ÖFFENTLICHKEIT VS. VERIFIZIERBARKEIT

- INWIEWEIT ERFÜLLT MATHEMATISCHE VERIFIZIERBARKEIT DEN GRUNDSATZ DER ÖFFENTLICHKEIT DER WAHL - [1]

Maria Henning[1], Denise Demirel[2], Melanie Volkamer[3]

[1]Wissenschaftliche Mitarbeiterin, Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Wilhelmshöher Allee 64-66, 34109 Kassel, DE, maria.henning@uni-kassel.de; http://provet.uni-kassel.de
[2]Wissenschaftliche Mitarbeiterin, TU Darmstadt, FB Informatik, Kryptographie und Computeralgebra, Hochschulstraße 10, 64289 Darmstadt, DE, denise.demirel@cased.de; www.cdc.informatik.tu-darmstadt.de
[3]Head of Group, SecUSo-IT Security, Usability and Society, Center for Advanced Security Research Darmstadt, TU Darmstadt, Hochschulstraße 10, 64289 Darmstadt, DE, melanie.volkamer@cased.de; www.secuso.cased.de

Schlagworte: ***Verifizierbarkeit, Öffentlichkeit, Kontrollierbarkeit, Wahrscheinlichkeit.***

Abstract: *Die Verfasser gehen der Frage nach, ob mathematische Verifizierbarkeit dem Kontrollerfordernis im Rahmen der Öffentlichkeit der Wahl entspricht. In diesem Zusammenhang werden nicht nur die Vorteile der Verifizierbarkeit, sondern auch die Schwachstellen derselben herausgearbeitet und diskutiert.*

1. Einleitung

Mit Urteil vom 3.3.2009 hat das Bundesverfassungsgericht die Verwendung von Wahlgeräten bei der Wahl zum 16. Deutschen Bundestag für unzulässig erklärt. Dabei hat der Zweite Senat seine Entscheidung nicht auf Sicherheitsmängel, sondern auf einen Verstoß gegen den in Art. 38 in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG verankerten Grundsatz der Öffentlichkeit der Wahl gestützt. Dieser gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen. Beim Einsatz elektronischer Wahlgeräte müssen daher die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne Sachkenntnis überprüft werden können.[2]

Das Wahlcomputerurteil hat der Diskussion um elektronische Wahlen neue Impulse verliehen. Im Zentrum rechts- und informationstechnischer Auseinandersetzung steht nunmehr die Möglichkeit einer sachkenntnisunabhängigen Kontrolle. Während die Rechtswissenschaft allerorts nach Öffentlichkeit ruft, antwortet die Informatik mit dem Begriff der Verifizierbarkeit. Diese ermöglicht dem Wähler, selbstständig zu überprüfen, ob seine Stimme richtig erkannt, gespeichert und gezählt wurde. Die Verfasser gehen der Frage nach, inwieweit mathematische Verifizierbarkeit dem Grundsatz der Öffentlichkeit der Wahl entspricht. Dabei konzentrieren sie sich in diesem Beitrag[3] auf den Aspekt der Kontrolle und lassen die Frage, ob die korrekte Erfassung der abgegebenen

---

[1] Diese Arbeit wurde im Tagungsband des 15. Internationalen Rechtsinformatik Symposions (IRIS 2012): Transformation juristischer Sprachen. Editoren: Erich Schweigehofer, Franz Kummer and Walter Hötzendorfer ©2012 Österreichische Computer Gesellschaft

[2] BVerfGE 123, 39 (71).

[3] Dieser Beitrag ist im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Projekts „VerkonWa“ – Verfassungskonforme Umsetzung von elektronischen Wahlen – entstanden.

Stimmen auch ohne Sachkenntnis nachvollziehbar ist, für einen gesonderten Aufsatz offen. Diese Vorgehensweise ist sinnvoll, da die Suche nach einem transparenten, das heißt jedermann zugänglichen Kontrollverfahren bereits begrifflich voraussetzt, dass eine Kontrolle möglich ist.

Im folgenden Beitrag erläutern die Verfasser zunächst den Grundsatz der Öffentlichkeit der Wahl (Abschnitt 2) und die Möglichkeit mathematischer Verifizierbarkeit (Abschnitt 3). Dabei stellen sie die unterschiedlichen Formen der Verifizierbarkeit und die sich daraus ergebenden Kontrollmöglichkeiten dar. Nach einer Zwischenbilanz, ob mathematische Verifizierbarkeit generell ein taugliches Instrument zur Realisierung der vom Bundesverfassungsgericht geforderten Kontrollmöglichkeit sein könnte (Abschnitt 4), arbeiten die Verfasser Schwachstellen mathematischer Verifizierbarkeit heraus und diskutieren diese aus rechtswissenschaftlicher Sicht (Abschnitt 5). Um die dargestellten Probleme anschaulich zu gestalten, betrachten sie den Ausgang der Landtagswahl 2011 in Baden-Württemberg für den Wahlkreis Tübingen, da hier nur 21 Stimmen zwischen den stärksten Kandidaten lagen. Abschließend werden die Ergebnisse zusammengefasst und offene Forschungsfragen daraus abgeleitet (Abschnitt 6).

