Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Änderung des Bundesgesetzes über die politischen Rechte (Überführung der elektronischen Stimmabgabe in den ordentlichen Betrieb): Fragebogen zum Vernehmlassungsverfahren

Vernehmlassung vom 19. Dezember 2018 bis zum 30. April 2019

Absender
Namen und Adresse des Kantons oder der Organisation
Alternative Linke Bern, Postfach 504, 3018 Bern

Kontaktperson für Rückfragen [Name, E-Mail, Telefon]
Klingsor Reimann, info@al-be.ch, 031 961 12 33
Raffael Joggi, raffael.j@gmx.ch

Vorbemerkung

Der elektronische Stimmkanal ist eine Gefahr für die demokratische Legitimation der politischen Institutionen der Schweiz.

Vollständige Verifizierbarkeit gibt es nicht: Kein Computerprogramm der Welt – also auch nicht E-Voting – kann sich selbst vollständig verifizieren. Dieser Umstand ist mathematisch und informatiktheoretisch bewiesen und gilt für alle Computer, wie wir sie heute kennen.

Nachvollziehbarkeit irgendwie ganz und gar nicht: Was ein E-Voting System *kann,* lässt sich lediglich an Hand dessen nachvollziehen, was das System *tut*. Es bleibt daher eine Blackbox, die nicht in seine Teile zergliedert und individuell nachvollzogen werden kann.

Beim Vertrauen aufs Ganze gehen: E-Voting Systeme sind inhärent manipulierbar und Manipulation betrifft immer das ganze System. Es reicht darum schon der Verdacht einer Manipulation, um das Vertrauen in den elektronischen Stimmkanal nachhaltig und rückwirkend zu erschüttern.

Einführung

Im Rahmen der Vernehmlassung *E-Voting als dritter ordentlicher Stimmkanal* zur Teilrevision des Bundesgesetztes über die politischen Rechte (BPR) vom 19. Dezember 2018 ist das vorliegende Argumentarium als Beilage für die Vernehmlassungsantwort gedacht. Ziel soll es sein auf zwei wesentliche und bisher ungenügend genannte Probleme des *elektronischen Stimmkanals* (hier auch *E-Voting*) hinzuweisen. Als wesentlich werden diese Probleme erachtet, da sie einem E-Voting System inhärent sind und weder auf mangelnde Vorsicht oder Fahrlässigkeit der Benutzer noch auf mangelnde technische Ausgereiftheit des Produkts zurückzuführen sind. Konkret handelt es sich um zwei prinzipielle Probleme von Computerprogrammen: der *inhärenten Manipulierbarkeit* und der *ungenügenden Nachvollziehbarkeit*. Der daraus resultierende potentielle Vertrauensverlust in den Abstimmungsprozess stellt eine Gefahr dar für die demokratische Legitimation der politischen Institutionen der Schweiz.

Viele stichhaltige, bereits an anderer Stelle geäusserte Bedenken in Bezug auf E-Voting wurden hier aus Platzgründen weggelassen (*Problem der unsicheren Plattform*, *„Man in the middle"-Attacken*, *„False positives"* bei der Verifizierung, Wahrung des Stimmgeheimnisses bei gleichzeitiger individueller Verifikation, hohe finanzielle Kosten, fehlende betriebliche Sicherheitskriterien, fehlende Konkurrenz der Anbieter etc.). Selbstverständlich sind wir der Auffassung, dass diese und auch die hier nicht explizit ausgeführten Probleme zentrale Gründe gegen eine Einführung eines ordent-

lichen elektronischen Stimmkanals darstellen und in ein umfassendes Argumentarium aufzunehmen sind.

„Vollständige Verifizierbarkeit“ gibt es nicht

Mittels der sogenannten „vollständigen Verifizierbarkeit“ (gemeint ist vermutlich eine Kombination aus *individueller Verifizierung* und *universeller Verifizierung*) als Sicherheitsanforderung an ein mögliches E-Voting System soll einerseits dafür gesorgt werden, dass die Abstimmende sicherstellen kann, dass ihre Stimme korrekt im System registriert wurde (individuelle Verifizierbarkeit) und andererseits, dass Abstimmungsverantwortliche überprüfen können, ob das E-Voting System als Ganzes manipuliert worden ist oder nicht (universelle Verifizierung).

