

Elektronische Wahlen durch Stimmzettelbelege?

Untersuchung möglicher Umsetzungen des Öffentlichkeitsgrundsatzes

Telekommunikations- und Medienrecht

Der Beitrag analysiert verschiedene Ansätze, die den Grundsatz der Öffentlichkeit der Wahl im Rahmen elektronischer Wahlen mithilfe sog. Stimmzettelbelege zu erfüllen suchen. Dabei wird zunächst geprüft, inwieweit die drei Stufen technischer Verifizierbarkeit – cast as intended, recorded as cast und tallied as recorded – geeignet sind, die gebotene Überprüfbarkeit der Wahlhandlung und Ergebnisermittlung zu realisieren. Anschließend werden Konzepte, die Belege der Klartextstim-

me generieren, und Konzepte, die Belege der kodierten Stimme erzeugen, dargestellt und vor dem Hintergrund des Wahlcomputerurteils vom 3.3.2009 juristisch bewertet. In diesem Kontext wird auch der Frage nachgegangen, ob kryptografiebasierte Wahlgeräte überhaupt geeignet sind, den Grundsatz der Öffentlichkeit der Wahl umzusetzen und wie viel technisches Verständnis dem Einzelnen hier zuzumuten oder gar abzuverlangen ist.

I. Einleitung

Zahlreiche Institutionen wie die *Deutsche Forschungsgemeinschaft* und die *Gesellschaft für Informatik* wählen ihre Gremien elektronisch. Anlass hierfür mag zum einen die Erwartung einer schnellen und fehlerfreien Ergebnisermittlung, zum anderen aber auch das Bestreben einer zeitgemäßen Stimmabgabe sein. Wir leben in einer Welt, die ohne Technik kaum noch denkbar ist. E-Mails werden nicht nur noch im Büro, sondern ebenso im Zug oder in der Straßenbahn beantwortet. Hotelbuchungen werden zwischen zwei Terminen von einem beliebigen Ort via Smartphone vorgenommen. Und selbst bei Steuererklärungen holt uns die Technik ein. Daher ist es nur folgerichtig, die Chancen moderner Informationstechnologien auch im Kontext von Wahlen zu nutzen.

Allerdings hat das *BVerfG* die Anforderungen an elektronische Parlamentswahlen mit U. v. 3.3.2009 deutlich erhöht. Hiernach ist der Einsatz rechnergesteuerter Wahlgeräte nicht nur an den fünf geschriebenen Wahlrechtsgrundsätzen, sondern auch am Grundsatz der Öffentlichkeit der Wahl nach Art. 38 i.V.m. Art. 20 Abs. 1 und Abs. 2 GG zu messen. Dieser „gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen.“¹ Vor diesem Hintergrund müssen insbesondere die „Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können.“² Diese Überprüfbarkeit wird bereits seit einigen Jahren unter dem Stichwort Verifizierbarkeit in der Wissenschaft diskutiert. Vielen Konzepten ist gemein, dass sie die Verifizierbarkeit der Wahlhandlung mithilfe sog. Stimmzettelbelege realisieren. Hier sind Belege der Klartextstimme ebenso denkbar wie Belege der kodierten Stimme. Nachfolgend soll untersucht werden, inwieweit diese Stimmzettelbelege den Grundsatz der Öffentlichkeit der Wahl gewährleisten. Der Fokus liegt dabei auf elektronischen Wahlgeräten, die im Wahlraum eingesetzt werden.

II. Öffentlichkeit und Verifizierbarkeit

Der Grundsatz der Öffentlichkeit der Wahl setzt zunächst die Existenz einer Überprüfungsmöglichkeit voraus, die die Wahlhandlung und die Ergebnisermittlung umfasst. Unter dem Begriff der Wahlhandlung ist das gesamte unter Leitung und Aufsicht der Wahlorgane stehende Verfahren am Wahltag zu verstehen. Es beginnt mit dem Zusammenritt des Wahlvorstands

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.³ Jedoch ist davon auszugehen, dass das *BVerfG*, wenn es von der Überprüfbarkeit der Wahlhandlung spricht, insbesondere die eigene Wahlhandlung und damit die Stimmabgabe des Wählers meint. So heißt es im Wahlcomputerurteil eben auch, dass ein „Wahlverfahren, in dem der Wähler nicht zuverlässig nachvollziehen kann, ob seine Stimme unverfälscht erfasst und in die Ermittlung des Wahlergebnisses einbezogen wird und wie die insgesamt abgegebenen Stimmen zugeordnet und gezählt werden“ nicht den verfassungsrechtlichen Anforderungen genügt.⁴ Insofern muss sich eine Überprüfungsmöglichkeit i.R.d. Wahlhandlung vor allem auf die korrekte Erfassung und Einbeziehung der eigenen Stimme beziehen.

