Fehlerhafte Interpretation der „Verifizierbarkeit“ bei E-Voting CH

Als Hauptargument für die Sicherheit wird die Verifizierbarkeit angeführt: die individuelle, das Recht des Bürgers, seine Stimme im Ziel überprüfen zu können, sowie die universelle, die Pflicht des Staates, die Richtigkeit des Ergebnisses zu überprüfen.

Mgmt Summary:

Die universelle Verifizierbarkeit ist zwar formell als "vollständige Verifizierbarkeit" von der Bundeskanzlei gefordert. Unter dem gleichzeitigen Anspruch der Stimmanonymität ist sie aber niemals zu erreichen, denn sie verlangt, dass zentral festgestellt werden kann, ob alle Stimmen der Stimmberechtigten korrekt angekommen sind und korrekt verarbeitet wurden. Wenn aber bereits im Benutzergerät das nicht garantiert werden kann (wegen des unsicheren Prozesses der Benutzerführung), so ist es auch auf dem ganzen Wege unmöglich. Diese Erkenntnis (Fehlende End-to-End-Sicherheit) wurde auch von der BFH, die als wissenschaftliche Beratung der Bundeskanzlei fungiert, kommuniziert. Trotzdem führt das bei der Bundeskanzlei zur Anerkennung der bestehenden Lösungen.

- **Warum braucht es die individuelle Verifizierbarkeit (i.V.)?**
  Mit der i.V. sichert der/die StimmbürgerIn sich Recht für sich zur sicheren Stimmabgabe. Mit der I.V. kann der/die StimmbürgerIn überprüfen, ob seine Stimme so angekommen ist, wie er sie eingeben wollte. Wenn der Ablauf auf dem Eingabegerät einwandfrei funktioniert und nicht verfälscht wird durch eine Cyberattacke, wird er benutzergeführt und weiss immer, was als nächstes kommt und wie er die Anzeigen interpretieren muss. Es wechseln sich Code – Eingaben und Code-Überprüfungen mit dem postalisch angekommenen Stimmrechtsausweis ab.
  Dieser Stimmrechtsausweis mit seinen Codes muss *postalisch* kommen, denn jeder elektronisch erzeugte Code könnte durch die gleiche Cyberattacke gefälscht sein und allenfalls das Gegenteil bewirken, von dem was der Nutzer will. Die Nutzung eines 2. Kommunikationsweges für die Codeübermittlung stellt einen Teil der Sicherheit dar, die man erzeugen will.
  Nur diese umständliche manuelle Prozedur garantiert die i.V. auf dem ungesicherten Eingabegerät. Wenn jetzt der Ablauf auf dem Eingabegerät (Handy, Computer) nicht mehr 100%ig korrekt läuft bzw. etwas Falsches angezeigt wird, muss dies der Benutzer erkennen und hat dann nur noch die Möglichkeit auf dem postalischen Weg oder mit dem Gang zur Urne abzustimmen.
  Leider ist er leicht zu überlisten mit manipulierten sprachlichen Angaben auf dem Bildschirm und Eingabeaufforderungen, die nicht beachtet werden dürften, um die i.V. nicht zu gefährden. Das Verpassen einer einzigen Codeüberprüfung oder des Finalisierungscodes bzw. das verfrühte Eingeben des Bestätigungscodes könnte zur Manipulation oder zur verpassten Stimmabgabe führen, was der Benutzer nur dann bemerkt, wenn der den komplizierten Ablauf auswendig beherrscht.
  Jede Art von Vereinfachung durch elektronische Hilfsmittel wie z.B. „neue Apps“, die zur Eingabe verwendet werden könnten, hätten wieder das Risiko einer Manipulation inhärent in sich und diese kann dann nicht mehr mit i.V. überwunden werden. Deshalb wäre jeder Ansatz, diese komplizierte Prozedur zu vereinfachen, der Todesstoss für die Verifizierbarkeit von E-Voting CH, denn die universelle Verifizierbarkeit, wie sie von E-Voting CH angeboten

wird, ist nicht unabhängig und funktioniert nur mit der lückenlosen Anwendung der i.V.. Anbieter von solchen Hilfsmitteln müssten sofort und unisono als potentielle Manipulatoren erkannt und deshalb verboten werden. Bei Bekanntwerden würde die BK sicher Empfehlungen ausgeben, diese ja nicht zu verwenden.
Da aber weder davon ausgegangen werden kann, dass alle Users sich richtig verhalten noch davon, dass nie der Anreiz entsteht, diese komplizierte Prozedur zu vereinfachen ist die i.V nur als *theoretische* Sicherstellung der Entdeckung einer allfälligen Manipulation anzuerkennen. Jedoch als Recht des Einzelnen erfüllt die Prozedur die Anforderungen.

