehlende postalische Infrastruktur ausgleichen zu können, würden nur komplett dematerialisierte E-Voting-Systeme helfen, um die es in der Vorlage jedoch gar nicht geht. Selbst wenn jegliche bereits vorgebrachten, demokratiepolitischen Argumente nicht gälten, würde selbst die Zuhilfenahme einer künftigen E-ID als Ersatz für die individuelle Verifizierbarkeit eine briefliche Zustellung derselben nicht ersetzen (Erläuternder Bericht, S. 27, Erläuterungen zum Anhang Ziff. 2.1 und Ziff. 4.12 VEleS). Offensichtlich wird der postalische Rückweg von Abstimmungscouverts zwar eingespart, zeitliche Einschränkungen hierbei könnten jedoch viel simpler und verfassungsmässig weit weniger prekär beispielsweise durch frühere Postzustellungen gelöst werden. Abgesehen davon würde die Neuausrichtung von E-Voting bei Auslandschweizer:innen auch keinerlei prozentualen Beschränkungen unterliegen, sondern direkt in den Live-Betrieb gehen.

Dasselbe gilt auch für Menschen mit Behinderung, was aufgrund der Möglichkeit zum Einscannen der Verifizierungsreferenz vorgängig zur Stimmabgabe jedoch als begrüssenswert einzustufen ist. Durch diese Erleichterung der individuellen Verifizierbarkeit können auch Menschen mit Sehbehinderung ihre eigene Stimmabgabe selbst und ohne fremde Hilfe überprüfen (Erläuternder Bericht, S. 26, Erläuterungen zum Anhang Ziff. 4.10 VEleS), und können so ihr Stimmgeheimnis effektiv wahren. Jedoch ist gerade bei Menschen mit Hörbehinderung die Informationszugänglichkeit, wie einfach verständliche Texte und Videos zur Entscheidungsfindung, wichtig und verbesserungswürdig – und nicht der Abstimmungsvorgang per se. Um Menschen mit Sehbehinderung die Stimmabgabe per Brief oder an der Urne ohne fremde Hilfe zu ermöglichen, könnten sogenannte Wahl- oder Abstimmungsschablonen zum Einsatz kommen, wie sie in vielen Ländern bereits im Einsatz sind.

Der Vollständigkeit halber soll an dieser Stelle noch ein häufiges Missverständnis ausgeräumt werden: Oftmals wird von Befürworter:innen des E-Voting angeführt, E-Banking sei heutzutage schliesslich auch eine Selbstverständlichkeit. Dass dessen Ziel jedoch die eindeutige Identifizierung einer Einzelperson ist, die beim E-Voting unter keinen Umständen erfolgen darf, wird hierbei völlig verkannt – weshalb der Vergleich mit der elektronischen Zahlungsabwicklung völlig unzulässig ist.

Technische Defizite

Selbstverständlich nehmen wir als Digitale Gesellschaft auch zum vertieft technischen Teil Stellung, wobei wir uns auf die unseres Erachtens schwerwiegendsten technischen Versäumnisse beschränkt haben. Es muss jedoch betont werden, dass die nachfolgenden Ausführungen keineswegs als generelle Zustimmung zu E-Voting-System verstanden werden dürfen, sondern vielmehr Anforderungen und Verbesserungsvorschläge ultima ratio darstellen. Will man sich wirklich nicht vom (offensichtlich gefährlichen) Weg abbringen lassen, sollten folgende Gesichtspunkte zwingend erneut beleuchtet werden:

Generell muss vorab angemerkt werden, dass wohl die allerwenigsten Vernehmlassungsteilnehmer:innen – geschweige denn die Schweizer Durchschnittbürger:in – den extensiven Anhang dieser Vorlage auch nur im Ansatz verstehen werden können. Bei gewissen Punkten scheint man sich entschieden zu haben, äusserst detaillierte Regulierungen zu erlassen, während gravierende, allgemeine Mängel nur spärlich adressiert wurden. Ob dies den Anschein erwecken soll, man habe alles durchdacht, sei an dieser Stelle dahingestellt.