Im Gegensatz zu der wohlbekannten *individuellen* und *universellen Verifizierbarkeit* ist nicht klar, was mit „vollständiger Verifizierbarkeit“ gemeint ist und es scheint sich um eine hausgemachte Wortschöpfung zu handeln. Dies ist bemerkenswert und es mag dabei der Wunsch des Vaters des Gedankens gewesen sein, denn auch wenn eine vollständige Verifizierung im Zusammenhang mit E-Voting sehr wünschenswert wäre, ist diese doch aus Informatik-theoretischen Überlegungen für Computerprogramme prinzipiell nicht zu haben.

Der Grund warum ein Computerprogramm nie vollständig verifiziert werden kann liegt darin, dass ein Computerprogramm prinzipiell, aus sich heraus, nicht ermitteln kann, ob es manipuliert worden ist. Diese Eigenschaft eines jeden Computerprogramms folgt aus dem bekannten, von Alan Turing beschriebenen *Halteproblem*. Das Halteproblem gilt für jedes auf einem Computer ausführbare Programm und damit auch für softwarebasiertes E-Voting. Es wird aus diesem Grund niemals abschliessend möglich sein zu überprüfen, ob ein E-Voting System manipuliert worden ist oder nicht. Es ist wichtig zu verstehen, dass das Halteproblem mathematisch bewiesen ist und damit für sämtliche Computer gilt, wie wir sie heute kennen. Hierbei sind jegliche kryptographischen Vorkehrungen insofern unerheblich, als dass diese bestenfalls Komponenten *innerhalb* der Software, nie aber die Software *als solches* verifizieren können. *Vollständige Verifizierbarkeit gibt es nicht.*

Nachvollziehbarkeit irgendwie ganz und gar nicht

Ein Problem, das in Bezug auf den elektronischen Stimmkanal oft genannt wird, ist die fehlende Nachvollziehbarkeit im Vergleich mit den herkömmlichen Abstimmungskanälen. Um zu verstehen, was damit gemeint ist, mag man sich fragen inwiefern die zwei bestehenden Abstimmungskanäle, also Urnen- und Briefabstimmung, nachvollzogen werden können. Bei genauerer Betrachtung ist die Antwort einfach: Im Gegensatz zu E-Voting ist der Abstimmungsprozess der beiden herkömmlichen Abstimmungskanäle naturgemäss in einzelne und voneinander unabhängig verständliche

Schritte gegliedert. Um das zu sehen, kann man sich exemplarisch die Arbeit einer Postbotin im Falle einer brieflichen Abstimmung vorstellen. Der Postdienst, der dabei vollbracht wird, also das Einsammeln und Überbringen des Abstimmungscouverts, kann als ein Schritt von vielen im Abstimmungsprozess begriffen werden. Des Weiteren können die für den Teilprozess „Postdienst“ wesentlichen *Erfolgsbedingungen* benannt werden (z.B. das Abstimmungscouvert wird abgeholt und landet in der Abstimmungszentrale). Die Möglichkeit, den Gesamtprozess in Teilschritte zu zergliedern und Erfolgsbedingungen für die Teilschritte zu benennen, ist es, was mit Nachvollziehbarkeit gemeint ist.

Vergleicht man das mit dem elektronischen Stimmkanal, müssen wir uns E-Voting als ein laufendes Computerprogramm in Betrieb vorstellen. Ob Laie oder Profi, für ein solches in Betrieb befindliches Computerprogramm kann keine Zergliederung vorgenommen werden, denn ist ein Computerprogramm erst einmal gestartet, verhält es sich für den Betrachter wie eine „Blackbox“: Was das Computerprogramm *kann*, lässt sich lediglich an dem ermitteln, was es *tut*. Und was ein Computerprogramm tut, ist Eingaben (Input) zu Ausgaben (Output) verarbeiten. Das heisst, um ein laufendes Computerprogramm zu verstehen, kann dieses lediglich als Funktion, also als *ein* Prozess, verstanden werden. Es ist dabei unerheblich, ob das Computerprogramm repliziert läuft, an verschiedenen Standorten betrieben wird, es sich um ein einzelnes Computerprogramm, oder einen ganzen Verbund von interagierenden Programmen handelt.