Die reine Existenz einer Überprüfungsmöglichkeit ist aber nicht ausreichend. Erforderlich ist auch, dass die Überprüfungsmöglichkeit benutzbar gestaltet ist. Das bedeutet, dass jeder Wähler in der Lage sein muss, die Überprüfung fehlerfrei auszuführen. Schließlich müssen die Informationen, die der Wähler erhält, auch nachvollziehbar sein. Es muss dem Wähler also klar sein, welchen wesentlichen Schritt der Wahl – Wahlhandlung oder Ergebnisermittlung – er gerade überprüft und ob dieser Schritt korrekt verlaufen ist. Die beiden Eigenschaften „Benutzbarkeit und Nachvollziehbarkeit“ setzen demnach die Anforderung des *BVerfG* nach einer sachkenntnisunabhängigen Überprüfbarkeit um. Darüber hinaus fordert das *Gericht*, dass die Stimmen nach der Stimmabgabe nicht ausschließlich auf einem elektronischen Speicher abgelegt werden.⁵

Die Überprüfungsmöglichkeit entspricht dem in der technischen Fachliteratur verwendeten Begriff der Verifizierbarkeit. Diese wird in drei Schritte unterteilt, je nachdem welcher Schritt der Wahlhandlung – Stimmabgabe (cast as intended) und Stimm-speicherung (recorded as cast) – oder der Ergebnisermittlung (tallied as recorded) überprüft werden kann.

¹ *BVerfG* MMR 2009, 316, 317.

² *BVerfG* MMR 2009, 316, 318, 320.

³ *Hahlen*, in: Schreiber, *BWahlG*, 9. Aufl. 2013, § 31 Rdnr. 1.

⁴ *BVerfG* MMR 2009, 316, 317.

⁵ *BVerfG* MMR 2009, 316, 318.

1. Cast as intended

Die Stimmabgabe ist cast as intended verifizierbar, wenn der Wähler überprüfen kann, dass seine eigene Stimme so erfasst wurde, wie er es beabsichtigt hat. Hat der Wähler z.B. Kandidat A angeklickt, so kann er überprüfen, ob das Wahlgerät auch tatsächlich Kandidat A aufgenommen und nicht eine andere Stimme erfasst hat. Dieser Schritt ist bei der traditionellen Papierwahl per se gegeben. Der Wähler gibt seine Stimme auf dem Papierstimmzettel mit einem Stift ab, kontrolliert sie noch einmal anhand des Augenscheins und wirft den Zettel anschließend in die Wahlurne ein. Insofern kann er davon ausgehen, dass seine Stimme korrekt erfasst in der Urne liegt.

2. Recorded as cast

Die Stimmabgabe ist recorded as cast verifizierbar, wenn der Wähler überprüfen kann, dass seine korrekt erfasste Stimme unverändert in der (elektronischen) Urne gespeichert wird und bleibt. In Anlehnung an das vorherige Beispiel kann der Wähler also kontrollieren, ob seine Stimme für Kandidat A weiterhin in der Urne liegt und nicht nachträglich entfernt oder durch eine Stimme für einen anderen Kandidaten ersetzt wurde. Dieser Schritt ist bei der traditionellen Papierwahl gegeben, wenn der Wähler nach der Stimmabgabe bis zur Schließung des Wahlraums vor Ort bleibt und sicherstellt, dass niemand die Urne öffnet, Stimmen austauscht und die Urne wieder schließt. Wäre der Wähler außerdem bereits bei Öffnung des Wahlraums anwesend, so könnte er die Überprüfung nicht nur für seine eigene Stimme, sondern auch für alle abgegebenen Stimmen durchführen (wobei er dies für ein kurzes Zeitfenster nicht kann, nämlich dann, wenn er selbst seine Stimme abgibt).

3. Tallied as recorded

Die Stimmabgabe ist tallied as recorded verifizierbar, wenn der Wähler überprüfen kann, dass seine Stimme so gezählt wird, wie sie in der (elektronischen) Urne gespeichert wurde. Vor dem Hintergrund des Wahlgeheimnisses ist es allerdings weder bei der traditionellen noch bei der elektronischen Wahl möglich, die eigene Stimme im Ergebnis zu identifizieren. Der Wähler kann jedoch überprüfen, dass alle Stimmen aus der Urne korrekt ausgezählt werden, und weiß dadurch, dass auch seine Stimme korrekt ausgezählt wird. Dieser Schritt ist bei der traditionellen Papierwahl gegeben, wenn der Wähler bei der Ergebnisermittlung anwesend ist und überprüft, dass die Mitglieder des Wahlvorstands die Stimmen korrekt auszählen. Da die Auszählung aber meist in mehreren Räumen und bei Kommunalwahlen sogar an mehreren Tagen stattfindet,⁶ ist eine vollständige Überprüfung hier nicht erreichbar.

