

Technical Report

Nr. TUD-CS-2014-0017
January 20th, 2014



Öffentlichkeitsgrundsatz und Stimmzettelbelege

Authors

Maria Henning, Jurlind Budurushi and Melanie Volkamer

Öffentlichkeitsgrundsatz und Stimmzettelbelege

1 Einleitung

Zahlreiche Institutionen wählen ihre Gremien elektronisch.¹ Anlass hierfür mag zum einen die Erwartung einer schnellen und fehlerfreien Ergebnisermittlung, zum anderen aber auch das Bestreben einer zeitgemäßen Stimmabgabe sein. Leben wir doch in einer Welt, die ohne Technik kaum noch denkbar ist. Technik ist in nahezu alle Bereiche unseres beruflichen und privaten Alltags integriert. E-Mails werden nicht nur noch im Büro, sondern ebenso im Zug oder in der Straßenbahn gelesen und bearbeitet. Hotelbuchungen werden zwischen zwei Terminen von einem beliebigen Ort via Smartphone vorgenommen. Und selbst bei Steuerklärungen und Überweisungen holt uns die Technik ein. Daher ist es nur folgerichtig, die Chancen moderner Informationstechnologien auch im Kontext von Wahlen zu nutzen.

Allerdings hat das Bundesverfassungsgericht die Anforderungen an elektronische Parlamentswahlen mit Urteil vom 3.3.2009 deutlich erhöht.² Hiernach ist der Einsatz rechnergesteuerter Wahlgeräte nicht nur an den fünf geschriebenen Wahlrechtsgrundsätzen, sondern auch am Grundsatz der Öffentlichkeit der Wahl nach Art. 38 in Verbindung mit 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.“³ Dabei müssen insbesondere die „Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können.“⁴

Mit diesen Worten hat das Bundesverfassungsgericht die Forschung rund um das Thema eVoting vor neue Herausforderungen gestellt und zahlreiche Folgefragen aufgeworfen, insbesondere, ob die Öffentlichkeit der Wahl auch unter Nutzung elektronischer Hilfsprogramme realisiert werden kann und wie viel technisches Verständnis dem Einzelnen in diesem Kontext überhaupt zuzutrauen oder gar abzuverlangen ist.⁵ Dabei wird die Überprüfbarkeit der Wahl bereits seit einigen Jahren in der Forschung unter dem Stichwort Verifizierbarkeit diskutiert. Vielen Konzepten ist gemein, dass sie die Verifizierbarkeit der eigenen Stimme mithilfe sogenannter Stimmzettelbelege⁶ realisieren. Hier sind Belege der Klartextstimme ebenso denkbar wie Belege der kodierten Stimme. Eine Untersuchung, inwieweit entsprechende Verifizierungsverfahren den Grundsatz der Öffentlichkeit der Wahl gewährleisten, ist jedoch bislang nicht erfolgt. Diese Frage soll nachfolgend für parlamentarische Wahlen diskutiert werden. Der Fokus liegt dabei auf elektronischen Wahlgeräten, die im Wahlraum⁷ eingesetzt werden, und auf Vorschlägen zur Umsetzung der Verifizierbarkeit der Wahlhandlung. Dabei können

¹ Beispielhaft wird hier auf die Gremienwahl des Graduiertenkollegs der Friedrich-Schiller-Universität Jena, die Fachkollegienwahl der Deutschen Forschungsgemeinschaft und die Vorstands- und Präsidiumswahl der Gesellschaft für Informatik hingewiesen.

² BVerfGE 123, 39.

³ BVerfGE 123, 39 (70).

⁴ BVerfGE 123, 39 (71, 83).

⁵ Darüber hinaus stellt sich die Frage, ob für Wahlen zu Organen der funktionalen Selbstverwaltung, Wahlen zu arbeitsrechtlichen Interessenvertretungen und Wahlen in privaten Körperschaften unter Umständen geringere Anforderungen gelten. Siehe hierzu: *Richter*, Wahlen im Internet rechtsgemäß gestalten, 2012.

⁶ Häufig auch als Quittungen bezeichnet.

⁷ Umgangssprachlich werden die verschiedenen Wahlräume eines Wahlbezirks oft als Wahllokal bezeichnet.

die Überlegungen ebenso für Wahlen in nicht parlamentarischen Bereichen herangezogen werden.

2 Öffentlichkeit und Verifizierbarkeit

Möchte man den Zusammenhang zwischen Öffentlichkeit und Verifizierbarkeit untersuchen oder die Frage, ob das eine dem anderen entspricht, behandeln, so muss man zunächst den Inhalt des Grundsatzes der Öffentlichkeit der Wahl herausarbeiten. Dieser lässt sich, obgleich ihn das Bundesverfassungsgericht nahezu formelhaft definiert, nicht mit einem Satz erfassen. Offensichtlich setzt die Gewährleistung der Öffentlichkeit der Wahl zunächst die Existenz einer Überprüfungsmöglichkeit voraus. Nur wenn der Wähler die Möglichkeit zur Überprüfung hat, kann er diese auch durchführen. Die Überprüfungsmöglichkeit muss die Wahlhandlung und die Ergebnisermittlung abdecken. Unter dem Begriff der Wahlhandlung ist zunächst das gesamte unter Leitung und Aufsicht der Wahlorgane stehende Verfahren am Wahltag zu verstehen. Es beginnt mit dem Zusammentritt des Wahlvorstandes und der Eröffnung der Wahlhandlung⁸ und endet nach Ablauf der in Deutschland traditionell von 8.00 bis 18.00 Uhr dauernden Wahlzeit mit der Erklärung des Wahlvorstehers,⁹ dass die Abstimmung geschlossen ist.¹⁰ Jedoch ist davon auszugehen, dass das Bundesverfassungsgericht, wenn es die Überprüfung der Wahlhandlung als einen wesentlichen Schritt der Wahl zugrunde legt, 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.¹¹ Insofern muss sich eine Überprüfungsmöglichkeit im Rahmen der 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 hier erhält, auch nachvollziehbar sein. Es muss dem Wähler also klar sein, welchen wesentlichen Schritt der Wahl – Wahlhandlung oder Ergebnisberechnung – er gerade überprüft und ob dieser Schritt korrekt verlaufen ist. Der Wähler muss somit in der Lage sein, die ihm zur Verfügung gestellten Informationen entsprechend ihrem Zweck, der Überprüfung der Wahlhandlung und Ergebnisermittlung, zu deuten. Dazu gehört auch das Wissen, ob er die Überprüfung nur für seine eigene Stimme oder für alle abgegebenen Stimmen durchführt. Die beiden Eigenschaften „Benutzbarkeit und Nachvollziehbarkeit“ setzen demnach die Anforderung des Bundesverfassungsgerichts nach einer sachkenntnisunabhängigen Überprüfbarkeit um. Darüber hinaus fordert das Gericht aber auch, dass die Stimmen nach der Stimmabgabe nicht ausschließlich auf einem elektronischen Speicher abgelegt werden.¹²

