Teilrevision der Verordnung über die politischen Rechte und Totalrevision der Verordnung der BK über die elektronische Stimmabgabe (Neuausrichtung des Versuchsbetriebs)

Vernehmlassung vom 28. April 2021 bis zum 18. August 2021

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, 079 437 02 94

Vernehmlassungsantwort

«Vollständige Verifizierbarkeit»

An sich wäre es begrüssen, dass mit der Teilrevision der Verordnung über die politischen Rechte (VPR) und die Totalrevision der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) die individuelle und universelle Verifizierbarkeit vorgeschrieben ist. Mit der Fokussierung auf die Wortschöpfung «Vollständige Verifizierbarkeit» wird nicht nur der falsche Eindruck einer vollständigen Sicherheit vor Manipulationen erweckt, sondern auch unzulänglich auf die folgenden sicherheitsrelevanten Punkte eingegangen:

1. «Vollständige Verifizierbarkeit» ist informatiktheoretisch prinzipiell nicht zu erreichen, da sich ein Computerprogramm theoretisch wie praktisch nicht selbst verifizieren kann. Verifikation ist von daher eben gerade nicht «vollständig» und geht also immer von einer verifizierenden Komponente aus die eine mit sich nicht identische Komponente verifiziert. Somit wird die verifizierende Komponente dabei nicht selbst verifiziert und kann daher prinzipiell unentdeckt manipuliert worden sein (Trojaner, Bugs etc.).
2. Individuelle und universelle Verifizierbarkeit ist immer nur in Bezug auf eine einzelne Systemkomponente realisierbar. Die Verifizierbarkeit einer solchen Systemkomponente kann allerdings jederzeit durch die Plattform (Betriebssysteme, Frameworks, Server), auf welcher sie betreiben wird oder eingebettet ist, kompromittiert werden.
3. Die folgenden, insbesondere im Anhang der VEleS beschriebenen, sicherheitstechnisch relevanten Systemteilnehmer unterliegen weder der individuellen noch der universellen Verifizierbarkeit: Druckkomponenten, Setup-Komponenten, technische Hilfsmittel der Prüfer:innen. Ihre «Vertrauenswürdigkeit» wird in der Verordnung lediglich vorausgesetzt. Jede dieser Komponenten kann jedoch manipuliert werden und kann damit auch die Verifizierbarkeit der anderen vertrauenswürdigen Systemteile kompromittieren.

Jeder der oben genannten Punkte ist für sich genommen hinreichend, um den in den Verordnungen formulierten Anspruch auf «vollständige Verifizierbarkeit» zu unterminieren. Es ist daher im Grundsatz zutreffend was im Erläuternden Bericht zu den Revisionen dazu festgehalten wird:

> «Die Sicherheitsziele (vgl. Art. 4 Abs. 3) lassen sich nicht mit hundertprozentiger Gewissheit erreichen.»
> Erläuternder Bericht vom 28. April 2021, S. 28

Was jedoch in der Teilrevision der VPR und der Totalrevision der VEleS fehlt, ist die Klarstellung, dass «vollständige Verifizierbarkeit» nur eine relative Sicherheit mit sich bringen wird. Nur wenn dies deutlich in der Revision kommuniziert wird, kann für den künftigen Versuchsbetrieb die in der Verordnung mehrfach geforderte Transparenz in Bezug auf eine realistische Risikoabschätzung und breit angelegte Debatte entstehen.

Die AL Bern fordert, dass die Totalrevision der VEleS im Sinne der Transparenz und Risikoabwägung explizit festschreibt, dass vollständige Verifizierbarkeit nicht bedeutet, dass das System vollständig sicher vor Manipulation ist.

Fehlende Nachvollziehbarkeit

Computersysteme sind grundsätzlich schwer nachzuvollziehen. Das hat, einerseits, damit zu tun, dass nur wenige Menschen vertieft fachkundig in Bezug auf Computertechnologie sind und, andererseits, insbesondere auch damit, dass sich ein in Ausführung befindliches Computerprogramm, selbst für Fachkundige, nur Anhand der getätigten Eingaben (Input) und Ausgaben (Output) nachvollziehen lässt. Das heisst: einem laufenden Computerprogramm sieht man nicht an, was es macht, sondern nur, was es ausgibt (auf einen Bildschirm, Terminal, Drucker etc.). Dieser Umstand macht es für Menschen allgemein schwierig nachzuvollziehen was bei einem Computersystem effektiv vor sich geht.