- **Warum braucht es die universelle Verifizierbarkeit?**
  Da obige Tatsache den auf diesem Gebiet wissenschaftlich arbeitenden Leuten bekannt ist, haben diese neben der individuellen Verifizierbarkeit auch die universelle Verifizierbarkeit gefordert. Hier geht es um die Überprüfung durch eine beliebige zentrale Stelle, ob das Gesamtresultat korrekt ist, wobei es sich hier um eine Pflicht des Staates handelt zur Gewährleistung der richtigen Ermittlung des Volkswillens.
  Jetzt müsste also jeder/jede StimmbürgerIn auf sichere Weise dem Staat kommunizieren können, ob seine Stimme korrekt angekommen ist. Wie wir bei der i.V. gesehen haben hat er das zwar eigentlich gemacht, aber eben nur in den Fällen, wo er kein manipuliertes Gerät benutzt oder die Manipulation desselben erkennt und anschliessend einen alternativen Abstimmungskanal benutzt.
  Alle übrigen Fälle (Nichterkennen, Aufgeben, Code-Diebstahl etc.) können nicht erkannt werden, es sei denn, jeder müsste öffentlich bekanntgeben, ob er die i.V. richtig bedienen konnte. Aber dies ist ja auch nicht möglich, denn diese Information unterliegt auch dem Abstimmungsgeheimnis. Es darf niemand gezwungen werden, bekanntzugeben, ob er abgestimmt hat oder nicht. Ausserdem würde wohl kaum einer öffentlich bekanntmachen, dass er die Prozedur nicht beherrscht, weil man ja nie ganz sicher ist, ob man alles richtig gemacht hat.
  Weil der Einzelne auch ein Recht auf die richtige Ermittlung des gesamten Volkswillens hat, und nicht nur das Recht, seine eigene Stimme korrekt zählen zu lassen, muss aber die universelle Verifizierbarkeit so erfolgen, dass sie nicht abhängig ist von allen übrigen StimmbürgerInnen, die vielleicht nicht alle die komplizierten Prozeduren verstanden haben oder von einer Cyberattacke überlistet wurden.
  Mit der aktuellen Konzeption von E-Voting CH ist dies nicht gewährleistet[1]. Deshalb kann man dies nicht Universelle Verifizierbarkeit nennen. Der Begriff „vollständige Verifizierbarkeit“, wie er von der Bundeskanzlei verwendet wird, stellt nichts weiter als einen Versuch dar, mit scheinbar wissenschaftlichen Begriffen das Problem zu vernebeln.
  Man teilt dort die Überprüfung in *Stimmabgabe* und *Stimmenauszählung*[2] auf und bindet das erstere (nur) an das Recht des Einzelnen und (nur) das zweite an die Pflicht des Staates. Es müsste aber beides für beides gelten.

[1] https://www.digitale-gesellschaft.ch/2016/08/13/evoting-in-der-schweiz-universelle-verifizierbarkeit-und-open-source-software-bleibt-wunsch/
[2] Oliver Spycher: https://www.netzwoche.ch/news/2018-10-17/verifizierbares-e-voting-ist-moeglich (18.10.2018)

Deshalb kommen wir zum Schluss, dass die universelle Verifizierbarkeit bei E-Voting CH unter den gegebenen rechtlichen Bedingungen *grundsätzlich* nicht möglich ist und sich mit dem Abstimmungsgeheimnis nicht verträgt.

Die Bundeskanzlei zählt darauf, dass einige, die eine Manipulation bemerken, sich doch melden würden. Das mag zwar stimmen, aber wie werden diese Leute danach behandelt und gehört? Und was soll man daraus letztendlich schliessen, wenn man weiss, dass es nur ein kleiner Bruchteil der Geschädigten ist, der sich meldet? Wer hat anschliessend das Sagen, was zu tun ist? Wollen wir die Abstimmung wiederholen oder nicht? Waren solche Meldungen vielleicht nur ein Vorwand, um eine Wiederholung zu erreichen? Wer soll das alles prüfen und wie? Vielleicht findet man Spuren, aber wie viele? Vielleicht findet man auch keine. Denn diese Untersuchungen sind beliebig aufwendig, langwierig und bedürfen forensischer Spezialkenntnisse von höchster Güte. Die Frist zur Einsprache gegen ein Abstimmungsresultat beträgt 6 Tage. In dieser Zeit wird die Verwaltung gar nichts erreichen.