Der Grundsatz der Öffentlichkeit der Wahl ist demnach erst dann gewährleistet, wenn die folgenden vier Punkte – Überprüfungsmöglichkeit, Benutzbarkeit und Nachvollziehbarkeit

⁸ Näheres in § 53 Bundeswahlordnung.

⁹ Näheres in § 60 Bundeswahlordnung.

¹⁰ *Schreiber* 2009, BWahlG, § 31, Rn. 1.

¹¹ BVerfGE 123, 39 (70).

¹² BVerfGE 123, 39 (73).

sowie die unabhängig vom elektronischen Medium erfolgte Speicherung der Stimmen – gegeben sind.

Wie bereits angedeutet, entspricht die Existenz der Überprüfungsmöglichkeit dem in der technischen Fachliteratur verwendeten Begriff der Verifizierbarkeit. Dabei wird die Verifizierbarkeit in drei Schritte unterteilt, je nachdem welcher Schritt der Wahlhandlung (Stimmabgabe und Stimmspeicherung) oder der Ergebnisermittlung überprüft werden kann. Diese Unterteilung ist sinnvoll, da für die unterschiedlichen Schritte in der Regel unterschiedliche Techniken im Einsatz sind. Die drei Teildefinitionen von Verifizierbarkeit bilden zusammen den Aspekt der Überprüfungsmöglichkeit des Öffentlichkeitsgrundsatzes. Die einzelnen Schritte werden im Folgenden erläutert. Außerdem wird aufgezeigt, inwieweit die heutige Papierwahl im Wahlraum diese Verifizierbarkeit und damit Überprüfungsmöglichkeit bietet.

2.1 Korrekte Interpretation der Stimme (cast as intended-Verifizierbarkeit)

Ein Wahlsystem ist *cast as intended*-verifizierbar, wenn der Wähler überprüfen kann, ob seine eigene Stimme so vom (elektronischen) Wahlsystem erfasst wurde, wie er es beabsichtigt hat. Hat der Wähler beispielsweise Kandidat A angeklickt, so muss er überprüfen können, ob das System auch tatsächlich Kandidat A aufgenommen hat und die Stimme nach dem Anklicken auf dem Bildschirm nicht in eine Stimme für einen anderen Kandidaten geändert wurde. 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. Wird von solcher Tinte abgesehen, die nach einer Weile nicht mehr auf dem Stimmzettel zu sehen ist, so ist eine weitere Überprüfung durch den Wähler bei der Stimmabgabe nicht erforderlich. Er kann davon ausgehen, dass seine Stimme korrekt erfasst in der Urne liegt. Aus dem gleichen Grund kann er auch mit Blick auf alle anderen Wähler davon ausgehen, dass deren Stimmen korrekt erfasst in der Urne liegen.

2.2 Korrekte Aufbewahrung oder Speicherung der Stimme (recorded as cast-Verifizierbarkeit)

Ein Wahlsystem ist *recorded as cast*-verifizierbar, wenn der Wähler überprüfen kann, ob seine vom Wahlsystem erfasste Stimme unverändert in der (elektronischen) Urne gespeichert wird. 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 theoretisch 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 danach 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).

2.3 Korrekte Ergebnisermittlung (tallied as recorded -Verifizierbarkeit)

Ein Wahlsystem ist *tallied as recorded*-verifizierbar, wenn der Wähler überprüfen kann, ob 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 Wäh-

ler 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 Wahlvorstandes die Stimmen korrekt auszählen. Da die Auszählung aber meist in mehreren Räumen und bei Kommunalwahlen sogar an mehreren Tagen stattfindet,¹³ ist eine vollständige Überprüfung hier nicht erreichbar. Möglich ist aber in jedem Fall ein Plausibilitätscheck dahingehend, ob die Mitglieder des Wahlvorstandes korrekt ausgezählt haben.

Nachdem eine Konkretisierung der Öffentlichkeit der Wahl hinsichtlich Benutzbarkeit und Nachvollziehbarkeit der Überprüfungsmöglichkeiten und damit der Verifizierbarkeit erfolgt ist, werden im Folgenden existierende Vorschläge zur Umsetzung der Verifizierbarkeit aus der technischen Literatur vorgestellt und hinsichtlich der Erfüllung dieser Kriterien diskutiert.

3 Klartextstimmzettelbelege

Klartextstimmzettelbelege sind Belege, die die getroffene Kandidatenauswahl des Wählers im Klartext – entweder ausschließlich in menschenlesbarer oder zusätzlich in maschinenlesbarer Form¹⁴ – wiedergeben. Sie bleiben im Wahlraum und werden dort nach der Stimmabgabe in einer Urne aufbewahrt.

Nachfolgend wird die Zulässigkeit von Klartextstimmzettelbelegen nach den in Kapitel zwei definierten Kriterien untersucht. Außerdem werden elektronische Wahlsysteme vorgestellt, die entsprechende Belege verwenden. Dabei ist allen Wahlsystemen gemein, dass die Wahlberechtigungsprüfung analog zur traditionellen Papierwahl durch Vorlage eines Identifikationsausweises und Abgleich mit dem Wählerverzeichnis erfolgt.