2. Der Grundsatz der Öffentlichkeit der Wahl

Nach den Ausführungen des Bundesverfassungsgerichts entsprachen die bei der Wahl zum 16. Deutschen Bundestag verwendeten Geräte „nicht den Anforderungen, die die Verfassung an die Verwendung elektronischer Wahlgeräte stellt“.[4] Der Einsatz von Wahlgeräten, die die Stimmen der Wähler elektronisch erfassen und das Wahlergebnis elektronisch ermitteln, sei nur dann mit dem Grundgesetz vereinbar, wenn die wesentlichen Schritte der Wahl vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.[5] Obgleich der Zweite Senat betont, dass der Gesetzgeber Ausnahmen vom Grundsatz der Öffentlichkeit der Wahl zulassen kann, um anderen verfassungsrechtlichen Belangen Geltung zu verschaffen, vermochte er solch gegenläufige Verfassungsprinzipien beim Einsatz der betroffenen Wahlgeräte nicht zu erkennen. Insbesondere sei das Bestreben, unbewusst falsche Stimmzettelkennzeichnungen, unwillentlich ungültige Stimmabgaben, unbeabsichtigte Zählfehler oder unzutreffende Deutungen des Wählerwillens bei der Stimmenauszählung auszuschließen, nicht geeignet, den Verzicht auf jegliche Nachvollziehbarkeit des Wahlakts zu rechtfertigen.[6]

Die grundsätzlich gebotene Öffentlichkeit umfasst das Wahlvorschlagsverfahren, die Wahlhandlung und die Ermittlung des Wahlergebnisses.[7] „Unter Wahlhandlung ist das gesamte unter Leitung und Aufsicht der Wahlorgane stehende Verfahren zu verstehen. Es beginnt mit dem Zusammentritt des Wahlvorstandes und der Eröffnung der Wahlhandlung und endet nach Ablauf der in Deutschland traditionell von 8.00 bis 18.00 Uhr dauernden Wahlzeit mit der Erklärung des Wahlvorstehers, dass die Abstimmung geschlossen ist.“[8] Die Wahlhandlung umfasst somit nicht nur den eigentlichen Wahlakt, sondern auch die Kontrolle der Wahlurne vor Beginn der Stimmabgabe (§ 53 Abs. 3 Satz 1 BWO). Da sich die Öffentlichkeit der Wahl hierauf bezieht, müsste ein Verifizierungsverfahren bereits hier ansetzen. Verfügt das Wahlgerät über einen Stimmenspeicher (elektronische Urne), so muss kontrollierbar sein, dass dieser vor Beginn der Stimmabgabe leer ist. Daneben müssen der Akt der Stimmabgabe als Mittelpunkt der Wahlhandlung und die Ermittlung und Feststellung des Wahlergebnisses verifizierbar sein. Allerdings gibt eine Passage der Urteilsbegründung Grund zu der Annahme, dass sich die geforderte Kontrolle nicht nur auf die Wahlhandlung, Ermittlung und Feststellung des Wahlergebnisses, sondern auch auf die Wahrung der geschriebenen

[4] BVerfGE 123, 39 (85).
[5] BVerfGE 123, 39 (71).
[6] BVerfGE 123, 39 (75).
[7] BVerfGE 123, 39 (68).
[8] *Schreiber, W.*, Bundeswahlgesetz, Kommentar, Carl Heymanns Verlag, Köln, § 31, Rn. 1 (2009).

Wahlgrundsätze erstrecken könnte.[9] So führt der Zweite Senat aus, dass „nur durch die Möglichkeit einer Kontrolle, ob die Wahl den verfassungsrechtlichen Wahlgrundsätzen entspricht", sichergestellt werden kann, dass die Delegation der Staatsgewalt an die Volksvertretung nicht an einem Defizit leidet.[10] Es ist jedoch zu beachten, dass die Wahlhandlung in ihrem Ablauf nicht verändert würde, wenn elektronische Wahlgeräte zum Einsatz kämen, die ausschließlich dazu dienen, eine elektronische Stimme zu erzeugen und zu speichern. So würde die Stimmabgabe ebenfalls in einer Wahlzelle (§ 50 BWO) stattfinden und der Wahlvorstand könnte weiterhin die Vorlage der Wahlbenachrichtigung (§ 56 Abs. 3 Satz 2 BWO) verlangen. Vor diesem Hintergrund wäre die Kontrolle der Wahlgrundsätze bei elektronischen Wahlen mit „einfachen Wahlgeräten" in weiten Teilen ebenso gewährleistet wie bei der traditionellen Papierwahl. Jedoch fordern die Grundsätze der freien, gleichen und geheimen Wahl eine über die visuelle Wahrnehmung hinausgehende Kontrolle, da der Grundsatz der gleichen Wahlen tangiert wäre, wenn Stimmen unbemerkt manipuliert würden und die Wahrung der geheimen Wahl in Frage stünde, wenn Dritte eine nachweisbare Verbindung zwischen Wähler und Wahlentscheidung herstellen könnten.[11] In diesem Fall würde auch eine Verletzung der Freiheit der Wahl in Betracht kommen, da ein Angreifer die Fähigkeit zur Offenlegung der Wahlentscheidung nutzen könnte, die Wähler vor Ausübung ihres aktiven Wahlrechts gezielt zu beeinflussen.

