Inga Lindenau
Siemensstraße 6
52428 Jülich

Rechtliche und tatsächliche Probleme der elektronischen Wahl

Masterarbeit
im
Ergänzungsstudiengang
Rechtsinformatik
an der Leibniz-Universität Hannover

Eulisp XII
WS 2006/07

Inhaltsverzeichnis

Literaturverzeichnis

Alkassar, Ammar/ Krimmer, Robert/ Volkamer, Melanie — Online-Wahlen für Gremien; DuD 2005, S. 480 ff.

Beiß, Willi — Pilotstudie zum Digitalen Wahlstift. Dokumentation; Hamburg 2005.
Zitiert: *Beiß*, Pilotstudie zum Digitalen Wahlstift, S.

Birkenmaier, Philipp — E-Democracy – Der Wandel der Demokratie durch das Internet; Dresden 2004.

Brandt, Martin/ Volkert, Bernd — E-Voting im Internet – Formen, Entwicklungsstand und Probleme; Stuttgart 2002.

Braun, Nadja/ Brändli, Daniel — Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed;
In: Electronic Voting 2006, Hrsg.: Krimmer, Robert, Bonn 2006, S. 27 ff.
Zitiert: *Braun/Brändli* in Krimmer, S.

Bremke, Nils — Internetwahlen – Eine Analyse einer Wahlverfahrensergänzung für das 21. Jahrhundert unter besonderer Berücksichtigung rechtlicher Anforderungen;
LKV 2004, S. 102 ff.

Bremke, Nils — Der Grundsatz der Öffentlichkeit der Wahl und Internetwahlen; MMR 2004, S. IX ff.

Buchsbaum, Thomas M. — Lessons learnt aus E-Voting-Einsätzen;
In: Effizienz von e-Lösungen in Staat und Gesellschaft: Aktuelle Fragen der Rechtsinformatik: Tagungsband des 8.

Internationalen Rechtsinformatik Symposions: IRIS 2005, Hrsg.: Schweighofer, Erich [et. al.], Stuttgart 2005, S. 278 ff.
Zitiert: *Buchsbaum* in Schweighofer, S.

Buchstein, Hubertus Online-Wahlen und das Wahlgeheimnis;
In: Online-Wahlen; Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 51 ff.
Zitiert: *Buchstein* in Buchstein/Neymanns, S.

Bundesamt für Sicherheit in der Informationstechnik Zertifizierungsreport BSI-PP-0031-2007 zu Schutzprofil Digitales Wahlstift-System, Version 1.0.1;
Abrufbar unter:
http://www.bsi.de/zertifiz/zert/reporte/pp0031a.pdf,
Stand: 05.06.07.
Zitiert: *BSI*, Zertifizierungsreport Schutzprofil Digitales Wahlstift-System.

California Institute of Technology/ The Massachusetts Institute of Technology Corporation Voting – What is, What could be;
Abrufbar unter:
http://www.vote.caltech.edu/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf,
Stand: 24.04.07.
Zitiert: *Caltech/MIT*, S.

Di Fabio, Udo Privatisierung und Staatsvorbehalt;
JZ 1999, S. 585 ff.

Election Data Services Voting Equipment Study 2006;
Abrufbar unter:
http://www.edssurvey.com/images/File/ve2006_nrpt.pdf,
Stand 22.04.07.
Zitiert: *Election Data Service*, Voting Equipment Study 2006, S.

Election Data Services Voting Equipment Study 2004;
Abrufbar unter:
http://www.edssurvey.com/images/File/VotingEquipStudies%20/ve2004_report.pdf,
Stand: 24.04.07.
Zitiert: *Election Data Service*, Voting Equipment Study 2004.

Esteve, Jordi Barrat A preliminary question: Is e-voting actually useful for our democratic institutions? What do we need it for?
In: Electronic Voting 2006, Hrsg.: Krimmer, Robert, Bonn 2006, S. 51 ff.
Zitiert: *Esteve* in Krimmer, S.

Feldmann, Ariel J./ Haldermann, J. Alex/ Felten, Edward W. Security Analysis of the Diebold AccuVote-TS Voting Machine;
Abrufbar unter: http://itpolicy.princeton.edu/voting/ts-paper.pdf,
Stand: 23.03.07.
Zitiert: *Feldmann/Haldermann/Felten*, Diebold Security Analysis, S.

Fischer, Eric A. Voting Technologies in the United States: Overview and Issues for Congress;
Abrufbar unter:
http://usinfo.state.gov/usa/infousa/politics/voting/rl30773.pdf,
Stand 22.04.07.
Zitiert: *Fischer*, S.

Fischer, Gerald/ Zuser, Wolfgang Sicherheitstheoretische Aspekte bei elektronischen Wahlen.
In: Effizienz von e-Lösungen in Staat und Gesellschaft: Aktuelle Fragen der Rechtsinformatik: Tagungsband des 8. Internationalen Rechtsinformatik Symposions: IRIS 2005;
Hrsg.: Schweighofer, Erich [et. al.], Stuttgart 2005, S. 286 ff.
Zitiert: *Fischer/Zuser* in Schweighofer, S.

Forschungsgruppe Internetwahlen i-vote Report - Chancen, Möglichkeiten und Gefahren der Internetwahl 2002;
Abrufbar unter:
http://www.hsw.bfh.ch/content/File/weiterbildung/egov/studien/i-vote-report-lang.pdf,
Stand: 21.06.07.
Zitiert: *Forschungsgruppe Internetwahlen*, i-vote Report, S.

Grimm, Rüdiger Technische Sicherheit bei Internetwahlen;
In: Elektronische Demokratie, Hrsg.: Holznagel, Bernd/ Grünwald, Andreas/ Hanßmann, Anika, München 2001, S. 86 ff.
Zitiert: *Grimm* in Holznagel, S.

Grimm, Rüdiger/ Krimmer, Robert/ Meißner, Nils/ Reinhard, Kai/ Volkamer, Melanie/ Weinand, Marcel/ Helbach, Jörg Security Requirements for Non-political Internet Voting;
In: Electronic Voting 2006, Hrsg.: Krimmer, Robert, Bonn 2006, S. 203 ff.
Zitiert: *Grimm/Krimmer/Meißner/Reinhard/Volkamer/ Weinand/Helbach* in Krimmer, S.

Dies. Security Requirements for Non-Political Internet Voting;
Abrufbar unter:
http://www.uni-koblenz.de/~aggrimm/arbeitsberichte/arbeitsberichte_6_2007.pdf,
Stand: 22.06.07.
Zitiert: *Grimm/Krimmer/Meißner/Reinhard/Volkamer/ Weinand/Helbach,* Security Requirements, S.

Hanßmann, Anika Möglichkeiten und Grenzen von Internetwahlen;
Baden-Baden 2004.

Hartmann, Volker/ Meißner, Nils/ Richter, Dieter Online-Wahlsysteme für nicht-parlamentarische Wahlen: Anforderungskatalog;
Abrufbar unter:
http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf,
Stand: 22.06.07.
Zitiert: *Hartmann/Meißner/Richter*, Anforderungskatalog, S.

Heckmann, Jörn Estland: E-Voting bei Kommunalwahl;
CR 2005, S. R142.

Hiekel, Sabine Presseinformation der Kreiswahlleiterin vom 14.10.06, Kommunalwahl 2003-2008;
Abrufbar unter:
http://www.wahlrecht.de/doku/presse/20061014.pdf,
Stand 30.04.07.
Zitiert: *Hiekel*, Pressemitteilung vom 14.10.06, S.

Hof, Sonja E-Voting and Biometric Systems?
In: Electronic Voting in Europe – Technology, Law, Politics and Society, Hrsg.: Prosser, Alexander/Krimmer, Robert, Bonn 2004, S. 63 ff.
Zitiert: *Hof* in Prosser/Krimmer, S.

Holznagel, Bernd/ Hanßmann, Anika Möglichkeiten von Wahlen und Bürgerbeteiligung per Internet;
In: Elektronische Demokratie, Hrsg.: Holznagel, Bernd/ Grünwald, Andreas/ Hanßmann, Anika, München 2001, S. 55 ff.
Zitiert: *Holznagel/Hanßmann* in Holznagel, S.

Jarass, Hans/ Pieroth, Bodo Grundgesetz für die Bundesrepublik Deutschland, Kommentar;
9. Auflage, München 2007.

Jones, Douglas W. The Evaluation of Voting Technology;
In: Secure Electronic Voting, Hrsg.: Gritzalis, Dimitris A.,

Norwell, Massachusetts, USA, S. 3 ff.
Zitiert: *Jones* in Gritzalis, S.

Karpen, Ulrich
Elektronische Wahlen?
Baden-Baden 2005.

Khorrami, Esfandiar
Bundestagswahlen per Internet;
Baden-Baden 2006.

Kubicek, Herbert/
Wind, Martin
Bundestagswahl per Computer?
In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 91 ff.
Zitiert: *Kubicek/Wind* in Buchstein/Neymanns, S.

Krimmer, Robert/
Volkamer, Melanie
Wählen auf Distanz: Ein Vergleich zwischen elektronischen und nicht elektronischen Verfahren;
In: Effizienz von e-Lösungen in Staat und Gesellschaft: Aktuelle Fragen der Rechtsinformatik: Tagungsband des 8. Internationalen Rechtsinformatik Symposions: IRIS 2005, Hrsg.: Schweighofer, Erich [et. al.], Stuttgart 2005, S. 265 ff.
Zitiert: *Krimmer/Volkamer* in Schweighofer, S.

Kurz, Constanze/
Rieger, Frank/
Gronggrijp, Rop
Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern;
Abrufbar unter:
http://www.ccc.de/press/releases/2007/20070609/nedapReport54.pdf
Stand: 11.06.07.
Zitiert: *Kurz/Rieger/Gonggrijp*, Nedap-Report, S.

Lange, Nico
Click'n'Vote – Erste Erfahrungen mit Online-Wahlen;
In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 127 ff.
Zitiert: *Lange* in Buchstein/Neymanns, S.

Leder, Martin Der Einsatz von Wahlgeräten und seine Auswirkungen auf die Amtlichkeit und Öffentlichkeit der Wahl;
DÖV 2002, S. 648 ff.

Maaten, Epp Towards remote e-voting: Estonian case;
In: Electronic Voting in Europe – Technology, Law, Politics and Society, Hrsg.: Prosser, Alexander/Krimmer, Robert, Bonn 2004, S. 83 ff.
Zitiert: *Maaten* in Prosser/Krimmer, S.

Madise, Ülle/ Martens, Tarvi E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world;
In: Electronic Voting 2006, Hrsg. Krimmer, Robert, Bonn 2006, S. 15 ff.
Zitiert: *Madise/Martens* in Krimmer, S.

Mason, Stephen Is There A Future For Internet Voting?
Computer Fraud & Security 03/04, S. 6 ff.

Meißner, Niels/ Hartmann, Volker/ Richter, Dieter Verifiability and Other Technical Requirements for Online Voting Systems;
In: Electronic Voting in Europe – Technology, Law, Politics and Society, Hrsg.: Prosser, Alexander/Krimmer, Robert, Bonn 2004, S. 101 ff.
Zitiert: *Meißner/Hartmann/Richter* in Prosser/Krimmer, S.

Nagel, Udo Hamburg-Wahlen 2008, Landespressekonferenz am 31.10.06;
Abrufbar unter:
http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2006/oktober/31/2006-10-31-bfi-pm-wahl-digitalerstift-folien-pdf,property=source.pdf,
Stand: 04.06.07.
Zitiert: *Nagel*, Hamburg-Wahlen 2008, S.

Nederlande Organisatie voor toegepaast-natuurwetenschappelijk onderzoek (TNO)	TNO-rapport EIB-RPR-020021, Keuring van de Nedap stemmachine ESD-1 met aanpassingen voor gebruik in Nederland; Abrufbar unter: http://www.wijvertrouwenstemcomputersniet.nl/images/2/27/20020212_tno_rapport_keuring_nedap_ESD1_met_aanpassingen_voor_gebruik_in_Nederland.pdf, Stand: 22.06.07. Zitiert: *TNO-rapport*, S.
Neymanns, Harald	Die Wahl der Symbole: Politische und demokratietheoretische Fragen zu Online-Wahlen; In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 23 ff. Zitiert: *Neymanns* in Buchstein/Neymanns, S.
Neymanns, Harald/ Buchstein, Hubertus	Einleitung; In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 7 ff. Zitiert: *Neymanns/Buchstein* in Buchstein/Neymanns, S.
Noack, Ulrich	Virtuelle Hauptversammlung; In: Handbuch Multimedia-Recht, Hrsg.: Hoeren, Thomas/ Sieber, Ulrich, München 2006, Kapitel 21.2, Stand Mai 2003. Zitiert: *Noack* in Hoeren/Sieber, Kap. 21.2 Rn.
Oostveen, Anne-Marie/ Besselaar, Peter van den	Security as belief – User's perceptions on the security of electronic voting systems; In: Electronic Voting in Europe – Technology, Law, Politics and Society, Hrsg.: Prosser, Alexander/ Krimmer, Robert, Bonn 2004, S. 73 ff. Zitiert: *Oostveen/Besselaar* in Prosser/Krimmer, S.

Open Rights Group May 2007 Election Report;
Abrufbar unter:
http://media.ito.com/kevinmarks/org_election_report.pdf,
Stand: 22.06.07.
Zitiert: *Open Rights Group*, Election Report, S.

Ortega y Gasset, José Der Aufstand der Massen;
Stuttgart 1977.

Ostler, Ulrike Knopfdruck statt Kreuzchen – Die Kölner stimmten per Wahlcomputer ab;
Computerwoche 1999, Nr. 37, S. 10 ff.

Otten, Dieter Modernisierung der Präsenzwahl durch das Internet;
In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 71 ff.
Zitiert: *Otten* in Buchstein/Neymanns, S.

Otten, Dieter Wählen wie im Schlaraffenland?
In: Elektronische Demokratie, Hrsg.: Holznagel, Bernd/ Grünwald, Andreas/ Hanßmann, Anika, München 2001, S. 73 ff.
Zitiert: *Otten* in Holznagel, S.

Physikalisch-Technische Bundesanstalt Prüfbericht – Baumusterprüfung eines Wahlgerätes;
Abrufbar unter:
http://www.wahlrecht.de/doku/doku/PB-ESD1-SW03.08-BTW.pdf,
Stand: 10.05.07.
Zitiert: *Physikalisch-Technische Bundesanstalt*, Prüfbericht, S.

Physikalisch-Technische Bundesanstalt Richtlinien für den Einsatz des Digitalen Wahlstift-Systems bei Wahlen zur Hamburgischen Bürgerschaft und Wahlen zu den Bezirksversammlungen sowie bei der Durchführung von

Volksentscheiden;
Abrufbar unter:
http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2006/oktober/31/2006-10-31-bfi-pm-wahl-digitalerstift-wahlgvo-pdf,property=source.pdf,
Stand: 06.06.07.
Zitiert: *Physikalisch-Technische Bundesanstalt*, Richtlinien Digitales Wahlstift-System.

Piswanger, Carl-Markus Kostenargument für Remote-E-Voting in einem vollelektronischen Prozess;
In: Effizienz von e-Lösungen in Staat und Gesellschaft: Aktuelle Fragen der Rechtsinformatik: Tagungsband des 8. Internationalen Rechtsinformatik Symposions: IRIS 2005, Hrsg.: Schweighofer, Erich [et. al.], Stuttgart 2005, S. 271 ff.
Zitiert: *Piswanger* in Schweighofer, S.

Rüß, Oliver Rechtliche Voraussetzungen und Grenzen von Online-Wahlen;
In: Online-Wahlen, Hrsg.: Buchstein, Hubertus/ Neymanns, Harald, Opladen 2002, S. 39 ff.
Zitiert: *Rüß* in Buchstein/Neymanns, S.

Rüß, Oliver Wahlen im Internet – Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen;
MMR 2000, S. 73 ff.

Rüß, Oliver E-democracy;
ZRP 2001, S. 518 ff.

Schreiber, Wolfgang Handbuch des Wahlrechts zum Deutschen Bundestag, 7. Auflage, Köln 2002.

Schwarz, Monika Die E-Voting-Empfehlung des Europarates – Ein erster internationaler Standard für elektronische Wahlen und

	Referenden; In: Effizienz von e-Lösungen in Staat und Gesellschaft: Aktuelle Fragen der Rechtsinformatik: Tagungsband des 8. Internationalen Rechtsinformatik Symposions: IRIS 2005, Hrsg.: Schweighofer, Erich [et. al.], Stuttgart 2005, S. 263 ff. Zitiert: *Schwarz* in Schweighofer, S.
Security and Transparency Subcommittee (STS)	Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC; Abrufbar unter: http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf, Stand: 23.03.07. Zitiert: *STS*, Recommendations, S.
Sietmann, Richard	E-Voting vs. Verfassung, Rechtliche Bedenken bei elektronischen Wahlmaschinen in Deutschland; c't 01/06, S. 80 ff.
Ders.	Der schleichende Verfall, Der 22C3 diskutiert über Wahlen per Internet und E-Voting; c't 02/06, S. 20 ff.
Ders.	Naive E-Wähler, Rechtliche und technische Probleme bei Wahlcomputern in Deutschland; c't 15/06 , S. 104 ff.
Ders.	Neue Bedenken gegen Wahlmaschinen; c't 16/06, S. 54 ff.
Ders.	Obskure Demokratiemaschine – Sind Wahlcomputer manipulationssicher? c't 20/06, S. 86 ff.

Ders. Eine neue Situation;
c't 24/06, S. 72 ff.

Ders. Der Urnen-Bypass, Ein elektronischer Wahlstift als Alternative zu Wahlmaschinen;
c't 26/06, S. 92 ff.

Ders. E-Voting-Aktivismus;
c't 05/07, S. 42 ff.

Skagestein, Gerhard/ Haug, Are Vegard/ Nødtvedt, Einar/ Rossebø, Judith How to create trust in electronic voting over an untrusted platform;
In: Electronic Voting 2006, Hrsg.: Krimmer, Robert, Bonn 2006, S. 107 ff.
Zitiert: *Skagestein/Haug/Nødtvedt/Rossebø* in Krimmer, S.

Solop, Frederic I. Digital Democracy comes of Age in Arizona: Participation and Politics in the First Binding Internet Election;
Abrufbar unter:
http://ball.tcnj.edu/pols291/readings/036015SolopFrede.pdf,
Stand: 15.06.07.
Zitiert: *Solop*, S.

Stadt Fellbach Jugendgemeinderatswahl 2001 in Fellbach – online;
Abrufbar unter:
http://www.fellbach.de/kommunalpolitik/Jugendgemeinderat/Dokumentation_JGROnlinewahl.PDF,
Stand: 15.06.07.
Zitiert: *Stadt Fellbach*, Jugendgemeinderatswahl 2001, S.

Stadt Mainz Test des Digitalen Wahlstifts, Landtagswahl 2006, Dokumentation;
Abrufbar unter:
http://www.mainz.de/C1256D6E003D3E93/files/dokumentatio

n_wahlstift_2006.pdf/%24FILE/dokumentation_wahlstift_2006.pdf,
Stand: 07.06.07.
Zitiert: *Stadt Mainz*, Test des Digitalen Wahlstifts, S.

Tauss, Jörg E-Vote: Die „elektronische Briefwahl“ als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten;
In: Multimedia@Verwaltung, Hrsg. Kubicek, Herbert, Heidelberg 1999, S. 285 ff.
Zitiert: *Tauss* in Kubicek, S.

Ullmann, Markus/ Koob, Frank/ Kelter, Harald Anonyme Online-Wahlen;
DuD 2001, S. 643 ff.

Volkamer, Melanie/ Grimm, Rüdiger Multiple Casts in Online Voting: Analyzing Chances;
In: Electronic Voting 2006, Hrsg.: Krimmer, Robert, Bonn 2006, S. 97 ff.
Zitiert: *Volkamer/Grimm* in Krimmer, S.