Dieser Punkt ist nicht eine Frage des technischen Knowhows, sondern liegt in der Natur der Sache: was ein Computerprogramm können soll, wird zuvor als Quellcode – sozusagen als Bauanleitung – verfasst. Aus dem Quellcode wird das Computerprogramm „gebaut“ (d.h. in für den Computer, aber nicht für Menschen verständliche Instruktionen übersetzt) und dann gestartet. Läuft das Computerprogramm einmal, ist diesem nicht mehr anzusehen mit welchem Quellecode es gebaut wurde und es lässt sich darum nur noch rein funktional – also anhand dessen was ein- und ausgegeben wird – beschreiben.

Zum Vergleich: Im Falle des Postdiensts ist es zwar möglich, dass auch hier die durchschnittliche Stimmberechtigte nicht notwendigerweise in der Lage sein wird jeden Aspekt des Überbingens eines Abstimmungscouverts im Detail zu verstehen, doch liegt zumindest eine vage Beschreibung des Teilprozesses vor, für den sehr wohl die Erfolgsbedingungen genannt werden können. Hier ist Nachvollziehbarkeit also möglich.

Führt man diesen Vergleich zu Ende, bedeutet dies, dass das, was am elektronischen Stimmkanal mit letzter Sicherheit nachvollzogen werden kann, das ist, was in ein E-Voting System *eingegeben* (Adresserfassung, Stimmabgabe etc.) und *ausge-*

geben (Drucken von Wahlzetteln, Darstellung des aggregierten Resultats der Abstimmung etc.) wird. Es ist keine Zergliederung in Teilprozesse möglich. Schlimmer noch, im Falle von laufenden Computerprogrammen fällt die für die Nachvollziehbarkeit des Abstimmungsprozesses zentrale Benennung der Erfolgsbedingungen mit dem zusammen, was überhaupt von einem E-Voting als Prozess verstanden werden kann – also was in das Programm ein- und ausgegeben wird. Damit ist jegliches Verständnis des Prozesses des elektronischen Stimmkanals nicht davon abhängig was ein E-Voting Computerprogramm tatsächlich *kann*, sondern lediglich davon was das E-Voting Computerprogramm vordergründig *tut*. E-Voting ist im Gegensatz zu den zwei herkömmlichen Abstimmungskanälen eine Blackbox bei der *Nachvollziehbarkeit irgendwie ganz und gar nicht* zu haben ist.

Beim Vertrauen aufs Ganze gehen

Fassen wir zusammen: Ein E-Voting System lässt sich nicht in Teilen nachvollziehen, sondern von aussen nur als Ganzes, also *vollständig* betrachten. Gleichzeitig ist ein E-Voting System aus Informatik-theoretischer Sicht nie *vollständig* verifizierbar. Das ist eine ungute Mischung mit erheblichem Gefahrenpotential für das in die Abstimmungskanäle und in die Abstimmung gesetzte Vertrauen. Vertrauen ist aber zentral, um die Legitimation demokratischer Institutionen zu gewährleisten.

Man denke sich eine Webseite einer kantonalen Behörde (für die freilich nicht die gleichen Sicherheitsrichtlinien gelten müssen wir für ein E-Voting System). Stellen wir uns weiter vor, diese wurde gehackt. Allerdings wurde dabei die Webseite der Behörde lediglich um ein Bild – sagen wir eines finster lächelnden Wladimir Putins – ergänzt. Nun besuchen Abstimmende die Webseite mit der Absicht, sich über diese in das E-Voting System einzuloggen. Was würde passieren? Es ist davon auszugehen, dass die Abstimmenden durch diese relativ harmlose Manipulation tief verunsichert wären und wohl lieber gänzlich auf die Stimmabgabe verzichteten, als sich in ein vordergründig manipuliertes E-Voting System einzuloggen.

Was in diesem kleinen Gedankenexperiment zum Ausdruck kommt, ist das grundsätzliche Problem der fehlenden Nachvollziehbarkeit bei gleichzeitig unvollständiger Verifizierung: Bereits der Anschein einer Manipulation genügt, um das Vertrauen in das ganze System nachhaltig zu erschüttern. Im Falle einer Manipulation der herkömmlichen Urnen- und Briefabstimmungen kann der Prozess zergliedert und damit die Manipulation identifiziert werden. Dies ist mit Computerprogrammen prinzipiell nicht möglich.

