



»Aber Kinder, wat macht ihr denn da?« –
»Wir spielen Reichstagswahl, Mama!«

Intransparent und unkontrollierbar

Wahlcomputer auf dem verfassungsrechtlichen Prüfstand

Seit 1961 können Wahlgeräte bei Wahlen in der Bundesrepublik eingesetzt werden. Lange Zeit handelte es sich dabei um mechanisch oder elektromechanisch arbeitende Maschinen. 1999 fanden dann zum ersten Mal Wahlcomputer Verwendung, rechtlich gefasst als »rechnergesteuerte Wahlgeräte«. Spätestens seit den US-Präsidentenwahlen 2000, bei denen das Versagen der Technik George Bush die Präsidentschaft einbrachte, stehen Wahlgeräte und Wahlcomputer in der öffentlichen Kritik. VON JÖRG POHLE

Aktuell steht das Bundesverfassungsgericht (BVerfG) vor einer weitreichenden Entscheidung über die Zukunft der Wahlcomputer in der BRD, nachdem die Bundestagswahl 2005 wegen der Verwendung ebensolcher Geräte angefochten wurde. Dieser Wahleinspruch wurde vom zunächst zuständigen Bundestag erwartungsgemäß und ohne inhaltliche Prüfung als »offensichtlich unbegründet«¹ zurückgewiesen. Damit wurde gleichzeitig der Weg zu einer Wahlprüfungsbeschwerde beim BVerfG freigemacht. Bisher zumindest hat es sich das BVerfG nicht ganz so einfach gemacht wie der Bundestag. Stattdessen hat es im Frühjahr 2007 eine Vielzahl schriftlicher Stellungnahmen von Betroffenen und

Interessierten eingefordert. Zu diesen gehörten das Bundesministerium des Innern (BMI) und die Physikalisch-Technische Bundesanstalt (PTB)² ebenso wie der Chaos Computer Club (CCC), einer der profiliertesten Kritiker des Wahlcomputereinsatzes. Nachdem Ende Oktober 2008 vor dem BVerfG eine öffentliche Anhörung stattfand, ist eine Entscheidung in der Sache bis spätestens Ende Januar 2009 zu erwarten.

Geschichte

Bereits die erste Verordnung des BMI zum Einsatz von Wahlgeräten von 1961 war ganz auf ein bereits existierendes Wahlgerätemodell zugeschnitten und

¹ Eine Darstellung der Kritik an dieser grundsätzlichen Ignoranz des Bundestages gegenüber Wahlfehlern findet sich bei Achterberg/Schulte, in: v. Mangoldt/Klein/Starck, GG II, Art. 41, Rn. 10.

² Die PTB ist für die Baumusterprüfung der Wahlgeräte und Wahlcomputer vor deren Zulassung verantwortlich.

überführte dabei dessen technische Eigenschaften in rechtliche Anforderungen, die für Bauartzulassung zu erfüllen sind. Gleiches geschah erneut 1999. Auch hier existierte vor der Novellierung der Bundeswahlgeräteverordnung (BWahlGV) ein fertiges Wahlcomputermodell, das sowohl technische Grundlage für die Festsetzung von Anforderungen als auch erster Prüfgegenstand nach der neuen Fassung war. Die PTB, die maßgeblich an der Formulierung beteiligt war, sieht darin bis heute kein Problem.³ Dabei ist offensichtlich, dass es für einen Prüfgegenstand fast unmöglich ist, an Anforderungen zu scheitern, die nach seinem Bilde geformt wurden.

Zu einem breiten Einsatz von mechanischen und elektromechanischen Wahlgeräten ist es dennoch nie gekommen, zu fehler- und ausfallanfällig waren die Geräte, zu teuer Kauf und Unterhalt, zu beschränkt ihre Einsatzmöglichkeiten. Erst den Wahlcomputern – alle aus dem Haus der niederländischen Firma Nedap – blieb ein größerer Erfolg vorbehalten. Ihren ersten Einsatz erlebten sie zur Kommunalwahl in Köln 1999, ihren vorerst letzten zur Kommunalwahl in Brandenburg im September 2008. Nach offizieller Aussage sind bisher weder bei Verwendung von Wahlgeräten noch von Wahlcomputern »größere« Probleme aufgetreten. Dass diese Aussage weder bewiesen wurde noch überhaupt beweisbar ist, wird dabei unter den Tisch fallen gelassen.

Im Folgenden sollen einige rechtliche und technische Probleme mit den Nedap-Geräten im Besonderen und mit Wahlcomputern im Allgemeinen näher beleuchtet werden.

