E-Voting – Das Ende der Demokratie?

#tldr: E-Voting birgt neben Chancen auch etliche technologische Risiken, welche die Glaubwürdigkeit von demokratischen Entscheidungen in Frage stellen könnten. Zumindest das Experiment sollte gewagt werden, weil E-Voting den Zugang zur Demokratie gerade für junge Stimmbürgerinnen erleichtert.

Gegner und Befürworter von E-Voting machen in der Schweiz gerade mobil, da die Einführung der elektronischen Stimmabgabe auf das Jahr 2019 vorgesehen ist. Während etliche europäische Länder die Lancierung von E-Voting aus Sicherheitsbedenken auf Eis gelegt haben, glaubt die Schweiz, dieser technologischen Herausforderung gewachsen zu sein. Die Technologien sind vorhanden. Nahezu alle Stimmbürger verfügen über elektronische Kommunkations-Geräte oder einem Zugang zu solchen und können diese - vielleicht auch nur unter Anleitung - bedienen. Gerade die ältere Generation ist im Bezug auf die Bedienung elektronischer Geräte nicht ganz sattelfest. Die Möglichkeit der brieflichen Stimmabgabe müsste für eine Übergangsphase bestehen bleiben. Zudem wäre eine pflegliche Begleitung der älteren Generation in die digitale Demokratie angezeigt.

> *Insgesamt aber sieht es auf den ersten Blick so aus, als ob sowohl der Staat als auch die Stimmbürgerinnen von E-Voting profitieren können.*

E-Voting verspricht auf den ersten Blick eine Vereinfachung und Beschleunigung der demokratischen Entscheidungsfindung. Die Administration von Wahlen und Abstimmungen, die Stimmabgabe und Stimmauszählung würde zweifellos schneller, komfortabler und kostensparender über die Bühne gehen. Ein vereinfachter Zugang zu Wahlen und Abstimmungen kann mehr Wählerinnen und Stimmbürgerinnen mobilisieren: ein Gewinn für die Demokratie. Würde dieser Effekt aber ausbleiben, wäre die viel beschworenen Politik-Verdrossenheit wohl Tatsache. Ferner ist zu hoffen, dass die Beschleunigung von demokratischen Prozessen durch E-Voting nicht zu einer Flut von Vorlagen führt, welche die Stimmbürgerinnen überrollt, überfordert und abstumpft. Insgesamt aber sieht es auf den ersten Blick so aus, als ob sowohl der Staat als auch die Stimmbürgerinnen von E-Voting profitieren können.

> *Tatsächlich dürfte es schwierig sein, das jetztige Wahl- und Stimm-Verfahren entscheidend zu verfälschen, da es auf dezentralen, von Menschen durchgeführten Checks und Gegenchecks beruht.*

Was spricht also gegen die Einführung von E-Voting? Gegner des E-Votings geben zu bedenken, dass Wahl- und Abstimmungsergebnisse dadurch leichter manipulierbar seien. Wenn Wahlen und Abstimmungen manipuliert werden können und somit nicht mehr den Willen des Stimmvolkes abbilden, ist die Demokratie

tatsächlich am Ende angelangt. Fraglich bleibt, warum wir bislang die Gewissheit hatten, dass die Demokratie mit dem System der brieflichen Stimmabgabe nicht manipuliert wurde. Diese Gewissheit beruht auf dem Vertrauen in das System. Tatsächlich dürfte es schwierig sein, das jetztige Wahl- und Stimm-Verfahren entscheidend zu verfälschen, da es auf dezentralen, von Menschen durchgeführten Checks und Gegenchecks beruht. Bei elektronischen Verfahren wiederum ist die genaue Funktionsweise vielleicht nicht einmal mehr für Experten nachvollziehbar. E-Voting setzt also voraus, dass wir jenen Experten, die das System entwickelt und überprüft haben, blind vertrauen müssen. Komplexe Software ist jedoch nie frei von Fehlern. Das Vertrauen in E-Voting-Software wackelt hier zum ersten Mal.