3.1 Verfassungsrechtliche Zulässigkeit von Klartextstimmzettelbelegen

Die verfassungsrechtliche Zulässigkeit von Klartextstimmzettelbelegen, die die Stimme ausschließlich in geschriebener und damit in menschenlesbarer Form wiedergeben, folgt bereits aus dem Wahlcomputerurteil selbst. Hiernach sind insbesondere Systeme 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.“¹⁵

Oggleich das Bundesverfassungsgericht keine weiteren Angaben zur Gestaltung des Papierprotokolls macht, ist davon auszugehen, dass es einen Klartextstimmzettelbeleg im Blick hatte, den der Wähler eigenständig mit dem menschlichen Auge überprüfen kann. Hierfür sprechen nicht nur die Wortwahl des Gerichts („kontrolliert werden kann“) und die genannten

¹³ Siehe hierzu: *Henning/Volkamer/Budurushi*, Transparentes eVoting – Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen, DÖV 2012, 789-796.

¹⁴ Beispiel für eine maschinenlesbare Darstellung: QR-Code.

¹⁵ BVerfGE 123, 39 (73).

Beispiele, sondern auch der mit dem Protokoll verfolgte Zweck: die unmittelbare Überprüfung der eigenen Stimme durch den Wähler und die Ermöglichung einer Nachprüfung durch den Wahlvorstand. Dies würde dafür sprechen, auf rein maschinenlesbare Klartextstimmzettelbelege zu verzichten, auch wenn dem Wähler hierfür entsprechendes Lese-Equipment 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 oder bei Unstimmigkeiten die menschenlesbare und vom jeweiligen Wähler überprüfte Stimme zählt. Offen bleibt hier allerdings, ob ein entsprechender Zusatz vom Wähler akzeptiert oder kritisch hinterfragt würde, weil er ohne passendes Equipment nicht kontrollieren kann, ob die menschenlesbare mit der maschinenlesbaren Stimme übereinstimmt. Außerdem kann er nicht sehen, ob zusätzliche, das Wahlgeheimnis gefährdende Informationen, wie der Zeitpunkt der Stimmabgabe, kodiert sind. Obwohl eine Verletzung des Wahlgeheimnisses durch das Abdrucken der Stimme in maschinenlesbarer Form durch organisatorische Maßnahmen praktisch ausgeschlossen werden kann, könnte Unkenntnis an dieser Stelle zu einem Vertrauensverlust führen. Dies gilt es in Zukunft zu untersuchen.

Leider macht das Bundesverfassungsgericht keine genauen Angaben zur Auszählung der Papierprotokolle. Denkbar wäre eine manuelle Auszählung aller Papierstimmzettel in allen Wahlräumen, eine manuelle Auszählung aller Papierstimmzettel in ein paar zufällig ausgewählten Wahlräumen, eine scannerbasierte Auszählung der Papierstimmzettel in allen oder einer Auswahl an Wahlräumen oder eine rein elektronische Auszählung so lange keine relevante Wahlbeschwerde vorliegt oder Plausibilitätsprüfungen auf Unstimmigkeiten hinweisen. Da eine Überprüfung durch den Wähler nur dann gegeben ist, wenn in seinem Wahlraum auch die Papierstimmzettel gezählt werden, ist davon auszugehen, dass gerade zu Beginn der Einführung eines entsprechenden elektronischen Wahlsystems alle Papierstimmzettel nachgezählt werden. Dies würde nach den negativen Schlagzeilen zu den Nedap-Geräten¹⁶ auch als vertrauensbildende Maßnahme dienen, selbst wenn dadurch der Vorteil der schnellen Ergebnisberechnung verloren ginge. Entsprechend der aktuellen Hochrechnung am Wahlabend wäre es jedoch denkbar, zunächst die elektronischen Ergebnisse zu veröffentlichen und dann die Papierstimmzettel auszuzählen.

3.2 Verifizierbarkeit durch Klartextstimmzettelbelege

In den U.S.A. werden in einigen Bundesstaaten¹⁷ Wahlsysteme eingesetzt, bei denen der Wähler seine Stimme an einem elektronischen Wahlgerät abgibt, das am Ende der Stimmabgabe einen sogenannten Voter Verifiable Paper Audit Trail (VV-PAT)¹⁸ generiert. Hierbei handelt es sich um einen Ausdruck der Klartextstimme, wobei der Ausdruck für den Menschen ohne weiteres Equipment lesbar ist und keine rein maschinenlesbaren Elemente enthält. Abbildung 1 zeigt beispielhaft ein solches System. Der Wähler kann den Ausdruck überprüfen und bestätigen, wenn die richtige Stimme abgedruckt ist. Dieser Ausdruck wird nach der Bestätigung freigegeben und je nach System automatisch oder manuell in die Wahlurne gelegt. Die elektronische Stimme wird vom Wahlsystem gespeichert.

¹⁶ *Gonggrijp/Hengeveld*, Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective, in: EVT 2007, 1.

¹⁷ <https://www.verifiedvoting.org/verifier/>.

¹⁸ *Mercuri*, Physical Verifiability of Computer Systems, in: 5th International Computer Virus and Security Conference 1992.

Eine ähnliche Umsetzung von Klartextstimmzettelbelegen bietet EasyVote,¹⁹ ein System, das speziell für komplexe Kommunalwahlen in Deutschland vorgeschlagen wurde. Abbildung 2 zeigt den Ausdruck eines von diesem System generierten Stimmzettelbelegs. Dieser zeigt die Stimme nicht nur in menschenlesbarer, sondern auch in maschinenlesbarer Form, hier als QR-Code.²⁰ Dieser QR-Code ermöglicht eine schnellere elektronisch unterstützte Auszählung der Papierstimmzettel. Das Verfahren kommt außerdem ohne die Speicherung elektronischer Stimmen aus, um das Wahlgeheimnis nicht zu gefährden (weil beispielsweise das Speichermedium Rückschlüsse auf die Reihenfolge der abgegebenen Stimmen zulässt).