III. Klartextstimmzettelbelege

Klartextstimmzettelbelege sind Belege, die die getroffene Kandidatenauswahl des Wählers im Klartext – entweder ausschließlich in menschenlesbarer oder zusätzlich in maschinenlesbarer Form⁷ – wiedergeben. Sie bleiben im Wahlraum und werden dort nach der Stimmabgabe vom Wähler in eine Urne geworfen.

1. Verfassungsrechtliche Zulässigkeit von Klartextstimmzettelbelegen

Die verfassungsrechtliche Zulässigkeit von Klartextstimmzettelbelegen, die die Stimme ausschließlich in menschenlesbarer Form wiedergeben, folgt bereits aus dem Wahlcomputerurteil selbst. Hiernach sind insbesondere Wahlgeräte denkbar, die „zusätzlich zur elektronischen Erfassung der Stimme ein für den jeweiligen Wähler sichtbares Papierprotokoll der abgegebenen Stimme ausdrucken, das vor der endgültigen Stimmabgabe kontrolliert werden kann und anschließend zur Ermöglichung der Nachprüfung gesammelt wird. Eine von der elektronischen Stimmerfassung unabhängige Kontrolle bleibt auch beim Einsatz von Systemen möglich, bei denen die Wähler einen Stimmzettel kennzeichnen und die getroffene Wahlentscheidung gleichzeitig (etwa mit einem „digitalen Wahlstift“, [...]) oder nachträglich (z.B. durch einen Stimmzettel-Scanner; [...]) elektronisch erfasst wird, um diese am Ende des Wahltages elektronisch auszuwerten.“⁸

Obgleich das *BVerfG* keine weiteren Angaben zur Gestaltung des Papierprotokolls macht, ist davon auszugehen, dass es einen Klartextstimmzettelbeleg im Blick hat. Hierfür sprechen nicht nur die Wortwahl des *Gerichts* („kontrolliert werden kann“) und die genannten Beispiele, sondern auch der mit dem Protokoll verfolgte Zweck: die unmittelbare Überprüfung der eigenen Stimme durch den Wähler. Dies würde dafür sprechen, auf rein maschinenlesbare Klartextstimmzettelbelege zu verzichten, auch wenn dem Wähler hierfür entsprechendes Leseequipment zur Hand gegeben werden könnte. Zulässig aus Sicht des Öffentlichkeitsgrundsatzes ist es dagegen, wenn der Klartextstimmzettelbeleg neben der menschenlesbaren Stimme auch eine maschinenlesbare Variante enthält, solange im Zweifel die menschenlesbare und vom jeweiligen Wähler überprüfte Stimme zählt. Offen bleibt hier allerdings, ob ein entsprechender Zusatz vom Wähler akzeptiert oder beispielsweise mangels Überprüfungsmöglichkeit kritisch hinterfragt würde.

Um eine vollständige Überprüfung durch den Wähler zu gewährleisten, müsste das elektronisch ermittelte Wahlergebnis anhand der Klartextstimmzettelbelege nachgezählt werden. Dies würde nach den negativen Schlagzeilen über die Nedap-Geräte⁹ auch als vertrauensbildende Maßnahme dienen, selbst wenn dadurch der Vorteil der schnellen Ergebnisberechnung verloren ginge.

2. Verifizierbarkeit durch Klartextstimmzettelbelege

In einigen Bundesstaaten der USA¹⁰ werden Systeme eingesetzt, bei denen der Wähler seine Stimme an einem elektronischen Wahlgerät abgibt, das am Ende der Stimmabgabe einen sog. Voter Verifiable Paper Audit Trail (VV-PAT)¹¹ generiert. Hierbei handelt es sich um einen Ausdruck der Klartextstimme, wobei der Ausdruck für den Menschen ohne weiteres Equipment lesbar ist. Der Ausdruck wird erst nach der Bestätigung durch den Wähler freigegeben und anschließend automatisch oder manuell in die Wahlurne gelegt. Die elektronische Stimme wird vom Wahlgerät gespeichert.

Eine ähnliche Umsetzung bietet EasyVote,¹² ein Konzept, das speziell für komplexe Kommunalwahlen in Deutschland vorgeschlagen wurde. Der hierdurch generierte Ausdruck zeigt die Stimme in menschen- und maschinenlesbarer Form, z.B. als QR-Code, an.¹³ Der QR-Code ermöglicht eine elektronisch unterstützte Auszählung der Papierstimmzettel. Das Verfahren kommt außerdem ohne die Speicherung elektronischer Stimmen bei der Stimmabgabe aus, um das Wahlgeheimnis nicht zu gefährden (weil etwa das Speichermedium Rückschlüsse auf die Reihenfolge der abgegebenen Stimmen zulässt).