3. Mathematische Verifizierbarkeit

Dem Grundsatz der Öffentlichkeit der Wahl steht die Möglichkeit mathematischer Verifizierbarkeit gegenüber. In der „Security Community" zählt die Verifizierbarkeit seit vielen Jahren zu einer wichtigen Anforderung an eVoting-Systeme.[12] Die Idee dabei ist, dass man dem Wahlgerät bei der Erfassung, Speicherung und Auszählung der Stimmen nicht vertrauen muss, sondern einen mathematischen Beweis für deren Korrektheit erhält.

3.1. Definition mathematischer Verifizierbarkeit

In Abhängigkeit vom Wirkungskreis der Verifizierbarkeit wird zwischen „individueller" und „universeller" Verifizierbarkeit unterschieden. Ermöglicht ein Wahlsystem beide Arten der Verifizierbarkeit, so bezeichnet man es als „Ende-zu-Ende verifizierbar". In diesem Fall bietet die mathematische Verifizierbarkeit dem Wähler eine weitgehende Kontrolle der Wahl.

Individuelle Verifizierbarkeit ist gegeben, wenn der Wähler überprüfen kann, dass seine Kandidatenauswahl von dem elektronischen Wahlsystem richtig erkannt, seine Stimme hierin entsprechend korrekt gespeichert wurde und bis zur Auszählung unverändert gespeichert bleibt. In diesem Zusammenhang haben sich die Begriffe „cast as intended" und „recorded as cast" durchgesetzt. Dabei sollen folgende Manipulationen aufgedeckt werden: Der Wähler wählt Kandidat A, aber das System speichert Kandidat B (cast as intended) oder das System speichert Kandidat A, aber die Datenbank wird vor der Auszählung ausgetauscht, so dass in der „neuen" Datenbank keine Stimme für Kandidat A, sondern eine Stimme für Kandidat B enthalten ist (recorded as cast).

Universelle Verifizierbarkeit ist gewährleistet, wenn jeder (inkl. Wähler, Interessierte und Wahlbeobachter) überprüfen kann, dass alle bei Beginn der Auszählung im Wahlsystem gespeicherten

---

[9] So auch *Richter, P.*, Briefwahl für alle? Die Freigabe der Fernwahl und der Grundsatz der Öffentlichkeit, DÖV 2010, S. 609 (606-610).

[10] BVerfGE 123, 39 (69).

[11] So auch *Will, M.*, Wahlcomputer auf dem verfassungsrechtlichen Prüfstand, CR 2008, S. 541 (540-546).

[12] Ein guter Überblick über die Entwicklung des Begriffs der Verifizierbarkeit findet sich in: *Langer, L./Schmidt, A./Volkamer, M./Buchmann, J.*, Classifying Privacy and Verifiability Requirements for Electronic Voting, GI, Bonn, 2009, 1837-1846.

Stimmen korrekt ausgezählt werden. Dabei kann der Wähler zwar die Auszählung seiner eigenen Stimme nicht einsehen. Da er aber überprüfen kann, dass alle Stimmen richtig ausgezählt werden, weiß er indirekt auch, dass seine eigene Stimme richtig ausgezählt wird. Diese Form wird oft mit dem Begriff „tallied as recorded“ umschrieben. Sie ermöglicht es, folgende Manipulation aufzudecken: Die Auszählungssoftware/-komponente des elektronischen Wahlsystems bekommt viele Stimmen als Input, liefert aber unabhängig von diesem Input ein vordefiniertes Ergebnis. Dabei ist zu beachten, dass die universelle Verifizierbarkeit dem Wähler ermöglicht, die Korrektheit der Auszählung von zu Hause aus zu überprüfen, d.h. es ist nicht erforderlich dem Prozess der Ergebnisermittlung im Wahllokal beizuwohnen.