Zunächst entspricht es zwar Schweizer Tradition wie auch Recht, dass wie im hier zugrundeliegenden Fall ein Vernehmlassungsverfahren durchgeführt wird. Der Diskurs zwischen Gesetzgeber, politischen Parteien, verschiedenen Interessensvertretungen, vor allem aber auch NGOs, ist immer begrüssenswert und gehört in der Schweizer Politik ebenso dazu wie Initiativen oder Referenden. Im Vergleich mit gewissen anderen Ländern ist dies vor allem beim Thema E-Voting auch wünschenswert, widerspräche es doch jeglichen Werten der Schweizer Demokratie, wenn hierzulande wie in Australien Strafandrohungen für den öffentlichen Diskurs zu Schwachstellen in E-Voting-Systemen ausgesprochen würden. Das andere Extrem in Estland mit langjährigen Erfahrungen im E-Voting ohne Rücksicht auf Verletzungen des Stimmgeheimnis' ist in der Schweiz ebenso wenig denkbar. In der internationalen

Fachwelt geniesst die Schweiz für Ihre E-Voting-Regulierung (nicht die Implementierung) einen guten Ruf. Für die aktuelle Debatte erwarten wir, dass zumindest juristisch und technisch den höchsten Ansprüchen gerecht wird. Daher erstaunt der Mangel an Organisationen mit technischem Fachwissen in der Adressatenliste dieser Vorlage. Logischerweise werden diese tatsächlichen Adressaten die technischen Feinheiten im Anhang wohl kaum kommentieren (können), wodurch sich gezwungenermassen die Frage stellt, ob in diesem Vernehmlassungsverfahren tatsächlich hilfreiche Anmerkungen, oder blosse Absegnungen angestrebt wurden.

Eine störende Diskrepanz ist ausserdem zwischen den Empfehlungen der Expert:innen aus dem Dialog mit der Wissenschaft und der jetzigen Regulierung feststellbar. Mehrmals haben diese Expert:innen bestimmte Regulierungen aufgrund stichhaltiger Argumente und im Vergleich zur Bundeskanzlei weitaus grösserer Sachkenntnis vorgeschlagen, die es aus unerfindlichen Gründen nicht in die zugrundeliegende Vorlage geschafft haben. Beispielsweise wird die Abweichung der von Expert:innen geforderten Open-Source-Lizenz weder im erläuternden Bericht, noch in den sonstigen Vernehmlassungsunterlagen erklärt. Stattdessen findet sich ohne Angabe von Gründen im **Artikel 27m VPR** nurmehr eine Offenlegungspflicht. Man müsste doch meinen, dass wenn man schon Expert:innen zu einem Dialog einlädt, dessen Resultate selbst in einer Zusammenfassung auf ganze 70 Seiten erwachsen, man zumindest im Ansatz die Abweichungen derselben erklären wollen würde. Auch im Hinblick auf das im erläuternden Bericht explizit genannte Ziel einer Reduzierung der Abhängigkeit von einzelnen Personen und Organisationen würde mit einem Zwang zu Open Source viel eher erreicht als durch die blosse Pflicht zur Veröffentlichung des Quellcodes (Erläuternder Bericht, S. 11 Erläuterungen zu Art. 27m Abs. 2 VPR).

Das aktuell bestehende Versäumnis eines fehlenden Zwangs zu Open Source hat negative Signalwirkung. Denn erstens sollten auch andere Länder diese Systeme nutzen können, sollte sich herausstellen, dass die Schweizer Bevölkerung mit der fehlenden Nachvollziehbarkeit einverstanden ist. Zweitens ist auch international bekannt, dass das teuerste Gut der Schweizer:innen die direkte Demokratie ist, erwuchs es doch schon vor langer Zeit zu einem tragenden Identitätsmerkmal unseres Landes (vgl. den Abschnitt zur historischen Komponente). Man kann vermuten, dass dann auch anderswo von Bürger:innen erwartet würde, dass sie dem Staat und undurchsichtigen Kontrollinstanzen (in unserem Fall dem Gremium der Prüfer:innen) glauben schenken, ihre jeweilige Demokratie sei nicht in Gefahr. In einem solchen Szenario wird dann erst recht zur Gretchenfrage, welches System eingesetzt wird und

wie dieses im Detail funktioniert, wodurch sich ein weiteres Argument für Open-Source-Software ergibt. Diese Signalwirkung ist im Übrigen auch hierzulande von Bedeutung. Es wäre äusserst wünschenswert, wenn jegliche E-Government-Unterfangen ausschliesslich unter Open-Source-Lizenz lanciert würden, da auch in zukunftsträchtigen Bereichen wie E-Health oder einer staatlichen E-ID die jeweiligen Systeme eines hohen Vertrauens der Bevölkerung in deren korrekte Funktionsweise bedürfen, um breite Nutzung zu finden. Durch eine rigorose Open-Source-Pflicht würden vielerlei Spekulationen um technische Spezifitäten und theoretische Angriffsvektoren gegenstandslos. Das in Folge einer Open-Source-Lizenzierung zu erwartende gesteigerte (internationale) Interesse an einer bestimmten Software dient gleichzeitig immer auch deren Qualitätssicherung und -steigerung. Denn je mehr Augen sich auf denselben Code richten, desto eher können latente Fehler gefunden bzw. ausgeschlossen werden. Verbleibt ein System jedoch unter proprietärer Lizenz, fehlt verständlicherweise der Anreiz für aussenstehende Akteure, Zeit und Geld in deren Analyse und Weiterentwicklung zu investieren. Aus einer ganz grundsätzlichen Erwägung heraus muss zudem aus öffentlichen Geldern finanzierte Software auch öffentlich bleiben und dem Ansatz «Public Money? Public Code!» folgen.