Ein drittes Verfahren, welches Klartextstimmzettelbelege vorsieht, ist der Digitale Wahlstift²¹, der in Hamburg entwickelt wurde und dort für Bürgerschaftswahlen eingesetzt werden sollte. Abbildung 3 zeigt das Ausfüllen eines Stimmzettels mithilfe des Digitalen Wahlstifts. Die Stimme wird hier, anders als in den beiden vorherigen Ansätzen, mit einem speziellen Stift auf einem perforierten Papierstimmzettel 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 Wahlsystem zu kopieren und vom Stift zu löschen.

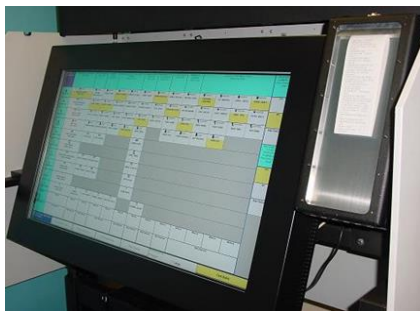


Abb. 1: VV-PAT.²²



Abb. 2: EasyVote.²³



Abb. 3: Digitaler Wahlstift.²⁴

In jedem Fall gewährleisten die drei vorgestellten elektronischen Wahlsysteme Überprüfungsmöglichkeiten in allen drei Phasen (*cast as intended*, *recorded as cast* und *tallied as recorded*), jeweils unter der Annahme, dass in allen Wahlräumen die Papierstimmzettel (zusätzlich) ausgezählt werden. Dabei ist es analog zur traditionellen Papierwahl erforderlich, dass der Wähler sowohl während der Wahlhandlung als auch während der Ergebnisermittlung im Wahlraum anwesend ist. Offen bleibt jedoch die Frage der Benutzbarkeit und Nachvollziehbarkeit. Für den Digitalen Wahlstift sollte beides gegeben sein, da der Klartextstimmzettelbeleg vom Wähler selbst erzeugt wird, indem er seine Stimme auf dem perforierten Papierstimmzettel abgibt. Die Benutzbarkeit der beiden anderen vorgestellten Ansätze sollte prinzi-

¹⁹ Volkamer/Budurushi/Demirel, Vote casting device with VV-SV-PAT for elections with complicated ballot papers, in: REVOTE 2011, 1-8.

²⁰ Andere Systeme speichern die Klartextstimme zusätzlich auf einem RFID Chip, wie etwa das argentinische System Vot.ar, siehe <http://www.vot-ar.com.ar/en/system-votation/>.

²¹ Arzt-Mergemeier/Beiss/Steffens, The Digital Voting Pen at Hamburg Elections 2008, in: VOTE-ID 2007, S. 88-98.

²² <http://www.avantetech.com/products/elections/dre/>.

²³ Volkamer/Budurushi/Demirel, Vote casting device with VV-SV-PAT for elections with complicated ballot papers, in: REVOTE 2011, 1-8.

²⁴ <http://www.hamburg.de/image/103302/digitaler-stift-400x518.jpg>.

piell ebenfalls gegeben sein, da der Wähler den Inhalt des Ausdrucks vor der eigentlichen Stimmabgabe lesen und überprüfen sowie bei der Auszählung anwesend sein kann.

Allerdings weisen einige der in den U.S.A. eingesetzten VV-PATs Mängel hinsichtlich der Benutzbarkeit auf, da der Ausdruck zu klein und unübersichtlich ist.²⁵ Insoweit sind in jedem Fall Benutzerstudien erforderlich, um dies abschließend für die jeweilige Umsetzung zu überprüfen. Hinsichtlich der Nachvollziehbarkeit ist festzustellen, dass diese für die Phasen *recorded as cast* und *tallied as recorded* analog zum traditionellen Papierwahlssystem gegeben ist. Mit Blick auf den ersten Überprüfungsschritt, *cast as intended*, ist unter Umständen Aufklärungsarbeit erforderlich. Dem Wähler muss verdeutlicht werden, dass er einer korrekten Bildschirmanzeige nicht ohne weiteres vertrauen darf und die Korrektheit des Stimmzettelbelegs selber überprüfen muss, da die hierauf befindliche Information in die Ergebnisermittlung einfließt.

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

4 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, das heißt, 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.

Da der Stimmzettelbeleg nur die kodierte Stimme darstellt, ist es dem Wähler möglich, seinen Beleg nach der Stimmabgabe mit nach Hause zu nehmen. Auf diese Weise kann er den zweiten Schritt der Überprüfbarkeit, *recorded as cast*, zeit- und ortsunabhängig durchführen. 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 sogenannte Web Bulletin Board) und dort alle kodierten Stimmzettelbelege angezeigt werden sowie nach einzelnen (insbesondere dem eigenen) gesucht werden kann. Da die Überprüfung, ob alle in der Urne gespeicherten Stimmen korrekt ausgezählt werden (*tallied as recorded*), von zu Hause aus durchgeführt werden kann, wird dem Wähler hier eine Überprüfungsmöglichkeit geboten, die nicht verlangt, dass er den ganzen Tag im Wahlraum verbleibt und sowohl die Wahlhandlung als auch die Ergebnisberechnung überwacht. Dies ist insofern von Interesse, als heute nur sehr wenige Menschen vom Öffentlichkeitsgrundsatz Gebrauch machen, da der zeitliche Aufwand hier zu groß ist.

Nachfolgend wird untersucht, ob kodierte Stimmzettelbelege ein zulässiges Instrument zur Umsetzung der Öffentlichkeit der Wahl sein können, auch wenn diese Form nicht explizit im Urteil des Bundesverfassungsgerichts genannt wurde. Danach werden unterschiedliche Ansätze, die kodierte Stimmzettelbelege zur Erfüllung der Öffentlichkeit der Wahl verwenden, beschrieben und nach den in Kapitel zwei definierten technischen Kriterien analysiert.

²⁵ Pilot Project Report, 2006 Georgia Accuracy in Elections Act, siehe <http://sos.georgia.gov/elections/VVPATreport.pdf>.