3.2. Umsetzung der Verifizierbarkeit

Beim Einsatz mathematischer Verifizierungsverfahren verschlüsselt das elektronische Wahlsystem die abgegebene Stimme.[13] Das dabei verwendete Verschlüsselungsverfahren ist probabilistisch, d.h. die Stimme wird unter Zuhilfenahme eines Zufallswertes verschlüsselt, wodurch gewährleistet ist, dass Stimmen für dieselben Kandidaten unterschiedliche Verschlüsselungstexte besitzen. Diese verschlüsselten Stimmen werden auf einem sogenannten Bulletin Board (einer Art Webseite) öffentlich zugänglich gemacht. An dieser Stelle ist es in der Regel noch erkennbar, welche verschlüsselte Stimme von welchem Wähler abgegeben wurde. Im Rahmen der Ergebnisberechnung werden die Stimmzettel sodann mittels eines sog. re-encryption Mix-Netzes[14] anonymisiert, entschlüsselt und anschließend ausgezählt.[15]

Um zu gewährleisten, dass die verschlüsselte Information der eigenen Kandidatenauswahl entspricht (*cast as intended*), erhält der Wähler einen Nachweis für die korrekte Verschlüsselung seiner Stimme. Dieser darf allerdings nicht als Beweis für die getroffene Kandidatenauswahl dienen. Um einen geeigneten Ausgleich zwischen Wahlgeheimnis und Verifizierbarkeit umzusetzen, verwenden viele Systeme folgenden Ansatz: Der Wähler kann vor der Stimmabgabe beliebig viele Teststimmen abgeben und verifizieren. Dabei wird mathematisch bewiesen, dass die Stimme korrekt verschlüsselt wurde. Dies kann der Wähler solange wiederholen, bis er davon überzeugt ist, dass sich das System ehrlich verhält. Da das System nicht in der Lage ist, zwischen Teststimmen und richtigen Stimmen zu unterscheiden, kann ein manipuliertes Wahlsystem einzelne Stimmen nur mit einer sehr geringen Wahrscheinlichkeit unbemerkt verändern. Für den Wähler bringt dies eine hohe Sicherheit mit sich, dass seine Stimme richtig verschlüsselt und gespeichert wurde. Allerdings ist zu beachten, dass er die endgültig abgegebene und damit am Ende gezählte Stimme nicht auf ihre Richtigkeit hin überprüfen kann.

Nach erfolgreicher Stimmabgabe erhält der Wähler einen Beleg, welcher die verschlüsselte Stimme repräsentiert, um den zweiten Schritt verifizierbar zu machen (*recorded as cast*). Durch diesen

---

[13] Dazu wird ein aus zwei Schlüsseln bestehendes Schlüsselpaar erzeugt, wobei ein Schlüssel öffentlich zugänglich ist und der andere geheim gehalten wird. Der öffentliche Schlüssel dient dazu, eine Stimme zu verschlüsseln und einen Schlüsseltext zu erzeugen, welcher die Stimmen in verschlüsselter Form darstellt. Der geheime Schlüssel ermöglicht es, diesen Text wieder zu entschlüsseln und die Stimme in Klartext zu extrahieren.

[14] Ein Mix-Netzwerk besteht aus mehreren Mix-Servern (auch Mix-Knoten genannt). Der erste Mix-Server erhält alle verschlüsselten Stimmen. Er kann diese zwar nicht entschlüsseln, da der Entschlüsselungsschlüssel geheim ist, allerdings kann er das Aussehen des Schlüsseltextes ändern ohne dabei die verschlüsselte Stimme zu verändern. Anschließend werden die Schlüsseltexte in einer anderen Reihenfolge ausgegeben. Nun weiß nur noch der Mix-Server welcher ausgegebene Schlüsseltext von welchem eingegebenen Schlüsseltext abstammt. Um zu verhindern, dass der Mix-Server diese Verbindung herstellen kann werden die Daten anschließend an einen anderen Mix-Server übergeben, welcher ebenfalls das Aussehen der Schlüsseltexte und ihre Reihenfolge ändert. Erst wenn alle Mix-Server des Mix-Netzwerks die Schlüsseltexte bearbeitet haben werden sie entschlüsselt und die Stimmen gezählt.

[15] Beim Einsatz von homomorphen Auszähltechniken werden die verschlüsselten Stimmzettel erst aufaddiert, dann die verschlüsselte Summe entschlüsselt. Da hierbei keine einzelnen Stimmen entschlüsselt werden, entfällt der Schritt der Anonymisierung. Da dieser Ansatz aber verschiedene Nachteile hat, wird er in diesem Beitrag nicht weiter betrachtet.

Beleg ist jeder Wähler mit einer Stimme verknüpft, d.h. darüber kann auf dem Bulletin Board jeder verschlüsselten Stimme ein Wähler zugeordnet werden. Der Wähler kann mit diesem Beleg also zu jedem Zeitpunkt inklusive kurz vor der Auszählung überprüfen, dass seine verschlüsselte Stimme korrekt auf dem Bulletin Board gespeichert und seit der Stimmabgabe nicht verändert wurde. Dies kann der Wähler von zu Hause oder über das Internet durchführen oder seinen Beleg einer Person seines Vertrauens geben. Diese Person kann den Schritt überprüfen, ohne dass dadurch das Wahlgeheimnis gefährdet wird, da die Kandidatenauswahl hierbei nicht offen gelegt wird. Die anschließende Anonymisierung, Entschlüsselung und Zählung werden so durchgeführt, dass die Korrektheit des Prozesses mathematisch bewiesen werden kann (*universelle Verifizierbarkeit*). Dazu reicht ein reines re-encryption Mix-Netz nicht aus. Hierbei könnte jeder Mix-Knoten unbemerkt einzelne verschlüsselte Stimmen austauschen. Gleiches gilt für den Entschlüsselungsalgorithmus. Daher werden diese Mix-Netze so erweitert, dass jeder Mix-Knoten einen Beweis liefert, dass das Wahlergebnis für die Input Stimmen gleich dem für die Output Stimmen ist. Hierzu werden so genannte Zero Knowledge Proofs[16] eingesetzt. Außerdem liefert der Entschlüsselungsalgorithmus einen Beweis für die korrekte Entschlüsselung. Da die Stimmen anschließend in entschlüsselter Form vorliegen, kann jeder Interessierte die Auszählung dieser Stimmen selbst durchführen und mit dem veröffentlichten Ergebnis vergleichen.