Das für sich genommen ist nicht neu und auch nicht per se problematisch, doch im Falle von e-Voting gelten erhöhte Anforderungen an die Nachvollziehbarkeit (vgl. *Grundsatz der Öffentlichkeit der Wahl*). Diesem Umstand wird in dem bemerkenswerten Urteilspruch des Bundesverfassungsgerichts Deutschland im Zusammenhang mit elektronischen Wahlmaschinen Ausdruck verliehen:

> «Der Einsatz von Wahlgeräten, die die Stimmen der Wähler elektronisch erfassen und das Wahlergebnis elektronisch ermitteln, genügt nur dann den verfassungsrechtlichen Anforderungen, wenn die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können. Während bei der herkömmlichen Wahl mit Stimmzetteln Manipulationen oder Wahlfälschungen unter den Rahmenbedingungen der geltenden Vorschriften jedenfalls nur mit erheblichem Einsatz und einem präventiv wirkenden sehr hohen Entdeckungsrisiko möglich sind, sind Programmierfehler in der Software oder zielgerichtete Wahlfälschungen durch Manipulation der Software bei elektronischen Wahlgeräten nur schwer erkennbar. Die große Breitenwirkung möglicher Fehler an den Wahlgeräten oder gezielter Wahlfälschungen gebietet besondere Vorkehrungen zur Wahrung des Grundsatzes der Öffentlichkeit der Wahl.»

> Urteil des Bundesverfassungsgericht vom 3. März 2009, 2 BvC 3/07, Pressemitteilung Nr. 19/2009 vom 3. März 209, verfügbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-019.html

Es ist klar, dass mit dem durch die Karlsruher Richter:innen festgestellten *Grundsatz der Öffentlichkeit der Wahl* in der Bundesrepublik Deutschland ein Versuchsbetrieb für die elektronische Stimmabgabe, wie ihn die Schweiz vorsieht, allein aufgrund der mangelhaften Nachvollziehbarkeit, als verfassungswidrige eingestuft würde. Der Grundsatz der Öffentlichkeit der Wahl ist auch für die Schweiz relevant. Es ist darum folgerichtig, dass die Nachvollziehbarkeit künftiger e-Votingsysteme auch in den vorliegenden Verordnungen, zumindest rhetorisch, einen gewissen Stellenwert geniesst:

> «Die Veröffentlichung von Informationen über System und Betrieb der elektronischen Stimmabgabe dient der Nachvollziehbarkeit der Abläufe.»
> Erläuternder Bericht vom 28. April 2021, S. 11

oder:

> «Alle Anforderungen an das kryptografische Protokoll sind über sämtliche Arbeitsergebnisse im Zusammenhang mit dem Softwareentwicklungsprozess hinweg nachvollziehbar.»
> Anhang zur VE-VEleS Rz. 25.1.2

Mit dieser und ähnlichen Ausführungen wird die Verordnung allerdings ihrem eigenen Anspruch nicht gerecht. Für die Akzeptanz eines erneuten Versuchsbetriebs für e-Voting ist entschieden auf die naturgemäss fehlende Nachvollziehbarkeit gegenüber Urnen- und Briefabstimmungen einzugehen. Das heisst, Nachvollziehbarkeit ist nicht etwa gleichzusetzen mit Transparenz – und kann darum nicht lediglich mittels einer Öffnung der Debatte und des Quellcodes begegnet werden. Vielmehr muss Nachvollziehbarkeit, für sich genommen, als eine zentrale technische Anforderung an die Umsetzung künftiger e-Votingsysteme verstanden werden. So könnten, entgegen gängiger Annahmen, beispielsweise gezielte «Medienbruchstellen» implementiert werden (d.h. ein e-Votingsystem wird in mehrere Einzelsysteme aufgeteilt, welche über für den Menschen nachvollziehbare, analoge Schnittstelle miteinander verbunden sind), um der vom deutschen Bundesverfassungsgericht festgestellten, naturgemäss «große Breitenwirkung möglicher Fehler an den Wahlgeräten oder gezielter Wahlfälschungen» entgegenzuwirken [https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-019.html] entgegenzuwirken.

Die AL Bern fordert, dass die Revision der Verordnungen im Sinne des Grundsatzes der Öffentlichkeit der Wahl die Nachvollziehbarkeit der e-Votingsysteme auch als spezifische, technische Anforderung für künftige e-Votingsysteme vorschreibt.