4.1 Verfassungsrechtliche Zulässigkeit von kodierten Stimmzettelbelegen

Kodierte Stimmzettelbelege werden unter Einsatz von Kryptografie erzeugt. Demnach ist die Durchführung einzelner Überprüfungsschritte nur mit Hilfe von (unabhängig vom eigentlichen elektronischen Wahlsystem) speziell entwickelten Hilfsprogrammen²⁶ möglich. Insoweit stellt sich für parlamentarische Wahlen die Frage nach der generellen Zulässigkeit kryptografischer Verfahren und der Verwendung entsprechender Hilfsprogramme bei Durchführung der Überprüfungsschritte. Das Wahlcomputerurteil sagt hierüber nichts aus. Dabei hat das Bundesverfassungsgericht auch keine ablehnende Haltung gegenüber entsprechenden Verfahren eingenommen oder diese gar als ungeeignet zurückgewiesen.

Da der Grundsatz der Öffentlichkeit der Wahl jedoch verlangt, dass die wesentlichen Schritte der Wahlhandlung und Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können, 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.²⁷ Insoweit verlangt das Bundesverfassungsgericht 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 Grundgesetzes, 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.²⁸ Insoweit ist nicht nur auf den Einzelnen, sondern auch auf die Gemeinschaft abzustellen. Dabei ist ferner zu bedenken, welchen Einzug die Technik in den vergangenen Jahrzehnten in das Leben des Einzelnen genommen hat. So wird unser Alltag, unabhängig davon, ob es sich um das Berufs- oder Privatleben handelt, immer mehr von Technik durchdrungen. Beispielhaft sei hier auch auf die elektronische Steuererklärung hingewiesen.²⁹ 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 (auch ohne Sachkenntnis) ist, bleibt offen und kann auch nur am konkreten technischen System entschieden werden. Hierzu werden in einem späteren Abschnitt bekannte elektronische Wahlsysteme, die auf kodierten Stimmzettelbelegen und damit auf Kryptografie aufbauen und Pro-

²⁶ Diese Programme werden von verschiedenen Anbietern bereitgestellt und der Wähler kann selbst entscheiden, welches Programm er verwenden möchte. Es ist auch möglich, unterschiedliche Programme zu verwenden.

²⁷ BVerfGE 123, 39 (73).

²⁸ BVerfGE 4, 7 (15 f.).

²⁹ <https://www.elster.de/>.

gramme zur Überprüfung benötigen, vorgestellt und analysiert. Aus juristischer Sicht ist aber zunächst die Frage, ob kodierte Stimmzettelbelege nach der Stimmabgabe vom jeweiligen Wähler mit nach Hause genommen werden dürfen, relevant.

Kodierte Stimmzettelbelege müssen nicht zwingend im Wahlraum verbleiben, da sie 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 Wahlheimnisses sichergestellt, können die Stimmzettelbelege vom Wähler mitgenommen werden, damit dieser den zweiten Schritt der Überprüfbarkeit, *recorded as cast*, zeit- und ortsunabhängig durchführen kann. Anders als bei der traditionellen Papierwahl kann ein Wähler dann aber nur noch seine eigene Stimme überprüfen. Da das Bundesverfassungsgericht fordert, dass „die Stimmen nach der Stimmabgabe nicht ausschließlich auf einem elektronischen Speicher abgelegt werden“³⁰ dürfen, muss eine Papierüberprüfungsmöglichkeit aller Stimmen auf jeden Fall im Wahlraum verbleiben. Insofern müssen die in der Literatur vorgeschlagenen Umsetzungen dahingehend erweitert werden, dass Wähler nur eine Kopie des eigenen Stimmzettelbelegs mit nach Hause nehmen können. Der Originalstimmzettelbeleg muss im Wahlraum bleiben, um eine Überprüfung der korrekten Speicherung aller Stimmen zu ermöglichen.

Die Mitnahme eines Stimmzettelbelegs birgt allerdings die Gefahr eines psychologischen, auf den Grundsatz der freien Wahl bezogenen Angriffs. So könnte ein Angreifer fälschlicherweise behaupten, die Stimme des Wählers aus dem Beleg ableiten zu können. Dieser Situation könnte durch Mitnahme eines beliebigen Stimmzettelbelegs begegnet werden. Ein entsprechendes Verfahren wird in der technischen Literatur bereits diskutiert.³¹ 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,³² dass Wähler mehrere Kopien von Stimmzettelbelegen inklusive des eigenen Belegs mit nach Hause nehmen können. Dabei wäre sichergestellt, dass jeder Wähler auch seine eigene Stimme überprüfen kann. Ob die Wähler aber davon überzeugt werden können, dass eine Rückführung des kodierten Stimmzettelbelegs und damit der kodierten Stimme auf die Klartextstimme nicht möglich ist, bleibt in entsprechenden Benutzerstudien zu untersuchen und kann daher hier nicht abschließend beurteilt werden.

4.2 Verifizierbarkeit durch kodierte Stimmzettelbelege

Nachfolgend werden die bekanntesten elektronischen Wahlsysteme beschrieben, bei denen kodierte Stimmzettelbelege zum Einsatz kommen. Die Systeme werden hierzu in zwei Gruppen unterteilt: Systeme, bei denen der kodierte Stimmzettelbeleg die Auswahl des Wählers mit einem kryptografischen Verschlüsselungsverfahren kodiert³³ und Systeme, bei denen der kodierte Stimmzettelbeleg auf die geheime zufällige Permutation der Kandidaten auf dem vom Wähler verwendeten Stimmzettel³⁴ verweist.

³⁰ BVerfGE 123, 39 (73).

³¹ *Araújo/Custódio/van de Graaf*, A Verifiable Voting Protocol Based on Farnel, in: *Towards Trustworthy Elections* 2010, 274-288.

³² Bei diesem Ansatz ist in Abhängigkeit des definierten Angreifermodells sicherzustellen (z.B. wenn Mitglieder des Wahlvorstandes Teil des Angreifermodells sind), dass der Wähler den eigenen Stimmzettelbeleg bekommt.