Volkamer, Melanie/ Vogt, Roland Common Criteria Schutzprofil Digitales Wahlstift-System;
Abrufbar unter:
http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf,
Stand: 05.06.07.

Wij vertrouwen stemcomputers niet Nedap/Groenendaal ES3B voting computer – a security analysis;
Abrufbar unter:
http://www.wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf,
Stand: 10.05.07.
Zitiert: *Wij vertrouwen stemcomputers niet*, security analysis, S.

Will, Martin Internetwahlen;
Stuttgart 2002.

Will, Martin Wahlen und Abstimmungen via Internet und die Grundsätze der allgemeinen und gleichen Wahl;
CR 2003, S. 126 ff.

Wilm, Peter Notwendige technische Anforderungen an eVoting-Systeme für staatliche Volksvertreter-Wahlen;
Abrufbar unter:
http://www.elektronische-wahlen.de/gi-edemocracy-workshop-2003/e-voting-anforderungen-kurzbeitrag.pdf,
Stand: 18.06.07.
Zitiert: *Wilm*, Technische Anforderungen, S.

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
DoS	Denial of Service
ESI	Elektronische Stimmabgabe im Internet
EPROM	Erasable Programmable Read Only Memory
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Persönliche Identifikationsnummer
PTB	Physikalisch-Technische Bundesanstalt
SMS	Short Message Service
SSL	Secure Sockets Layer
TAN	Transaktionsnummer
VVPAT	Voter Verified Paper Audit Trail

Im Übrigen wird verwiesen auf:

Kirchner, Hildebert/	Abkürzungsverzeichnis der Rechtssprache;
Butz, Cornelie	6. Auflage, Berlin 2007.

Kapitel 1: Einleitung

A. Hinführung zum Thema

„Das Heil der Demokratien, von welchem Typ und Rang sie immer seien, hängt von einer geringfügigen technischen Einzelheit ab: vom Wahlrecht. Alles andere ist sekundär. […] Ohne die Stütze einer vertrauenswürdigen Abstimmung hängen die demokratischen Institutionen in der Luft.“[1]

Diese Stütze der vertrauenswürdigen Abstimmungen wird in Deutschland seit geraumer Zeit in hohem Maße herausgefordert: durch die Debatte über die Einführung von elektronischen Wahlen. Dass es sich hierbei um alles andere als eine geringfügige Veränderung einer technischen Einzelheit handelt, ist allen Beteiligten bewusst. Schließlich steht die herausragende Bedeutung von Wahlen für die Demokratie außer Frage. Ob in der Verwendung von Informationstechnologie bei Wahlen aber vor allem ein Risiko für die Vertrauenswürdigkeit der Abstimmungen oder das große bislang ungenutzte demokratietheoretische Potential der Zukunft liegt, wird sehr kontrovers beurteilt.

Der nicht nur in Deutschland, sondern in vielen Ländern, vorherrschende Stand der Diskussion ist von großer Skepsis und Unsicherheit geprägt. Während in Estland die ersten rechtsverbindlichen parlamentarischen Internetwahlen stattgefunden haben, stehen in Irland einige Tausend Wahlcomputer original verpackt in Lagerhallen und warten seit 4 Jahren auf ihren Einsatz. Auch in Deutschland ist die Diskussion über die flächendeckende Einführung von Wahlcomputern durch den Nedap-Hack endgültig öffentlich entbrannt und in weiten Teilen Europas scheint die „Wahl im Unterhemd“ vom heimatlichen Sofa aus in weite Ferne gerückt. Ist womöglich die Vertrauenswürdigkeit der Abstimmung unmittelbar an Wahlzettel und Kugelschreiber geknüpft und bleibt die elektronische Wahl ein Wunschkonstrukt von einzelnen ehrgeizigen, technik-affinen Politikern?

Wohl kaum. Ungeachtet der Rückschläge des letzten Jahres und der bestehenden Sicherheitsbedenken lässt sich eine unaufhaltsame Tendenz zur Substitution der herkömmlichen Wahlutensilien durch elektronisch

[1] *Ortega y Gasset*, S. 188.

unterstützte Systeme erkennen. Lange Zeit nach der Wirtschaft hat nun auch der Staat die Vorteile der digitalen Technik für sich uns seinen Verwaltungs-, Justiz- und eben auch Legislativapparat entdeckt. Das „e“ erhält Einzug in den Staatsapparat. Unter den Schlagwörtern „eDemocracy“ und „eGovernment“ werden Steuererklärungen online angenommen, Vergabeforen etabliert, das Grundbuch digital zugänglich gemacht und Wahlcomputer regional eingesetzt. Die elektronische Wahl fungiert hierbei als Leitbild der zu entwickelnden „eDemocracy“, soll sozusagen ihre Krönung darstellen.[2] Hintergrund für diese Entwicklung ist dabei keineswegs eine bloß populistische Technisierung nach dem Motto „What can be done, is done“. Die unangefochtene Akzeptanz der Wahl mit Stift und Papier in der Bevölkerung darf nicht darüber hinwegtäuschen, dass auch diese traditionelle Methode an einigen Schwachstellen und Defiziten krankt. Zwar hat es in Deutschland noch keines mit den Vorkommnissen bei den Präsidentschaftswahlen 2000 in Florida vergleichbares Wahldesaster gegeben.[3] Dennoch ist die Fehleranfälligkeit bei Papierwahlen in dem Sinne groß, als davon ausgegangen wird, dass viele ungültige Stimmen nicht absichtlich ungültig abgegeben werden.[4] Zudem ist die Durchführung einer Wahl mit Wahlzetteln ein extremer wirtschaftlicher und organisatorischer Aufwand, da viele freiwillige Helfer benötigt werden und enorme Materialkosten anfallen.[5]

Elektronische Wahlen werden deswegen zum einen als Chance gesehen, diese Schwächen der herkömmlichen Stimmabgabe jedenfalls langfristig zu überwinden. Zum andern wird der neuen Technologie das Potential zugeschrieben, den gestiegenen Mobilitätserfordernissen der heutigen Gesellschaft gerecht zu werden und eine Mobilisierung insbesondere der Jungwähler zu erreichen.[6]

---

[2] *Birkenmaier*, S. 47.
[3] Aufgrund von kompliziertem Stimmzetteldesign in Verbindung mit veralteten Wahlmaschinen kam es zu Tausenden von semigültigen Stimmen: *Neymanns* in Buchstein/Neymanns, S. 30.
[4] *Neymanns* in Buchstein/Neymanns, S. 30.
[5] Vgl. BR-Drucksache 595/99; *Neymanns* in Buchstein/Neymanns, S. 31; für Österreich: *Piswanger* in Schweighofer, S. 271, 273.
[6] *Bremke*, LKV 2004, S. 102, 104.

Die technischen Ausgestaltungsmöglichkeiten der elektronischen Wahlsystem-Alternativen zum herkömmlichen papiernen Wahlzettel sind vielfältig und eine abschließende Darstellung würde den Rahmen dieser Arbeit sprengen. Die vorliegende Arbeit konzentriert sich deshalb nach einer kurzen Begriffserläuterung zunächst auf die beiden aktuell in der Bundesrepublik Deutschland zur Anwendung kommenden und in Rede stehenden elektronischen Methoden, dem elektronischen Wahlgerät und dem Wahlstift. Die beiden Systeme sollen anhand einer umfassenden sicherheitstechnischen Analyse auf ihre verfassungsrechtliche Zulässigkeit überprüft werden.

Schließlich wird auf die als in der politischen Diskussion als erstrebenswertes Endziel deklarierte Internetwahl vom heimischen Computer einzugehen sein. Auch hier stehen die Darstellung der sicherheitstechnischen Bedrohungen und die Frage nach einer verfassungsrechtskonformen Ausgestaltung des Systems im Vordergrund. In die Beurteilung aller drei Wahlsysteme sollen bereits gemachte Erfahrungen im In- und Ausland einfließen.

In der abschließenden Schlussbetrachtung soll ein Fazit über die rechtliche Zulässigkeit der bereits durchgeführten Einsätze der verschiedenen elektronischen Wahlsysteme in Deutschland gezogen werden, sowie ein Ausblick über die Zukunft der elektronischen Wahl im Kontext politischer Wahlen gegeben werden.

B. Elektronische Wahl – was ist das?

Die Diskussion rund um die Digitalisierung der Mitbestimmungsmöglichkeiten und -rechte der Bürger ist von vielen verschiedenen Begrifflichkeiten durchsetzt, die es zunächst zu definieren und einzuordnen gilt. „E-Voting“[7], „Online-Wahlen“[8], „elektronische Wahlen“[9], „i-voting“, „Internetwahlen“, „online-voting“[10] sind die Termini, die in der Diskussion auftauchen[11] und doch oft mit

[7] *Brandt/Volkert*, S. 2.
[8] *Neymanns/Buchstein* in Buchstein/Neymanns, S. 7, 16.
[9] *Otten* in Holznagel, S. 73, 75.
[10] *Holznagel/Hanßmann* in Holznagel, S. 55, 58.
[11] *Khorrami*, S. 28 ff.; *Birkenmaier*, S. 47 f.

unterschiedlicher Bedeutung oder fälschlicherweise synonym benutzt werden.

I. Begrifflichkeiten

Als gemeinsamer Oberbegriff für jegliche Art der Wahrnehmung politischer Mitbestimmungsrechte unter Verwendung von Informationstechnologie bietet sich der Begriff der „elektronischen Wahl", des „electronic voting" oder des „e-voting" an.[12]

Politisch gesehen unterfallen der elektronischen Wahl damit jegliche Wahl- und Abstimmungsrechte, aber auch solche Rechte, ein Bürgerbegehren oder einen Bürgerbescheid zu initiieren.[13] Da die direktdemokratischen Partizipationsmöglichkeiten und die Abstimmungen auf Bundesebene (so gut wie) keine Relevanz haben,[14] wird sich die vorliegende Arbeit ausschließlich mit der stärksten Beteiligungsform, der rechtsverbindlichen Wahl, befassen. Deshalb wird im Folgenden der Begriff „Elektronische Wahl" lediglich in seiner engsten Bedeutung verwendet.[15]

Technisch gesehen ist der Terminus der „elektronischen Wahl" so weit gefasst, dass davon jegliche Nutzung von Computern als Medien der Stimmabgabe und Stimmenauszählung umfasst ist.[16] Damit unterliegen dieser Begriffsgruppe neben Computern auch mobile elektronische Endgeräte und auch elektro-mechanische Geräte.[17]

Die teilweise synonyme Verwendung der Termini „elektronische Wahl/e-voting"[18] mit „i-Voting", „Online-Wahlen"[19] und „Internetwahlen"[20] hingegen ist irreführend.[21] Während das „e-voting" als Oberbegriff für jegliche auf Informations- und Kommunikationstechnologien basierende Wahlen steht, bezeichnen die anderen Begriffe die Verwendung einer

[12] *Birkenmaier*, S. 47; *Brandt/Volkert*, S. 2; *Khorrami*, S. 28; *Will*, S. 67. Die drei Begriffe werden im Folgenden synonym verwendet.
[13] *Brandt/Volkert*, S. 2 f.; *Khorrami*, S. 28.
[14] *Birkenmaier*, S. 48.
[15] Zu Meinungsumfragen, Abstimmungen und anderen Partizipationsmöglichkeiten mittels elektronischer Verfahren s. aber instruktiv: *Brandt/Volkert*, S. 32 ff.
[16] *Neymanns/Buchstein* in Buchstein/Neymanns, S. 7, 16.
[17] *Khorrami*, S. 28.
[18] *Birkenmaier*, S. 50.
[19] *Neymanns/Buchstein* in Buchstein/Neymanns, S. 7, 16.
[20] *Birkenmaier*, S. 47.
[21] So auch: *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 93.

ganz bestimmten Informationstechnologie. Als „Online-Wahlen“ sind Wahlen zu verstehen, bei denen die Datenübertragung über ein offenes oder internes Kommunikationsnetz stattfindet;[22] bei „Internetwahlen“ ist dieses Netz einzig das World Wide Web und keine Art von geschlossenem Netz.[23] Allerdings wird insbesondere der Terminus „Online-Wahlen“ im deutschsprachigen Raum oft synonym für die der Internetwahl zu Grunde liegenden Technik verwendet.[24]

Zur besseren Verständlichkeit sind in der vorliegenden Arbeit deshalb die Begriffe „elektronische Wahl/e-voting“ als Oberbegriffe für jegliche verbindliche Stimmabgabe mittels Informationstechnologie zu verstehen. „Online-Wahlen/online-voting“ hingegen bezeichnet eine elektronische Wahl, bei der die Datenübertragung mittels eines offenen oder internen Netzes geschieht, und „Internetwahlen/i-voting“ steht im Folgenden für die Stimmabgabe mit Computern, die über das Internet mit einander verbunden sind.

II. Arten der elektronischen Wahl

Die Bandbreite der technischen Wahlsysteme lässt sich am Besten in drei verschiedene Haupttypen unterteilen, die sich durch verschieden ausgeprägte Technisierungsgrade auszeichnen und wiederum Untermodelle hervorgebracht haben. Da die Unterschiedlichkeit der zugrunde liegenden Technik nicht ohne Auswirkung auf sicherheitstechnische und verfassungsrechtliche Aspekte bleibt, ist es erforderlich eine genaue Differenzierung vorab vorzunehmen.

1. Machine Counting

Die papiernen per Hand ausgezählten Wahlzettel haben vor allem in den USA seit der ersten Häflte des 20. Jahrhunderts Konkurrenz durch „machine counting“-Systeme („maschinelles Zählen“) bekommen, bei

[22] *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 93; a.A. *Holznagel/Hanßmann* in Holznagel, S. 55, 58.
[23] *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 93; *Will*, S. 67.
[24] *Holznagel/Hanßmann* in Holznagel, S. 55, 58; *Neymanns* in Buchstein/Neymanns, S. 23, 26 f.; *Rüß* in Buchstein/Neymanns, S. 39.

denen das Auszählen der Stimme mittels technischer und mechanischer Geräte erfolgt.[25]

Zu unterscheiden sind hier solche Systeme, bei denen ein vom Wähler ausgefüllter papierner Wahlschein durch ein technisches Gerät eingelesen wird, und solche, bei denen kein Papierdokument des Wählers existiert, sondern das Gerät die Stimme mechanisch registriert.[26]

a) Die Lochkarte

Prominenteste und ursprünglichste Ausgestaltung der ersten Gruppe ist das Lochkarten-System („Punchcard"), welches noch bis vor 2 Jahren in großen Teilen der USA bei Wahlen eingesetzt wurde.[27] Hierbei gibt der Wähler seine Stimme ab, indem er auf einer mit vorperforierten Löchern versehenen Lochkarte, die dem Kandidaten zugeordnete Stelle ausstanzt und in die Wahlurne wirft.[28] Das Ausstanzen erfolgt entweder mit einer bereitstehenden Maschine oder aber mit einem ausgehändigten Stecker.[29] Die markierten Karten werden nach Wahlschluss mit Hilfe eines Computerlesegerätes ausgewertet und gezählt.

Während die Vorteile im Vergleich zum handausgezählten Wahlzettel klar in der völlig objektiven und sehr viel zügigeren Auszählung liegen, hat sich das Design der Lochkarten in Verbindung mit überalterten Geräten als sehr fehleranfällig erwiesen.[30] Hierbei hat sich auch die theoretisch bestehende Möglichkeit der Nachzählung per Hand als extrem schwierig und willkürlich herausgestellt, da keine klaren Regelungen über die genaue Beschaffenheit des ausgestanzten Papiers bestehen, damit dieses als gültige Stimme angesehen werden kann.[31]

---

[25] *Caltech/MIT*, S. 18; *Jones* in Gritzalis, S. 3, 5 f.; *Khorrami*, S. 28 f.
[26] *Caltech/MIT*, S. 18; *Khorrami*, S. 29 f.
[27] *Jones* in Gritzalis, S. 3, 6 f.; *Election Data Services*, Voting Equipment Summary 2004, abrufbar unter: http://www.edssurvey.com/images/File/VotingEquipStudies%20/ve2004_report.pdf, (Stand: 24.04.07).
[28] S. zu den zwei grundlegenden Lochkarten-Systemen: *Fischer*, S. 3 f.
[29] *Khorrami*, S. 29.
[30] *Jones* in Gritzalis, S. 3, 6 f.; *Fischer*, S. 7; insbesondere auch zu den Problemen bei den Präsidentschaftswahlen 2000 in Florida: *Caltech/MIT*, S. 6 f.
[31] Zu den Folgen dieser Unsicherheiten bei den Präsidentschaftswahlen in Florida: *Caltech/MIT*, S. 6 f.

b) Optical Scan

Als Reaktion auf die Schwierigkeiten mit der Lochkarte hat sich in den USA als Alternative nunmehr das Optical Scan-System durchgesetzt.[32] Der hierbei vom Wähler auszufüllende Wahlzettel unterscheidet sich von dem bei herkömmlichen Papierwahlen verwandten nur unwesentlich durch ein Lokalisierungsraster für den Scanner und die Markierungsinstruktionen für den Wähler.[33] Hierin wird der Wähler aufgefordert das Kästchen oder Oval neben dem Kandidaten vollständig auszufüllen, damit diese Stelle vom Scanner als Stimmabgabe erkannt werden kann.

Die Fehleranfälligkeit dieses Modells liegt weniger in der inzwischen ausgefeilten Hard- und Software als vielmehr in der Unfähigkeit mancher Wähler den Instruktionen zu folgen, so dass die Fehlerquote trotz intelligenter Technik nicht zu verachten ist.[34] Immerhin ist aber aufgrund des existierenden Papier-Belegs eine Nachzählung möglich.

c) Mechanical Lever Machine

Hierin liegt gerade der Unterschied zu dem Modell der „mechanical lever machine“ (mechanische Hebelmaschine), das ohne einen Papier-Wahlzettel operiert. Den einzelnen zur Wahl stehenden Kandidaten ist stattdessen jeweils ein eigener Hebel der Maschine zugeteilt.[35] Die Stimmabgabe erfolgt, indem der Wähler nach Freischaltung des Gerätes den dem Kandidaten entsprechenden Hebel betätigt und die Stimmentscheidung sodann durch die Bewegung eines Rädchens im Inneren der Maschine aufgezeichnet wird.[36] Wegen der fehlenden Nachzählmöglichkeit und einer sehr komplexen und schwer zu kontrollierenden Technik der Maschinen werden mechanische Hebelmaschinen nur noch sehr begrenzt eingesetzt.[37]

---

[32] Zum heutigen Stand der eingesetzten Wahltechniken in den USA: *Election Data Services*, Voting Equipment Study 2006, S. 2; *Fischer*, S. 4.
[33] *Jones* in Gritzalis, S. 3, 8.
[34] *Jones* in Gritzalis, S. 3, 9.
[35] *Fischer*, S. 3.
[36] *Khorrami*, S. 30.
[37] *Election Data Services*, Voting Equipment Study 2006, S. 2 und zur Entwicklung S. 3.