⁶ S. hierzu Henning/Volkamer/Budurushi, DÖV 2012, 789.

⁷ Beispiel für eine maschinenlesbare Darstellung: QR-Code.

⁸ *BVerfG* MMR 2009, 316, 318.

⁹ Gonggrijp/Hengeveld, in: EVT 2007, S. 1.

¹⁰ <https://www.verifiedvoting.org/verifier/>.

¹¹ Mercuri, in: 5th International Computer Virus and Security Conference 1992, S. 1.

¹² Volkamer/Budurushi/Demirel, in: REVOTE 2011, S. 1.

¹³ Andere Systeme speichern die Klartextstimme zusätzlich auf einem RFID Chip, wie etwa das argentinische System *Vot.ar*, s. hierzu <http://www.vot-ar.com.ar/en/system-votation/>.

Ein drittes Verfahren, das Klartextstimmzettelbelege vorsieht, ist der Digitale Wahlstift,¹⁴ der in Hamburg entwickelt wurde und dort für Bürgerschaftswahlen eingesetzt werden sollte. Die Stimme wird hier, anders als in den beiden vorherigen Ansätzen, mit einem speziellen Stift auf Papier abgegeben. Dieser Stift erfasst über eine eingebaute Kamera die abgegebene Stimme während des Setzens der Kreuze gleichzeitig in elektronischer Form. Den ausgefüllten Papierstimmzettel wirft der Wähler in die Wahlurne. Der Digitale Wahlstift wird gleichzeitig vom Wähler in eine Docking Station beim Wahlvorstand gesteckt, um den „elektronischen Stimmzettel“ in das elektronische System zu kopieren und vom Stift zu löschen.

Die drei vorgestellten Konzepte gewährleisten Überprüfungsmöglichkeiten in allen drei Phasen (cast as intended, recorded as cast und tallied as recorded), jeweils unter der Annahme, dass in allen Wahlräumen die Stimmzettelbelege (zusätzlich) ausgezählt werden. Dabei ist es analog zur traditionellen Papierwahl erforderlich, dass der Wähler die gesamte Zeit im Wahlraum anwesend ist. Für den Digitalen Wahlstift sollte sowohl die Benutzbarkeit als auch die Nachvollziehbarkeit gegeben sein, da der Klartextstimmzettelbeleg vom Wähler selbst erzeugt wird, indem er seine Stimme auf dem entsprechenden Papierstimmzettel abgibt. Die Benutzbarkeit der beiden anderen vorgestellten Ansätze sollte ebenfalls gegeben sein, da der Wähler den Inhalt des Ausdrucks vor der Stimmabgabe überprüfen und bei der Auszählung anwesend sein kann. Allerdings weisen einige der in den USA eingesetzten VV-PATs Mängel bei der Benutzbarkeit auf, da der Ausdruck zu klein und unübersichtlich ist.¹⁵ Hinsichtlich der Nachvollziehbarkeit ist festzustellen, dass diese für die Phasen recorded as cast und tallied as recorded analog zur traditionellen Papierwahl gegeben ist. Mit Blick auf den ersten Überprüfungsschritt, cast as intended, muss dem Wähler bei den ersten beiden Ansätzen jedoch verdeutlicht werden, dass er die Korrektheit des gedruckten Stimmzettelbelegs unbedingt überprüfen muss.

Da alle drei Ansätze sowohl benutzbar als auch nachvollziehbar gestaltet werden können, sind sie mit dem Grundsatz der Öffentlichkeit der Wahl vereinbar – unter der Voraussetzung, dass alle Papierstimmzettel nachträglich ausgezählt werden können.

IV. Kodierte Stimmzettelbelege

Kodierte Stimmzettelbelege sind Belege, die unter Einsatz von Kryptografie erzeugt werden und die getroffene Auswahl des Wählers ausschließlich in kodierter Form darstellen. Diese Stimmzettelbelege sind ohne den Besitz eines entsprechenden Geheimnisses nicht lesbar, d.h., sie sagen nichts über die Klartextstimme des Wählers aus. In den meisten Fällen handelt es sich bei dem Geheimnis um einen kryptografischen Schlüssel. Dieser Schlüssel ist in der Regel auf mehrere Wahlorgane verteilt, damit eine einzelne Person nicht in der Lage ist, die Klartextstimme aus dem kodierten Stimmzettelbeleg zu berechnen und damit das Wahlgeheimnis zu brechen.