³³ Diese Funktion ist probabilistisch. Das bedeutet, dass eine Zufallszahl mit in die Funktion einfließt. Dadurch unterscheiden sich die Chiffretexte zweier Stimmen, auch wenn die Klartextstimme identisch ist.

³⁴ Die Permutation der Kandidaten auf dem Stimmzettel wird geheim gehalten.

4.2.1 Verschlüsselte Stimmzettelbelege

Bei Wahlsystemen, 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.³⁵ Um die Handhabung für den Wähler zu erleichtern, wird dabei regelmäßig nicht der gesamte Schlüsseltext, sondern nur dessen Fingerabdruck (kryptografischer Hashwert) abgedruckt³⁶ oder der Schlüsseltext wird in einem QR-Code kodiert.³⁷ Nachdem der Stimmzettelbeleg gedruckt wurde, kann der Wähler entweder seine Auswahl bestätigen oder überprüfen, ob das Wahlgerät seine Auswahl korrekt erfasst hat, das heißt, 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.³⁸ Anhand der Kopie des entsprechenden Stimmzettelbelegs kann der Wähler 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 Pseudonym³⁹ angezeigt wird, kann der Wähler alternativ auch nach diesen Informationen suchen und überprüfen, ob seiner Identität der Chiffretext auf seinem Stimmzettelbeleg zugeordnet ist.

Wenn der Wähler sich entscheidet, den Stimmzettelbeleg nicht direkt zu bestätigen, sondern erst zu überprüfen, ob die richtige Stimme verschlüsselt wurde, verwendet er ein entsprechendes Prüfprogramm, das ihm bereitgestellt wird. Dieses bekommt alle zur Überprüfung erforderlichen Daten und zeigt dem Wähler die Stimme im Klartext an. Der Wähler kann dann überprüfen, ob das die Stimme war, die er zuvor am Wahlgerät abgegeben hat. Um das Wahlgeheimnis sicherstellen zu können, ist es allerdings erforderlich, die Stimme erneut mit dem Wahlgerät zu verschlüsseln und einen neuen Stimmzettelbeleg zu erzeugen. Sodann kann der Wähler entscheiden, ob er diesen bestätigen oder eine weitere Überprüfung durchführen möchte.

Dieser Mechanismus ermöglicht demnach 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

³⁵ Chaum, Secret-Ballot Receipts: True Voter-Verifiable Elections, in: Security and Privacy 2004, 38-47.

³⁶ Benaloh, Simple Verifiable Elections, in: EVT 2006.

³⁷ Ben-Nun/Fahri/Llewellyn/Riva/Rosen/Ta-Shma/Wikström, A New Implementation of a Dual (Paper and Cryptographic) Voting System, in: Electronic Voting 2012, 315-329; Vegas, The New Belgian E-voting System, in: Electronic Voting 2012, 199-211.

³⁸ Um die Integrität des Web Bulletin Boards (der elektronischen Urne) zu gewährleisten, können beispielsweise zu jeder Zeit Abzüge hiervon durch andere vertrauenswürdige Instanzen (z.B. Wahlorgane oder das Bundesamt für Sicherheit in der Informationstechnik) angefertigt und zur gegenseitigen Kontrolle verwendet werden. Entsprechende Abzüge können nach einer bestimmten Anzahl abgegebener Stimmen oder nach Ablauf einer bestimmten Zeitperiode, z.B. alle zehn Minuten, angefertigt werden.

³⁹ Dies ist erforderlich, um sogenannte Clash-Attacks zu verhindern. Siehe hierzu: Kusters/Truderung/Vogt, Clash Attacks on the Verifiability of E-Voting Systems, in: Security and Privacy 2012, 395-409.

Wahlgerät mit sehr hoher Wahrscheinlichkeit korrekt verhalten. Das Wahlgerät ist quasi “verpflichtet”, die Auswahl des Wählers korrekt zu erfassen und zu verschlüsseln, da die Manipulation sonst bei einer Überprüfung des Stimmzettels entdeckt werden würde. Die Wahrscheinlichkeit für den Wähler, eine Manipulation seines eigentlichen Stimmzettelbelegs aufzudecken, steigt mit der Anzahl der durchgeführten Überprüfungen. Durch die Abgabe von Teststimmen kann der Wähler “begründetes Vertrauen” in die korrekte Anzeige seiner tatsächlich abgegebenen Stimme auf dem Web Bulletin Board erlangen. Ob dies ausreicht, um den Grundsatz der Öffentlichkeit der Wahl hinreichend zu gewährleisten, kann letztlich nur nach einer Gegenüberstellung mit den Vorteilen für die beiden anderen Schritte (*recorded as cast* und *tallied as recorded*) beantwortet werden.

Der dritte Schritt der Überprüfung der eigenen Wahlhandlung, *tallied as recorded*, kann mit Hilfe des Stimmzettelbelegs nicht überprüft werden. Die beschriebenen 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.

Abschließend bleibt festzuhalten, dass sowohl die *recorded as cast*- als auch die *tallied as recorded* -Verifizierbarkeit bei diesen Verfahren gegeben ist. Ob die Stimme wie beabsichtigt vom System aufgenommen worden ist (*cast as intended*), kann nicht im vollen Umfang überprüft werden, da der Wähler die Stimme, die er letztendlich abgibt, nicht einsehen kann. Daher können Zweifel bestehen bleiben, ob das Wahlgerät nicht doch einen anderen als den angeklickten Kandidaten verschlüsselt und gespeichert und auch für diesen einen Chiffretext gedruckt hat.

Die Benutzbarkeit hängt stark von der Umsetzung ab. Da bislang keiner der vorgestellten Ansätze einer Benutzerstudie unterzogen oder im Rahmen einer Wahl im Wahlraum untersucht worden ist, kann dies hier nicht abschließend entschieden werden. Offen bleibt auch, ob man die Nachvollziehbarkeit erreicht, das heißt die Funktion der einzelnen Programme sowie der möglichen Ausgaben verständlich kommunizieren kann. Hier sind entsprechende Benutzerstudien erforderlich.