2. Computer Voting

Ursprünglich den mechanischen Hebelmaschinen nachempfunden, aber auf Computertechnik gestützt und inzwischen den PCs oder Bankautomaten angenähert, sind die „Direct Recording Electronic Voting"- oder „Computer Voting"-Systeme.[38] Ebenso wie ihr analoges Pendant verzichten diese Geräte auf die Verwendung eines papiernen Wahlzettels. Stattdessen erfolgt die Stimmabgabe durch Betätigung eines Knopfes oder durch Berührung einer Fläche auf dem Bildschirm („touch screen"), wodurch wiederum eine automatische Aufzeichnung der Stimme durch die Maschine erfolgt.[39] Abgelegt wird die Stimme automatisch in einem elektronischen Speichermedium wie einer Diskette, einem Speicher-Cardridge oder einer Smart Card, welches nach Wahlschluss daraufhin ausgelesen und -gezählt wird.[40] Wie bei der „lever voting machine" liegt die Schwäche hier in dem fehlenden unabhängigen Beleg der Stimmabgabe und der fehlenden Kontrollmöglichkeit des technischen Aufzeichnungsvorgangs; positiv zeichnet sich das System durch eine hohe Benutzerfreundlichkeit aus.[41]

3. Internetwahl

Herzstück der momentanen Diskussion im Bereich der elektronischen Wahl ist die Einführung von Internetwahlen. Als solches können nur die Wahlsysteme bezeichnet werden, bei denen entweder die Stimme schon über das Internet abgegeben wird, oder aber die Wahlcomputer der zuständigen Stellen untereinander über das Internet miteinander verbunden sind und zur Auszählung die Stimmen hierüber übertragen.[42] Nicht davon erfasst sind hingegen Systeme, bei denen nicht das Internet, sondern geschlossene Netze zur Datenübertragung hinzugezogen werden.[43] Auch bei der Stimmabgabe mittels des Internets sind verschiedene Modelle denkbar und in der Erprobung. Aus der Perspektive juristischer Problemstellungen bietet sich hier eine

[38] *Fischer*, S. 4; *Jones* in Gritzalis, S. 3, 9 f.; *Caltech/MIT*, S. 20.
[39] *Fischer*, S. 4 f.
[40] *Khorrami*, S. 31.
[41] *Leder*, DÖV 2002, S. 648.
[42] *Khorrami*, S. 32.
[43] *Will*, S. 67.

Differenzierung danach an, welche Kontrollmöglichkeiten öffentlichen Stellen bezüglich des Ablaufs der Wahl zukommt. Da die Überwachungsintensität maßgeblich davon abhängig ist, inwieweit der Wähler die Öffentlichkeit ausschließen kann, ist eine Unterscheidung nach dem Ort der Stimmabgabe zu machen.
Unter verfassungsrechtlichen Aspekten spielt es zudem eine große Rolle, um welche Form von Wahl es sich handelt: politische, gar parlamentarische, oder private Wahl.

a) Unterscheidung nach Ort der Wahl

Mit absteigender Intensität der Kontroll- und Überwachungsmöglichkeiten durch öffentliche Stellen, lassen sich daher drei Stufen der Internetwahlen unterscheiden: die Wahl im Wahllokal, an anderen öffentlichen Wahlstationen und im individuellen Bereich.[44]

aa) Internetwahl im Wahllokal

Bei der Internet Wahl im Wahllokal („Polling Place Internet Voting“) findet die Stimmabgabe an dort aufgestellten öffentlichen Eingabegeräten statt. Diese übermitteln die Stimmen anschließend über das Internet an andere zentralisierte Wahlcomputer, wo die Auszählung stattfindet.[45]
Wie bei der traditionellen Wahl ist die Kontrolle des Wahlablaufs durch die Öffentlichkeit gewährleistet und eine technische Überprüfung der Geräte durch die zuständige öffentliche Stelle deswegen möglich, weil die Wahlcomputer in ihrem Eigentum stehen.[46]

bb) Kiosk-Wahl

Bei der Kiosk-Wahl werden die öffentlichen Eingabegeräte nicht (nur) in Wahllokalen, sondern an Orten des öffentlichen Raumes aufgestellt, die für den Wähler u.U. noch leichter und schneller zu erreichen sind.[47] Denkbar sind hier insbesondere Einkaufspassagen, Bahnhöfe, Postfilialen, Büchereien und Schulen. Die Wahlterminals, PCs oder Touch-Screen-Wahlmaschinen, übermitteln die Stimmen wiederum über das Internet.

---

[44] *Khorrami*, S. 32; *Neymanns* in Buchstein, Neymanns, S. 23, 26; *Will*, S. 68.
[45] *Will*, S. 68.
[46] *Khorrami*, S. 32 f.
[47] *Will*, S. 68.

Auch bei diesem Modell ist eine gewisse Kontrolle des Wahlablaufs durch die Präsenz der Öffentlichkeit gegeben; die Wahlgeräte unterliegen der technischen Überprüfung durch die zuständigen Stellen.[48]

cc) Internetwahl aus dem individuellen Bereich

Die brisanteste Form der Internetwahl stellt diejenige aus dem individuellen Bereich dar („Remote Internet Voting"), bei der die Stimmabgabe von jedem beliebigen internetfähigen Gerät aus erfolgen kann. Das können neben dem heimischen PC auch der PC am Arbeitsplatz, im Internetcafé oder auch internetfähige Mobiltelefone[49] oder PDA sein.[50] Entscheidend ist, dass die Übertragungstechnik auf dem Internet basiert, die Stimmabgabe aus dem öffentlichen Raum in die Privatsphäre verschoben ist und folglich auch keine öffentliche Kontrolle der Geräte und des Wahlablaufs besteht.[51] Demgegenüber steht als Vorteil die absolute Unabhängigkeit und Flexibilität für den Wähler.

b) Unterscheidung nach Charakter der Wahl

Eine Unterscheidung der Internetwahlen[52] nach ihrem Charakter ist deswegen geboten, weil sich für politische Wahlen einerseits und private Wahlen andererseits unterschiedliche wahlrechtliche Anforderungen aus der Verfassung ergeben.

aa) Politische Wahlen

Die Wahlen zu den Parlamenten auf Bundes-, Landes- und kommunaler Ebene unterliegen den strikten Wahlrechtsgrundsätzen des Art. 38 Grundgesetz.[53] Hiernach sind die politischen Entscheidungsträger in

---

[48] *Khorrami*, S. 33 f.

[49] Nicht unter das „Remote Internet Voting" hingegen fällt die Stimmabgabe per SMS, da hierbei die Stimmübermittlung nicht auf der Internettechnologie basiert; nicht klargestellt von *Neymanns* in Buchstein/Neymanns, S. 23, 27; zur Wahl per SMS in der Schweiz: *Heckmann*, CR 2005, S. R124.

[50] *Neymanns* in Buchstein/Neymanns, S. 23, 27; *Will*, S. 69.

[51] *Khorrami*, S. 33.

[52] Richtigerweise ist die Differenzierung nach Art der Wahl auch auf die anderen Formen der elektronischen Wahl anzuwenden. Allerdings ist der Einsatz von nicht auf das Internet gestützten Wahlcomputern im nicht-parlamentarischen Bereich zu vernachlässigen, so dass es auf die Unterscheidung maßgeblich nur im Kontext der Internetwahlen ankommt.

[53] Für die Wahlen zu den Landesparlamenten und Kommunalorganen ergibt sich dies aus Art. 28 I 2 GG i.V.m. Art. 38 GG; *Schreiber*, Teil 1 Rn. 16.

allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl zu bestimmen. Aus diesen Wahlrechtsgrundsätzen i.V.m. den entsprechenden Wahlgesetzen ergeben sich sehr hohe Einzelvorgaben an die genaue technische Ausgestaltung internetbasierter Wahlen.[54]

bb) Private Wahlen

Angelehnt an die Grundsätze des Art. 38 I GG sind zwar meist auch die Anforderungen, die an private Wahlen gestellt werden. Dass sich das Wahlreglement, das sich die Firmen, Vereine oder private Organisationen selbst geben, konform zu den verfassungsrechtlichen Grundsätzen aus Art. 38 GG verhält, ist aber nicht zwingend. Der Spielraum für Internetwahlen im privaten Bereich ist somit sehr viel größer als im politischen Bereich. Genutzt wird diese Ausgestaltung der Wahl bislang vor allem in Aktionärsversammlungen,[55] Universitäten, Vereinen,[56] bei der Wahl der Kanzlerkandidaten auf den Parteitagen,[57] und bei Gewerkschaften.[58]

[54] *Buchstein* in Buchstein/Neymanns, S. 51 f.; *Khorrami*, S. 34; *Will*, S. 153.
[55] *Buchstein* in Buchstein/Neymanns, S. 52.
[56] *Alkassar/Krimmer/Volkamer*, DuD 2005, S. 480 ff.
[57] *Rüß*, ZRP 2001, S. 518, 519 m.w.N; http://www.virtueller-parteitag.de.
[58] *Buchstein* in Buchstein/Neymanns, S. 51, 52; *Khorrami*, S. 34, 41.

Kapitel 2: Wahlcomputer

Die vorliegende Arbeit konzentriert sich im Folgenden auf die drei elektronischen Wahlmethoden, die in Deutschland zum Teil bereits in (Test-)Wahlen eingesetzt wurden, bzw. hier besonders im Fokus der Diskussion um die zukünftige Einführung elektronischer Wahlen stehen: Der Wahlcomputer, der Wahlstift und die Internetwahl aus dem individuellen Bereich. Alle drei Wahlmethoden sollen dabei auf ihre Vereinbarkeit mit verfassungsrechtlichen Wahlgrundsätzen untersucht und die ihnen spezifischen technischen Eigenheiten, Stärken und Schwächen festgestellt werden.

Der Wahlcomputer war zeitweise schon auf dem besten Weg zum Durchbruch (als die Wahlgeräteverordnung 1999 explizit hierfür geändert wurde und die ersten Geräteeinsätze im Herbst des gleichen Jahres erfolgreich und problemlos verliefen); aber im Oktober 2006 kam es in den Niederlanden zu einem Ereignis, das die weitestgehend unbeobachtete Einführung der Wahlgeräte in Deutschland zunächst vereitelte: Die Bürgerinitiative „Wij vertrouwen stemcomputers niet“ (Wir vertrauen Wahlcomputern nicht) knackte erfolgreich einen Wahlcomputer der Firma Nedap und manipulierte das Gerät in der Weise, dass darauf Schach gespielt werden konnte.[59] Der „Nedap-Hack“ von Anfang Oktober 2006 hat die Befürworter der Wahlgeräte so gut wie „zurück auf Los!“[60] geschickt und die Diskussion über die Einführung erstmals aus dem kleinen Expertenkreis in die – wenn auch nicht breite - Öffentlichkeit gebracht. Politiker und Behörden haben dem Wahlcomputer als Wahlsystem der Zukunft zwar als Reaktion noch keine endgültige Absage erteilt, die flächendeckende Einführung dieses Systems ist aber zunächst stark in die Kritik geraten und zum Teil sind akute Anschaffungen gestoppt worden.[61]

[59] *Wilkens*, Heise-News vom 05.10.06, abrufbar unter: http://www.heise.de/newsticker/meldung/79052, (Stand: 28.04.07).
[60] So der Vergleich von *Sietmann*, c’t 24/06, S. 72.
[61] *Sietmann*, Heise-News vom 19.01.07, abrufbar unter: http://www.heise.de/newsticker/meldung/84396, (Stand: 30.04.07).

Ob das Aufsehen erregende Ereignis in den Niederlanden jedoch zum endgültigen Scheitern des Wahlcomputer-Systems in Deutschland führen wird, ist aus politischer Perspektive noch völlig offen.

Das folgende Kapitel soll nach einer kurzen Darstellung des Status quo, die durch den Wahlcomputer tangierten wahlrechtlichen Probleme erläutern und sich kritisch mit der technischen Konzeption der für Deutschland vorgesehenen Wahlcomputer auseinandersetzen.

A. Historie

I. Deutschland

Als bundesweit erste Stadt ließ Köln 1999 bei der Europawahl und den anschließenden Landtags- und Kommunalwahlen ihre Bürger an Abstimmungsgeräten wählen.[62] Das bei den Wahlen in Köln eingesetzte Wahlgerät ESD-1 von Nedap stieß bei den Wählern, gerade auch denen der älteren Generation, aufgrund seiner hohen Benutzerfreundlichkeit auf große Akzeptanz. [63] Die Wahlen konnten mangels negativer Zwischenfälle als voller Erfolg verbucht werden und fungierten im weiteren Verlauf als positives Vorreitermodell für andere Städte.[64]

So entschieden sich schon bei den Bundestagswahlen 2002 etliche Städte für den Austausch von Papier und Wahlzettel durch elektronische Stimmabgabegeräte.

Bei den Bundestagswahlen 2005 addierte sich die Anzahl der bundesweit eingesetzten Wahlcomputer (Nedap Typ ESD-1) bereits auf eine Gesamtsumme von 1831 Geräten, aufgeteilt auf 38 Wahlkreise in 5 Ländern,[65] was einen Anteil der Gesamtstimmen von ca. 2,25 Prozent ausmachte. [66] Wiederum waren keine technischen Störungen oder sonstige Probleme mit der neuen Technik zu verzeichnen.

---

[62] *Leder*, DÖV 2002, S. 648 f.
[63] *Ostler*, Computerwoche 1999, Nr. 37. S. 10 ff.
[64] *Leder*, DÖV 2002, S. 648, 649.
[65] *Chaos Computer Club*, Einsatz von Nedap-Wahlgeräten bei der Bundestagswahl 2005; abrufbar unter: https://berlin.ccc.de/mediawiki/images/f/fa/Einsatz_Nedap_BTW_2005.pdf, (Stand: 28.04.07).
[66] *Oswald*, System der kollektiven Sicherheit, SZ vom 04.12.2006, abrufbar unter: http://www.sueddeutsche.de/computer/artikel/656/93563/, (Stand: 28.04.07).

Zum Teil weniger erfolgreich verliefen die im Jahr 2006 abgehaltenen Landtags- und Kommunalwahlen, bei denen auf den Einsatz von Wahlcomputern gesetzt wurde:

Im Landkreis Darmstadt-Dieburg führten diverse Software- und ein Programmierungsfehler zu starken Verzögerungen bei der Auszählung der Stimmen zur Kreistagswahl, so dass das offizielle Endergebnis erst drei Tage nach dem Wahltag bekannt gegeben werden konnte.[67] Insbesondere das System des Panaschierens und Kumulierens zeigte die Grenzen der angewandten Software auf.[68]

Auch bei den Kreistagswahlen im Rheingau-Taunus konnten die Stimmen des Wahlkreises Niedernhausen, der als einziger auf die vermeintliche Schnellig- und Bequemlichkeit der Technik setzte, aufgrund von Softwareproblemen erst zwei Tage später zum vorläufigen Endergebnis hinzugezählt werden.[69]

In Cottbus haben bereits neunmal computerbasierte Wahlen stattgefunden.[70] Doch auch hier hinterlässt der „Nedap-Hack“ Spuren und es muss umgedacht werden: Zwar wurde bei der Oberbürgermeisterwahl im Oktober 2006 noch ganz auf die innovative Technik gesetzt.[71] Aber es sind auch hier deutliche Anzeichen von Unsicherheit zu entdecken: So fühlte sich die Kreiswahlleiterin Sabine Hiekel aufgrund der Ereignisse in den Niederlanden genötigt, die Cottbusser Wahlgeräte im Vorfeld der Wahl eingehend durch Experten des Physikalisch-Technischen Bundesanstalt (PTB) überprüfen zu lassen und in einer offiziellen Stellungnahme deren Sicherheit zu garantieren.[72] Doch auch diese Maßnahme scheint die Bedenken der Offiziellen selbst nicht gänzlich ausgeräumt zu haben, wie sich im Januar 2007 zeigte, als offenkundig wurde, dass der schon beschlossene Miet-Kauf von 74

[67] *Echo Online*, Computer vergibt zu viele Stimmen, abrufbar unter: www.echo-online.de/kundenservice/a_detail.php3?id=363894, (Stand: 30.04.07).
[68] *Echo Online*, Computer vergibt zu viele Stimmen, abrufbar unter: www.echo-online.de/kundenservice/a_detail.php3?id=363894, (Stand: 30.04.07).
[69] *Wiesbadener Kurier* vom 29.03.2006, abrufbar unter: http://www.wiesbadener-kurier.de/region/objekt.php3?artikel_id=2328290, (Stand: 30.04.07).
[70] *Hiekel*, Pressemitteilung vom 14.10.06, S. 1.
[71] *Chaos Computer Club*, Bericht der CCC-Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus, abrufbar unter: http://www.ccc.de/updates/2006/bericht-ob-wahl-cottbus, (Stand: 30.04.07); *Kleinz*, Heise-News vom 14.10.2006, abrufbar unter: http://www.heise.de/newsticker/meldung/79480, (Stand: 13.01.07).
[72] *Hiekel*, Pressemitteilung vom 14.10.06, S. 2 f.

Nedap-Wahlcomputern [73] storniert wurde. [74] Die angemieteten Wahlgeräte hat die Stadt bereits wieder dem Eigentümer zurückgegeben. Hinsichtlich der Diskussion über die bei der Wahl 2008 einzusetzende Wahlmethode muss Cottbus nun erneut bei Null anfangen.

II. International

Wie in Deutschland, werden auch im europäischen Ausland unterschiedliche Erfahrungen mit dem Einsatz von Wahlcomputern gemacht.

Bislang unprätentiöser Vorreiter seit fast zwei Jahrzehnten sind die Niederlanden, die schon Anfang der neunziger Jahre von Papierstimmzetteln auf Computerwahlsysteme umstellten. Nahezu flächendeckend wurden die Wahlen im Nachbarland mit Hilfe von Geräten von Nedap (Typ ES3B) und SDU durchgeführt. [75] Umso unvorbereiteter traf das Land nun der „Nedap-Hack" und die daraus resultierende Diskussion über die Sicherheit von Wahlcomputern insgesamt und Nedap-Geräten im Speziellen. Zwar erscheint die Interpretation der Lage der Regierungskreise als „total panisch" und der Zukunft des Wahlcomputers als „völlig offen"[76] ein wenig zu dramatisch. Tatsächlich ist aber die niederländische Regierung wachgerüttelt worden und sah sich zum Erlass von Maßnahmen gezwungen. So wurden zu den Parlamentswahlen am 22. November 2006 nur noch Geräte der Firma Nedap Typ ES3B, nicht aber der Firma SDU, zugelassen und einige sicherheitstechnische Maßnahmen angeordnet. [77] Dass dies eine ausreichende und für die Bürgerinitiative „Wij vertrouwen stemcomputers niet" zufrieden stellende Reaktion auf den spektakulären

[73] *Stadt Cottbus*, Vorlage-II-025-30/06 vom 27.09.06, abrufbar unter: http://cottbus.avc-online.de/abfrage/senator/index.pl?G_CONTEXT=_xvMgaTNxNLMDNydS7RqFw&G_ID=0:Vorlage:2431, (Stand: 30.04.07).

[74] *Stadt Cottbus*, Vorlage II-004/07 vom 31.01.07, abrufbar unter: http://cottbus.avc-online.de/abfrage/senator/index.pl?S_SID=eQ01ORd3DCtLCcztf5cDZg:15a&G_CONTEXT=_xvMgaTNxNLMDNydS7RqFw&G_ID=0:Vorlage:5492, (Stand: 30.04.07); *Sietmann*, Heise-News vom 29.02.07, abrufbar unter: http://www.heise.de/newsticker/meldung/84396, (Stand: 05.03.07).

[75] *Kleijn*, Heise-News vom 31.10.06, abrufbar unter: http://www.heise.de/newsticker/meldung/80316, (Stand: 30.04.07).

[76] *Sietmann*, c't 05/07, S. 42, 44.

[77] *Kleijn*, Heise-News vom 31.10.06, abrufbar unter: http://www.heise.de/newsticker/meldung/80316, (Stand: 30.04.07).

„Nedap-Hack“ darstellt, erscheint jedoch mehr als fraglich. Womöglich muss sich die niederländische Regierung ähnlich wie die deutsche auf einen offeneren Diskurs mit ihren Kritikern und der alarmierten Bevölkerung einlassen.

Italien hat nach dem Verdacht einer inkorrekten Stimmerfassung bei der Übertragung von manuellen Ergebnissen auf Zähl-PCs bei den Präsidentschaftswahlen im Mai 2006 das Aus für jegliche Art der elektronischen Stimmabgabe oder -auswertung erklärt.[78] Es sieht die Gefahren einer weit reichenden Manipulation bei Papierwahlen als sehr viel geringer an und verzichtet daher auf die Technisierung der Wahl.