4. Öffentlichkeit vs. Verifizierbarkeit

Mathematische Verifizierbarkeit befähigt den Wähler, die eigene Stimmabgabe und die Ermittlung des Gesamtergebnisses im dargestellten Umfang zu kontrollieren. Ob sie daher als taugliches Instrument zur Realisierung der vom Bundesverfassungsgericht geforderten Kontrollmöglichkeit angesehen werden kann, soll im Folgenden diskutiert werden. Dabei ist zu beachten, dass das Gericht konkrete Vorschläge zur Umsetzung der seinerseits geforderten Richtigkeitskontrolle unterbreitet hat. So differenziert der Zweite Senat zunächst zwischen Geräten, die zusätzlich zur elektronischen Erfassung der Stimme ein für den jeweiligen Wähler sichtbares Papierprotokoll der abgegebenen Stimme ausdrucken, und Systemen, bei denen die Wähler einen Stimmzettel kennzeichnen und die getroffene Wahlentscheidung gleichzeitig oder nachträglich elektronisch erfasst wird.[17] Beiden Verfahren ist gemein, dass die Stimme des Wählers neben der elektronischen Speicherung anderweitig erfasst wird. Dies entspricht auch den Anforderungen des Bundesverfassungsgerichts, wonach „die Stimmen nach der Stimmabgabe nicht ausschließlich auf einem elektronischen Speicher abgelegt werden“ dürfen.[18] Ob daraus aber geschlussfolgert werden kann, dass eine zuverlässige Richtigkeitskontrolle *nur* anhand eines Ausdrucks der Klartextstimme umsetzbar ist, erscheint fraglich.

Mathematische Verifizierungsverfahren ermöglichen die Nachvollziehbarkeit der Stimmabgabe und Ergebnisermittlung auf der Basis eines verschlüsselten Belegs. Obgleich das Bundesverfassungsgericht diese Möglichkeit der Kontrolle nicht aufgeführt hat, sollte sie als zulässig erachtet werden, da das Gericht die benannten Verfahren nur als „denkbar“[19] und damit nur als „obiter dictum“[20] (lat.: nebenbei Gesagtes) dargestellt und die Frage nach anderen technischen Möglichkeiten der verfassungskonformen Umsetzung von elektronischen Wahlen ausdrücklich offen gelassen hat.[21] Darüber hinaus gewinnt der Wähler im Vergleich zur Beobachtung der Stimmzettelauswertung bei der Papierwahl an Kontrollkompetenzen hinzu. So verschafft die individuelle Verifizierbarkeit dem

---

[16] Zero Knowledge Proofs sind mathematische Beweise, die es ermöglichen, die Kenntnis eines Geheimnisses zu beweisen, ohne dass das Geheimnis offen gelegt werden muss.
[17] BVerfGE 123, 39 (73).
[18] BVerfGE 123, 39 (73).
[19] BVerfGE 123, 39 (73).
[20] *Buchmann, J./Roßnagel A.*, Das Bundesverfassungsgericht und Telemedienwahlen, K&R 2009, S. 545 (543-548).
[21] BVerfGE 123, 39 (73 f.).

Wähler einen Vorteil, da er die korrekte Erfassung der eigenen Stimme auch nach der Stimmabgabe noch einsehen und gezielt kontrollieren kann. Die öffentliche Verifizierbarkeit ermöglicht ihm schließlich die zeitpunktunabhängige und beliebig oft wiederholbare Kontrolle *aller in allen Wahllokalen* abgegebenen Stimmen. Damit gehen mathematische Verifizierungsverfahren weit über die Möglichkeiten der Papierwahl hinaus. Sie sollten somit generell als taugliches Instrument zur Realisierung der geforderten Kontrollmöglichkeit angesehen werden.

5. Verfassungskonforme Umsetzung mathematischer Verifizierbarkeit

Nachfolgend werden Grenzen mathematischer Verifizierbarkeit erklärt und analysiert.