Und was bedeutet das dann? All diese Fragen zum Risiko –Management sind bei der Einführung von E-Voting CH ungeklärt. Das einzig sichere Resultat eines solchen Vorganges ist ein riesiges Chaos und der Verlust des Vertrauens in die demokratischen Prozesse.

- **Wie funktioniert die „vollständige Verifizierbarkeit" der POST (Sicherstellung der Auszählungs-Authentizität)?**

  Bei der Auszählungsüberprüfung wird bei der POST[3] davon ausgegangen, dass ein allfälliges Problem (Cyberattacke) sich auf einem Teil der Anlage befindet und wenn man dieses Teil redundant führt und den Ablauf über beide Redundanzen führt, dass man den Fehler durch Differenzbildung entdeckt. Diese Annahme ist zwar grundsätzlich richtig, aber sie enthält enorm viele Tücken.

  Man kann zwar Systemkomponenten redundant führen aber man müsste auch den Hersteller (nicht nur den Lieferanten) redundant führen. Die Frage ist, ob man wirklich weiss, wer der Hersteller meines Systemteils ist? Was, wenn der „Hersteller 1" seine Teile (Chips, Middleware, Software, Compiler etc.) auch vom gleichen Sublieferanten bezieht wie der „Hersteller 2"? Wer in der IT arbeitet, weiss, dass er all diese Informationen nie und nimmer hat und viele Systembausteine aus den gleichen Grosskonzernen stammen (Intel, AMD, Microsoft, Apple etc.). Das führt zur Erkenntnis, dass Schwachstellen sich automatisch auch auf redundanten Systemen befinden.

  Ausserdem müsste man auch die Betreiber dieser Systeme trennen, weil sonst nicht sichergestellt ist, dass irgendeiner der Betreiber beide Systeme manipuliert, wenn er dazu einen entsprechenden Anreiz hat. Man müsste auch die Ansteuerung der Betreiber redundant führen, denn sonst könnte irgendein Vorgesetzter eine entsprechende Manipulation initiieren z.B. unter dem Vorwand eines notwendigen Updates.

  Wegen der Komplexität dieser Differenz-Überprüfungen aller Systemteile braucht man auch entsprechende Hilfsprozeduren, die die Unterschiede und daher auch die Authentizität der Auszählungsergebnisse anzeigen. Wenn diese keine Differenz anzeigen geht man von der Annahme aus, dass sie korrekt sind. Jetzt muss man aber sicherstellen, dass diese Prozeduren auch nicht manipuliert sind. Auch das kann man nur sicherstellen, wenn man weitere Hilfsmittel hat, die das prüfen. Diesen Kreislauf könnte man noch eine Weile so weiterführen bis zum Punkt wo ein cleverer Chef-Betreiber sagt, „ich habe alles voll im Griff". Aber er ist

[3] Video der POST https://www.youtube.com/watch?v=2UI3VsszqPE

wohl dann der Einzige, der das beurteilen kann. Oder spricht er aus mangelnder Erfahrung oder aus massloser Selbstüberschätzung, weil er seine Gegner nicht kennt? Und: können bzw. sollen wir ihm vertrauen?

Selbst wenn alles perfekt gemacht wäre und Mitarbeiter vertrauenswürdig sind: Es ist beliebig komplex und für Aussenstehende nicht überblickbar, schon gar nicht durch die Wahlkommission, die dafür zuständig ist.

Das Parlament hat am 11.9.2018 einen Vorstoss[4] versenkt, der die Transparenz der Vorgänge verlangt, so wie das auch als Teil der Menschenrechte für die Glaubwürdigkeit einer Demokratie verlangt wird. Man sieht dort mit dieser Auflage keine Möglichkeit mehr, E-Voting zu verwenden und verweist auf Vorgänge, die auch bei der klassischen Wahl nicht mehr jedermann ohne spezifische Kenntnisse versteht. Der eklatante Unterschied zwischen den Anforderungen zum Verständnis des „doppelten Pukelsheim“ und der modernen IT wird elegant übergangen. Ein zweiter Vorstoss[5], der nur ein Moratorium verlangte, hatte ebenfalls keine Chance.

Es bleibt eine Konsequenz: Aus der Demokratie wird eine Expertokratie. Die Frage ist nur: Wollen wir das?

[4] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180420
[5] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170471