Auch in Irland ist es bislang noch zu keinem Einsatz der elektronischen Wahlgeräte gekommen. Das Kuriose im Fall Irlands ist allerdings, dass die irische Regierung in vorauseilendem Eifer für die Europawahl 2004 schon Wahlgeräte der Firma Nedap (Typ ESI2), ähnlich wie sie in Deutschland auch zum Einsatz kommen sollen, für 51 Millionen Euro erstanden hat.[79] Dass die Iren aber bislang immer noch mit Papier und Stift wählen und die original verpackten Geräte unberührt in Lagerhallen geblieben sind, ist auf die Initiative „Irish Citizens for Trustworthy E-Voting“ zurückzuführen.[80] Die Gruppe provozierte eine Diskussion über die bis dato an der Öffentlichkeit vorbei manövrierte Einführung der Wahlcomputer und zwang die Regierung letztlich dazu nachträglich eine Studie über die Sicherheit und Eignung der Nedap-Geräte in Auftrag zu geben.[81] Zwar bescheinigte dieses Gutachten den Wahlmaschinen eine generelle Eignung, bemängelte aber das im Vergleich zur Papierwahl fehlende Audit[82] und stellte dem System daher ein entscheidendes

[78] *Sietmann*, c’t 05/07, S. 42.
[79] *Sietmann*, c’t 16/06, S. 54.
[80] *Sietmann*, c’t 05/07, S. 42, 44; *Sietmann*, Heise-News vom 09.02.07, abrufbar unter: http://www.heise.de/newsticker/meldung/85092, (Stand: 05.03.07).
[81] *Sietmann* c’t 05/07, S. 42, 44; *Sietmann*, Heise-News vom 09.02.07, abrufbar unter: http://www.heise.de/newsticker/meldung/85092, (Stand: 05.03.07).
[82] S. die Berichte der Kommission von 2004 und 2006, abrufbar unter: http://www.cev.ie/htm/report/, (Stand: 30.04.07); *Sietmann*, c’t 16/06, S. 54.

Defizit aus, was schließlich zu der teueren Einmottung der Geräte[83] führte.

Beim jüngsten Einsatz von Wahlcomputern im Ausland, bei den Präsidentschaftswahlen in Frankreich im Mai dieses Jahres, sorgte die Technik vielfach für Verdruss: Die extrem hohe Wahlbeteiligung führte bei zu schmaler Infrastruktur (ein Wahlcomputer ersetzte teilweise vier Wahlkabinen) und zeitraubenden Bedienungsschwierigkeiten mancherorts zu Wartezeiten von mehr als einer Stunde.[84] In Einzelfällen resultierte dies in derartigem Verdruss der Wähler, dass diese ohne Stimmabgabe unverrichteter Dinge den Heimweg antraten.

In den USA hatte sich vor allem Florida nach dem Wahldebakel von 2000 um die Einführung von Wahlcomputern bemüht. Doch auch mit dem Nachfolgersystem der „Touchscreen Direct-Recording-Electronic"-Geräten hatte der Bundesstaat kein glückliches Händchen. Bei den Kongresswahlen im November 2006 kam es erneut zum nicht nachvollziehbaren Verlust von 18.000 Stimmen, die womöglich auf technische Ungenauigkeiten zurückzuführen sind.[85] Nun steht in Florida ein erneuter Umschwung von den Touchscreen-Wahlgeräten auf Wahlzettel-Scanner an, nachdem das Fehlen eines papiernen Wahlbelegs und damit einer akkuraten Wahlüberprüfung beim Touchscreen-System als entscheidendes Defizit empfunden wurde.[86]

B. Funktionsweise

Für den Wähler beginnt der Stimmabgabeprozess wie bislang auch zunächst mit seiner Identifikation und Authentifikation beim Wahlvorstand durch Vorlage des Personalausweises und der Wahlbenachrichtigung. Zwar ist theoretisch sowohl der Einsatz von Smartcards als auch von biometrischen Identifikationsdaten auf lange

[83] Allein die Aufbewahrung der Wahlcomputer in einer sicheren Umgebung kostet Irland jährlich 700.000 Euro: *Sietmann*, c't 16/06, S. 54.
[84] *Ziegler*, Heise-News vom 23.04.07, abrufbar unter: http://www.heise.de/newsticker/meldung/88653, (Stand: 30.04.07).
[85] *Sietmann*, Heise-News vom 20.04.07, abrufbar unter: http://www.heise.de/newsticker/meldung/88566, (Stand: 05.03.07).
[86] *Braun*, Heise-News vom 03.02.07, abrufbar unter: http://www.heise.de/newsticker/meldung/84751, (Stand: 05.03.07).

Sicht denkbar und wurde im Ausland auch schon erfolgreich erprobt.[87] Für das in Deutschland relevante System der Nedap-Geräte, ist eine solche rein technisch-basierte Identifikation bislang weder angedacht noch von Nöten, da das System ohnehin auf einen vor Ort anwesenden Wahlvorstand setzt.[88] Die Stimmabgabe selbst findet nach der Identifikation des Wählers nicht in der herkömmlichen Wahlkabine, sondern am Wahlcomputer statt:

Der Wahlcomputer – bezogen auf den Gerätetyp Nedap ESD-1[89] - kommt äußerlich relativ unscheinbar daher: Aufbewahrt in einem Koffer stellt das 30 kg schwere Gerät aufgebaut Wahlkabine, Wahlurne und Stimmzettel zugleich dar. Die Benutzerfläche, wie sie sich dem Wähler präsentiert, besteht aus einer 85x46cm großen Folie und einem Display am oberen Rand des Gerätes. Die justierbare Folie stellt den Gerätestimmzettel dar und gibt die Kandidaten und Parteien wie auf dem traditionellen Papierstimmzettel angeordnet wieder. Per Knopfdruck auf die dem Kandidaten zugeordnete Taste kann der Wähler seine Stimme abgeben. Auf dem Display erscheint daraufhin die getroffene Auswahl und es wird zum jeweils nächsten Wahlschritt aufgefordert (Bestätigung der Auswahl, Abgabe der Zweitstimme etc.). Eine Taste für eine Wahlenthaltung („ungültig“) ist ebenso vorgesehen wie eine Korrekturtaste.

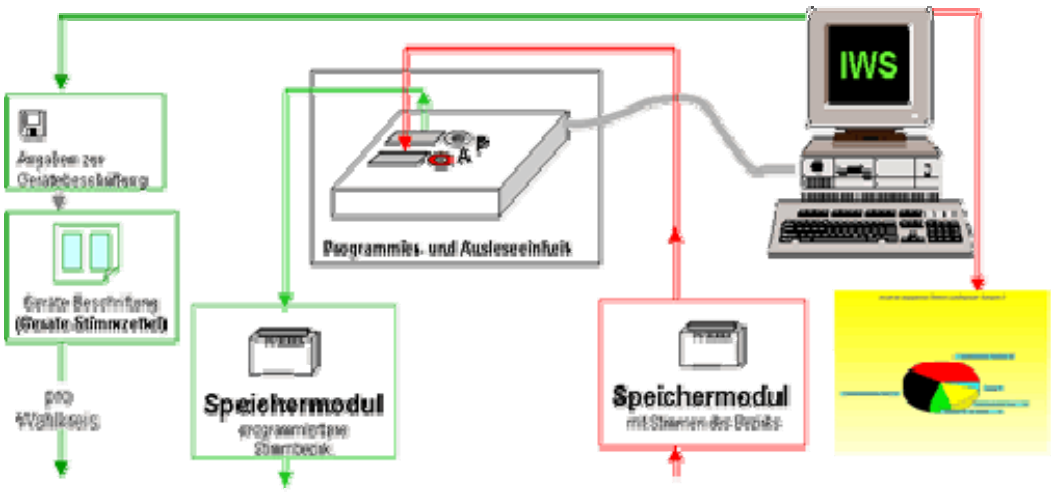
Hinter dieser äußeren Einfachheit steckt jedoch ein hochkomplexes technisches Hard- und Software-System, das im Folgenden vereinfacht auf Grundlage des PTB-Prüfberichts[90] erläutert und anhand der Grafik veranschaulicht werden soll:

[87] Bei den Präsidentenwahlen 2002 in Mérignac, Frankreich, mussten sich die Wähler mit ihrem Fingerabdruck und einer smart card, auf der die biometrischen Daten des Fingerabdrucks zum Abgleichen gespeichert waren, identifizieren. Vgl. *Will*, S. 51.

[88] Sicherheitsrechtlich bedenklich erscheint eine Authentifikation mittels Biometrie im Bereich der Wahlen ohnehin. Vgl. *Hof* in Prosser/Krimmer, S. 63, 71.

[89] Vgl. zu den technischen Angaben: *Physikalisch-Technische-Prüfanstalt*, Prüfbericht, S. 4 ff.; vgl. auch *Sietmann*, c’t 20/06, S. 86, 93.

[90] *Physikalisch-Technische Bundesanstalt*, Prüfbericht, S. 4 ff.; vgl. auch *Sietmann*, c’t 20/06, S. 86, 93.



Das Speichermodul wird vor der Wahl in das Wahlgerät eingesetzt.		Das Speichermodul wird dem Gerät nach der Wahl entnommen.

Es folgt die Wahl

Nedap/HSG Wahlsysteme: Der Gesamtablauf des Integralen Wahlsystems[91]

Die elektronische Ausstattung des Wahlgeräts stellen ein Motorola-M68000-Prozessor und zwei die Anwendung speichernde EPROMs des Typs 27C512 dar. Auf der Geräte-Rückseite integriert ist ein Thermoprinter, der nach Abschluss aller Stimmabgaben das Wahlergebnis und -protokoll in Form eines Kassenbelegs ausdruckt. Hauptelement des Wahlgeräts selbst ist ein herausnehmbares Stimmspeichermodul, das zwei Flash EEPROMs des Typs 28F512 enthält und die Wahlurne elektronisch ersetzt. Hier wird jede Stimme auf den zur Verfügung stehenden 2x64 Kilobyte selbsttätig, ohne Möglichkeit der Rückverfolgung oder Reproduktion, anonym und an völlig zufälliger Position abgespeichert.

Ebenfalls auf diesem Speichermodul ist die Zuordnung und Freigabemöglichkeit der wahlspezifisch belegten Tasten zu den

[91] http://www.wahlsysteme.de/Homepage.htm, (Stand: 22.06.07).

Kandidaten festgehalten (Initialisierungsdaten). Die - von insgesamt 1116 auf dem Wahltableau zur Verfügung stehenden - nicht programmierten Felder sind funktionslos und werden bei Einschub des Speichermoduls in das Hauptgerät nicht frei geschaltet.

Zur Kontrolle und Freischaltung des Speichermoduls bedient sich der Wahlvorstand am Wahltag selbst einer eigenen Bedieneinheit, die via Signalkabel mit dem Wahlgerät verbunden ist. Mit diesem Gerät können die Wahlvorgänge freigeschaltet, der reibungslose technische Ablauf überwacht und – wo vorgesehen – übliche wahlstatistische Daten hinzugefügt werden. Nach jeder abgeschlossenen Wahl und dem individuellen Wahlvorgang sperrt sich das Wahlgerät automatisch.

Auch für die Vorbereitung und Auswertung der Wahl wird über das eigentliche Wahlgerät hinaus eine weitere technische Einheit benötigt: ein normaler PC, der mit einem separaten Programmier- und Auslesegerät ausgestattet ist. Die Wahlvorbereitung liegt darin, dass mit Hilfe der „Integrierten Wahlsystem"-Software iws.exe das Speichermodul spezifisch für den jeweiligen Wahl-/Stimmbezirk auf dem ersten Steckplatz der separaten Programmier- und Speichereinheit programmiert wird. Im Gegenzug dient der zweite Auslese-Steckplatz nach Abschluss der Wahl zum Auswerten des Speichermoduls, so dass die Ergebnisse nachfolgend mit Hilfe eines Tabellenkalkulationsprogramms auf dem Rechner zur weiteren Analyse zur Verfügung stehen.

C. Rechtliche Zulässigkeit und technische Probleme

Durch den Nedap-Hack[92] wurden gravierende, da sicherheitstechnisch sehr sensible, Schwachstellen beim Wahlcomputer Typ ES3B der Firma Nedap aufgedeckt. Die rechtliche Zulässigkeit des Einsatzes der Wahlgeräte Nedap Typ ESD-1 und ESD-2, die in Deutschland zum Teil bereits verwendet wurden, ist durch dieses Ereignis deshalb nun auch

[92] *Sietmann*, Heise-News vom 05.10.06, abrufbar unter: http://www.heise.de/newsticker/meldung/79052, (Stand: 05.03.07).

stark in Frage gestellt worden, weil die drei Gerätetypen bezüglich der aufgedeckten Sicherheitslücken nahezu baugleich sind.[93]

Ob der Einsatz von Wahlcomputern generell und im speziellen Fall der Geräte Nedap Typ ESD-1 und ESD-2 unter den bestehenden rechtlichen Vorgaben in Deutschland unzulässig ist, soll im Folgenden erläutert werden.

I. Relevante Normen und Gesetze

Zwar sind für die Durchführung sowohl von Bundestags- und Europawahlen als auch von Landtagswahlen in Deutschland die Städte und Gemeinden zuständig. Ihnen obliegt es das jeweilige Wahlverfahren – also papierner Wahlzettel oder elektronische Wahl – zu bestimmen und die nötigen Anschaffungen zu tätigen. Der Einsatz von Wahlgeräten kann dennoch nur erfolgen, insoweit die einzusetzenden Wahlgeräte zugelassen sind und ihre Verwendung den gesetzlichen Anforderungen entspricht.[94]

1. Bundestags- und Europawahlen

Der Einsatz von Wahlgeräten bei Bundestags- und Europawahlen[95] muss den Vorgaben, die § 35 Bundeswahlgesetz (BWG) und die Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag (BWahlGV) aufstellen, genügen. Über die rechtlichen Anforderungen, die an einen zulässigen Einsatz von Wahlgeräten generell zu stellen sind, entscheidet nach § 35 II BWG das Bundesinnenministerium in einem zweistufigen Verfahren. Die vom Gerätehersteller beantragte Bauartzulassung wird dabei erst nach eingehender Prüfung [96] des Gerätetyps durch die PTB anhand der vom Bundesinnenministerium erlassenen Anforderungen der BWahlGV gegeben. Nach erfolgter

[93] Vgl. *TNO-rapport*, S. 3 f.; *Chaos Computer Club*, Wahlcomputer, abrufbar unter: https://berlin.ccc.de/wiki/Wahlcomputer, (Stand: 10.05.07).
[94] Schematische Darstellung des Zulassungsverfahrens: *Sietmann*, c't 24/06, S. 72, 75.
[95] Vgl. für die Europawahlen: § 17 Europawahlgesetz.
[96] Die Prüfberichte werden grundsätzlich weder von der PTB noch vom BMI veröffentlicht. Im Einverständnis mit dem Hersteller HSG Wahlsysteme GmbH ist aber nun ein Prüfbericht über das Gerät Nedap ESD-1 abrufbar unter: http://www.wahlrecht.de/doku/doku/PB-ESD1-SW03.08-BTW.pdf, (Stand: 10.05.07).

genereller Zulassung muss zudem noch die Zulassung zum Einsatz bei der jeweiligen Wahl beim Bundesinnenminister eingeholt werden.[97]
Bislang haben als mikroprozessorgesteuerte Wahlmaschinen nur die Wahlgeräte von Nedap Typen ESD-1 und ESD-2 die Bauartzulassung des Bundesinnenministeriums erhalten.[98]

2. Landtagswahlen

Für den Bereich der Landtagswahlen haben bislang lediglich sieben Bundesländer den rechtlichen Rahmen für den Einsatz von Wahlgeräten geschaffen: [99] In Baden-Württemberg, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt und Schleswig-Holstein wurden Wahlgeräteverordnungen erlassen, die - an der BWahlGV orientiert - ebenso ein zweistufiges Bauartzulassungs- und Verwendungsgenehmigungsverfahren durch die Landesinnenminister vorsehen. Zwar erlassen die Länder formal gesehen eine eigene Bauartzulassung; mangels Beteiligung einer eigenen technischen Landesbehörde stützen sie sich aber prüftechnisch gesehen im Wesentlichen auf das Ergebnis der PTB und erheben dieses als Grundlage für die eigene Gerätezulassung.[100] Eine originäre Kontrolle findet somit insbesondere bezüglich landesspezifischer Wahlsystemanforderungen statt, die eine Eignung des Gerätetyps ausschließen könnten.

II. Rechtliche Zulässigkeit der Wahlgerätesysteme

Die Nedap Wahlgeräte Typen ESD-1 und ESD-2 haben vom Bundesinnenministerium die Bauartzulassung und die Verwendungsgenehmigung für die Europa- sowie Bundestagswahlen 1999 bzw. 2005 erhalten. Die beim Nedap-Hack aufgedeckten Sicherheitslücken und Manipulationsmöglichkeiten drängen aber den Gedanken auf, dass die Geräte weder den rechtlichen Anforderungen, die das BWG und die BWahlGV aufstellen, gerecht werden, noch im

[97] *Schreiber*, § 35 Rn. 6.
[98] *Chaos Computer Club*, Wahlcomputer, abrufbar unter: https://berlin.ccc.de/wiki/Wahlcomputer, (Stand: 10.05.07).
[99] *Heckmann*, CR 2005, S. R124; *Leder*, DÖV 2002, S. 648, 650.
[100] *Leder*, DÖV 2002, S. 648, 650 f.

Hinblick auf verfassungsrechtliche Wahlgrundsätze zum Einsatz kommen dürften. Welchen genauen Anforderungen die Wahlcomputer einfachgesetzlich entsprechen müssen und ob sie geeignet sind auch die verfassungsrechtlichen Wahlgrundsätze einzuhalten, ist im Folgenden zu erörtern.