Jetzt mag man sich fragen – wenn schon das Computerprogramm an sich Manipulation nicht vollständig ausschlissen kann – ob nicht wenigstens die Infrastruktur, auf der E-Voting betrieben werden soll, vollständig sicher gestaltet werden kann. Weit

gefehlt. Alle Sicherheitsprobleme, die auf der Anwenderseite bestehen (z.B. Computer oder Netzwerkverbindung der Abstimmenden wurden gehackt etc.) einmal ausser Acht gelassen; für ein manipulations-freies E-Voting System muss, wie bereits erwähnt, darauf vertraut werden, dass das entsprechende Computerprogramm mit guten Absichten initial gebaut, installiert, gestartet und zu jeder Zeit überwacht wurde. Nun ist es aber so, dass neben den in der Informationstechnologe immer vorhandenen Sicherheitsrisiken auch nur schon kompromittierte Hardware (Server- wie auch Netzwerk-Infrastruktur) ausreicht, um die darauf betriebene Software gleichsam zu kompromittieren. Wenn man bedenkt, dass Experten schon heute davor warnen, dass weite Teile des Internets und möglicherweise auch bereits Teile der IT-Infrastruktur der Bundesverwaltung aus verwanzter Hardware bestehen könnten, ist Manipulation von in der Schweiz betriebenen Computerprogrammen immer möglich. Somit kann auch auf Ebene Infrastruktur die nötige vollständige Sicherheit nicht gewährleistet werden.

Mit Verunsicherung und daraus resultierendem Vertrauensverlust in den elektronischen Stimmkanal ist schon beim *Anschein einer Manipulation* zu rechnen, aber doch es kommt noch schlimmer. Für einen nachhaltigen Vertrauensverlust scheint es bereits ausreichend, das hier vorgebrachte *zu glauben*. Es wäre gut denkbar, dass ohne nachweisliche Manipulation allein der gesellschaftliche Diskurs und die Wahrnehmung das Vertrauen in den elektronischen Stimmkanal erschüttern könnte. Dies würde sich dann auch nicht nur im fehlenden Vertrauen in Bezug auf inskünftige Abstimmungen niederschlagen, sondern könnte sich auch rückwirkend auf bereits abgehaltene Abstimmungen negativ auswirken.

Schliesslich könnte eingewendet werden, dass bereits eine *teilweise Verifizierung*, oder Betrachtung des Ganzen E-Voting Systems *ohne Nachvollzug seiner Teile* für eine Erhöhung der Sicherheit und des Vertrauens in den elektronischen Stimmkanal sorgten. Das mag sein. Doch geht es hier um nichts weniger als die demokratische Legitimation der wesentlichsten politischen Institution der Schweiz. Ledigliche „Erhöhung der Sicherheit wird darum nicht reichen. Eine vernünftige Güterabwägung, gemessen an der Wichtigkeit des Abstimmungsprozesses für die Demokratie, sieht darum wie folgt aus: Entweder sind Abstimmungen mittels E-Voting nachvollziehbar und nicht manipulierbar oder es sollte aus Sicherheits- und Vertrauensgründen ganz auf den elektronischen Stimmkanal verzichtet werden. Es ist anzunehmen, dass die durch die Bundeskanzlei erlassenen, erneut erhöhten Anforderungen in Bezug auf den Umfang der Verifizierbarkeit von E-Voting Systemen und die Offenlegung ihres Quellcodes (vgl. *Freesoftware* bzw. *Opensource*) Ausdruck dieser Überlegungen sind – nun gilt es diese noch konsequent zu Ende zu denken: Der elektronische

Stimmkanal ist eine Gefahr für die demokratische Legitimation der politischen Institutionen der Schweiz.

1. Allgemeine Bestimmungen zu den Stimmabgabeverfahren

1.1. Sind Sie mit der Neuordnung der Grundsätze der Stimmabgabe und der einheitlichen Festlegung der Anforderungen an die Verfahren der Stimmabgabe einverstanden (Art. 5 und 6 E-BPR)?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:
Da die technischen Voraussetzungen nach wie vor nicht gegeben sind, um die elektronische Stimmabgabe sicher, vollständig nachvollziehbar etc. abzugeben, gehört der so genannte dritte Weg der Stimmabgabe (E-Voting) bis auf weiteres nicht als ordentliches Verfahren ins Gesetz.

1.2. Begrüssen Sie die Verankerung der Stimmabgabe an der Urne am Wahl- und Abstimmungstag und die Änderung bezüglich der vorzeitigen Stimmabgabe (Art. 7 E-BPR)?