1. Verfassungsrechtliche Zulässigkeit von kodierten Stimmzettelbelegen

Die Durchführung der dargestellten Überprüfungsschritte mittels kodierter Stimmzettelbelege ist nur unter Einbindung spezieller (unabhängig vom elektronischen Wahlgerät) entwickelter Hilfsprogramme möglich. Da der Grundsatz der Öffentlichkeit der Wahl jedoch verlangt, dass die wesentlichen Schritte der Wahlhandlung und Ergebnisermittlung vom Bürger ohne besondere Sachkenntnis überprüft werden können, ist zu diskutieren, ob diese Hilfsprogramme zulässig sind. Insofern ist es von entscheidender Bedeutung, wie viel Sachkenntnis dem Einzelnen im Umgang mit Technik zuzutrauen ist und ob eine Öffnung

gegenüber technischem Fortschritt verlangt werden kann. Für die Bejahung der letzten Frage spricht bereits die grundsätzliche Aussage des *Gerichts*, wonach der Gesetzgeber nicht gehindert ist, elektronische Wahlgeräte zur Stimmabgabe einzusetzen, wenn die verfassungsrechtlich gebotene Möglichkeit einer zuverlässigen Richtigkeitskontrolle gesichert ist.¹⁶ Insofern verlangt das *BVerfG* auf der Ebene der Allgemeinheit der Wahl bereits eine Öffnung gegenüber technischem Fortschritt, da es dem Einzelnen die elektronische Stimmabgabe einerseits zutraut, andererseits auferlegt. Dies spricht dafür, dass auch auf der Ebene der Öffentlichkeit der Wahl eine Öffnung gegenüber technischem Fortschritt möglich ist. Ein anderes Ergebnis wäre widersprüchlich, da das *Gericht* nicht einerseits die elektronische Stimmabgabe als verfassungskonform, ihre elektronische Kontrolle aber als verfassungswidrig darstellen kann. Dafür, vom Einzelnen die Öffnung gegenüber technischem Fortschritt verlangen zu können, spricht schließlich auch das Menschenbild des GG, das eben nicht das eines isolierten, souveränen Individuums, sondern das des Einzelnen in der Gemeinschaft ist. Die Verfassung hat sich für die „Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person“ entschieden.¹⁷ Insofern ist nicht nur auf den Einzelnen, sondern auch auf die Gemeinschaft abzustellen. Dabei ist ferner zu bedenken, welchen Einzug Technik in den vergangenen Jahrzehnten in das Leben des Einzelnen genommen hat. Diese gesellschaftliche Entwicklung kann bei Beantwortung der Frage, ob eine Öffnung gegenüber technischem Fortschritt verlangt werden kann, nicht unbeachtet bleiben. Vor diesem Hintergrund ist eine Überprüfung der wesentlichen Schritte der Wahl unter Heranziehung entsprechender Hilfsprogramme nicht zu beanstanden. Ob diese Programme allerdings benutzbar sind und das Ergebnis der Überprüfung für den Wähler nachvollziehbar ist, bleibt offen und kann auch nur am konkreten technischen System entschieden werden.

Aus juristischer Sicht ist außerdem zu klären, ob kodierte Stimmzettelbelege nach der Stimmabgabe vom jeweiligen Wähler mit nach Hause genommen werden dürfen. Grundsätzlich ist dies möglich, da die Belege weder die Stimme im Klartext zeigen noch eine Antwort darauf geben, ob der Wähler eine gültige oder ungültige Stimme abgegeben hat. Ist die Einhaltung des Wahlgeheimnisses sichergestellt, können die Belege also vom Wähler mitgenommen werden, damit dieser den zweiten Schritt der Überprüfbarkeit, recorded as cast, zeit- und ortsunabhängig durchführen kann. Der Wähler kann also von zu Hause aus feststellen, ob seine Stimme unverändert in der Urne liegt. Dies ist möglich, da die Urne als Webservice implementiert ist (das sog. Web Bulletin Board) und dort alle kodierten Stimmzettelbelege angezeigt werden. Anders als bei der traditionellen Papierwahl kann ein Wähler dann aber nur noch seine eigene Stimme überprüfen. Da das *BVerfG* fordert, dass die Stimmen nach der Stimmabgabe nicht ausschließlich auf einem elektronischen Speicher abgelegt werden¹⁸ und die gesamte Öffentlichkeit die Möglichkeit zur Überprüfbarkeit im Wahlraum haben sollte, muss eine Papierüberprüfungsmöglichkeit aller Stimmen im Wahlraum verbleiben. Insofern müssen die in der Literatur vorgeschlagenen Umsetzungen dahingehend erweitert werden, dass der Wähler nur eine Kopie des eigenen Stimmzettelbelegs mit nach Hause nehmen kann. Um psychologische, auf den Grundsatz der freien Wahl bezogene Angriffe auszuschließen, werden in der Literatur auch Verfahren diskutiert, die die

¹⁴ *Arzt-Mergemeier/Beiss/Steffens*, in: VOTE-ID 2007, S. 88.