Wegen der geforderten Speicherung auf Papier bleibt festzustellen, dass nur das Abdrucken eines reinen Hashwertes nicht zulässig ist. Dieser mag – wie der RFID-Chip oder der QR-Code – aus anderen Gründen enthalten sein (beispielsweise um eine Überprüfung zu erleichtern). Da die Stimmen aber nicht ausschließlich auf einem elektronischen Speicher abgelegt werden dürfen, muss daneben der gesamte Chiffretext abgedruckt sein.

4.2.2 Permutation der Kandidatenreihenfolge

Diese Wahlsysteme 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.⁴⁰ Auf dem anderen Teil wird die Auswahl eines Kandidaten durch manuelles Markieren mit einem Stift getätigt. Dieser Teil enthält außerdem einen verschlüsselten Wert.⁴¹ Der Klar-

⁴⁰ Wiederholungen der Permutation sind jedoch unvermeidbar, da es in Abhängigkeit von der Anzahl der Wahlbewerber nur eine feste Anzahl an Optionen gibt.

⁴¹ Hier ist anzumerken, dass in der Regel nicht der komplette Chiffretext abgebildet ist, sondern – analog zu 4.3.1 – nur ein Hashwert oder ein Verweis zu dem vollständig verschlüsselten Wert. Dies wäre aber entspre-

text hinter diesem verschlüsselten Wert definiert die Kandidatenreihenfolge auf diesem Stimmzettel.

Das bekannteste Wahlsystem dieser Art ist Prêt à Voter.⁴² Ähnlich arbeitet auch das System Scantegrity.⁴³ Abbildung 4 zeigt beispielhaft einen Prêt à Voter-Stimmzettel.

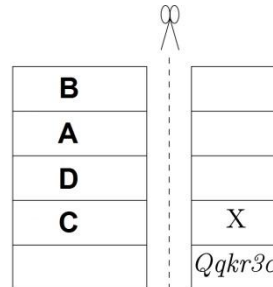


Abb. 4: Prêt à Voter Stimmzettel.⁴⁴

Nach der Stimmabgabe trennt der Wähler noch in der Wahlkabine die beiden Teile voneinander. Der Teil mit der Kandidatenreihenfolge (bei Prêt à Voter der linke Teil) wird vernichtet und der rechte 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 rechten Teils, das heißt des kodierten Stimmzettelbelegs, mit nach Hause nehmen, um zu überprüfen, ob seine Stimme in der Urne (auf dem Web Bulletin Board) gespeichert ist (*recorded as cast*). Dazu besucht er auch hier die entsprechende Wahlwebseite und sucht nach seinem auf dem Stimmzettelbeleg abgedruckten verschlüsselten Wert. Da auf dem Web Bulletin Board zu jedem Wähler ebenfalls dessen Identität oder ein Pseudonym angezeigt wird, kann der Wähler alternativ auch nach diesen Informationen suchen und 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. So könnte es sein, dass die Klartextpermutation des Stimmzettels aus Abbildung 4 an vierter Stelle nicht C, sondern D vorsieht. Demnach wäre hier nicht der Wählerwille, sondern der Wille des Angreifers kodiert. Um dieser Problematik zu begegnen, werden bei entsprechenden Systemen mehr Papierstimmzettel erzeugt, als erforderlich sind. Hiervon wird vor der Wahl eine zufällig ausgewählte Anzahl kontrolliert. Dabei 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.

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. Eine unmittelbare Überprüfung kann sich ebenfalls nur

chend der Diskussion in 4.3.1 über Stimmzettelbelege, die nur den Hashwert enthalten, nicht zulässig. Daher ist hier davon auszugehen, dass der vollständig verschlüsselte Text abgebildet ist, auch wenn dies dazu führt, dass mehr Informationen abgedruckt werden als das in Abbildung 4 der Fall ist.

⁴² Chaum/Ryan/Schneider, A Practical Voter-Verifiable Election Scheme, in: ESORICS 2005, 118-139.

⁴³ Chaum/Carback/Clark/Essex/Popoveniuc/Rivest/Ryan/Shen/Sherman, Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes, in: EVT 2008, 1-13.

⁴⁴ Siehe hierzu: Chaum/Ryan/Schneider, A Practical Voter-Verifiable Election Scheme, in: ESORICS 2005, 118-139.

auf Teststimmen beziehen. Dieses Verfahren bietet dennoch eine hohe Sicherheit, wenn eine genügend große Anzahl an zufällig ausgewählten Stimmzetteln überprüft wird. Da der Druckdienstleister, der die Stimmzettel erzeugt, nicht weiß, welche Stimmzettel überprüft werden und welche nicht, wird er sich mit sehr hoher Wahrscheinlichkeit korrekt verhalten. Er ist ebenfalls quasi “verpflichtet”, die Stimmzettel korrekt zu erzeugen. Würde die verschlüsselte Permutation nicht zu der Klartextpermutation passen, so würde die Manipulation bei der Überprüfung der Stimmzettel entdeckt werden. Die Wahrscheinlichkeit einer solchen Entdeckung hängt entscheidend von der Menge und der Zufälligkeit der überprüften Stimmzettel ab. Am Rande sei angemerkt, dass hier, anders als bei dem Verfahren, das in Kapitel 4.2.1 diskutiert wurde, *cast as intended* nur dann gegeben ist, wenn der Wähler den Prozess der Überprüfung der Korrektheit der erstellten Stimmzettel im Vorfeld der eigentlich Wahl nicht scheut und ununterbrochen beobachtet, insbesondere, dass die Auswahl zufällig erfolgt. Ob dies ausreicht kann auch bei diesem Ansatz letztlich nur infolge einer Gegenüberstellung von Vor- und Nachteilen für die Verwirklichung des Grundsatzes der Öffentlichkeit der Wahl entschieden werden.

Der dritte Schritt der Überprüfung der eigenen Wahlhandlung, *tallied as recorded*, kann mit Hilfe dieser Stimmzettelbelege nicht überprüft werden. Die beschriebenen elektronischen Wahlsysteme Prêt à Voter und Scantegrity ermöglichen aber durch die Bereitstellung von mathematischen Beweisen die Auszählung nachzurechnen und das Ergebnis nachzuvollziehen. Hierzu müssten analog zu den Verfahren in Kapitel 4.3.1 entsprechende Programme von unabhängigen Institutionen bereitgestellt werden. Unter diesen Umständen wäre *tallied as recorded* gegeben.