☐ Ja ☒ Ja mit Vorbehalt ☐ Nein

Anmerkungen:
Die Stimmabgabe an der Urne ist (auch wenn der elektronische Weg als ordentlicher dritter Weg im Gesetz verankert wird) jederzeit für alle Stimmberechtigten zu gewährleisten. Dazu soll die Stimmabgabe an der Urne an mindestens zwei der vier Tage vor der Abstimmung gewährleistet sein.

2. Bestimmungen betreffend die elektronische Stimmabgabe

2.1. Erachten Sie eine Bewilligung durch den Bundesrat für den Einsatz der elektronischen Stimmabgabe im ordentlichen Betrieb für sinnvoll?

☐ Ja ☒ Ja mit Vorbehalt ☐ Nein

Anmerkungen:
Grundsätzlich ist eine Bewilligung durch den Bundesrat zu begrüssen, da die Bedingungen im Falle der elektronischen Stimmabgabe unbedingt zentral durch den Bund geregelt werden müssen.
Es sind jedoch einige Grundvoraussetzungen, die der Vortrag zum Gesetz vorsieht, zu kritisieren: Die Privatisierung von hoheitlichen Staatsaufgaben wie Volksabstimmungen und Wahlen sind nicht zulässig. Auch wenn Kantone formell zuständig bleiben, verlieren sie, die für die Sicherheit nötige, technische Kompetenz an den Hersteller.
Die Sicherstellung der Demokratie wird hiermit an Private und gar an ausländische Einflussnehmer (im aktuellen Fall Scytl) ausgelagert. Ein privater Anbieter von E-Voting kann die Sicherheit alleine nicht gewährleisten und eine hoheitliche Kontrolle bedingt viel mehr technische Kompetenz und Aufwand bei Bund

und Kantonen als heute an Ressourcen vorhanden und zukünftig vorgesehen sind.
In der ganzen Diskussion wurde es verpasst, vorab eine fundierte Bedarfsabklärung zu machen. Der Bedarf wird auf unqualifizierte Umfragen abgestützt und die Öffentlichkeit wird hinsichtlich der Risiken nicht hinreichend informiert. Die Erkenntnisse, dass wichtige sicherheitstechnische Versprechungen nicht erfüllbar und widerlegt sind, werden in der öffentlichen Kommunikation unterdrückt.

2.2. Ist der Geltungsbereich des Öffentlichkeitsgrundsatzes in Artikel 8c E-BPR genügend klar abgesteckt?

☒ Ja ☐ Ja mit Vorbehalt ☐ Nein

Anmerkungen:
Es muss, wie die aktuelle Situation bei der Veröffentlichung des Quellcodes beim System der Post zeigt, klar definiert werden, was unter öffentlich zugänglichem und dokumentiertem Quellcode verstanden wird.

2.3. Halten Sie das Bewilligungsverfahren auf Gesetzesstufe für ausreichend und zweckmässig geregelt?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:
Der Artikel ist aufgrund der aktuellen Ereignisse nicht praktikabel. Die Formulierung von „hinreichend geringen Risiken“ ist zu unpräzise respektive braucht es einen Grundsatz, dass der Bundesrat die Verantwortung dafür hat, dass die „hinreichend geringen Risiken“ ausreichend definiert sind.
Zudem muss im Zusammenhang mit der Zertifizierung gewährleistet werden, dass die für die Zertifizierung zuständige Firma / Stelle unabhängig von der Herstellerfirma ist und es keine Interessensbindungen zwischen der zertifizierenden Stelle und der Herstellerfirma gibt.

2.4. Halten Sie die in Artikel 8e E-BPR vorgesehene Möglichkeit einer Anmeldung für die elektronische Stimmabgabe, die mit Einschränkungen bei der Nutzung der anderen Stimmkanäle verbunden ist, für sinnvoll?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:
Eine Anmeldung einzig für den elektronischen Stimmkanal ist nicht praktikabel respektive steht im Widerspruch dazu, dass sich eine Person jederzeit frei für einen anderen Stimmkanal entscheiden können soll. Zudem ist unklar, wie die Möglichkeit aufrechterhalten werden soll im Falle eines Systemfehlers.

2.5. Ist die in Artikel 8e Absatz 1 Buchstabe b E-BPR vorgesehene Möglichkeit, an der Urne abzustimmen und zu wählen, wenn die elektronische Stimmabgabe nicht möglich ist, ausreichend, um die Ausübung der politischen Rechte sicherzustellen?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:
Siehe Punkt 2.4.