Zudem ist hinderlich, dass die Post mit dem derzeit einzigen verbliebenen System kommerzielle Interessen verfolgt. Die Weiterentwicklung der Schweizer Demokratie darf nicht davon abhängig sein. Der Bund und die Kantone sollen deshalb selbst grössere Verantwortung für die Entwicklung des Systems übernehmen und dies nicht einem einzigen kommerziellen Anbieter überlassen. Insbesondere während des Versuchsbetriebs erscheint es illusorisch, dass der Zielkonflikt zwischen Weiterentwicklung der Demokratie, Sicherheit und kommerziellen Interessen erfolgreich gelöst werden kann. Die Abstimmung über die E-ID vom März 2021 hat gezeigt, dass die Bevölkerung privatwirtschaftlichen Akteuren gegenüber wenig Vertrauen hat, wenn es um Kernprozesse unseres Staates geht. Dazu gehört auch das Wählen und Abstimmen.

Bereits im Vorfeld der nun geplanten Neuausrichtung des Versuchsbetriebs, die nur eine Offenlegungspflicht verlangt, konnte die Post ihre geschäftlichen Interessen durchsetzen. Der Konzern hat bis heute bereits 20 Millionen Franken in das Projekt investiert und sieht durch eine Open-Source-Lizenzierung sein Geschäftsmodell gefährdet (wie die Republik berichtet: «Wird eine Open-Source-Lizenz verlangt, zieht sich die Post zurück» sowie «Wir könnten das E-Voting-Programm bei verbindlicher Open-Source-Lizenz gleich abbrechen»). Da die Kantone jedoch auf die (einzige

verbliebene) Anbieterin angewiesen scheinen, haben sie sich für die Interessen des Konzerns stark gemacht. Gemeinsam konnten sie sich gegen die Forderung einer Open-Source-Lizenzierung von Seiten der Expert:innen durchsetzen. Für die Kantone, die auf Biegen und Brechen einen möglichst schlüsselfertigen E-Voting-Dienst beziehen möchten, scheint das Vorgehen erklärbar. Für die Sicherheit und das Vertrauen in die Demokratie hingegen ist diese «Geiselhaft» verheerend, wären doch gerade die Kantone für die Risikobeurteilung und den Einbezug der Öffentlichkeit bei der Durchführung von E-Voting verantwortlich.

Der zweite Satz in Artikel 27m Abschnitt 2 VPR muss daher lauten:

> *Sie legen die entsprechende Dokumentation offen, machen den Entwicklungsprozess transparent und veröffentlichen den Quellcode unter einer Open-Source-Lizenz.*

Die Ausführungen zu **Artikel 27i VPR** bezüglich Plausibilisierung sind begrüssenswert, wenn auch imperfekt. Eine Plausibilisierung ist eine statistische Methode, durch die sich krasse Auffälligkeiten im Stimmverhalten erkennen liessen. An sich keine schlechte Idee, müssen die Methoden hierzu jedoch teilweise erst noch entwickelt werden: Die Vermutung liegt nahe, dass diese Unklarheit sogar Absicht seitens der Bundeskanzlei gewesen ist, nämlich um die Kantone dazu zu bringen, diese Tools selbst (potenziell in Zusammenarbeit mit Universitäten) zu entwickeln und untereinander auszutauschen. Für eine öffentlich nachvollziehbare Plausibilisierung ist es jedoch notwendig, dass die elektronischen von den analogen Stimmen getrennt werden. Würden nun nur einzelne Personen in einem kleinen Stimmkreis elektronisch abstimmen – wie beispielsweise Menschen mit Behinderung –, bestünde stets eine latente Verletzungsgefahr des Stimmgeheimnisses. Inwiefern dieses Problem abgeschwächt wird, oder ob es den Verfassern dieser Vorlage überhaupt bewusst ist, wird weder in der Vorlage selbst noch im erläuternden Bericht erwähnt.

Begrüssenswert ist jedoch, dass nun eine Verifizierung selbst – und nicht mehr nur die Möglichkeit zur Plausibilisierung – verlangt wird. Zudem wird diese Aufgabe nun klar den Kantonen zugewiesen, während im Abs. 2 der vorgängigen Verordnung nicht geregelt war, wer genau verifizieren soll. Die aktuelle Vorlage bedingt mehr Know-How auf Kantonsebene und reduziert die Macht des Systemanbieters, was unter Anbetracht des derzeitigen Monopols der Post zu begrüssen ist.