5.1. Wahrscheinlichkeit einer Manipulation trotz mathematischer Verifizierbarkeit

Die Wahrscheinlichkeit, dass eine Manipulation im Rahmen der Verschlüsselung der Stimme entdeckt wird (cast as intended), hängt von der Anzahl durchgeführter Testwahlen und der Anzahl an Stimmen ab, die manipuliert werden müssten, um das Wahlergebnis zu verändern. Verifiziert jeder Wähler vor der endgültigen Stimmabgabe nur eine Teststimme und wird parallel dazu eine manipulierte Stimme in das System eingeschleust, liegt die Wahrscheinlichkeit bei 50 %, dass die Manipulation nicht entdeckt wird. Dies liegt darin begründet, dass jeder Wähler zwei Stimmzettel erhält, wobei einem Wähler ein korrekt erzeugter und ein manipulierter Stimmzettel vorliegen werden. Die Wahrscheinlichkeit, dass er den korrekt erzeugten Stimmzettel verifiziert, liegt bei 50 % (1:2). Werden zwei manipulierte Stimmzettel eingeschleust, muss es zweimal gelingen, dass sich der jeweilige Wähler dazu entscheidet den korrekt erzeugten Stimmzettel zu verifizieren, wodurch sich sie Wahrscheinlichkeit einer unentdeckten Manipulation entsprechend reduziert (multipliziert; also 25 %). Es ist jedoch zu beachten, dass es jedem Wähler frei gestellt ist, ob er überhaupt verifiziert und wie oft er dies tut. Klar ist jedoch, dass der Ablauf der Wahl behindert werden würde, wenn jeder Wähler 100 Teststimmen verifizieren würde.

Zur Veranschaulichung des verbleibenden Restrisikos wird das knappe Wahlergebnis für den Wahlkreis Tübingen bei der Landtagswahl am 17.3.2011 in Baden-Württemberg betrachtet.[22] Insgesamt wurden bei dieser Wahl 95.804 Stimmen abgegeben, wobei 30.479 Stimmen auf die CDU und 30.500 Stimmen auf die Grünen entfielen. Die Differenz betrug demnach nur 21 Stimmen. Um den Ausgang der Landtagswahl im Wahlkreis Tübingen zu ändern, hätte das Wahlsystem 11 Stimmzettel unbemerkt manipulieren müssen. Die Wahrscheinlichkeit dafür, dass dies gelungen wäre, obwohl jeder Wähler eine der beiden Stimmen auf ihre Korrektheit hin hätte überprüfen können, liegt bei 0,04883 %.[23] Zu beachten ist jedoch, dass die Anzahl der Wahlhandlungen, die zu Testzwecken durchgeführt werden müssen, um die Wahrscheinlichkeit einer Manipulation niedrig zu halten, vor Durchführung der Wahl festgelegt werden muss. Dazu besteht die Möglichkeit, eine maximale Wahrscheinlichkeit für eine erfolgreiche Manipulation zu berechnen, indem davon ausgegangen wird, dass bereits eine falsche Stimme das Wahlergebnis signifikant ändern kann. In Abhängigkeit dieses Ergebnisses besteht die Möglichkeit eine minimale Anzahl von Stimmzetteln zu definieren, die pro Wähler verifiziert oder im Rahmen einer öffentlichen Verifizierung überprüft werden muss. Als Alternative zur Wahrscheinlichkeitsberechnung könnte man die jeweilige Verschlüsselung der Stimme direkt kontrollieren. Dies würde allerdings das Wahlgeheimnis gefährden.

Eine Manipulation, infolge derer die abgegebene Stimme falsch im Wahlsystem gespeichert wurde (recorded as cast), kann der Wähler durch Abgleichen seines verschlüsselten Belegs mit dem

---

[22] Statistik über die Wahlen in Baden-Württemberg für den Wahlkreis Tübingen. http://www.statistik.baden-wuerttemberg.de/Wahlen/Landtagswahl_2011/Wahlkr.asp?62, aufgerufen: 31.10.2011 (2011).

[23] Die Wahrscheinlichkeit einer erfolgreichen Manipulation wird potenziert: (1/2)^11 = 0,00048828125 ~ 0,04883 %.

Bulletin Board eindeutig aufdecken. Bei der Verwendung eines re-encryption Mix-Netzes existieren bereits Verifizierungsverfahren, welche anhand eines Zero Knowledge Arguments auch die korrekte Auszählung (tallied as recorded) zeigen können.[24] Einige elektronische Wahlsysteme hingegen verwenden nach wie vor Methoden, welche keine 100%tige Garantie für eine korrekte Arbeitsweise bieten (z.B. verwendet Scantegrity III Randomized Partial Checking[25]). Die Wahrscheinlichkeit modifizierte Stimmen zu erkennen ist bei diesen Verfahren zwar relativ hoch, ob sie jedoch ausreicht muss im Einzelfall entschieden werden.