3. Dematerialisierung der Stimmunterlagen für die elektronische Stimmabgabe

3.1. Sind Sie der Auffassung, die Bundesgesetzgebung solle die Kantone ermächtigen, die Stimmunterlagen unter Bedingungen ganz oder teilweise zu dematerialisieren?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:
Eine Dematerialisierung ist nicht praktikabel. Im Falle eines Systemfehlers bspw. können Bürger*innen ihr Wahl- oder Stimmrecht nicht mehr wahrnehmen und die Möglichkeit, dass sich Bürger*innen jederzeit frei für einen anderen Kanal entscheiden können kann nicht gewährleistet werden.
Zudem werden die Sicherheitsrisiken des elektronischen Stimmkanals noch grösser, wenn sämtliche Informationen und Grundlagen elektronisch versandt werden.

Artikelweise Detailerörterung / Discussions, article par article du projet / Esame del progetto erticolo per articolo

BPR Art. Art. LDP LDP art.	Nötig? Nécessaire? Necessaria?	Tauglich? Adéquat? Adeguata?	Praktikabel? Applicable? Realizzabile?	Aenderungsvorschlag? Autre proposition? Proposta di modifica?	Bemerkungen Remarques Osservazioni
5 I	Nein	Nein	Nein	„elektronisch“ streichen.	Aufgrund von Sicherheitsbedenken ist es verfrüht, den elektronischen Abstimmungskanal als dritten Weg im Gesetz zu verankern. Es fehlt der Nachweis einer prinzipiell ausreichend sicheren Methode E-Voting Software zu betreiben. So lange diese fehlt, ist eine gesetzliche Regelung obsolet. Wenn der „elektronische“ Weg nicht gestrichen wird, dann sind die Bemerkungen zu den folgenden Artikeln zu berücksichtigen
5 II	Nein	Nein	Nein		Der zweite Satz muss gestrichen werden (Begründung siehe Art 5 Abs. I).
6 I	Ja	Ja	Ja		
6 II	Ja	Ja	Ja		Dieser Artikel ist sinnvoll.
7 I	Ja	Ja	Ja		
7 II	Ja	Nein	Nein	Siehe Bemerkungen.	Die Stimmabgabe an der Urne soll an mindestens zwei der vier Tage vor der Abstimmung gewährleistet sein.
8 I^{bis}	Ja	Ja	Ja		Es muss sichergestellt werden, dass die briefliche und elektronische Stimmabgabe nicht vom selben Anbieter abgedeckt wird.
8a I	Ja	Ja	Ja		Falls eine elektronische Stimmabgaben vorgesehen wird, macht es Sinn, dass es schweizweit eine Bewilligungsbehörde gibt und nicht jeder Kanton selber verantwortlich ist.
8a II	Ja	Ja	Ja		Siehe 8^{a} I.

8b I	Ja	Nein	Nein		Der Grundsatz, dass Stimmberechtigte nachvollziehen können sollen, ob ihre Stimme gemäss ihrem Willen erfasst worden ist (individuelle Verifizierbarkeit), ist elementar. Die Forderung ist jedoch bei der elektronischen Stimmabgabe weder tauglich noch praktikabel: Die Konzeption der Sicherung als individuelle Verifizierbarkeit gegen Manipulation ist ungenügend. Zum einen stellt sie zu hohe Anforderungen an den Benutzer des E-Votingsystems, da nicht erwartet werden kann, dass die Abstimmenden erkennen, ob ihr Gerät oder die Software manipuliert worden ist. Zum anderen kann die individuelle Verifizierbarkeit Manipulation des Systems nicht sicher ausschliessen. Erschwerend kommt hinzu, dass eine individuelle Verifizierbarkeit das Abstimmungsgeheimnis aufweicht, da unklar ist, wie verhindert werden kann, dass Abstimmungsnachweise erbracht werden, welche auch für Dritte einsehbar sind.
8b II	Ja	Nein	Nein		Die Komponenten eines Systems sind einerseits nie unabhängig und können so nicht die Nachvollziehbarkeit des Ergebnisses garantieren. Die Komponenen eines Systems sind andererseits nie unabhängig und können nie individuell nachvollzogen und verifiziert werden. Dieser Artikel verhindert nicht, dass es an Sicherheitsvorkehrungen gegen eine Manipulation des Ergebnisses und gegen den Bruch des Abstimmungsgeheimnisses mangelt. Es sind für die Öffentlichkeit keine geeigneten konkreten Kriterien sichtbar. Eine elektronische Erstellung und Auszählung von Stimmen ohne die Möglichkeit einer Nachzählung der Gesamtheit aller willentlich abgegebenen JA- und NEIN-Stimmen durch den Stimmbürger stellt für diesen – und das ist neu – einen intransparenten und daher nicht vertrauenswürdigen Prozess dar und widerspricht so den Anforderungen der Demokratie.