1. Vereinbarkeit mit BWG und BWahlGV

Einfachgesetzlich sind die Anforderungen, die an Wahlgeräte gestellt werden, in § 35 BWG niedergelegt und in der BWahlGV näher ausgestaltet. Aber auch die übrigen Vorschriften des BWG bleiben von § 35 BWG unberührt und müssen deshalb Beachtung finden.[101]

a) Wahlgeheimnis

Der Geheimhaltungs-Wahlgrundsatz ist in § 35 II BWG einfachgesetzlich normiert und bestimmt, dass die einzusetzenden Geräte insbesondere die Geheimhaltung der Stimmen gewährleisten müssen. Während die PTB dem Gerätetypus Nedap ESD-1 in seinem Prüfbericht noch die Einhaltung des Wahlgeheimnisses bescheinigte,[102] offenbarte der Nedap-Hack eine andere Realität:[103]

Aus einer Entfernung von einigen Metern konnte die Gruppe um Rop Gonggrijp elektromagnetische Emissionen feststellen. Es wurden von den Wahlgeräten abstrahlende Signale ausfindig gemacht, die unter bestimmten Umständen Rückschlüsse auf das Stimmabgabeverhalten der Wähler zuließen.[104] Aus dieser Erkenntnis heraus leitet die niederländische Initiative einen massiven Verstoß gegen den Geheimhaltungsgrundsatz ab und fordert den Nichteinsatz aller Wahlcomputer.[105] Dagegen versucht Jan Groenendaal, Geschäftsführer von Nedap/Groenendaal, die Sicherheitsanalyseergebnisse ganz erheblich

[101] *Leder*, DÖV 2002, S. 648, 652.
[102] *Physikalisch-Technische Bundesanstalt*, Prüfbericht, S. 28.
[103] S. den gesamten Sicherheits-Analyse-Bericht: *Wij vertrouwen stemcomputers niet*, Nedap/Groenendaal ES3B voting computer – a security analysis, abrufbar unter: http://www.wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf, (Stand: 10.05.07).
[104] Zu der technisch detaillierten Analyse: *Wij vertrouwen stemcomputers niet*, Security Analysis, S. 14 ff.
[105] *Wij vertrouven stemcomputers niet*, Pressebericht vom 01.11.06, abrufbar unter: http://www.wijvertrouwenstemcomputersniet.nl/Persbericht_1_nov_2006, (Stand: 11.05.07).

dadurch zu relativieren, dass er Beispiele anderer Wahlsysteme anbringt, die das Wahlgeheimnis ebenfalls nicht bis zur letzten Instanz zu wahren geeignet sind, und dennoch seit langem kritiklos eingesetzt werden.[106] Während er damit allerdings keineswegs die theoretisch technische Möglichkeit des Abhörens dementiert, wehrt sich auf Seiten der deutschen Verantwortlichen PTB-Direktor Dieter Richter gegen den Vorwurf der Abhörbarkeit.[107] Anders als bei den in den Niederlanden verwendeten und gehackten Wahlgeräten des Typus ES3B, wären Signalabstrahlungen in solcher Intensität und Reichweite, dass das Wahlgeheimnis gefährdet sei, bei den in Deutschland eingesetzten Geräten (ESD-1 und ESD-2) nicht festzustellen gewesen.[108] Dies sei auf einen anders gearteten mechanischen Aufbau, insbesondere auf eine verbesserte Abschirmung, zurückzuführen.[109] Unglücklicherweise ist diese aber in keinem der Prüfberichte technisch nachvollziehbar dokumentiert. Vielmehr bestätigt eine neue Studie des Chaos Computer Clubs auch für die in Deutschland eingesetzten Wahlgeräte das Risiko „kompromittierender Emissionen".[110]

b) Korrekte Durchführung des Wahlprozesses

Noch viel größere Zweifel hinsichtlich der Vereinbarkeit der Wahlgeräte mit dem geltenden Recht bringt die beim Nedap-Hack vollzogene Manipulation der Geräte hervor: In einem kaum fünf-minütigen Eingriff tauschten die Hacker das Steuerungsprogramm des Wahlgerätes aus, indem sie die zwei herausnehmbaren EPROMS mit eigenen gefälschten Komponenten ersetzten.[111] Dieser Hack lässt starke Zweifel an der Vereinbarkeit der Nedap-Geräte[112] mit den Anforderungen der akkuraten

---

[106] *Groenendaal*, Wahlnachrichten November 2006, abrufbar unter: http://www.wahlsysteme.de/Wahlnachrichten/2006_Abhoeren_von_Wahlgeraeten.pdf, (Stand: 11.05.07).

[107] Richter in *Sietmann*, c't 24/06, S. 72, 74 f.; *Richter*, PTB Presseinformation vom 09.10.2006, abrufbar unter: http://www.ptb.de/de/aktuelles/archiv/presseinfos/pi2006/pitext/pi061009.htm, (Stand: 11.05.07).

[108] Richter in *Sietmann*, c't 24/06, S. 72, 74 f.

[109] *Richter*, PTB Presseinformation vom 09.10.2006, abrufbar unter: http://www.ptb.de/de/aktuelles/archiv/presseinfos/pi2006/pitext/pi061009.htm, (Stand: 11.05.07).

[110] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 45 ff.

[111] Zur Ausführlichen technischen Dokumentation: *Wij vertrouwen stemcomputers niet*, security analysis, S. 4 ff.

[112] Typen ES3B und ESD-1 und ESD-2 sind diesbezüglich baugleich.

und sicheren Stimmzählung und –speicherung sowie der korrekten Durchführung des Wahlprozesses insgesamt gemäß Anlage 1, Ziff. 3.4 (6) zur BWahlGV aufkommen.

Dass das Öffnen der Wahlcomputer und das Austauschen der EPROMS keine großen Schwierigkeiten machen würden, war spätestens seit dem Bericht der irländischen Untersuchungskommission [113] ein offenes Geheimnis.[114] Warum es aber erst dieses Hacks bedurfte, um wenigstens eine geringfügige technische Verbesserung hieran vorzunehmen (zusätzliche Versiegelung der EPROMS in den Niederlanden und auch in Cottbus)[115], bleibt unklar und schürt das Misstrauen bezüglich eines verantwortlichen Umgangs mit der Thematik.

Unerwartet traf die Verantwortlichen von Nedap/Groenendaal hingegen das Ausmaß der inhaltlichen Manipulationsmöglichkeit der Wahlgeräte:

Die vor laufender Kamera demonstrierte Umfunktionierung des Stimmabgabegeräts zu einem Schachcomputer ist zwar in erster Linie als publikumswirksamer Show-Effekt und Reaktion auf Jan Groenendaals Provokation[116] anzusehen. Ernstlich in Sorge versetzen muss einen dabei aber, dass den Hackern auch ohne Kenntnis des Quellcodes eine Manipulation dergestalt möglich war, dass gezielt Stimmen transferiert werden konnten. Entgegen der Behauptungen des Bundesinnenministeriums, dass im schlimmsten Fall allenfalls eine blinde Manipulation zu befürchten sei, weil den Hackern im Vorfeld der Wahl die Zuordnung der Listenplätze nicht bekannt wäre,[117] schaffte die niederländische Bürgerinitiative hingegen eine gezielte Manipulation zu

---

[113] *Commission on Electronic Voting*, First Report December 2004, Part 4.2 and Appendix 2B, abrufbar unter: http://www.cev.ie/htm/report/first_report.htm, (Stand: 12.05.07).

[114] *Richter*, PTB Presseinformation vom 09.10.2006, abrufbar unter: http://www.ptb.de/de/aktuelles/archiv/presseinfos/pi2006/pitext/pi061009.htm, (Stand: 11.05.07); *Sietmann*, c't 24/06, S. 72.

[115] *Fehndrich*, Wahlrecht-Nachrichten vom 19.10.2006, abrufbar unter: http://www.wahlrecht.de/news/2006/20, (Stand: 12.05.07); *Hiekel*, Pressemitteilung vom 14.10.06, S. 2.

[116] *Groenendaal*, WIJVERTROUWENSTEMCOMPUTERSNIET, abrufbar unter: http://www.election.nl/bizx_html/ISS/documents/WIJVERTROUWENSTEMCOMPUTERSNIET.pdf , (Stand: 12.05.07): „Und hinsichtlich der Behauptung, dass unser Geräte Schach spielen kann: Das würde ich gerne demonstriert sehen." (S.2).

[117] Vgl. *Sietmann*, c't 15/06, S. 104, 105.; *BMI*, Stellungnahme des Bundesinnenministeriums zu den Wahleinsprüchen 76/05, 108/05, 145/05, Ziffer 3.2.3, abrufbar unter: http://www.ulrichwiesner.de/stellungnahme_BMI.html, (Stand: 15.05.07).

Gunsten eines bestimmten Listenkandidaten oder einer Partei, da die hierfür notwendigen Informationen aus der Wahlkonfiguration des Stimmspeichermoduls ausgelesen werden konnten.[118]

Diesen allzu überwältigenden Manipulationsnachweisen aus dem Nedap-Hack begegnen die Verantwortlichen in Deutschland weiterhin dennoch mit dem Argument, dass in Deutschland die Manipulationsgefahr durch ein Gesamtpaket von Maßnahmen ausreichend ausgeschlossen werden kann.[119]

c) Aufdeckbarkeit von Manipulationen

Insbesondere der Anforderung aus BWahlGV Analge 1, Punkt 2.1, dass jegliche Manipulation an den Geräten nicht unentdeckt bleiben dürfen, werde in Deutschland dadurch entsprochen, dass eine Reihe von organisatorischen Maßnahmen zu einer lückenlosen Überwachung und zu einem nahezu 100%igen Ausschluss der Manipulationsmöglichkeit führte.[120] Zu diesem gedachten Gesamtkonzept von Maßnahmen gehöre neben der sicheren Aufbewahrung bei den Kommunen und den Kontrollen vor Wahlbeginn auch die Annahme, dass ohne den Quellcode eine Manipulation der Software in sinnvoller Weise nicht möglich sei.[121] Hinsichtlich des letzten Gesichtspunkts mussten sich die deutschen Verantwortlichen durch den Nedap-Hack nun eines Besseren belehren lassen. Aber auch die Verlässlichkeit der anderen angeführten Maßnahmen muss stark angezweifelt werden: Weder in der BWahlGV noch in ihrem Anhang 1 findet sich die verbindliche Anordnung zu einer durchgängig sicheren Verwahrung der Geräte zwischen den Wahleinsätzen. Und dass die Annahme Richters, dies sei eine

---

[118] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 13.

[119] *Anwendergemeinschaft Elektronischer Wahlgeräte*, Presseinformation zum 31.05.2006, abrufbar unter: http://www.hsg-wahlsysteme.de/Wahlnachrichten/2006_Presseinfo_Anwendergemeinschaft.pdf, (Stand: 16.05.07); *Schulze Geiping*, HSG-Wahlsysteme Wahlnachrichten Oktober 2006, abrufbar unter: http://www.wahlsysteme.de/Wahlnachrichten/2006_Niederlaender_hacken_Wahlgeraet01.pdf, (Stand: 16.05.07); Richter in *Sietmann*, c't 24/06, S. 72, 73.

[120] Richter in *Sietmann*, c't 24/06, S. 72, 73; *Richter*, PTB Presseinformation vom 09.10.2006, abrufbar unter: http://www.ptb.de/de/aktuelles/archiv/presseinfos/pi2006/pitext/pi061009.htm, (Stand: 11.05.07).

[121] Richter in *Sietmann*, c't 24/06, S. 72, 73; *BMI*, Stellungnahme des Bundesinnenministeriums zu den Wahleinsprüchen 76/05, 108/05, 145/05, Ziffer 3.2.2, abrufbar unter: http://www.ulrichwiesner.de/stellungnahme_BMI.html, (Stand: 15.05.07).

Selbstverständlichkeit für die Kommunen, gutgläubig, wenn nicht gar naiv ist, illustriert die Reportage der Bürgerinitiative um Rop Gongriijp für den Fall der Niederlande sehr anschaulich.[122] In einer Lagerhalle in Rotterdam werden 8.000 bei landesweiten Wahlen eingesetzte Wahlcomputer aufbewahrt, ohne dass der Zutritt zu dem Lagerraum mit Sicherheitskameras oder anderweitigen Zutrittskontrollen erschwert würde. Auch während des Transports der Computer in die jeweiligen Wahllokale sind die Geräte vor Zugriffen Dritter nicht geschützt.[123]
Ebenso lässt die BWahlGV eine Anordnung zur Versiegelung der EPROMS vermissen. Dieses nicht nachvollziehbare Defizit wird in Deutschland als Folge des Nedap-Hacks nun ernsthaft überdacht werden müssen und nicht bloß zu Einzelnachrüstungen, wie sie in Cottbus stattfanden, führen. Als relativ leicht umzusetzende technische Maßnahme wäre dies zumindest ein kleiner Schritt in die Richtung den gesetzlichen Vorgaben, die weniger nach einem organisatorischen Überwachungsgesamtkonzept, als vielmehr nach einem technischen Manipulationsschutz verlangen,[124] zu entsprechen.

d) Vereinbarkeit von Wahlgeräten mit Wahlrechtsgrundsätzen

Neben den Vorgaben der BWahlGV und ihren Anlagen schließt § 35 BWG aber auch die Anwendbarkeit der übrigen Vorschriften des BWG und natürlich der Verfassung beim Einsatz von Wahlgeräten keineswegs aus.[125] Die Zulässigkeit der Verwendung von Wahlcomputern muss sich deswegen auch an den übrigen Wahlrechtsgrundsätzen messen lassen, insbesondere am Öffentlichkeitsgrundsatz und am Grundsatz der Amtlichkeit.

---

[122] *Eén vaandag* vom 4.10.2006, abrufbar unter: http://player.omroep.nl/?aflID= 3355684&md5=e83e151c120fb91b83739b61fda939e6, (Stand: 13.05.07).
[123] S. auch: *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 39.
[124] Vgl. den Wortlaut Anlage 1, Ziffer 2.1. zur BWahlGV: „Das Wahlgerät ist so konstruiert, dass eine Veränderung des technischen Aufbaus und bei rechnergesteuerten Geräten auch der installierten Software durch unbefugte Dritte nicht unbemerkt bleibt."
[125] *Leder*, DÖV 2002, S. 648, 653.

aa) Öffentlichkeit der Wahl

Der Öffentlichkeitsgrundsatz, als ungeschriebener Verfassungsgrundsatz dem Demokratieprinzip (Art. 20 II GG) zu entnehmen,[126] ist im BWG in den Paragraphen 10 I und 31 einfachgesetzlich derart ausgestaltet, dass danach alle Entscheidungen der Wahlorgane in öffentlicher Sitzung und die Wahlhandlung an sich öffentlich zu erfolgen haben. Die Nachvollziehbarkeit und Transparenz der ordnungsgemäßen Wahlhandlung für jedermann gelten als Grundpfeiler einer demokratischen Willensbildung.[127] Das von der Bundesregierung mit den Wahlgeräten praktizierte Sicherheitskonzept wird diesen Anforderungen aber kaum gerecht: Hier wird stattdessen auf das schon lange überholte Modell des „security by obscurity", also die Geheimhaltung des Quellcodes als Kernsicherheitsmaßnahme, gesetzt.[128] Dass diese Herangehensweise aus technischer Sicht ohne Zukunft ist, hat der Nedap-Hack endgültig klar bewiesen. Gleichzeitig hält dieses Konzept aber auch den rechtlichen Anforderungen nicht stand. Anstatt eines leicht nachvollziehbaren Stimmabgabe-Modus wie bei der papiernen Stimmzettelwahl, wird die Überprüfung der Ordnungsmäßigkeit der Wahl aus dem öffentlichen Wahllokal heraus auf eine Überprüfung durch wenigen Experten verlagert.[129]

Zwar wird zum einen am Wahltag selbst durch den Wahlvorstand kontrolliert, dass die Zähl- und Speichervorrichtungen auf Null stehen und nicht genutzte Speicherplätze gesperrt sind (§ 10 I Ziff. 3, 4 BWahlGV). Diese dem Öffentlichkeitsgrundsatz womöglich noch annähernd gerecht werdende Schlusskontrolle ist aber für die Transparenz der elektronischen Stimmabgabe nicht der entscheidende Schritt. Die davor erfolgte Auswahl der Wahlgeräte, die Bauartzulassung und die Baugleichheitserklärung von einzusetzendem und zugelassenem

[126] Karpen in *Sietmann*, c't 01/06, S. 80 f.
[127] *Schreiber*, § 31 Rn. 2.
[128] *Sietmann*, c't 02/06, S. 20, 21; Wiesner in *Wolz*, FAZ vom 03.01.07, abrufbar unter: http://www.faz.net/s/RubFC06D389EE76479E9E76425072B196C3/Doc~ED7BB8B33DC2A4CCC8701C8B0672E58FF~ATpl~Ecommon~Scontent.html, (Stand: 05.03.07).
[129] *Karpen*, S. 36; *Leder*, DÖV 2002, S. 648, 652.

Gerät, finden außerhalb jeder Öffentlichkeit statt.[130] Hier entscheiden einige wenige Experten, im praktisch wahrscheinlichsten und durch § 7 BWahlGV zugelassenen Fall sogar der Hersteller selbst, über die Zulässigkeit und Funktionsfähigkeit der Geräte.[131] Den Wahlvorständen fehlt meist jegliche Expertise um den technischen Vorgang im Inneren der Geräte auch nur annähernd nachzuvollziehen, geschweige denn eine Manipulation aufdecken zu können. Selbst mit gewisser Expertise wäre aus technischer Sicht am Wahltag selbst eine Kontrolle, dass die Software des Gerätes nicht manipuliert worden ist, vor Ort nicht möglich: Die Software der Wahlmaschine identifiziert sich über eine Versionsnummer und zwei Prüfnummern, die das Gerät aber selbst generiert.[132] Eine Authentizitätsabgleichung mit der von der PTB zugelassenen Software kann also in den Wahllokalen gar nicht stattfinden. Das Bundesinnenministerium verweist als ausreichende, vorgelagerte öffentliche Kontrolle auf die Baumusterprüfung durch die PTB.[133] Auch diese findet aber ohne Anwesenheit der Öffentlichkeit statt und eine Offenlegung des Quellcodes wird aus Gründen der Wahrung von Geschäftsgeheimnissen des Herstellers Nedap abgelehnt.[134]

Aus dem für die breite Öffentlichkeit nachvollziehbaren Willensbildungsprozess wird demnach ein „Black-Box-Voting“[135], das den Wahlgrundsätzen der Verfassung keineswegs mehr entspricht,[136] weil die Stimmabgabe per Wahlgerät für den einzelnen Wähler nicht mehr nachzuvollziehen ist.[137] Eine Offenlegung des Quellcodes[138] oder

[130] *Hanßmann*, S. 188; *Leder*, DÖV 2002, S. 648, 652; *Sietmann*, c’t Hintergrund vom 21.02.07, abrufbar unter: http://www.heise.de/ct/hintergrund/meldung/85615, (Stand: 06.03.07).
[131] *Karpen*, S. 36; *Sietmann*, c’t 15/06, S. 104, 105.
[132] *Sietmann*, c’t 15/06, S. 104; *Sietmann*, c’t 20/06, S. 86 ff.
[133] Das gesteht auch das Bundesinnenministerium zu: *BMI*, Stellungnahme des Bundesinnenministeriums zu den Wahleinsprüchen 76/05, 108/05, 145/05, abrufbar unter: http://www.ulrichwiesner.de/stellungnahme_BMI.html, (Stand: 15.05.07); bzw. *Sietmann*, c’t 15/06, S. 104, 105.
[134] *BMI*, Stellungnahme des Bundesinnenministeriums zu den Wahleinsprüchen 76/05, 108/05, 145/05, abrufbar unter: http://www.ulrichwiesner.de/stellungnahme _BMI.html, (Stand: 15.05.07); *Sietmann*, c’t 15/06, S. 104, 105.
[135] Wiesner in *Wolz*, FAZ vom 03.01.07, abrufbar unter: http://www.faz.net/s/Rub FC06D389EE76479E9E76425072B196C3/Doc~ED7BB8B33DC2A4CCC8701C8B 0672E58FF~ATpl~Ecommon~Scontent.html, (Stand: 15.05.07).
[136] Karpen in *Sietmann*, c’t 01/06, S. 80 ff.
[137] *Karpen*, S. 36; *Schreiber*, § 35 Rn. 4.

eine technische Umgestaltung der Geräte derart, dass sie ein Trusted Platform Module erhalten, welches eine externe Überprüfung ermöglicht, [139] würde eine verlässliche Identifikation der Geräteprüfsummen im Wahllokal durch den Wahlvorstand oder die Öffentlichkeit garantieren.

bb) Amtlichkeit der Wahl

Auch eine rechtliche Vereinbarkeit des Einsatzes der Nedap-Wahlgeräte nach der BWahlGV mit dem Grundsatz der Amtlichkeit der Wahl, wird stark angezweifelt. [140] Während dieser Grundsatz besagt, dass die wahlbezogenen Handlungen von einem Amtsträger im Rahmen seiner Zuständigkeit vorgenommen werden müssen, eröffnet die BWahlGV hingegen in § 7 I BWahlGV die Möglichkeit, die Überprüfung der Funktionstüchtigkeit der Wahlgeräte vor der Wahl anstelle von einem Amtsträger auch durch den Hersteller selbst vornehmen zu lassen. Diese Alternative der Inanspruchnahme von Privaten zur Erfüllung von Staatsaufgaben ist zwar per se nicht ausgeschlossen. Doch muss dem Staat, hier also den Kreiswahlleitern, die tatsächliche Sachherrschaft über den Wahlablauf vorbehalten sein. [141] Diese ist aber dann nicht mehr anzunehmen, wenn die Verwaltungsangestellten nicht mehr in der Lage sind, die Funktionsfähigkeit der Geräte selbst zu überprüfen. Im Fall des Einsatzes von Wahlgeräten kann den Wahlvorständen in der Regel kein solcher technischer Sachverstand bezeugt werden, dass sie in der Lage wären eine Kontrolle der Geräte auf Ordnungsmäßigkeit durchzuführen. Stattdessen wird sich hier oft auf die Expertise des Herstellers oder anderer privater Spezialisten verlassen, was dem Grundsatz der Amtlichkeit klar widerspricht. [142]

---

[138] *Wiesner*, Wahlprüfbeschwerde 2 BvC 3/07, S. 80 f., abrufbar unter: http://www.ulrichwiesner.de/wp/070212_wahlpruefbeschwerde.pdf, (Stand: 15.05.07).
[139] *Sietmann*, c't 20/06, S. 86 ff.
[140] *Karpen*, S. 35 f.; *Leder*, DÖV 2002, S. 648, 651; *Wiesner*, Wahlprüfbeschwerde 2 BvC 3/07, S. 67, abrufbar unter: http://www.ulrichwiesner.de/wp/070212_ wahlpruefbeschwerde.pdf, (Stand: 15.05.07).
[141] *Di Fabio*, JZ 1999, S. 585, 591.
[142] *Leder*, DÖV 2002, S. 648, 651; *Sietmann*, c't Hintergrund vom 21.02.07, abrufbar unter: http://www.heise.de/ct/hintergrund/meldung/85615, (Stand: 06.03.07).