5.2. Beweisschwierigkeiten im Rahmen mathematischer Verifizierbarkeit

Diskutiert man den Einsatz von Verifizierungsverfahren, so geht man grundsätzlich von dem Idealfall aus, dass keine Unstimmigkeiten auftreten, der Wähler also die korrekte Abgabe und Speicherung seiner Stimme verifizieren kann (individuelle Verifizierbarkeit). Treten jedoch Beschwerden von Seiten der Wähler auf, so stellt sich die Frage, wie mit diesen umzugehen ist und welche Kompetenzen dem Wahlvorstand in dieser Situation zustehen. Nach § 40 Satz 1 BWahlG entscheidet der Wahlvorstand über alle bei der Wahlhandlung und der Ermittlung des Wahlergebnisses sich ergebenden Anstände.[26] Gemäß § 7 Satz 1 BWO sorgt er für die ordnungsgemäße Durchführung der Wahl. Unabhängig von der Frage, welche Kompetenzen hieraus folgen, ist zu beachten, dass viele Wahlsysteme nicht unterscheiden können, ob der Wähler zurecht behauptet, dass die ihm zugänglichen Informationen nicht seiner Stimme entsprechen oder ob der Wähler diese Behauptung zu Unrecht vorbringt, da sich das System ehrlich verhalten, der Wähler einen Fehler gemacht hat oder einen „denial-of-service-Angriff“[27] begehen will.

Eine Möglichkeit, dieser Situation zu begegnen, wäre es, die Wahl ab einer bestimmten Anzahl an Beschwerden abzubrechen und an einem anderen Zeitpunkt zu wiederholen. Diese Vorgehensweise steht jedoch der Funktionsfähigkeit der Wahl selbst entgegen. „Der reibungslose Ablauf einer Parlamentswahl erfordert, dass die Rechtskontrolle der zahlreichen Einzelentscheidungen der Wahlorgane während des Wahlverfahrens begrenzt und im Übrigen dem nach der Wahl stattfindenden Wahlprüfungsverfahren vorbehalten bleibt.“[28] Dies geht auch aus Art. 41 Abs. 1 Satz 1 GG hervor, wonach die Wahlprüfung Sache des Bundestages ist. Nach § 1 Abs. 1 WahlPrüfG besteht die Wahlprüfung in der Entscheidung „über die Gültigkeit der Wahlen zum Bundestag“. Diese Kompetenz umfasst die Befugnis zur rechtlichen Kontrolle des gesamten Wahlgeschäfts auf das Vorliegen von Wahlfehlern, wobei das Wahlgeschäft die Wahlvorbereitung, die Wahldurchführung, die Ergebnisermittlung und -feststellung umfasst.[29] Ein Wahlfehler liegt vor, wenn ein Verstoß gegen zwingende Wahlrechtsvorschriften bei der Vorbereitung, Durchführung oder Ergebnisermittlung der Bundestagswahl gegeben ist.[30] Ist ein Wähler der Ansicht, eine andere Stimmabgabe vorgenommen zu haben, als aus dem Beleg ersichtlich, so könnte ein Verstoß gegen den Grundsatz der Gleichheit der Wahl vorliegen. Da dieser als Wahlfehler der Wahlprüfung

---

[24] Zum Beispiel das Verifizierungsverfahren von Bayer und Groth: *Bayer S./ Groth J.*, Efficient Zero-Knowledge Argument for Correctness of a Shuffle, Manuscript, 2011.

[25] *Sherman A.T./ Fink R.A./ Carback R./ Chaum D.*, Scantegrity III: automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability, USENIX Association, Berkeley, CA, USA, 2011.

[26] Hier kommen alle Vorkommnisse von einiger Bedeutung während der Wahlhandlung und der Ergebnisermittlung in Betracht (*Schreiber, W.*, Bundeswahlgesetz, Kommentar, Carl Heymanns Verlag, Köln, § 40, Rn. 3 (2009).

[27] Hierunter versteht man einen Angriff, der darauf gerichtet ist, die Funktionsweise eines informationstechnischen Systems zum Erliegen zu bringen. Dabei könnte eine Gruppe von Wählern oder Wahlbeobachtern fälschlicherweise behaupten, dass die ihnen nach der Stimmabgabe ausgehändigten Belege nicht der jeweiligen Kandidatenauswahl entsprechen, um den Ablauf der Wahl zu gefährden.

[28] *Schreiber, W.*, Bundeswahlgesetz, Kommentar, Carl Heymanns Verlag, Köln, § 49, Rn. 10 (2009).

[29] *Schreiber, W.*, Das Bundesverfassungsgericht als Wahlprüfungsgericht, DVBl. 2010, S. 609 (609-618).

[30] *Morlok , M.*, in: Dreier, Grundgesetz, Kommentar, Mohr Siebeck, Tübingen, Art. 41, Rn. 17 (2006).

unterfällt und somit Sache des Bundestages ist, vermag der Wahlvorstand hierüber nicht zu entscheiden und kann dies zunächst nur protokollieren.