8b III	Ja	Nein	Nein		Die zuverlässige Nachvollziehbarkeit ist nicht identisch mit vollständiger Verifizierbarkeit. Ein System kann sich nie vollständig verifizieren. Die sogenannte „universelle Verifizierbarkeit“ der Schweizerischen POST erfüllt die Anforderungen dieses Begriffes nicht, sondern höchstens das ungenügende Regulativ der Bundeskanzlei mit dem Neu-Begriff „vollständige Verifizierbarkeit“. Es wird vorausgesetzt, dass die Software fehlerfrei installiert ist und das kann, sobald das System installiert ist, nicht mehr überprüft werden. Was, wenn ein System fünf Tage vor dem Abstimmungstag abstürzt? Wie kann rückverfolgt werden, wer schon abgestimmt hat? Wenn zehnmal mit denselben Rohdaten gezählt wird, kommt logischerweise wieder dasselbe Resultat hervor. Es ist deshalb nicht nachvollziehbar, ob und wenn ja was falsch gelaufen ist. Die Einplanung von Sicherheitskosten in der Zukunft fehlt.
8c	Ja	Ja	Ja	Die Sicherheitsanforderungen an den Betrieb müssten genauer geregelt werden.	Vor dem Hintergrund der aktuellen Ereignisse um den Quellcode des letzten verbliebenen Anbieters, der Post, ist es wichtig, dass dieser Artikel in dieser Version enthalten ist.
8d I	Ja	Nein	Nein		Der Artikel ist aufgrund der aktuellen Ereignisse nicht praktikabel. Die Formulierung von „hinreichend geringen Risiken“ ist zu unpräzise respektive braucht es einen Grundsatz, dass der Bundesrat die Verantwortung dafür hat, dass die „hinreichend geringen Risiken“ ausreichend definiert sind. Zudem muss im Zusammenhang mit der Zertifizierung gewährleistet werden, dass die für die Zertifizierung zuständige Firma / Stelle unabhängig von der Herstellerfirma ist und es keine Interessensbindungen zwischen der zertifizierenden Stelle und der Herstellerfirma gibt.
8d II	Ja	Ja	Ja		
8d III	Ja	Ja	Ja	Ergänzung Abs. III siehe Be-	Sowohl die Zertifizierung wie auch die Ergebnisse von

				merkung.	Risikoanalysen soll öffentlich zugänglich sein. Auf Verordnungsebene soll auch Transparenz hinsichtlich der Zertifizierungsstellen gewährleistet sein.
8e I	Ja	Nein	Nein	Der Artikel ist zu streichen.	Absatz a und b wiedersprechen sich, die Formulierung ist unklar Der Artikel muss gestrichen werden. Eine Dematerialisierung ist nicht praktikabel. Im Falle eines Systemfehlers bspw. können Bürger*innen ihr Wahl- oder Stimmrecht nicht mehr wahrnehmen und die Möglichkeit, dass sich Bürger*innen jederzeit frei für einen anderen Kanal entscheiden können kann nicht gewährleistet werden. Zudem werden die Sicherheitsrisiken des elektronischen Stimmkanals noch grösser, wenn sämtliche Informationen und Grundlagen elektronisch versandt werden.
8e II	Nein	Nein	Nein	Der Artikel ist zu streichen.	Der Absatz muss gestrichen werden (Begründung siehe Art 8e I).
12 I–III 38 I, IV–V 49 I–III	Nein	Ja	Ja		Siehe Art. 5 Abs I.
47 I^{ter}	Nein	Ja	Ja		Siehe Art. 5 Abs I.
84 II	Nein	Ja	Ja		Siehe Art. 5 Abs I.
84 III	Ja	Ja	Ja	Die Plausibilisierung der Abstimmungsergebnisse ist auf E-Voting auszuweiten.	Auch die Resultate von E-Voting sollen mittels statistischer Methoden überprüft und plausibilisiert werden.