¹⁵ Pilot Project Report, 2006 Georgia Accuracy in Elections Act, s. hierzu <http://sos.georgia.gov/elections/VVPATreport.pdf>.

¹⁶ *BVerfG* MMR 2009, 316, 318.

¹⁷ *BVerfGE* 4, 7, 15 f.

¹⁸ *BVerfG* MMR 2009, 316, 318.

Mitnahme einer beliebigen Stimmzettelkopie vorsehen.¹⁹ Hier stellt sich jedoch die Frage, ob diese Technik verfassungskonform ist, da der Wähler nicht mehr seine eigene, sondern nur die Wahlhandlung anderer Wähler überprüfen kann. Denkbar ist auch,²⁰ dass Wähler mehrere Kopien von Stimmzettelbelegen inklusive des eigenen Belegs mit nach Hause nehmen. Dabei wäre sichergestellt, dass jeder Wähler auch seine eigene Stimme überprüfen kann.

2. Verifizierbarkeit durch kodierte Stimmzettelbelege

Nachfolgend werden zwei Gruppen kryptografiebasierter Konzepte vorgestellt:

a) Verschlüsselte Stimmzettelbelege

Bei Konzepten, die verschlüsselte Stimmzettelbelege verwenden, trifft der Wähler nach erfolgreicher Überprüfung der Wahlberechtigung durch den Wahlvorstand seine Auswahl an einem elektronischen Wahlgerät. Die Auswahl des Wählers wird mit einem öffentlichen Wahlschlüssel verschlüsselt und der daraus resultierende Chiffretext auf den Stimmzettelbeleg gedruckt.²¹ Um die Handhabung für den Wähler zu erleichtern, wird dabei regelmäßig nicht der gesamte Schlüsseltext, sondern nur dessen Fingerabdruck (kryptografischer Hashwert) abgedruckt²² oder der Schlüsseltext wird in einem QR-Code kodiert.²³ Nachdem der Stimmzettelbeleg gedruckt wurde, kann der Wähler entweder seine Auswahl bestätigen oder überprüfen, ob das Wahlgerät seine Auswahl korrekt erfasst hat, d.h., ob der Stimmzettelbeleg tatsächlich seine Auswahl enthält. Wenn der Wähler den Stimmzettelbeleg bestätigt, ist der Vorgang der Stimmabgabe beendet und die auf dem Stimmzettelbeleg gedruckte kodierte Stimme wird auf dem Web Bulletin Board elektronisch gespeichert und veröffentlicht.²⁴

Anhand eines dafür konzipierten Prüfprogramms kann der Wähler überprüfen, ob die richtige Stimme verschlüsselt wurde. Das Programm bekommt alle hierfür erforderlichen Daten und zeigt dem Wähler die Stimme im Klartext an. Dieser Mechanismus ermöglicht jedoch keine unmittelbare *cast as intended* Verifizierung, denn vor dem Hintergrund des Wahlgeheimnisses ist es nicht möglich, die Stimme, die überprüft wurde, auch tatsächlich abzugeben. Es handelt sich bei der überprüften Stimme also nur um eine Teststimme. Der Mechanismus bietet dennoch eine hohe Sicherheit, wenn mehrfach überprüft wird. Dadurch, dass das Wahlgerät den Stimmzettelbeleg druckt, zu diesem Zeitpunkt aber noch nicht weiß, ob der Wähler diesen Beleg überprüft oder nicht, wird sich das Wahlgerät mit sehr hoher Wahrscheinlichkeit korrekt verhalten. Die Wahrscheinlichkeit für den Wähler, eine Manipulation seines eigentlichen Stimmzettelbelegs aufzudecken, steigt mit der Anzahl der durchgeführten Überprüfungen. Hierdurch kann der Wähler begründete

Vertrauen in die Korrektheit seiner tatsächlich abgegebenen Stimme auf dem Web Bulletin Board erlangen.

Anhand der Kopie seines Stimmzettelbelegs kann der Wähler anschließend von zu Hause oder jedem beliebigen Ort aus überprüfen, ob seine Stimme in der Urne (auf dem Web Bulletin Board) gespeichert ist (*recorded as cast*). Dazu besucht er die entsprechende Wahlwebseite und die Webseite einer anderen, die Integrität des Web Bulletin Boards kontrollierenden Instanz und sucht nach seinem Chiffretext oder seinem Hashwert. Da auf dem Web Bulletin Board zu jedem Wähler auch dessen Identität oder ein Pseudonym²⁵ angezeigt wird, kann der Wähler alternativ auch nach diesen Informationen suchen und überprüfen, ob seiner Identität der Chiffretext auf seinem Stimmzettelbeleg zugeordnet ist.