> *Zweifellos gibt es mächtige staatliche und private Gruppierungen, welche zu solchen Infiltrationen und Manipulationen in der Lage sind.*

Ein möglicher Angriffsvektor ist die Manipulation der Software auf den Servern oder auf den Abstimmungsgeräten (Computern, Tablets, Smartphones) der Stimmbürgerinnen. Die Gefahr eines erfolgreichen Angriffs auf die IT-Infrastruktur eines Landes ist reel, wie der aktuelle «Hack» des deutschen Bundestages unterstreicht. Auch der schweizerische Rüstungskonzern Ruag wurde schon digital unterwandert. Sollte es Angreifern gelingen, in sensibelste Bereiche der E-Voting-Infrastruktur vorzudringen, ist es um die Demokratie geschehen. Die Erfahrung zeigt, dass solche gezielten Angriffe stattfinden und vielfach den beabsichtigten Schaden herbeiführen. Zweifellos gibt es mächtige staatliche und private Gruppierungen, welche zu solchen Infiltrationen und Manipulationen in der Lage sind. Auch die Motivation für solche Angriffe ist gegeben, zumal es bei Abstimmungen wie bspw. über die Beschaffung von Kampfflugzeugen um Milliarden von Franken geht. Anderseits fliessen aber die Erkenntnisse über mögliche Angriffsvektoren in die Entwicklung der E-Voting-Software ein. Die Entwickler werden versuchen, die Software und die Hardware gegen alle denkbaren Angriffe zu härten.

> *Wer kann aber schon garantieren, dass neuere Prozessoren keine neuen Schwachstellen enthalten?*

Auch wenn wir der Software vertrauen könnten, darf die Sicherheit der Hardware, der Elektronik, nicht aus den Augen verloren werden. Leider ist das Vertrauen in die Hardware erschüttert, seit bekannt wurde, dass jahrelang gravierende Sicherheitslücken in fast allen modernen Prozessoren klafften. «Meltdown» und «Spectre» wurden diese beiden Angriffsvektoren getauft. Diese Sicherheitslücken erlaubten oder erlauben noch immer das unberechtigte Auslesen von hochsensiblen Daten wie Passwörtern auf allen Betriebssystemen. Die einzig wirkliche Abhilfe für dieses Problem ist eine neue Prozessorgeneration, welche auf einer anderen Architektur beruht. Es wird wahrscheinlich noch ein Jahrzehnt vergehen, bis die letzten der anfälligen

Prozessoren nicht mehr zum Einsatz kommen. Wer kann aber schon garantieren, dass neuere Prozessoren keine neuen Schwachstellen enthalten? Diese Garantie ist angesichts der zunehmenden Komplexität von Technologie nicht vorhanden.

> *Sollten bei einer umstrittenen Abstimmung auch nur zwei Prozent dieser Geräte manipulierte Stimmen abgeben, könnte das Abstimmungsresultat entscheidend verfälscht werden.*

Auch die Endgeräte der Stimmbürgerinnen sind leider alles andere als sicher. Etliche Computer und Smartphones sind infiziert mit Trojanern und Viren. Deren Nutzerinnen haben die Kontrolle über ihre «Zombie-Geräte» verloren, ohne es überhaupt zu merken. Sollten bei einer umstrittenen Abstimmung auch nur zwei Prozent dieser Geräte manipulierte Stimmen abgeben, könnte das Abstimmungsresultat entscheidend verfälscht werden. Es ist gewiss hilfreich, das Sicherheitsbewusstsein der Geräte-Nutzerinnen fortlaufend zu schärfen, um die Stabilität der gesamten IT-Infrastruktur zu stärken. Geben wir es zu: die technologischen Voraussetzungen für E-Voting sind insgesamt nicht makellos oder sogar bedenklich. Berücksichtigen wir aber, dass die gesamte Wirtschaft, unsere Banken, unser Sozial- und Privatleben trotz all dieser Anfälligkeiten noch nicht zusammengebrochen sind, sollten wir dem Experiment «E-Voting» mit der gebotenen Vorsicht eine Chance geben. Sollte es funktionieren, kann die Demokratie damit vereinfacht und sogar neu belebt werden. Andernfalls muss bei den geringsten Anzeichen von Manipulation sofort der Stecker gezogen werden.