Die Praxis der Ignoranz

Derzeit sind etwa ein halbes Dutzend unterschiedlicher Modelle von Nedap-Wahlcomputern für Bundestagswahlen geprüft und zugelassen. Rechtliche Bedingung für eine erfolgreiche Baumusterprüfung ist insbesondere die Erfüllung der technischen Anforderungen, wie sie in Anlage 1 zu § 2 BWahlGV niedergelegt sind. Diese »Richtlinien für die Bauart von Wahlgeräten« enthalten dabei etwa die Maßgabe, dass Wahlcomputer eine »eindeutige Identifikation der installierten Software« zu ermöglichen haben. Aus rechtlicher Sicht ist der Inhalt dieser Anforderung evident: Der Wahlcomputer hat seine Identität nicht nur zu *behaupten*, sondern zu *beweisen*. Dass dennoch Wahlcomputermodelle eine Bauartzulassung erhielten, die diese Anforderung nicht erfüllten, erklärte das BMI in einer von der

PTB an den Wahlprüfungsausschuss gerichteten Stellungnahme⁴ mit einer begrifflichen Trennung zwischen »Identifikation« und »Authentifizierung«. Demnach erfülle bereits die Ausgabe von Prüfsummen⁵ durch die Wahlcomputer die Anforderung zur Identifikation, eine darüber hinausgehende Authentifizierung sei nicht erforderlich. Diese Ansicht entspreche dabei der Verwendung der Begriffe in der Informatik. Dies ist jedoch nur teilweise korrekt.⁶ Richtig muss hier vielmehr auf die *Eindeutigkeit* der Identifikation abgestellt werden, wie sie in der BWahlGV gefordert wird. Unter einer solchen »eindeutigen Identifikation« kann auch aus Sicht der Informatik nur ein Beweis verstanden werden.

Hilfsweise verweisen PTB und BMI auf das Prinzip der »sicheren Lagerung« von Wahlcomputern zwischen den Wahlen, wodurch es ausgeschlossen sei, dass Unbefugte Zugriff erhalten und Manipulationen durchführen könnten. Die Realität sieht allerdings, wie etwa die Wahlbeobachtung des CCC in Hessen im Januar 2008⁷ gezeigt hat, völlig anders aus.

»Sichere« Lagerung

Nachdem die ersten Designprobleme und daraus folgende Manipulationsmöglichkeiten aufgezeigt wurden, mussten PTB und BMI ihre Begründungen für die Sicherheit der eingesetzten Wahlcomputer neu formulieren. Während bisher als allgemein akzeptiert galt, dass die Wahlcomputer selbst manipulationssicher konstruiert sein müssen, wurde nun auf »organisatorische Maßnahmen« verwiesen, die diese Sicherheit garantieren sollen. Eine solche Maßnahme sei, so wiederholen die Verantwortlichen seitdem mantrahaft, die Lagerung der Wahlcomputer in »geschützten Umgebungen«. In solchen Umgebungen könnten Angriffe auf die Sicherheit der Wahlcomputer effektiv verhindert werden, insbesondere würden restriktive Zugangsmechanismen und -kontrollen Unbefugte fernhalten können. Eine solche »sichere« Lagerung in »geschützten Umgebungen« ist bis heute nicht gesetzlich geregelt und auch die PTB hat diese Anforderung erst im Oktober 2007 in ihre Prüfberichte zur Baumusterprüfung aufgenommen. Es kann deshalb nicht überraschen, dass der Begriff der »geschützten Umgebung« in der Praxis offenbar weit ausgelegt wird.

Im hessischen Niederrhein wurden die Wahlcomputer in der Nacht vor der Wahl in den Privatwohnungen von Lokalpolitikern gelagert mit der Begründung, dies sei »gängige Praxis«. Weder die

3 Sietmann, Richard: »Eine neue Situation«, in: *c't* – magazin für computer technik, 24 (2006), S. 72.

4 www.ulrichwiesner.de/stellungnahme_BMI.html (Abruf: 12. 12. 2008).

5 Prüfsummen sind vergleichbar mit Quersummen bei natürlichen Zahlen. Sie dienen der Erkennung von Fehlern, etwa bei einer Datenübertragung. Eine Maßnahme zur Erhöhung der Sicherheit können sie nicht darstellen, weil sie vom Wahlcomputer selbst berechnet und ausgegeben werden.

6 In der Informatik werden Identifikation (Behauptung einer Identität) und Authentifizierung (Beweis einer Behauptung) getrennt betrachtet, weil in manchen Zusammenhängen nur eines der Prinzipien Anwendung finden soll: In Internet-Foren etwa reicht oftmals eine Identifizierbarkeit der einzelnen AutorInnen, und die Authentifizierung kann sich auch auf andere Merkmale beziehen, etwa den Besitz eines bestimmten Schlüssels.