2. Sicherheit

Aus den verfassungsrechtlichen Wahlgrundsätzen des Art. 38 I 1 GG lässt sich die Anforderung an die Wahlgeräte ableiten, dass sie frei von jeglicher Manipulation bleiben. In seinem Bericht für das Bundesverfassungsgericht gibt der Chaos Computer Club einen umfassenden Überblick über die gravierenden Sicherheitsmängel der Nedap-Geräte.[143] Neben den bereits angeführten Defiziten bezüglich einer Manipulationsfreiheit der Wahlgerätekomponenten selber, besteht auch die Möglichkeit der Angriffe auf die Speichermodule, die zur Auswertung auf einem Zentral-PC ins Gemeindewahlamt gebracht werden. Ebenso ist die dort eingesetzte Auswertungssoftware mannigfaltiger Bedrohungen von Hackern und Innentätern ausgesetzt.[144]
Als völlig ungeeignet stellen sich insbesondere auch die physischen Sicherheitsmaßnahmen dar. Die Schlüsselsysteme, die den Zugriff von außen auf das Geräteinnere verhindern, und die Siegel, die die Unversehrtheit der einzelnen Gerätekomponenten dokumentieren sollen, sind von billigster Machart und können leicht auf dem freien Markt nachgekauft und gefälscht werden.[145]
Den hohen Anforderungen, die an die Sicherheit von bei parlamentarischen Wahlen einzusetzenden Wahlgeräten zu stellen sind, werden die Nedap-Wahlgeräte damit keinesfalls gerecht.[146]

3. Effektivität der Wahlprüfung

Des Weiteren führt die mangelnde Einhaltung des Öffentlichkeitsprinzips in einem nächsten Schritt auch dazu, dass es an einer effizienten Wahlprüfungsmöglichkeit fehlt. Um einen substantiierten Sachvortrag als Grundlage eines Einspruchs zur Erzwingung eines Wahlprüfungsverfahrens i.S.d. Art. 41 GG an den Bundestag vorbringen zu können, ist der Beschwerdeführer darauf angewiesen, dass er von den Tatsachen des Wahlhergangs Kenntnis erlangen kann. Dies wird ihm

[143] *Kurz/Rieger/Gonggrijp*, Nedap-Report, abrufbar unter: http://www.ccc.de/press/releases/2007/20070609/nedapReport54.pdf, (Stand: 11.06.07).
[144] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 19 f.
[145] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 33 ff.
[146] Ähnliche Sicherheitsmängel weisen die in den USA eingesetzten Diebold-Geräte auf: *Feldmann/Haldermann/Felten*, Diebold Security Analysis, abrufbar unter: http://itpolicy.princeton.edu/voting/ts-paper.pdf, (Stand: 23.03.07).

grundsätzlich nur durch die Öffentlichkeit der Wahlhandlung und der Stimmauszählung ermöglicht, welche im Fall der Wahlgeräte aber gerade nicht garantiert ist. Auch werden, anders als beim herkömmlichen Wahlverfahren, die für das Endergebnis wesentlichen Verfahrensschritte nicht in der Weise dokumentiert, dass der Beschwerdeführer sie zur Überprüfung vorlegen könnte. Denn der Vergleich von den Daten auf dem Stimmspeicher mit dem, was der geräteeigene Drucker nach Abschluss der Wahl ausgegeben hat, erlaubt nur einen Rückschluss auf die Funktionsfähigkeit des Druckers. Eine Überprüfung dahingehend, dass die tatsächlich abgegebenen Stimmen richtig gespeichert und zusammengezählt wurden, lässt das System damit nicht zu.[147]

Darüber hinaus auferlegt das Bundesinnenministerium die Beweislast einer tatsächlichen Wahlmanipulation dem Beschwerdeführer und lässt den Vorwurf einer rein theoretisch bestehenden Manipulationsmöglichkeit rechtlich nicht zu.[148]

Im Zusammenspiel mit dem tatsächlich nicht zu führenden Beweis einer Wahlmanipulation wegen des Fehlens einer geräteunabhängigen technischen Softwarekontrolle und der Transparenz ist eine effiziente Wahlüberprüfung folglich ausgeschlossen.[149]

III. Sonstige Anforderungen an Wahlgeräte

Insbesondere aus den negativen Wahlszenarien in den USA heraus, werden immer mehr Stimmen laut, die nach einem papiernen Stimmabgabebeleg verlangen, mit dem die Nachvollziehbarkeit des Zustandekommens des Wahlergebnisses gewährleistet würde.[150] Gemeint ist hierbei ausdrücklich nicht ein solcher Abschlussbeleg über das Geräte-Gesamtergebnis des Wahltags wie es auch die Nedap-Geräte vorsehen, sondern ein papierner Beleg jeder einzelnen Stimmabgabe, die gegebenenfalls auch durch den Wähler selbst noch bestätigt werden muss

[147] *Leder*, DÖV 2002, S. 648, 652.
[148] *Sietmann*, c't 20/06, S. 86 ff.; BT-Beschluss zum Wahleinspruch WP 145/05, Rn. 168; abrufbar unter: http://www.wahlrecht.de/wahlpruefung/20061214145.htm, (Stand: 16.05.07).
[149] *Sietmann*, c't 20/06, S. 86 ff.
[150] *CalTech/MIT*, S. 24; *Karpen*, S. 36 f.; *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 53 f., *Leder*, DÖV 2002, S. 648, 653; *STS*, Recommendations, S. 5 f.

(„voter-verified-paper-audit-trail“, im Folgenden: VVPAT).[151] Ein solches System würde nicht nur technisch die Nachprüfung im Manipulationsverdacht ermöglichen, sondern wäre auch aus soziologischen Gründen vorteilhaft.[152] Die Skepsis in der Bevölkerung gegenüber den komplexen Systemen der Wahlcomputer, ist im Zuge der Wahldesaster von Florida,[153] der Debakel mit den Sicherheitsvorkehrungen bei Diebold-Geräten[154] und schließlich durch den Nedap-Hack stetig gewachsen und intensiviert worden. Um den Glauben an ein sicheres Wahlsystem zu stärken ohne auf die Vorteile der elektronischen Stimmabgabe ganz verzichten zu müssen, wäre die Umrüstung auf Wahlcomputer mit VVPAT-Fähigkeit sinnvoll und geeignet.[155] Damit könnte auch dem Fehlen der öffentlichen Kontrolle und Transparenz des Verfahrens zumindest ansatzweise beigekommen werden.[156]

Zur Verbesserung der Sicherheit der Wahlgeräte wird zudem gefordert, dass die zu unterscheidenden Wahlschritte, Erzeugung der Stimme einerseits und Abgabe der Stimme andererseits, auch technisch klar voneinander abzugrenzen seien, indem hierzu zwei voneinander getrennte Geräte benutzt würden.[157] So sei ein System denkbar bei dem der Wähler eine Stimmkarte ausgehändigt bekommt, auf der alle Wahlzettel-Informationen abgespeichert sind. Diese Karte würde dann in ein Gerät eingeführt, dass die Angaben abbildet und dem Wähler die Stimmerzeugung durch Auswahl ermöglicht. Sodann wird die Karte in ein zweites Geräte eingeführt, wo der Wähler seine Stimme überprüfen und endgültig abgeben kann. Diese Stimmabgabe wird von diesem Gerät gespeichert und die Karte als Stimmbeleg einbehalten.[158] Ein solches System hätte den Vorteil, dass eine Kommunikation zwischen

---

[151] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 51; *Leder*, DÖV 2002, S. 648, 653.
[152] *Oostveen/Besselaar* in Prosser/Krimmer, S. 73 ff.
[153] *CalTech/MIT*, S. 6 ff.; *Sietmann*, Heise-News vom 20.04.07, abrufbar unter: http://www.heise.de/newsticker/meldung/88566, (Stand: 23.06.07).
[154] *Feldmann/Haldermann/Felten*, Diebold Security Analysis, S. 2 ff.; *Ziegler*, Heise-News vom 26.01.07, abrufbar unter: http://www.heise.de/newsticker/meldung/84345, (Stand: 23.06.07).
[155] *Oostveen/Besselaar* in Prosser/Krimmer, S. 73 ff.
[156] *Kurz/Rieger/Gonggrijp*, Nedap-Report, S. 51 f.; *Leder*, DÖV 2002, S. 648, 654.
[157] *CalTech/MIT*, S. 58 ff.; *Leder*, DÖV 2002, S. 648, 653 f.
[158] *CalTech/MIT*, S. 58 ff.

Stimmerzeugungs- und Stimmspeichereinheit technisch ausgeschlossen ist und ein geräteunabhängiger Beleg generiert wird.

IV. Geplante Einsätze und Initiativen gegen Wahlcomputer

Der Einsatz von Wahlgeräten stößt im In- und Ausland zunehmend auf harsche Kritik und vehementen Widerstand. Die ungelösten Sicherheitsrisiken und das Unterlaufen demokratischer Grundsätze haben die Wahlcomputer-Gegner auf die politische und rechtliche Bühne geholt.

1. Deutschland

In Deutschland wehrt sich der Physiker und Software-Spezialist Ulrich Wiesner durch alle Instanzen gegen den Einsatz von Wahlcomputern der Firma Nedap bei der Bundestagswahl 2005. Nachdem sein Wahlprüfungseinspruch im Oktober vom Bundestag als offensichtlich unbegründet abgelehnt wurde,[159] bemängelt er nun im Rahmen einer Verfassungsbeschwerde vor dem BVerfG vor allem die Verletzung des Öffentlichkeitsprinzips und die fehlende Transparenz des Wahlcomputersystems.[160] Erklärtes Ziel des Antrags ist formal die Wiederholung der Wahl und hilfsweise – und wegen der Dauer des Verfahrens bereits einschlägig – die Feststellung, dass der Einsatz der Nedap-Wahlgeräte gegen das Grundgesetz verstößt.[161] Das Verfahren liegt dem BVerfG nunmehr zur Entscheidung vor.

Zugleich muss sich der Petitionsausschuss des Bundestages mit einer Petition des Berliners Tobias Hahn befassen, die auf die Abschaffung des § 35 BWG als gesetzliche Grundlage für den Einsatz von Wahlcomputern gerichtet ist.[162] Auch Hahn begründet seine Petition mit der fehlenden Kontrollfähigkeit der Wahlgeräte und der mangelnden

---

[159] *Wahlprüfungsausschuss*, Beschlussempfehlung zum WP 145/05, BT-Drucksache 16/3600, S. 7 ff.; *Sietmann*, c't Hintergrund vom 21.02.07, abrufbar unter: http://www.heise.de/ct/hintergrund/meldung/85615, (Stand: 06.03.07).

[160] *Wiesner*, Wahlprüfbeschwerde 2 BvC 3/07, abrufbar unter: http://www.ulrichwiesner.de/wp/070212_Wahlpruefbeschwerde.pdf, (Stand: 15.05.07).

[161] *Wiesner*, Wahlprüfbeschwerde 2 BvC 3/07, S. 2 f., abrufbar unter: http://www.ulrichwiesner.de/wp/070212_wahlpruefbeschwerde.pdf, (Stand: 15.05.07).

[162] *Kleinz*, Heise-News vom 20.10.06, abrufbar unter: http://www.heise.de/newsticker/meldung/79791, (Stand: 06.03.07); Petition abrufbar unter: http://itc.napier.ac.uk/e-Petition/bundestag/view_petition.asp?PetitionID=294, (Stand: 06.03.07).

Öffentlichkeit und fand die Unterstützung von mehr als 45.000 Unterzeichnern, u.a. auch von Abgeordneten der Grünen.[163] In einer ersten Anhörung im Petitionsausschuss, blieben die Vertreter des Bundesinnenministeriums ihrer Linie treu und zeigten sich weiterhin überzeugt von der Manipulationssicherheit der Wahlgeräte, eine Revision der BWahlGV sei aber in Arbeit.[164]

2. Europa

Auch im übrigen Europa formieren sich die E-Voting-Aktivisten:
Die Niederlande sehen sich spätestens seit dem Nedap-Hack einer neuen öffentlichen Diskussion über ihr schon zwei Jahrzehnte lang eingesetztes Wahlsystem gegenüber. Die Bürgerinitiative „Wij vertrouwen stemcomputers niet“ [165] stellt das in den neunziger Jahren ohne öffentliche Diskussion eingeführte System erfolgreich in Frage und entwickelt sich zu einer der aktivsten Gruppen in Europa.
Zunächst sehr erfolgreich war auch das Vorgehen der Gruppe „Irish Citizens for Trustworthy E-Voting“ in Irland, der es gelang, dass die bereits für 51 Millionen Euro angeschafften Nedap-Wahlcomputer seit 2004 in Lagerräumen auf ihren ersten Einsatz warten.[166] Auf Initiative der Bürgerbewegung gab die Regierung ein Gutachten über die Geräte in Auftrag, welches zum Ergebnis kam, dass die Geräte grundsätzlich zwar für Wahlen geeignet seien, hinsichtlich einer Wahlüberprüfungsmöglichkeit der Papierwahl aber nachstehen und deswegen zunächst nicht eingesetzt werden sollten.[167] Einen Dämpfer verpasste Information Officer Emily O’Reilly aber kürzlich dem E-Voting-Aktivismus in Irland. Sie entschied, dass das Innenministerium Informationen über die Funktions- und Sicherheitsarchitektur der Wahlgeräte zurückhalten darf, da dem Geschäftsgeheimnis der Firma Nedap und der Geheimhaltung des Quellcodes aus Sicherheitsaspekten

[163] *Sietmann*, c’t 05/07, S. 42.
[164] *Sietmann*, Heise-News vom 18.06.07, abrufbar unter: http://www.heise.de/newsticker/meldung/91330, (Stand: 23.06.07).
[165] http://www.wijvertrouwenstemcomputersniet.nl.
[166] *Sietmann*, c’t 05/07, S. 42, 43.
[167] *Commission on Electronic Voting*, Second Report, July 2006, Part 5.5.2., S. 153 f., abrufbar unter: http://www.cev.ie/htm/report/second_report/pdf/Part%205%20Comparative%20Assessment.pdf, (Stand: 24.05.07).

eine höhere Bedeutung zukomme als der Informationsfreiheit der Bürger.[168] Wie in Deutschland setzen die Verantwortlichen also auch hier auf das Konzept des „Security by Obscurity".

In Frankreich flammte insbesondere vor den Präsidentschaftswahlen im Mai dieses Jahres die öffentliche Kritik und Sorge um die Stimmabgabe am Wahlcomputer auf. Im Zentrum der Kritik stehen auch hier das Fehlen einer Code-Inspektion der Software, des Prüfmechanismus zur Verifikation der Rechnerauthentizität und ein Papier-Audit zur geräteunabhängigen Nachzählung.[169] Die Petition der Bürgerinitiative „Citoyens et informaticiens pour un vote vérifié par l'écteur"[170] zur Beibehaltung der Papierzettel-Wahl haben mittlerweile über 86.000 besorgte Franzosen unterzeichnet.

Auch in Italien, Belgien und Großbritannien haben sich die Wahlcomputer-Gegner formiert; allerdings mit sehr unterschiedlichen Erfolgen: Während in Italien jegliche E-Voting-Experimente zu Gunsten der traditionellen Papierzettelwahl eingestellt wurden,[171] wird in Belgien noch immer an technisch völlig veralteten Wahlcomputern gewählt.[172] In Großbritannien hat sich die Open Rights Group im University College London[173] den Kampf gegen die Pläne der Regierung, das E-Voting wieder aufleben zu lassen, auf die Fahne geschrieben.

Bei den Parlamentswahlen in Schottland im Mai 2007 konnte die Gruppe größere prozessuale und technische Probleme beobachten, die auch den Medien nicht verborgen blieben[174] und zu einer umfassenden Neubeurteilung des E-Voting in Großbritannien führen könnten. Die

---

[168] *Sietmann*, Heise-News vom 30.03.07, abrufbar unter: http://www.heise.de/newsticker/meldung/87641, (Stand: 24.05.07).
[169] *Sietmann*, Heise-News vom 11.04.07, abrufbar unter: http://www.heise.de/newsticker/meldung/88064, (Stand: 25.05.07).
[170] http://www.ordinateurs-de-vote.org.
[171] *Ziegler*, Heise-News vom 30.11.06, abrufbar unter: http://www.heise.de/newsticker/meldung/81832, (Stand: 24.05.07).
[172] *Sietmann*, c't 05/07, S. 42 f.
[173] http://www.openrightsgroup.org/category/evoting/.
[174] *Electronicsweekly* vom 04.05.07, abrufbar unter: http://www.electronicsweekly.com/Articles/2007/05/04/41323/E-voting+policy+review+after+Scottish+ballot+chaos.htm, (Stand: 24.05.07).

aufgetretenen Probleme mit den Wahlcomputern wurden nunmehr in einem Gutachten ausführlich analysiert.[175]

Von Großbritannien geht auch die Bestrebung aus, die europäischen E-Voting-Aktivisten auf Gemeinschaftsebene in einem gemeinsamen Workshop („European Electronic Voting Activism") zu bündeln. Schwierigkeiten liegen hierbei darin, dass die Auffassungen der einzelnen Gruppen im Detail und im Ergebnis divergieren; kleinster gemeinsamer Nenner bleibt aber die Forderung nach der Einhaltung sämtlicher Wahlgrundsätze.[176]

3. USA

Anders als in Europa, bedurfte es in den USA keiner Bürgerinitiative um die Schwachstellen und Defizite der Wahlcomputertechnik an die Öffentlichkeit zu bringen. Die Skandal-Wahlen in Florida 2000 und 2004, sowie die bei den Diebold-Wahlmaschinen aufgedeckten Sicherheitslücken trugen maßgeblich dazu bei, dass sich Computer-Spezialisten und nationale technische Prüfbehörden mit der fehlerhaften Technik kritisch auseinandersetzen mussten.[177] Angeprangert wurden bei dem in Florida eingesetzten System zunächst das unübersichtliche und verwirrende Design der Touchscreens und schließlich vor allem das Fehlen eines geräteunabhängigen Stimmbelegs, das eine Nachzählung unmöglich machte. Inzwischen reagierte der Bundesstaat Florida auf die Wahlprobleme und will in Zukunft Wahlzettel-Scanner anstelle der Touchscreen-Geräte einsetzen.[178]

Die Firma Diebold trug zu den ohnehin schon kursierenden Negativ-Schlagzeilen über die Sicherheitsprobleme der AccuVote-TS-Geräte[179]

---

[175] *Open Rights Group*, Election Report, abrufbar unter: http://media.ito.com/kevinmarks/org_election_report.pdf, (Stand: 22.06.07).