Open Source bedeutet Lizenzierung

Es ist zu begrüssen, dass in den hier vorliegenden Verordnungen viel von «Open Source» die Rede ist:

> «Der Kanton sorgt dafür, dass folgende Unterlagen offengelegt werden: a. der Quellcode der Software des Systems einschliesslich der Dateien mit relevanten Parametern»
> VE-VEIeS Art. 11 Abs. 1 lit. a

und:

> «Jede Person darf den Quellcode zu ideellen Zwecken untersuchen, verändern, kompilieren und ausführen sowie Studien dazu verfassen. Sie darf Studien und Erkenntnisse zu Mängeln publizieren. Sie darf sich insbesondere für die Fehlersuche mit weiteren Personen austauschen und dabei aus den offengelegten Informationen zitieren.»
> VE-VEIeS Art. 12 Abs. 3

Für die Vertrauensbildung ist Transparenz wichtig. Und Transparenz in ein Computerprogramm kann unter anderem mit der öffentlichen Zugänglichkeit seines Quellcodes verbessert werden. Doch scheint in den hier vorliegenden Verordnungen vergessen gegangen zu sein, dass das Prinzip «Open Source» nicht allein die Offenlegung des Quellcodes, sondern in erster Linie ein bestimmtes Lizenzierungsmodell vorschreibt. Die Vorentwürfe der Verordnungen legen hingegen nirgends fest, dass der Quellcode nicht nur einsehbar, sondern auch frei weiterverwendet und weiterentwickelt werden darf. Es ist allgemein bekannt und diesem Umstand wird auch in den Verordnungen mehrfach Rechnung getragen, dass der freie gebraucht und die Weiterentwicklung erheblich zur Verbesserung und Sicherheit der unter den Open Source Modell lizenzierten Software führt. Es ist darum nicht nachzuvollziehen, warum sich die Verordnungen zwar den Quellcode, gemäss den Open Source Standards öffentlich machen will, sich aber über die konkrete Open Source Lizenzierung ausschweigt. Schliesslich ist es wünschenswert ein Lizenzmodell zu wählen, welches erfolgte Modifikationen zwingend zurückfliessen lässt.

Die AL Bern fordert, dass die Revision der Verordnungen für die künftigen e-Votingsysteme das Open Source Lizenzmodell explizit und zwingend vorschreibt.

Verordnung für eine spezifische technische Lösung geschrieben

Die vorliegenden Verordnungen und insbesondere deren Anhänge sind in Bezug auf die technische Umsetzung ungewöhnlich detailliert. Das ist nach dem Debakel mit vergangenen e-Voting Projekten bis zu einen gewissen Grad verständlich, doch läuft die Revision der Verordnungen damit auch Gefahr eine bestimmte technische Lösung vorzuschreiben. So entsteht über weite Teile des Anhangs zur VE-VEleS der Eindruck, dass dieser für einen ganz bestimmten kryptografischen Ansatz (vgl. *CHVote*) geschrieben wurde. Zum heutigen Zeitpunkt ist jedoch mitnichten klar, welcher Ansatz am erfolgversprechendsten sein wird (bspw. bilden dezentrale Konsensus-Algorithmen, die heute vor allem in Block-Chain-Technologie ihre Anwendung finden, eine erfolgversprechende Alternative zu den aktuell angestrebten zentralisierten e-Voting Lösungsansätzen).

Schliesslich lässt sich sagen, dass der hohe technische Detaillierungsgrad des Anhangs zur VEleS vor allem zwei Probleme birgt:

1. Er erschwert es alternativen, möglicherweise heute noch nicht bekannten technologischen e-Voting Lösungsansätzen, sich für den Versuchsbetrieb zu qualifizieren.
2. Über die Kompetenz zur Änderungen des Anhangs der VEleS, wird der Bundeskanzlei unvermittelt die Rolle zugewiesen, über technisch höchst detaillierte Anforderungen für künftige e-Voting Lösungsansätze zu befinden und diese verbindlich festzulegen.

Selbstredend ist es zum heutigen Zeitpunkt nicht klar, wie sich in den nächsten Jahren die e-Voting-Technologie weiterentwickeln wird. Einer Verordnung zum «Versuchsbetrieb» würde es daher besser zu Gesichte stehen, hier die technischen Vorschriften allgemeiner zu halten und damit die Innovation neuer Ansätze den gesetzlichen Rahmen zu geben.

Die AL Bern empfiehlt, dass der Anhang zur Totalrevision der VEleS die technischen Anforderungen allgemeiner formuliert, anstatt einen konkreten Lösungsansatz de facto vorzuschreiben.