7 ccc.de/updates/2008/wahlbeobachtungen-hessen (Abruf: 12. 12. 2008).



InnentäterInnen

lokalen Verantwortlichen noch der hessische Landeswahlleiter konnten darin ein Problem erkennen. Bei der Kommunalwahl in Bayern im März 2008 wurden Computer zur Stimmzählung⁸ eingesetzt, die vorher von Privatpersonen, unter ihnen amtierende Stadträte, von zu Hause mitgebracht wurden. Vor der Kommunalwahl in Brandenburg – fast ein Jahr nach ihrer offiziellen »Einführung« – bestanden die »geschützten Umgebungen« aus unverschlossenen Hinterzimmern von als Wahllokalen benutzten Kindergärten und Schulen.

Als sicher sollen die »geschützten Umgebungen« dabei vor allem deshalb gelten, weil sie Unbefugte vom Zugriff auf Wahlcomputer abhalten würden. Dadurch würden Manipulationen gleichzeitig grundsätzlich verhindert. Dieser Schluss ist nur möglich, weil nach offizieller Einschätzung die Gefahr ausschließlich von Außenstehenden ausgehen soll.

Die oft wiederholte Behauptung,⁹ InnentäterInnen würden keine Gefahr für die Sicherheit von Wahlcomputern darstellen, lässt sich vor dem Hintergrund vergangener Wahlfälschungen nicht halten. So wurden etwa im Frühjahr 2002 in Dachau Wahlfälscher überführt, die eingestanden, bereits seit den 1980er Jahren Manipulationen durchzuführen. Dabei handelte es sich um Mitglieder des Stadtrats und Verwaltungsangehörige, die nach der derzeitigen Rechtslage legal Zugriff auf Wahlcomputer zwischen den Wahlen besitzen. Dass der Fall überhaupt öffentlich wurde, lag an der Entdeckung einer großen Menge ausgefüllter Stimmzettel auf der örtlichen Deponie. Und trotz der erdrückenden Beweise weigerte sich der CSU-geführte bayerische Landtag monatelang, das Ergebnis der gefälschten Kommunalwahl in Dachau für ungültig zu erklären. Auch 2008 wurde aus Bayern wieder ein Fall von Wahlfälschung bekannt: Ein SPD-Mitglied mani-

⁸ In Bayern werden keine Wahlcomputer verwendet, sondern mit Barcodes versehene Stimmzettel, die zur Auszählung mit Scannern eingelesen werden. Die Auszählung findet dann ausschließlich elektronisch statt.

⁹ Vgl etwa den bei der PTB für die Baumusterprüfung Verantwortlichen, Dieter Richter. Richter: Wahlgeräte in Deutschland: Eine Erwidern, Informatik Spektrum, Dezember 2007, S. 440.

pulierte das Stimmenergebnis in einem Wahllokal während der Auszählung zugunsten seiner Partei, unbemerkt von den anderen Mitgliedern des Wahlvorstandes. Die Manipulation fiel erst auf, als eine Bürgerinitiative das Wahlergebnis statistisch auswertete, dabei über signifikante Auffälligkeiten stolperte und eine Nachzählung erkämpfte.

Schwerwiegender als Fehler im praktischen Einsatz konkreter Wahlcomputermodelle wiegen allerdings fundamentale Probleme, die Wahlcomputern konstruktionsbedingt innewohnen. Sie haben modellunabhängig Auswirkungen auf Wahlen und stellen einen möglichen Einsatz von Wahlcomputern grundsätzlich verfassungsrechtlich infrage.