[176] *Sietmann*, c't 05/07, S. 42, 43.

[177] S. *CalTech/MIT*, Voting Technology Project 2001, abrufbar unter: http://www.vote.caltech.edu/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf, (Stand 23.03.07); *Feldmann/Haldermann/Felten*, Diebold Security Analysis, abrufbar unter: http://itpolicy.princeton.edu/voting/ts-paper.pdf, (Stand: 23.03.07); *STS*, Recommendations, abrufbar unter: http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf, (Stand: 23.03.07).

[178] *Braun*, Heise-News vom 03.02.07, abrufbar unter: www.heise.de/newsticker/meldung/84751, (Stand: 24.05.07).

[179] Vgl. die Analyse von *Feldmann/Haldermann/Felten*, Diebold Security Analysis, abrufbar unter: http://itpolicy.princeton.edu/voting/ts-paper.pdf, (Stand: 23.03.07).

noch selbst bei, indem sie auf ihrer eigenen Homepage über längere Zeit eine so detailgetreue Abbildung von Schlüsseln, mit denen das Gehäuseinnere vor Zugriffen geschützt wird, zeigten, dass Hackern die Nachproduktion der Schlüssel und das Öffnen der Gehäuse möglich wurde.[180] Spätestens nach diesem Fauxpas kursieren die Gerüchte um den Rückzug der US-Firma aus dem Wahlgeräte-Segment.[181]

Um die Zuverlässigkeit und Korrektheit zukünftiger Wahlen mit Wahlgeräten zu garantieren, hat sich die Regierung nun in die Zertifizierung der Wahlmaschinentestlabors eingeschaltet und wählt über das National Institute for Standards and Technology (NIST) die fünf offiziellen Testlabors aus, die ihrerseits die einzusetzenden Wahlgeräte kontrollieren.[182] Die Sicherheit und Vertrauenswürdigkeit der Wahlmaschinen hängt laut Expertenmeinung weiterhin maßgeblich von einem papiernen Stimmbeleg („paper-audit“) ab; technisch sei eine ausreichende Sicherheit bei Software-unabhängigen und papierlosen Audit-Systemen noch nicht erreicht.[183] Empfohlen wird zum einen diese Systemtechnologien voranzutreiben und zunächst aber auch die Handhabbarkeit der mit Papierbelegen operierenden Systeme zu verbessern.[184]

V. Zusammenfassung

Wie die Analyse gezeigt hat, basiert das Wahlgerätesystem sowohl auf technischen als auch organisatorischen Elementen, die in sicherheitstechnischer und -rechtlicher Hinsicht nicht den gesetzlichen Anforderungen entspricht. Der Einsatz der Nedap-Geräte bei parlamentarischen Wahlen birgt eine hohe Gefahr der gezielten Manipulation, welche - mangels Effizienz - auch nicht durch die proklamierte Schutzumgebung verhindert werden kann. Zudem steht das Wahlgerätesystem in seiner heutigen technischen und organisatorischen

[180] *Ziegler*, Heise-News vom 26.01.07, abrufbar unter: www.heise.de/newsticker/meldung/84345, (Stand: 24.05.07).
[181] *Ziegler*, Heise-News vom 05.03.07, abrufbar unter: www.heise.de/newsticker/meldung/86239, (Stand: 24.05.07).
[182] *Ziegler*, Heise-News vom 22.02.07, abrufbar unter: www.heise.de/newsticker/meldung/85744, (Stand: 25.05.07).
[183] *STS*, Recommendations, S. 9 f.
[184] *STS*, Recommendations, S. 5 f.

Ausgestaltung im Widerspruch mit dem verfassungsrechtlichen Öffentlichkeits- und Amtlichkeitsgrundsatz. Unter geltendem Recht ist der Einsatz der Nedap-Geräte in Deutschland deswegen unzulässig.

Kapitel 3: Wahlstift

Als Vorreiter in Deutschland beschreitet Hamburg momentan als einziger den Weg eines elektronischen Wahlsystems mit Papier-Audit. Der Senat der Freien und Hansestadt beschloss am 31.10.2006 die Einführung des „Digitalen Wahlstifts“ für die Bezirksversammlungs- und Bürgerschaftswahlen 2008 und hat mittlerweile auch die Bestellung von 12.000 Wahlstiften aufgegeben. [185] Die Hamburger sahen die Notwendigkeit einer technischen Stimmabgabelösung gegeben, weil ihr Wahlsystem die Möglichkeit des Panaschierens und Kumulierens vorsieht und die Wahlen zu einem so komplexen Vorgang macht, dass es ohne technische Unterstützung am Wahlabend nicht mehr zur Bekanntgabe der vorläufigen Wahlergebnisse kommen könnte.[186] Nicht ganz zu vernachlässigen sind auch die ökonomischen Vorteile der Einführung des „Digitalen Wahlstifts“. Hamburg erhofft sich durch die Umstellung der Wahltechnik Einsparungen in Höhe von 3 Millionen Euro im Vergleich zur traditionellen Papierwahl und noch höhere Einsparung im Vergleich zu einer Einführung von Nedap-Wahlcomputern.[187]

Bei den Bundestagswahlen 2005 war der Einsatz des „Digitalen Wahlstifts“ in zwei Wahllokalen in Hamburg im Rahmen einer Pilotstudie [188] bereits erfolgreich erprobt worden: Die durchgeführte Parallelwahl, nicht verbindlich und zusätzlich zur eigentlichen Bundestagswahl, wurde von den angesprochenen Wählern und Wahlhelfern ganz überwiegend positiv bewertet und die Handhabbarkeit und Akzeptanz des Systems damit bestätigt.[189]

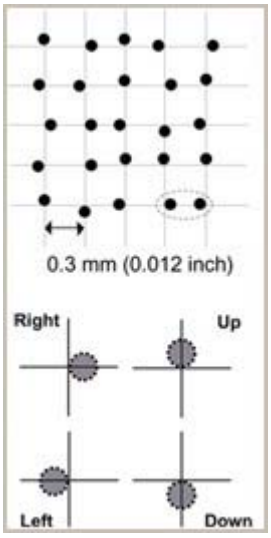
Dennoch stehen dem Einsatz des „Digitalen Wahlstifts“ bei den Bürgerschaftswahlen 2008 von anderer Seite starke Bedenken und Einwände entgegen. Ob der „Digitale Wahlstift“ die

[185] *Welt-Online* vom 23.01.07, abrufbar unter: http://www.welt.de/print-welt/article 710675/Hamburg_bestellt_12_000_digitale_Wahlstifte_fuer_2008.html, (Stand: 05.06.07).
[186] *Sietmann*, c’t 26/06, S. 92.
[187] *Sietmann*, c’t 26/06, S. 92 f.
[188] *Beiß*, Pilotstudie zum digitalen Wahlstift.
[189] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 20; Anhang VIII, S. 2 ff.

verfassungskonforme Alternative zum Wahlcomputer ist, ist daher im Folgenden näher zu erläutern.

A. Funktionsweise

Das Wahlstift-System kommt den Wählern in der Art der Bedienung sehr entgegen: Wie bei der traditionellen Wahl bekommt der Wähler einen papiernen Wahlzettel und einen Kugelschreiber ausgehändigt, mit dem er auf dem Wahlzettel seine Stimmabgabe durch ein Kreuz markiert. Die Qualität von Wahlzettel und Kugelschreiber allerdings differiert entscheidend von den traditionellen Utensilien:



Das Papier

Der Stift

Grafiken: Anoto[190]

Das Papier des Wahlzettels ist mit Punkten im Abstand von 0,3 mm fein gerastert und jeweils 6x6 Punkte sind als eine Koordinate auf dem Zettel genau bestimmt. Nur die Rasterung, nicht aber der übrige Inhalt des Wahlzettels, ist mit kohlenstoffhaltiger Tinte gedruckt, die ein Infrarotsignal reflektiert.[191] Der Stift verfügt neben seiner Funktion als Kugelschreiber zudem noch über eine Mini-Kamera, einen Drucksensor, einen Prozessor, einen Speicher und eine Batterie. Beim Aufsetzen des Stiftes registriert der Minendrucksensor des Wahlstiftes den Kontakt mit

[190] http://www.anoto.com/?id=906 und http://www.anoto.com/?id=908, (Stand: 23.06.07).
[191] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 12.

dem Papier und kann anhand der Koordinaten und der Infrarot-Beleuchtung auch die exakte Position der Stiftspitze erkennen.[192] Die ausgeführten Bewegungen des Stifts auf dem Stimmzettel werden von der digitalen Kamera im Stiftinneren aufgezeichnet und vom Prozessor abgespeichert (Anoto-Technik).[193] Sodann werfen die Wähler den Wahlzettel in die Wahlurne und geben den Wahlstift an den Wahlvorstand zurück. Dieser überträgt mit Hilfe einer Docking-Station und einem sicheren Kabel die Daten vom Wahlstift auf einen PC, wo sie in einem binären Code, kryptisch und in der Reihenfolge zufällig in einer Datenbank gespeichert werden.[194]

Die Auswertung erfolgt daraufhin mittels einer Software, in der gültige Ankreuzfelder und ungültige Koordinatenbereiche definiert sind. Die Stimmzettel-Datensätze werden anhand festgelegter Definitionen den Kategorien „gültig", „ungültig" oder „noch zu prüfen" zugeordnet.[195] Als Maßstab für eine Gültigkeitsmarkierung sind die Parameter des Markierungs-/Lesefelds sowie ein durch zwei – in einem Winkelbereich von 20° bis 160° angeordnete – Linien gebildetes Kreuz ausschlaggebend. Dem Wahlvorstand ist es möglich, sich jeden Stimmzettel-Datensatz, insbesondere solche in der Kategorie „noch zu prüfen", visualisiert in einem XML-Format anzeigen zu lassen und eine Entscheidung über die Einordnung des Wählerwillens und die Gültigkeit der Stimmabgabe zu treffen. Nach eindeutiger Zuordnung jedes Stimmdatensatzes liegt das Ergebnis der Wahl digital vor und wird auf einem portablen Speichermedium gesichert.

Eine erhöhte Sicherheit des Systems wird dadurch erzielt, dass der Stift an verschiedenen Docking-Stationen aktiviert, ausgelesen sowie entleert wird und die Ordnungsmäßigkeit der Datenübertragung vom Wahlvorstand auf einem Display kontrolliert werden kann.[196]

---

[192] *Nagel*, Hamburg-Wahlen 2008, Landespressekonferenz am 31.10.06, S. 4 f., abrufbar unter: http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2006/oktober/31/2006-10-31-bfi-pm-wahl-digitalerstift-folien-pdf,property=source.pdf, (Stand: 04.06.07).

[193] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 12.

[194] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 13.

[195] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 13.

[196] *Sietmann*, c't 26/06, S. 92.

B. Rechtliche Zulässigkeit und technische Anforderungen

Der Wahlstift hat die Testwähler und die Verantwortlichen in Hamburg und Mainz überzeugt: Die Wähler hatten keine Probleme das neue System zu bedienen; die Verantwortlichen sehen darin eine kostengünstige technische Lösung die Ergebnisse auch komplexer Wahlsysteme noch am Wahlabend selbst bekannt geben zu können. Darüber hinaus scheint der „Digitale Wahlstift“ anders als die kostenintensivere Alternative des Wahlcomputers auch das Vertrauen von Wählern und Wahlvorständen zu genießen. Die Kritik am „Digitalen Wahlstift“ ist verhalten. Ob dies womöglich aber in erster Linie auf die bislang flächenmäßig sehr begrenzte Ausbreitung des Wahlstift-Systems zurückzuführen ist, oder ob das System tatsächlich die sicherheitstechnischen und rechtlichen Schwächen des Wahlcomputers bei Aufrechterhaltung der Vorteile der technischen Unterstützung eliminiert, ist Gegenstand der folgenden Betrachtung.

I. Relevante Normen und Gesetze

Auch das Wahlstift-System muss sich an den rechtlichen Vorgaben für Wahlsysteme messen lassen, insbesondere also im Einklang stehen mit der Wahlgeräteverordnung und den verfassungsrechtlichen Grundsätzen. Weil das Wahlstift-System ursprünglich für den Einsatz auf Landes- und Kommunalebene entwickelt worden ist, sollen zunächst deren rechtliche Rahmenbedingungen und anschließend diejenigen eines Einsatzes bei Bundestagswahlen erörtert werden.

1. Landesebene am Beispiel Hamburg

Für das in Hamburg einzusetzende digitale Wahlstift-System dotvote[197] gelten im Vergleich zum Einsatz von Nedap-Wahlcomputern verschärfte Sicherheitsvoraussetzungen: Das System muss dem nach internationalem Standard speziell entwickelten Schutzprofil gegen Manipulationen der Software entsprechen (Commons Criteria Schutzprofil), d.h. es muss hinsichtlich der analysierten möglichen Bedrohungen entsprechende Schutzmechanismen selbst vorsehen. Das Digitale Wahlstiftsystem

[197] Abrufbar unter: http://www.dotvote.de, (Stand: 05.06.07).

dotvote wurde nach eingehender Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)[198] als mit den Common Criteria Anforderungen vereinbar erklärt und dementsprechend zertifiziert.[199] Der Zertifizierung des Wahlstift-Systems soll erwartungsgemäß im Juli die Zertifizierung des Produkts selbst, also des „Digitalen Wahlstifts", durch das BSI im Rahmen der Baumusterprüfung durch die PTB folgen. In einem nächsten Schritt, voraussichtlich Ende August, wird überprüft, ob der „Digitale Wahlstift" mit der Hamburgischen Wahlgeräteverordnung im Einklang steht und bei positivem Ergebnis findet eine Abnahme und Zulassung hiernach statt. In die noch zu erlassene Hamburgische Wahlgeräteverordnung werden die von der PTB aufgesetzten „Richtlinien für den Einsatz des Digitalen Wahlstift-Systems in Hamburg"[200], die sich stark an der BWahlGV orientieren, einfließen.[201]

2. Bundesebene

Ein Einsatz auf Bundesebene stand bislang nicht im Mittelpunkt der Diskussionen und ist de lege lata auch nicht zulässig. Maßstab für einen solchen Einsatz wäre zunächst die WahlGV des Bundes. Diese ist aber von Anfang an auf den Einsatz und die Zulassung von Wahlcomputern der Firma Nedap zugeschnitten gewesen und lässt von ihrem Wortlaut her eine Erweiterung auf Wahlgeräte ganz anderer Techniken kaum zu. Ein Wahlgerät i.S.v. § 1 BWahlGV ist, wie sich aus Abschnitt A der Anlage 1 zur BWahlGV ergibt, dadurch definiert, dass es sich um ein in einem Gehäuse verschlossenes System handelt. Dies lässt sich mit dem Konzept des „Digitalen Wahlstifts" ebenso wenig vereinbaren wie die weitere Voraussetzung, dass das Wahlgerät die Wahlvorschläge gemäß dem herkömmlichen Stimmzettel „auf der Vorderseite des Wahlgerätes

[198] *Volkamer/Vogt*, Common Criteria Schutzprofil Digitales Wahlstift-System, abrufbar unter: http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf, (Stand: 05.06.07).
[199] *BSI*, Zertifizierungsreport Schutzprofil Digitales Wahlstift-System, abrufbar unter: http://www.bsi.de/zertifiz/zert/reporte/pp0031a.pdf, (Stand: 05.06.07).
[200] *Physikalisch-Technische Bundesanstalt*, Richtlinien Digitales Wahlstift-System, abrufbar unter: http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2006/oktober/31/2006-10-31-bfi-pm-wahl-digitalerstift-wahlgvo-pdf,property=source.pdf, (Stand: 06.06.07).
[201] *Sietmann*, c't 26/06, S. 92, 94.

gut erkennbar“[202] darzustellen hat. Dass der „Digitale Wahlstift“ diesen Anforderungen nicht gerecht werden kann, deutet weniger auf seine Unzulässigkeit hin, als vielmehr darauf, dass der Gesetzgeber bei Ausarbeitung der BWahlGV einzig den Nedap-Wahlcomputer-Typus vor Augen hatte.[203] Vor einem zulässigen Einsatz des „Digitalen Wahlstift-Systems“ bei Bundestags- und Europawahlen bedarf es folglich einer erweiterten Anpassung der BWahlGV auf alternative spezifische Wahlgeräte-Techniken.

II. Vereinbarkeit mit bestehendem Recht

Aber selbst bei Betrachtung der geltenden Rechtslage unter Einbeziehung der noch nicht erlassenen, aber auf den Richtlinien der PTB beruhenden und an die BWahlGV angelehnten, Hamburgischen Wahlgeräteverordnung müssen Bedenken gegen die Zulässigkeit des Systems geäußert werden.

1. Vereinbarkeit mit WahlGV

Wie schon bei den Wahlcomputern sind zwei Gruppen von Bedrohungsszenarien zu unterscheiden: eine physische und eine elektronische Manipulierbarkeit.

Genau wie die BWahlGV im Fall der Wahlcomputer, wird die Hamburgische WahlGV aus sicherheitsrechtlichen Aspekten für das „Digitale Wahlstift-System“ verlangen, dass jegliche physische Manipulierbarkeit ausgeschlossen ist, bzw. jedenfalls nicht unentdeckt bleibt.[204]

Die einzige Zeit zu der eine Komponente des „Digitalen Wahlstift-Systems“, nämlich der Wahlstift selbst, nicht der ständigen Kontrolle des Wahlvorstands unterliegt, ist die Zeitspanne während der der Wähler sich mit dem Stift in der Wahlkabine aufhält. [205] Eine adäquate

[202] Abschnitt 3.3 der Anlage 1 zur BWahlGV: „Alle Angaben, die auf den amtlichen Stimmzetteln enthalten sind, können auf der Vorderseite des Wahlgerätes gut erkennbar angebracht werden, z.B. in waagerechter oder senkrechter Anordnung.“

[203] *Sietmann*, c’t 20/06, S. 86 ff.

[204] Vgl. Abschnitt 2.1 der Anlage 1 zur BWahlGV und 4.1 der PTB-Richtlinien zum Digitalen Wahlstift-System.

[205] *Volkamer/Vogt*, Common Criteria Schutzprofil Digitales Wahlstiftsystem, abrufbar unter: http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf, (Stand: 05.06.07).

Sicherheitsvorkehrung zur Verhinderung einer unerkannten Manipulation wäre z.B. das Anbringen eines Siegels auf den aufmachbaren Gerätekomponenten. Dem heimlichen Austausch des gesamten Wahlstifts gegen ein manipuliertes Gerät kann dadurch begegnet werden, dass der Wahlstift bei jeder Freischaltung mit einer elektronischen Signatur versehen wird, die beim Auslese- und Übertragungsvorgang auf ihre Korrektheit überprüft werden kann. Eine Manipulation oder ein kompletter Austausch des Stifts bleiben somit nicht unentdeckt.

Dass der Hamburgische „Digitale Wahlstift" genau diese Sicherheitsmaßnahmen vorsieht, ist ebenso wenig aus dem Zertifizierungsreport ersichtlich wie die Frage beantwortet wird, ob die einzelnen Komponenten des „Digitalen Wahlstift-Systems" zwischen den Wahleinsätzen in einer absolut sicheren Umgebung aufbewahrt werden.