Um eventuellen Beschwerden dennoch gerecht zu werden, könnte betroffenen Wählern die Möglichkeit offeriert werden, bis zum Ablauf der Wahlzeit eine neue Stimmabgabe – unter Streichung der vorherigen – vorzunehmen.[31] Über den Beleg wäre die Stimme im System auffindbar und könnte somit gelöscht werden. Die Frage, ob und unter welchen Voraussetzungen der Wähler eine erneute Stimmabgabe vornehmen darf, betrifft die technische Seite des Wahlvorgangs und somit das Wahlsystem. Dieses auszugestalten, ist gemäß Art. 38 Abs. 3 GG Aufgabe des Bundesgesetzgebers. Hierbei hat er sich jedoch an die Vorgaben des Art. 38 Abs. 1 Satz 1 GG zu halten. Der erneuten Stimmabgabe in Form einer Stimmkorrektur könnte der Grundsatz der Gleichheit der Wahl entgegenstehen. Dieser verlangt, dass jeder nach den allgemeinen Vorschriften Wahlberechtigte seine Stimme wie jeder andere abgeben darf und dass die gültig abgegebene Stimme genauso bewertet wird wie alle anderen Stimmen.[32] Wird die Stimme, von welcher der Wähler glaubt, dass sie falsch ins System gegangen sei, wieder gelöscht, so hätte er bei erneuter Stimmabgabe nicht mehr Stimmen als jeder andere Wähler. Die Zählwertgleichheit wäre hiernach gewahrt. Kann ein System aber nicht zwischen begründeten und unbegründeten Beschwerden differenzieren, so müsste die Möglichkeit einer Stimmkorrektur jedem Wähler offen stehen. Dies könnte jedoch den ordnungsgemäßen Ablauf der Wahl gefährden. Ferner ist die Möglichkeit einer erneuten Stimmabgabe dem geltenden Wahlrecht fremd. Zwar darf der Wahlvorstand dem Wähler nach § 56 Abs. 8 BWO einen neuen Stimmzettel aushändigen, wenn der Wähler seinen Stimmzettel verschrieben oder versehentlich unbrauchbar gemacht hat oder eine Zurückweisung des Wählers erfolgt, weil dieser seinen Stimmzettel außerhalb der Wahlzelle gekennzeichnet oder gelfaltet hat. § 56 Abs. 8 BWO geht jedoch davon aus, dass der „erste“ Stimmzettel noch nicht in die Urne eingeworfen wurde, das aktive Wahlrecht somit noch besteht.

Der Umgang mit Beschwerden bei der Stimmenspeicherung (recorded as cast) gestaltet sich einfacher. Der Wähler verfügt in der Regel über einen signierten Beleg, dessen korrekte Erstellung er bei der Stimmabgabe verifiziert hat. Hierdurch ist seine Beschwerde entweder begründet (stimmt nicht mit dem Bulletin Board überein) oder unbegründet (stimmt mit dem Bulletin Board überein). Dies gilt ebenfalls für die Verifizierung der Auszählung. Anhand der veröffentlichten Daten kann die korrekte Arbeitsweise mathematisch verifiziert (der mathematische Beweis kann nur richtig oder falsch sein) und die Berechnung von unabhängigen Instanzen beliebig oft wiederholt werden.

6. Schlussfolgerungen

Mathematische Verifizierbarkeit bietet sowohl dem Wähler als auch der Öffentlichkeit eine über das Maß der Papierwahl hinausgehende Kontrollmöglichkeit, da sie die Kontrolle aller in allen Wahllokalen abgegebenen Stimmen ermöglicht. Unabhängig von der Transparenz (Kontrolle ohne besondere Sachkenntnis), welche im Rahmen dieses Beitrags nicht thematisiert wurde, weist sie jedoch Schwachstellen auf, die aus juristischer Sicht diskussionswürdig sind. So ist insbesondere der Umstand, dass eine lückenlose Nachvollziehbarkeit der eigenen Stimmabgabe aufgrund des Wahlgeheimnisses nicht möglich ist, von Bedeutung. Daher können mathematische Verifizierungsverfahren Manipulationen nur mit einer sehr hohen Wahrscheinlichkeit aufdecken, nicht aber zu 100 %. Eine künftige Forschungsfrage wird schließlich sein, wie Beschwerden nach Durchführung der Wahlhandlung zu handhaben sind. Daneben muss untersucht werden, wie mathematische Verifizierbarkeit dargestellt werden kann, um sie für jedermann verständlich zu gestalten. Die aufgezeigten Vorteile, namentlich die Befähigung zu einer weitgehenden Kontrolle

---

[31] Vgl. *Will, M.*, Internetwahlen, Richard Boorberg Verlag, Stuttgart, S. 123 (2002). Will thematisiert die Möglichkeit der erneuten Stimmabgabe im Rahmen von Internetwahlen zur bestmöglichen Sicherung der freien Wahl.

[32] BVerfGE 16, 130 (138).

der eigenen Stimme und der gesamten Ergebnisermittlung, sind jedoch derart zu gewichten, dass eine weitere Analyse mathematischer Verifizierungsverfahren als lohnenswert anzusehen ist.