Öffentlichkeitsprinzip

Eines der wesentlichen Fundamente der politischen Entscheidungsfindung ist das aus dem demokratischen und dem republikanischen Prinzip folgende Öffentlichkeitsprinzip.¹⁰ Dieses Prinzip findet seinen Ausdruck etwa in § 31 Bundeswahlgesetz (BWahlG), der die Öffentlichkeit der Wahlhandlung fordert. Nach § 54 Bundeswahlordnung (BWahlO) erfolgen auch Ermittlung und Feststellung des Wahlergebnisses öffentlich. Die Durchsetzung dieses Prinzips dient dabei unter anderem der Verhinderung von Manipulationen des Wahlergebnisses durch Mitglieder der Wahlvorstände.¹¹ Für Wahlen unter Verwendung von Papierstimmzetteln lässt sich diese Vorgabe auch unschwer umsetzen. Nachdem der Wahlvorstand durch Vorzeigen beweist, dass die Wahlurne leer ist, wird diese verschlossen und versiegelt. Da die Wahlurne nicht in der Lage ist, eingeworfene Stimmzettel zu manipulieren, ist deren Integrität garantiert, solange die Wahlurne selbst nicht in ihrer Integrität beeinträchtigt wird. Eine solche Beeinträchtigung lässt sich ausschließen, wenn und solange die Wahlurne öffentlich einsehbar ist. Auch die Stimmzettel können sich nicht selbst manipulieren. Durch die Öffentlichkeit der Wahlhandlung lässt sich damit eine geschlossene Vertrauenskette vom Beginn der Wahlhandlung bis zum Ende der Stimmenauszählung bilden, sie garantiert damit die Integrität der abgegebenen Stimmen und die Manipulationsfreiheit des Wahlergebnisses insgesamt.

Eine solche Vertrauenskette existiert bei der Verwendung von Wahlcomputern explizit nicht. Der »Nachweis« der Nullstellung der Stimmzähler, der die anfängliche Leere von Wahlurnen entspricht, wird vom Wahlcomputer selbst erzeugt: Dieser gibt

einfach einen Kassenzettel mit einer aufgedruckten »0« aus. Die Nullstellung ist objektiv, also ohne Nutzung des Computers, nicht überprüfbar. Auch sonst handelt es sich bei Wahlcomputern um die Umsetzung einer sogenannten Black-Box-Technologie: Weder die Dateneingabe noch die Datenspeicherung oder -verarbeitung findet im Bereich des von Menschen Wahrnehmbaren statt, Einblicke in die konkrete Arbeit sind nicht möglich. Der Ablauf der Stimmenauszählung bleibt allen Beobachtenden verborgen. Zwar können sie offenkundige Manipulationen durch Mitglieder der Wahlvorstände oder Dritte immer noch entdecken, zumindest wenn diese während der Wahlhandlung oder der Auszählung stattfinden, aber an zwei Stellen ist die Vertrauenskette unterbrochen: Erstens gibt es keinen »Vertrauensanker«, an dem die Kette beginnt. Die Wahlhandlung beginnt eben gerade nicht mit leeren Stimmzetteln und einer leeren Wahlurne, deren initiale Zustände durch eigene Beobachtung nachvollzogen werden können. Die Vertrauenskette hängt hier also förmlich in der Luft.

Zweitens sind die einzelnen Kettenglieder und ihre Verbindung untereinander nicht »atomar«¹² und/oder nicht beobachtbar. Während etwa der Übergang eines Stimmzettels vom Einwurf in die Wahlurne bis zu seiner Entnahme nach Schließung der Wahlhandlung atomar ist und dabei insbesondere nicht durch eine Manipulation unterbrochen werden kann, weil diese beobachtbar ist, fehlt es bei der Verarbeitung der Stimmdateien im Wahlcomputer sowohl an der Atomarität als auch an der Beobachtbarkeit. Auch die Auszählung der Stimmen findet im Wahlcomputer unter Ausschluss aller Beobachtungsmöglichkeiten statt, die bei manueller Auszählung eine Manipulation zu verhindern im Stande wäre.

Der Schutzzweck des Öffentlichkeitsprinzips bei Wahlen – die Verhinderung von Manipulationen – und sein Wirkmechanismus – sozialer Druck durch mögliche Anwesenheit von Beobachtenden und das dadurch stark erhöhte Entdeckungsrisiko für Manipulierende – werden damit durch die Verwendung von Wahlcomputern unterminiert.

Integrität und Überprüfbarkeit

Während die Öffentlichkeit von Wahlhandlung und Auszählung Manipulationen während der Wahl verhindern oder zumindest stark erschweren soll, regelt Art. 41 Grundgesetz (GG) grundsätzlich, wer Wahlergebnisse und deren Entstehung wie

¹⁰ Der Begriff

»Republik« leitet sich von »res publica« – »öffentliche Angelegenheit« – ab.

¹¹ Vgl. BAGE 86, 117, 121.

¹² Der Begriff der

Atomarität beschreibt vereinfacht ausgedrückt die Eigenschaft von Übergängen oder Veränderungen, entweder wie ein unteilbarer Schritt oder gar nicht abzulaufen, unabhängig von deren interner Komplexität.

überprüfen darf, wenn ihre Echtheit bezweifelt oder andere Wahlfehler behauptet werden. Implizit geht Art. 41 GG dabei davon aus, dass eine solche Überprüfung von Wahlabläufen und -ergebnissen objektiv möglich ist. Dies wird – mit gutem Grund – von KritikerInnen bei Wahlcomputern infrage gestellt.