Der dritte Schritt der Überprüfung der eigenen Wahlhandlung, *tallied as recorded*, kann mithilfe des Stimmzettelbelegs nicht durchgeführt werden. Die dargestellten Verfahren ermöglichen aber durch die Bereitstellung von mathematischen Beweisen nach der Auszählung, diese nachzurechnen und das Ergebnis nachzuvollziehen. Hierzu müssten von unabhängigen Institutionen entsprechende Programme bereitgestellt werden. Unter diesen Umständen wäre *tallied as recorded* gegeben.

Wegen der geforderten Speicherung auf Papier ist das alleinige Abdrucken eines Hashwerts nicht zulässig. Dieser mag aus anderen Gründen dargestellt sein (z.B. um eine Überprüfung zu erleichtern). Da die Stimmen aber nicht ausschließlich auf einem elektronischen Speicher abgelegt werden dürfen, muss daneben der gesamte Chiffretext der Stimme abgedruckt sein.

b) Permutation der Kandidatenreihenfolge

Diese Konzepte verwenden eine besondere Form von Stimmzetteln, wobei der Stimmzettel aus zwei voneinander trennbaren Teilen besteht. Der eine Teil des Stimmzettels enthält eine zufällig permutierte Kandidatenreihenfolge. Diese ist auf jedem Stimmzettel unterschiedlich.²⁶ Auf dem anderen Teil wird die Auswahl eines Kandidaten durch manuelles Markieren mit einem Stift getätigt. Dieser Teil enthält außerdem einen kodierten Wert. Der Klartext hinter diesem kodierten Wert definiert die Kandidatenreihenfolge auf diesem Stimmzettel.

Das bekannteste Konzept dieser Art ist *Prêt à Voter*.²⁷ Ähnlich arbeitet auch *Scantegrity*.²⁸ Bei beiden Systemen trennt der Wähler den Stimmzettel noch in der Wahlkabine. Der Teil mit der Kandidatenreihenfolge (bei *Prêt à Voter* der linke Teil) wird vernichtet und der andere Teil, der nur die Position, nicht aber den vom Wähler ausgewählten Kandidaten verrät, wird gescannt und somit elektronisch erfasst. Der Wähler kann auch hier eine Kopie des kodierten Teils mit nach Hause nehmen, um zu überprüfen, ob seine Stimme in der Urne (auf dem Web Bulletin Board) gespeichert ist. Dazu besucht er auch hier die entsprechende Wahlwebseite und sucht nach seinem auf dem Stimmzettelbeleg abgedruckten verschlüsselten Wert. Alternativ dazu kann er überprüfen, ob seiner Identität der Chiffretext auf seinem Stimmzettelbeleg zugeordnet ist.

Der Wähler kann jedoch nicht überprüfen, ob der verschlüsselte Wert tatsächlich die Permutation der Kandidaten enthält, die er vorab auf dem ausgedruckten Stimmzettel gesehen hat. Daher werden bei entsprechenden Systemen mehr Papierstimmzettel erzeugt, als erforderlich sind. Hiervon wird vor der Wahl eine zufällig ausgewählte Menge an Stimmzetteln kontrolliert. Insofern wird überprüft, ob die auf der rechten Seite befindliche verschlüsselte Permutation der Kandidaten der permutierten Kandidatenreihenfolge auf der linken Seite des Stimmzettels entspricht. Dieser Überprüfungsprozess findet öffentlich statt und kann von allen Wählern und der gesamten interessierten Öffentlichkeit beobachtet werden.

¹⁹ Araújo/Custódio/van de Graaf, in: *Towards Trustworthy Elections 2010*, S. 274.

²⁰ Bei diesem Ansatz ist in Abhängigkeit des definierten Angreifermodells sicherzustellen (z.B. wenn Mitglieder des Wahlvorstands Teil des Angreifermodells sind), dass der Wähler den eigenen Stimmzettelbeleg bekommt.

²¹ Chaum, in: *Security and Privacy 2004*, S. 38.

²² Benaloh, in: *EVT 2006*, S. 5.

²³ Ben-Nun/Fahril/Llewellyn/Rival/Rosen/Ta-Shma/Wikström, in: *Electronic Voting 2012*, S. 315; Vegas, in: *Electronic Voting 2012*, S. 199.