Im Absatz 1 Bestimmung b des **Artikel 13 VEleS** werden Denial-of-Service-Angriffe aus den öffentlichen Sicherheitstests ausgenommen. Obwohl absolut üblich, müssen

solche Testangriffe trotzdem zwingend durchgeführt und die Resultate publiziert werden, wovon in der Vorlage leider nirgendswo die Rede ist.

Die mehrmalige Nennung von Bug-Bounty-Programmen kann ebenfalls nur als Augenwischerei bezeichnet werden, spricht jedoch eine eindeutige Sprache: Das Schweizer Volk soll jetzt also darauf hoffen, dass die besten Hacker:innen der Welt bitte unbedingt an all den Fehlersuchen mitmachen, sodass ja alle Fehler und Risiken aufgedeckt werden und nicht zu einem späteren Zeitpunkt von noch Fähigerenen zum Schaden unserer Demokratie ausgenutzt werden können. Zudem handelt es sich hierbei nicht um Standard-Software oder -Komponenten, sondern um höchst komplexe IT-Systeme, weshalb nicht davon ausgegangen werden kann, dass Systemfehler spätestens beim Bug-Bounty-Programm zu Tage treten. Es bleibt auch nach solch öffentlichkeitswirksamen Auftritten wahrscheinlich, dass nicht alle potenziellen Sicherheitslücken aufgedeckt werden, wie die Geschehnisse vor zwei Jahren eindrücklich bewiesen haben.

Schlussbemerkungen

Nach dem Gesagten kann nur noch auf einige besorgniserregenden Äusserungen im erläuternden Bericht verwiesen werden, die einem den Kern des E-Voting-Dilemmas erneut vor Augen führen: «Kein Beweis kann mit absoluter Sicherheit bestätigen, dass alle Stimmen im Sinne der Anforderungen in Artikel 5 Absätze 2 und 3 korrekt verarbeitet wurden» (Erläuternder Bericht, S. 15, Erläuterungen zu Art. 6 VEleS). Und auch: «Die Sicherheitsziele (vgl. Art. 4 Abs. 3) lassen sich nicht mit hundertprozentiger Gewissheit erreichen» (Erläuternder Bericht, S. 28, Erläuterungen zum Anhang Ziff. 13 VEleS). Wenn diese schwerwiegenden, zugestandenen Risiken objektiv abgeschätzt würden, müsste man von einer erneuten Aufnahme des E-Voting-Betriebes – selbst von Versuchsbetrieben – aufgrund kaum überzeugender Argumente absehen.

Nach mehr als 20 Jahren will man noch immer nicht einsehen, dass E-Voting in der Schweiz fehlgeschlagen ist. Diese Tatsache versucht man nicht einmal zu verheimlichen, benennt der erläuternde Bericht doch eindeutig den einzigen Grund für die Neuausrichtung: «Mit der Weiterführung der Versuche in einzelnen Kantonen würde schliesslich nur angestrebt, dass die vorhandenen Ressourcen und Know-how sowie bereits getätigte Investitionen bei den Kantonen und den Systemanbietern nicht verloren gehen.» Ja, E-Voting entspricht theoretisch dem digitalen Zeitalter und selbstverständlich könnten derart komplexe IT-Systeme theoretisch funktionieren,

doch die Praxis lehrte uns leider zu oft das Gegenteil.

Hinweis: Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Digitale Gesellschaft zu solchen Regelungen verbunden.

Mit freundlichen Grüssen

Erik Schönenberger
Geschäftsleiter

Quellen

- Cottier, T., & Liechti, R. (2008). Schweizer Spezifika: Direkte Demokratie, Konkordanz, Föderalismus und Neutralität als politische Gestaltungsfaktoren. Die Schweiz im europäischen Integrationsprozess, Baden-Baden, 39-61.
- Ghielmini, S., Kaufmann, C., Post, C., Büchler, T., Wehrli, M., & Amacker, M. (2021). Grund-und Menschenrechte in einer digitalen Welt. buch & netz.
- Killer, C., & Stiller, B. (2019). The Swiss Postal Voting Process and its System and Security Analysis
- Lauer, T. W. (2004). The risk of e-voting. Electronic Journal of E-government, 2(3), 177-186.
- Markić, L. (2019). Die elektronische Stimmabgabe im Lichte des Prinzips der Öffentlichkeit:E-Voting im Spannungsverhältnis zwischen dem Ruf nach mehr digitaler Demokratie und der Wahl- und Abstimmungsfreiheit
- Tanner, J. (2015). Demokratie, ein Auslaufmodell? Tages-Anzeiger vom 15. Juli 2015.
- Tschopp, S. S. (2012). Politische Systembildung aus dem Geist der Geschichte: Zu den kulturellen Wurzeln der direkten Demokratie in der Schweiz.