Die Integrität der abgegebenen Stimmen, die Korrektheit der Auszählung und die sich unter anderem daraus ableitende Korrektheit des Wahlergebnisses ist durch die Wahlvorstände sicherzustellen, wie aus der Anforderung der Gleichheit der Wahl in Art. 38 GG folgt. Dieser Forderung können Wahlvorstände weder objektiv noch subjektiv nachkommen, wenn Wahlcomputer eingesetzt werden. Die objektive Unmöglichkeit folgt aus technischen Beschränkungen der Wahlcomputer selbst. In der Forschung ist bis heute keine Methode bekannt, die nicht auf der Durchführung forensischer Untersuchungen basiert, um Manipulationen an Software oder Hardware zu erkennen, nachdem sich ein Computer in der Hand potentieller AngreiferInnen befand.¹³ Da Innen-täterInnen nicht a priori ausgeschlossen werden können, handelt es sich bei allen, die zwischen den Wahlen Zugriff auf die Wahlcomputer besitzen, um potentielle AngreiferInnen.

Selbst wenn Manipulationen im Einzelfall objektiv bei einer eingehenden Prüfung der Wahlcomputer vor Beginn der Wahlhandlung, wie sie von der BWahlGV explizit gefordert wird, erkennbar sein würden, fehlt der großen Mehrheit der Mitglieder von Wahlvorständen grundsätzlich das Wissen und die Fähigkeit, diese subjektiv erkennen zu können. Damit stehen sie allerdings nicht allein. Tatsächlich ist die IT-Forensik auch innerhalb der Informatik ein wenig durchdrungenes Exotenfach. Auch nach einer Wahl lassen sich Manipulationen nicht mit Sicherheit erkennen, etwa weil Software grundsätzlich in der Lage ist, sich selbst zu verändern. Damit könnte eine manipulierte Software zum Beispiel erst die abgegebenen Stimmen ändern und sich nach Abschluss der Wahlhandlung mit einer Originalversion überschreiben, die dann einer nachträglichen Überprüfung standhält. Auch eine Manipulation der Hardware, wie etwa ein Austausch des Prozessors, lässt sich derart durchführen, dass eine Prüfung nicht mehr zerstörungsfrei durchführbar ist, eine zerstörende Prüfung würde jedoch oft schlicht an den Kosten scheitern, vor allem weil dabei *alle* Bauteile eines zu überprüfenden Wahlcomputers auseinander genommen werden müssten.

Verständnis der Technik

Nicht nur Mitgliedern von Wahlvorständen mangelt es an technischem Verständnis für die Funktionsweise und die inhärenten Beschränkungen der eingesetzten Wahlcomputer und die daraus folgenden Anforderungen an deren sichere Verwendung. Gleiches gilt natürlich auch für eine große Mehrheit der Wahlbevölkerung. Die Durchführung von Wahlen mit technischen Geräten, deren Funktionsweise sich den Betroffenen nicht erschließt und erschließen kann, lässt sich in einer Demokratie nicht legitimieren. Dass die politisch Verantwortlichen auf die weitere Verwendung von Wahlcomputern insistieren, entspricht der politischen Entmündigung der Wahlbevölkerung und dem Ausschluss der Öffentlichkeit aus politischen Prozessen, wie sie etwa ihren Ausdruck in der Verlagerung der Entscheidungsfindung in nicht-öffentliche »Beratungen«, sogenannte Expertengremien oder auf die europäische Ebene finden.

Hingenommen werden kann eine solche Entwicklung nicht. Die verfassungsrechtlichen Bedenken konnten bisher nicht ausgeräumt und die grundlegenden technischen Probleme nicht gelöst werden. Es bleibt zu hoffen, dass das BVerfG wieder einmal steuernd eingreift und die Wahlcomputer dorthin befördert, wo sie in einem demokratischen System hingehören: in die Versenkung. ☐

¹³ Kurz/Rieger/Gonggrijp: Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern, www.ccc.de/press/releases/2007/20070609/nedapReport54.pdf (Abruf: 12.12.2008).

Anzeige



Antifaschistisches Blatt info

Nr.81 | Winter 2008/2009



**Pro und Contra -
Bürgerbewegung Pro und
Gegenaktivitäten**

Kostenloses Probeexemplar:

Antifaschistisches Infoblatt
Gneisenaustr. 2a | 10961 Berlin
e-mail: mail@antifainfoblatt.de
web: www.antifainfoblatt.de

Einzelexemplar 3,10 Euro
Abo 15,50 Euro (fünf Ausgaben)