²⁴ Um die Integrität des Web Bulletin Boards (der elektronischen Urne) zu gewährleisten, können zu jeder Zeit spezifizierte Abzüge hiervon durch andere vertrauenswürdige Instanzen (z.B. Wahlorgane oder das Bundesamt für Sicherheit in der Informationstechnik) angefertigt und zur gegenseitigen Kontrolle verwendet werden.

²⁵ Dies ist erforderlich, um sog. *Clash-Attacks* zu verhindern, s. hierzu Kusters/Truderung/Vogt, in: *Security and Privacy 2012*, S. 395.

²⁶ Wiederholungen der Permutation sind jedoch unvermeidbar, da es in Abhängigkeit von der Anzahl der Wahlbewerber nur eine feste Anzahl an Optionen gibt.

²⁷ Chaum/Ryan/Schneider, in: *ESORICS 2005*, S. 118.

²⁸ Chaum/Carback/Clark/Essex/Popoveniuc/Rivest/Ryan/Shen/Sherman, in: *EVT 2008*, S. 1.

Damit bietet auch dieser Ansatz keine unmittelbare cast as intended Verifizierung, denn zur Sicherung des Wahlgeheimnisses ist es nicht möglich, die im Vorfeld überprüften Stimmzettel zur Stimmabgabe zu verwenden. Die Wahrscheinlichkeit einer Manipulationsentdeckung hängt entscheidend von der Menge und der Zufälligkeit der im Vorfeld überprüften Stimmzettel ab.

Der dritte Schritt der Überprüfung der eigenen Wahlhandlung, tallied as recorded, kann auch hier mithilfe der Stimmzettelbelege nicht überprüft werden. Die beschriebenen elektronischen Konzepte Prêt à Voter und Scantegrity ermöglichen aber durch die Bereitstellung mathematischer Beweise, die Auszählung nachzurechnen und das Ergebnis nachzuvollziehen. Hierzu müssten analog zu den Verfahren in Kap. IV.2.a) entsprechende Programme von unabhängigen Institutionen bereitgestellt werden. Gemäß den obigen Ausführungen ist das Abdrucken eines reinen Hashwerts nicht zulässig.

V. Fazit

Wie sollen elektronische Wahlen einerseits das Wahlgeheimnis gewährleisten und andererseits eine sachkenntnisunabhängige Überprüfbarkeit der Wahlhandlung und Ergebnisermittlung ermöglichen? Der Beitrag hinterfragt die Tauglichkeit von Konzepten, die diesen Anforderungen mithilfe von Stimmzettelbelegen begegnen. Während die Überprüfbarkeit der Wahlhandlung mithilfe von Klartextstimmzettelbelegen ohne weiteres Equipment möglich und vor dem Hintergrund der Öffentlichkeit der Wahl nicht zu bestanden ist, kann die Überprüfbarkeit kodierter Stimmzettelbelege nur unter Heranziehung entsprechender Hilfsprogramme erfolgen. Dem steht zwar aus Sicht des Öffentlichkeitsgrundsatzes grundsätzlich nichts entgegen. Es besteht jedoch noch großer Forschungsbedarf zur Benutzbarkeit und Nachvollziehbarkeit dieser Ansätze. Um die recorded as cast und

tallied as recorded Verifizierbarkeit zeit- und ortsunabhängig im Hinblick auf die eigene Stimme durchführen zu können, darf der Wähler bei diesen Ansätzen eine Kopie des Stimmzettelbelegs mit nach Hause nehmen, solange der Originalbeleg im Wahlraum verbleibt. Um aber auch dem Wahlvorstand die Überprüfung aller abgegebenen Stimmen zu ermöglichen, muss der gesamte Chiffretext auf dem Stimmzettelbeleg abgedruckt sein. Insgesamt bleibt festzuhalten, dass weitere Forschung im Kontext verifizierbarer Wahlen notwendig und geboten ist, da entsprechende Verfahren großes Potenzial haben, die Überprüfbarkeit der eigenen Wahlhandlung und Ergebnisermittlung ortsunabhängig zu gestalten. Abschließend sei angemerkt, dass diese Überlegungen ebenso für gegenwärtig praktizierte Wahlen in nicht parlamentarischen Bereichen herangezogen werden können.



Ass. jur. Maria Henning

ist Doktorandin und Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel.



M.Sc. Inf & M.Sc. IT-Sich. Jurlind Budurushi

ist Doktorand der Forschungsgruppe „SecUSo – Security, Usability and Society“ im Fachbereich Informatik an der TU Darmstadt und im Forschungszentrum „CASED – Center for Advanced Security Research Darmstadt“.



Prof. Dr. Melanie Volkamer

ist Leiterin der Forschungsgruppe „SecUSo – Security, Usability and Society“ im Fachbereich Informatik an der TU Darmstadt und im Forschungszentrum „CASED – Center for Advanced Security Research Darmstadt“.