Abschließend bleibt festzuhalten, dass sowohl die *recorded as cast*- als auch die *tallied as recorded*-Verifizierbarkeit bei diesem Verfahren gegeben ist und eine Überprüfung von einem beliebigen Ort zu einer beliebigen Zeit durchgeführt werden kann. Für die Durchführung müssen entsprechende Programme bereitgestellt werden. Allerdings ist die Durchführung der *cast as intended*-Verifizierbarkeit nicht im vollen Umfang möglich, da der Stimmzettel, den der Wähler für seine Stimmabgabe nutzt, nicht hinsichtlich der korrekt verschlüsselten Permutation überprüft werden kann. Insofern könnten Zweifel bestehen bleiben, ob der Druckdienstleister nicht doch manipulierte Stimmzettel generiert hat, die eben nicht von der Überprüfung betroffen waren und nun von einzelnen Wählern verwendet werden. In der Praxis ist eine Aufdeckung bei diesem Ansatz allerdings eher gegeben als bei dem vorherigen, weil es dort dem Wähler überlassen ist, zu überprüfen oder nicht, während hier die Überprüfung Teil des Prozesses ist.

Die Benutzbarkeit der *cast as intended*-Verifizierbarkeit ist gegeben, da diese in der Öffentlichkeit durchgeführt wird. Die Benutzbarkeit der anderen beiden Verifizierungen hängt stark von der Umsetzung ab. Da diese Systeme zwar implementiert und teilweise auch zu kleinen Wahlen⁴⁵ eingesetzt, aber bislang keine umfassenden Benutzerstudien oder Wählerbefragungen durchgeführt wurden, bleibt die Benutzbarkeit offen. Dies gilt auch für die Nachvollziehbarkeit der *recorded as cast*- und *cast as intended*-Verifizierbarkeit, also für die Frage, ob man die Funktion der einzelnen Programme sowie der möglichen Ausgaben verständlich kommunizieren kann. Hier sind entsprechende Benutzerstudien erforderlich.

Wegen der geforderten Speicherung auf Papier bleibt festzustellen, dass nur das Abdrucken eines reinen Hashwertes oder ähnlichem – wie vorab – nicht zulässig ist. Dieser mag aus an-

⁴⁵ Bismark/Heather/Peel/Schneider/Xia/Ryan, Experiences Gained from the first Prêt à Voter Implementation, in: REVOTE 2009, 19-28; <http://www.scantegrity.org/elections.php>.

deren Gründen, etwa der Benutzbarkeit der *recorded as cast*-Verifizierbarkeit enthalten sein. Wichtig ist aber, dass zusätzlich der vollständige Chiffretext der Permutation abgedruckt wird.

5 Fazit

Wie sollen elektronische Wahlen einerseits das Wahlgeheimnis gewährleisten und andererseits eine sachkenntnisunabhängige Überprüfbarkeit der Wahlhandlung und Ergebnisermittlung ermöglichen? Der Beitrag hinterfragt die Tauglichkeit solcher Wahlsysteme, die diesen Anforderungen mithilfe von Stimmzettelbelegen begegnen. Die hierdurch gewährleistete Überprüfbarkeit der Wahlhandlung entspricht aber nur dem Grundsatz der Öffentlichkeit der Wahl, wenn sie auch benutzbar und nachvollziehbar gestaltet ist. Dabei sind Stimmzettelbelege der Klartextstimme ebenso denkbar wie solche, die die Stimme des Wählers in kodierter Form wiedergeben. Zahlreiche Systeme ermöglichen auf diese Weise die Verifizierbarkeit der eigenen Wahlhandlung und damit die Überprüfbarkeit der Frage, ob die Stimme wie beabsichtigt vom Wahlsystem erfasst (*cast as intended*) und im Folgenden unverändert im System gespeichert wurde (*recorded as cast*). 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 Verbesserung und Evaluation der Benutzbarkeit und Nachvollziehbarkeit kodierter Stimmzettelbelege und hinsichtlich der auf mathematischen Beweisen beruhenden Verfahren für die Verifizierbarkeit der Ergebnisermittlung (*tallied as recorded*). Der letztlich erreichte Grad an Benutzbarkeit und Nachvollziehbarkeit muss in Bezug gesetzt werden zur Stärkung des Öffentlichkeitsgrundsatzes gegenüber dem einzelnen Wähler, da dieser anders als bei der Generierung von Klartextstimmzettelbelegen nicht den ganzen Tag im Wahlraum verbleiben muss, sondern die *recorded as cast*- und *tallied as recorded*-Verifizierbarkeit von überall zu jeder Zeit über einen Web Service durchführen kann. Hierzu darf er eine Kopie des Stimmzettelbelegs mit nach Hause nehmen, solange der Originalbeleg im Wahlraum verbleibt. Dies ist angesichts der Forderung, eine von der elektronischen Speicherung der Stimmen losgelöste Überprüfungsmöglichkeit bereitzuhalten, erforderlich. Um aber dem Wahlvorstand auch eine *recorded as cast*- und *tallied as recorded*-Verifizierbarkeit aller abgegebenen Stimmen zu ermöglichen, darf nicht nur der reine Hashwert, sondern es muss der gesamte Chiffretext auf dem Stimmzettelbeleg abgedruckt sein. Das zusätzliche Abdrucken eines Hashwertes oder QR-Codes ist hingegen zulässig.

Insgesamt bleibt festzuhalten, dass weitere Forschung im Kontext verifizierbarer Wahlen notwendig und geboten ist, da entsprechende Verfahren großes Potential haben, die Überprüfbarkeit der eigenen Wahlhandlung benutzbar und nachvollziehbar zu offerieren. Dabei können die Überlegungen ebenso für gegenwärtig praktizierte Wahlen in nicht parlamentarischen Bereichen, beispielsweise in Vereinen oder an Universitäten, herangezogen werden.