Dennoch bezeugt das BSI dem „Digitalen Wahlstift-System" durch die spezifische Zertifizierung, dass das Common Criteria Schutzprofil eingehalten und somit die Verhinderung und Aufdeckung einer elektronischen Manipulation, d.h. einer unerkannten Veränderungen an der Software, garantiert wird.[206]

Eine weitere Bedrohung wird vom Schutzprofil zwar erkannt, aber bewusst außen vorgelassen: die Manipulationsmöglichkeiten durch den Wahlvorstand selbst oder durch andere Innentäter.[207] Denkbar wäre hier z.B., dass verfälschte Stimmzettel gedruckt und eingeschleust werden, bei denen das kohlenstoffhaltige Raster so verändert wurde, dass die Schraffur für alle Kästchen der einer bestimmten Partei entspricht und die Kamera somit alle Kreuze als Stimmen für ein- und dieselbe Partei registriert.[208]

Es ist nicht nachvollziehbar, warum dieses Bedrohungspotenzial völlig aus dem Schutzprofil herausgenommen wurde, da es schwere Zweifel an der Systemsicherheit aufkommen lässt und die Vereinbarkeit mit der WahlGV erneut in Frage stellt.

---

[206] *BSI*, Zertifizierungsreport Schutzprofil Digitales Wahlstift-System, abrufbar unter: http://www.bsi.de/zertifiz/zert/reporte/pp0031a.pdf, (Stand: 06.05.07).
[207] *Volkamer/Vogt*, Common Criteria Schutzprofil Digitales Wahlstift-System, S. 13.
[208] Vgl. *Chaos Computer Club*, Wahlcomputer, abrufbar unter: https://berlin.ccc.de/wiki/Wahlcomputer, (Stand: 06.06.07).

2. Vereinbarkeit mit Geheimhaltungsgrundsatz

Um die Einhaltung des Wahlgeheimnisses aus Art. 38 I 1 GG zu garantieren hält das „Digitale Wahlstift-System“ einige technische und organisatorische Spezifikationen bereit. Die Stimmabgabe selbst findet wie bei der herkömmlichen Wahl völlig verdeckt in der Wahlkabine statt und stellt kein wahlrechtliches Problem dar. Damit die Übertragung der Datensätze vom Wahlstift auf den PC aber auch völlig geheim und nicht auslesbar erfolgt, muss die Bluetooth-Funktionalität des Wahlstifts unterbunden und die Übertragung einzig über die Docking-Station und ein sicheres Kabel erlaubt werden. Die Übertragungsfunktionalität des Systems, nicht aber der Inhalt der Datensätze, kann vom Wähler auf einem zu ihm ausgerichteten Monitor oder Display selbst kontrolliert werden,[209] wodurch das Vertrauen in die Geheimhaltung gestärkt werden soll. Ursprünglich war der Kontrollmonitor einzig zum Wahlvorstand ausgerichtet, was bei der Testwahl in Hamburg zur Irritation der Wähler geführt hatte, die ein Auslesen ihrer Stimmentscheidung befürchteten.[210] Die Übertragungstechnik muss außerdem so ausgestaltet sein, dass der Übertragungsvorgang immer gleich lang andauert, unabhängig davon wie viele Stimmen der Wähler abgegeben hat oder ob er sich gänzlich enthalten hat. Nur so bleibt der Geheimhaltungsgrundsatz gewahrt.

3. Vereinbarkeit mit Öffentlichkeitsgrundsatz

Substantiierte Kritik wird am Wahlstift aber hinsichtlich der Einhaltung des Öffentlichkeitsgrundsatzes geübt. Zwar scheint das „Digitale Wahlstift-System“ auf den ersten Blick genau der Schwäche der Nedap-Wahlcomputer zu begegnen. Diesen wird mangels Papierbeleg vorgeworfen, dass sie die Nachvollziehbarkeit der Stimmauswertungen völlig aus dem Bereich der Öffentlichkeit hin in die Hände von einigen wenigen Experten verlagern.[211] Das Wahlstift-System hingegen setzt auf die Parallelität von papierner und elektronischer Speicherung der Stimmen und erhält den herkömmlichen Wahlzettel. Dadurch wird zwar

[209] *Volkamer/Vogt*, Common Criteria Schutzprofil Digitales Wahlstiftsystem, S. 9.
[210] *Beiß*, Pilotstudie zum digitalen Wahlstift, S. 19.
[211] Anstelle vieler: *Wiesner*, Wahlprüfbeschwerde 2 BvC 3/07, S. 68 ff., abrufbar unter: http://www.ulrichwiesner.de/wp/070212_wahlpruefbeschwerde.pdf, (Stand: 15.05.07).

zunächst deutlich mehr Transparenz als bei den Nedap-Wahlcomputern erzielt; je nach praktischem Umgang mit dieser Parallelität ist dieser Vorteil aber dennoch hinfällig:[212] Wird die digitale Stimmauswertung lediglich dazu benutzt zeitnah ein vorläufiges Endergebnis zu ermitteln, das amtliche Endergebnis aber dennoch auf eine Papierstimmzettelauswertung gestützt, so wird zwar dem Öffentlichkeitsprinzip gerecht, der Stift entbindet dann aber nicht von der kostenintensiven Handauszählung.

In der wahrscheinlicheren, ökonomisch sinnvollen und von der Stadt Hamburg auch geplanten Handhabungsvariante[213] wird die elektronische Stimmauswertung als Grundlage für die Feststellung des amtlichen Endergebnisses herangezogen. Die papiernen Wahlzettel dienen nur als „Backup“ für den Fall eines Wahlmanipulationsverdachts. Da schon jetzt ersichtlich ist, dass eine stichprobenartige Handauszählung in Höhe von 1% in Hamburg nur für den erstmaligen Einsatz des „Digitalen Wahlstift-System“ 2008 vorgesehen ist,[214] werden der Öffentlichkeits- und Transparenzgrundsatz auch durch dieses System verletzt.

Die prinzipielle Nachzählmöglichkeit aufgrund des existierenden Papierbelegs bleibt erwartungsgemäß eine rein theoretische Option, da sie womöglich mit der Argumentation abgewiegelt werden wird, dass das System hinreichend sicher und dem Wahlvorstand kein Verdacht der Manipulation bekannt sei.[215]

Auch für den Fall einer Nachzählung muss vorweg die Frage beantwortet werden, welcher Ergebnisfeststellung, der elektronischen oder der papiernen, Verbindlichkeit zukommen soll. Wenn - wie in Belgien[216] - selbst bei einer Abweichung von 8 % an der Elektronik festgehalten wird, so stellt dies das begründete Vertrauen der Wähler ebenso wie verfassungsrechtliche Grundsätze in erheblichem Maße in Frage.

---

[212] *Sietmann*, c’t 26/06, S. 92, 93 f.
[213] *Sietmann*, c’t 26/06, S. 92, 93 f.; *Nagel*, Hamburg-Wahlen 2008, S. 6 f.
[214] *Nagel*, Hamburg-Wahlen 2008, S. 7; *Sietmann*, c’t 26/06, S. 92, 93 f.
[215] *Chaos Computer Club*, Wahlcomputer, abrufbar unter: https://berlin.ccc.de/wiki/Wahlcomputer, (Stand: 06.06.07).
[216] *Association Electronique Libre*, Electronic Voting Paper Audit Trail, abrufbar unter: http://wiki.ael.be/index.php/ElectronicVotingPaperAuditTrail, (Stand: 07.06.07).

Auch das „Digitale Wahlstift-System“ verletzt damit in der geplanten Handhabungsvariante den Öffentlichkeitsgrundsatz und ist somit nicht mit der Verfassung zu vereinbaren.

4. Geplante Einsätze

Das „Digitale Wahlstift-System“ hat bislang keine große Ausbreitung gefunden. Nur in Hamburg und Mainz, wo sehr komplexe Wahlsysteme mit den Möglichkeiten des Kumulierens und Panaschierens praktiziert werden, hat das System ernsthaftes Interesse hervorgerufen. Der weltweit erste Einsatz bei den Bürgerschafts- und Bezirksversammlungswahlen in Hamburg 2008 ist beschlossene Sache und wird mangels lauter Bedenken oder Kritik an der juristischen Zulässigkeit wohl auch ohne rechtliche Überprüfung unbehelligt vollzogen werden.

Mainz denkt über den Einsatz des Systems im Superwahljahr 2009 nach, wenn dort Europa-, Bundestags-, Kommunal- und Ausländerbeiratswahlen stattfinden werden. [217] Eine endgültige Entscheidung für das „Digitale Wahlstift-System“ oder andere elektronische Stimmabgabe-Systeme ist hier aber noch nicht getroffen worden.

Die rechtlichen Bedenken, die auch gegen den „Digitalen Wahlstift“ geäußert werden, haben den Weg in die Öffentlichkeit, anders als die harsche Kritik an den Nedap-Wahlcomputern, kaum gemacht. Es wurden auch von Experten bislang keinerlei rechtliche Schritte im Vorfeld gegen den Einsatz des Systems eingeleitet.

III. Zusammenfassung

Das „Digitale Wahlstift-System“ krankt zwar nicht in gleichem Maße an einem Verstoß gegen das verfassungsrechtliche Öffentlichkeitsprinzip wie die Nedap-Wahlgeräte, weil es die Parallelität von Papierstimmzettel und digitaler Stimme vorsieht. Da sich die Pilotstadt Hamburg aber im Fall einer Wahlüberprüfung dennoch auf die digitale Auswertung verlassen will, bleibt die Nachprüfbarkeit lediglich als theoretische Möglichkeit bestehen. Für die Wählerschaft bedeutet dies aber im

[217] *Stadt Mainz*, Test des Digitalen Wahlstifts, S. 5.

praktischen Anwendungsfall keine Verbesserung ihrer Position. In der Ausgestaltung, wie die Stadt Hamburg den „Digitalen Wahlstift“ einzusetzen gedenkt, begegnet auch diese elektronische Wahlmethode erheblichen verfassungsrechtlichen Bedenken.

Kapitel 4: „Remote Internetvoting“

Wahlcomputer und Wahlstift – für einige fallen diese elektronischen Wahlsysteme gar nicht unter den eigentlichen Begriff des „elektronischen Wählens“, und wenn doch, dann jedenfalls nur als notwendige Zwischenstationen auf dem Weg zum vermeintlich unvermeidbaren Ziel der Internetwahl von jedem beliebigen Ort aus („Remote Internet Voting“). Das Bild des „Wählers im Unterhemd“, der bequem von zu Hause aus seine Stimme abgibt oder sich von unterwegs per Mobiltelefon an der Wahl beteiligt, mutiert zum Sinnbild der Modernisierung unserer Demokratie und übt einen starken Reiz auf Politiker und Wähler gleichermaßen aus.[218] Die Flexibilisierung der Beteiligung am demokratischen Entscheidungsprozess durch Loslösung von örtlicher Gebundenheit an Wahllokale wird als adäquates und gar notwendiges Pendant zur vom Wähler abverlangten Mobilität in der heutigen Informationsgesellschaft angesehen. Was auf den ersten Blick vor allem bürgerfreundlich und bequem erscheint, hält für viele Politiker und Wissenschaftler darüber hinaus ein weit reichendes ökonomisches und soziologisches Potential vor. Dass der Einsatz der neuen Technologien für Wahlen aber gleichzeitig ein hohes Gefahrenpotential beinhaltet, wird teilweise nur allzu gern übersehen und verschwiegen.

A. Attraktivitäts- und Gefahrenpotential

I. Vorteile

Die Liste der von den Befürwortern von Internetwahlen vorgebrachten positiven Aspekte des Systems ist lang und vielfältig.[219] Sie reicht von rein ökonomischen bis hin zu soziokulturellen Aspekten.[220]

1. Rationalisierung des Wahlprozesses

Nach allgemeiner Meinung würde die Einführung von Internetwahlen zu einer Rationalisierung des Wahlprozesses führen.[221]

---

[218] *Otten* in Holznagel, S. 75.
[219] *Otten* in Holznagel, S. 75; *Rüß* in Buchstein/Neymanns, S. 39, 41 f.; *Schreiber*, § 35 Rn. 9; *Will*, S. 18.
[220] *Birkenmaier*, S. 51 ff.

a) Kostenreduzierung

In erster Linie versprechen sich Politiker eine deutliche Kostenreduzierung durch die Umstellung vom herkömmlichen Wahlverfahren auf die digitale Stimmerfassung und –auswertung.[222] Die Organisation der herkömmlichen Papierwahl verursacht durch den Druck von Stimmzetteln, Versand der Wahlbenachrichtigungen und Briefwahlunterlagen, die Benennung von Wahlvorständen und Wahlhelfern, das Anmieten von Wahllokalen und die Wahlermittlung Kosten in erheblicher Höhe. Für die Bundestagswahlen 2002 musste der Bund über 62 Millionen Euro an die Länder und Kommunen zahlen. Da dieser Betrag aber lediglich die Kosten für Porto und das Erfrischungsgeld für die ca. 630.000 Wahlhelfer beinhaltete, nicht aber Aufwendungen für Anmietung und Reinigung der Wahllokale, sind die tatsächlichen Ausgaben für den Wahlprozess noch weitaus höher anzusetzen.[223]

Eine Umstellung des Wahlsystems auf „Remote Internet Voting“ würde den Großteil dieser Kostenfaktoren durch einen massiven Abbau des Wahlpersonals und eine deutlich schnellere Ergebnisermittlung eliminieren. Die Reduzierung des organisatorischen Aufwands hätte mithin zwangsläufig eine Kostensenkung zur Folge, so die Befürworter.[224]

b) Beschleunigung des Wahlprozesses

Als politisch vergleichbar wünschenswerter Effekt würde durch die Wahl per Internet eine Beschleunigung des Wahlprozesses, insbesondere im Stadium der Stimmauswertung, erreicht.[225] Per Knopfdruck liegt bei der Internetwahl das amtliche Endergebnis bereits wenige Minuten nach Wahlschluss vor und kann bekannt gegeben werden. Insbesondere in Kommunen, in denen das Wahlrecht das Kumulieren und Panaschieren

---

[221] *Birkenmaier*, S. 51 ff.; *Rüß* in Buchstein/Neymanns, S. 39, 41 f.; *Schreiber*, § 35 Rn. 9; *Will*, CR 2003, S. 126, 127.

[222] *Birkenmaier*, S. 51; *Bremke*, LKV 2004, S. 102, 104; *Otten* in Buchstein/Neymanns, S. 73, 75; *Rüß* in Buchstein/Neymanns, S. 39, 41; *Will*, S. 19.

[223] Hahlen in *Petersen*, fluter.de Archiv Nr. 40 vom 12.09.05, abrufbar unter: http://fluter.de/look/archiv_article.tpl?IdLanguage=5&IdPublication=2&NrArticle=4179&NrIssue=40&NrSection=11, (Stand: 11.06.07).

[224] *Birkenmaier*, S. 51.

[225] *Karpen*, S. 16; *Will*, S. 19.

vorsieht, könnte durch die technische Unterstützung ein ansonsten einige Tage lang andauerndes Auswerten der Stimmzettel ausbleiben. Der Beschleunigungseffekt beim relativ einfach gehaltenen Bundestagswahlrecht hingegen ist vergleichsweise gering, da trotz Handauszählung bislang nach ca. zwei Stunden das amtliche Endergebnis bereits vorliegt.

c) Vereinfachung des Wahlsystems

Einen weiteren Vorteil bietet die digitale Stimmabgabe übers Internet in der Hinsicht, dass die Anzahl unbewusst ungültig abgegebener Stimmen reduziert werden kann.[226] Insbesondere bei komplizierten Wahlsystemen mit Kumulieren und Panaschieren sind offensichtlich unbewusst ungültig abgegebene Stimmen keine Seltenheit. Hier kann das Programm eine Fehlermeldung vorsehen, die den Wähler auf die Ungültigkeit der Stimmabgabe hinweist und zur erneuten Bestätigung oder Korrektur auffordert und somit zur Ermittlung des wahren Wählerwillens entscheidend beiträgt.

2. Mobilisierung der Wähler

Vermeintliches Potential birgt die Internetwahl auch im Hinblick auf ein Entgegenwirken bezüglich der zunehmenden schlechten Wahlbeteiligung. Erhofft und erwartet wird vor allem der Politikverdrossenheit der jungen Nichtwähler entgegenzuwirken und deren Wahlbeteiligung dadurch zu erhöhen, dass diese mit einem modernen und ihnen vertrauten Medium angesprochen werden.[227] Übersehen wird bei dieser Hoffnung allerdings, dass die Gründe für die niedrige Wahlbeteiligung von Jungwählern sehr vielschichtig sind und nicht allein durch eine flexible und neue Wahltechnik aufgefangen werden können.[228] So liegen die Motive für eine Wahlenthaltung häufig darin, dass Jungwähler spontane Formen politischer Partizipation, wie z.B. Demonstrationen, bevorzugen.[229] Dass die Stimmabgabe via Internet zu einem dauerhaften

[226] *Bremke*, LKV 2004, S. 102, 103; *Will*, S. 19.
[227] *Bremke*, LKV 2004, S. 102, 103; *Khorrami*, S. 180; *Will*, S. 18.
[228] *Khorrami*, S. 181 ff.
[229] *Khorrami*, S. 184 f.

Wahlbeteiligungsanstieg führen kann ist empirisch bislang nicht belegt und bleibt daher höchst zweifelhaft.[230]

Vorteilhaft würde sich die neue Wahltechnik jedenfalls für körperlich Behinderte, v.a. Sehbehinderte und Blinde, auswirken. Während sie sich bei der herkömmlichen Wahlzettel-Stimmabgabe oft Problemen gegenüber sahen und auf die Hilfe einer Vertrauensperson angewiesen waren und damit ihr Recht auf Wahlgeheimnis preisgeben mussten, kann ihnen durch die Internetwahl eine autonome Stimmabgabe ermöglicht werden.[231]

3. Flexibilisierung des Wahlprozesses

Schließlich wird die Internetwahl als eine logische Reaktion auf die gestiegenen Mobilitätsanforderungen unserer heutigen Gesellschaft angesehen.[232] Die Einführung des „Remote Internet Voting" schafft eine örtlich und zeitlich flexible Stimmabgabealternative zur Urnen- und Briefwahl und ermöglicht es so auch denjenigen, die sich kurzfristig nicht in ihrem Wahlkreis an der demokratischen Willensbildung beteiligen können, ihre Stimme abzugeben.[233]

Dieses Potential liegt jedenfalls dann in der Wahl via Internet, wenn man von einem „i-voting" ohne vorherige Anmeldung ausgeht und auf das Erfordernis, dass ähnliche Ausnahmegründe wie bei der Briefwahl vorzuliegen haben,[234] verzichtet.[235]

II. Gefahrenpotential

Dem vielschichtigen Attraktivitätspotential des „Remote Internet Voting" steht allerdings ein nicht zu unterschätzendes und ähnlich facettenreiches Gefahrenpotential gegenüber.

---

[230] *Birkenmaier*, S. 53 m.w.N.; *Khorrami*, S. 185; *Schreiber*, § 35 Rn. 9; a.A. *Bremke*, LKV 2004, S. 102, 104.
[231] *Bremke*, LKV 2004, S. 102, 103; *Esteve* in Krimmer, S. 51, 53; *Will*, S. 18.
[232] *Birkenmaier*, S. 54; *Otten* in Holznagel, S. 73, 74 f.; *Rüß*, ZRP 2001, S. 518, 519.
[233] *Will*, S. 18.
[234] Vgl. § 25 BWO.
[235] So *Birkenmaier*, S. 54; kritisch hierzu: *Karpen*, S. 21; *Rüß*, MMR 2000, S. 73, 74 f.; *Will*, S. 154; *Will*, CR 2003, S. 126, 130.

1. Symbolik der Wahl

Zunächst einmal wird von Kritikern des „Remote Internet Voting“ hervorgebracht, dass diese neue Wahltechnik den Symbolcharakter und damit einen Teil des Sinnes von Wahlen beseitigt.[236] Wahlen dienen zwar in erster Linie dazu die Volksvertreter zu ermitteln; gleichzeitig kommt in der Ausgestaltung der Wahl, also im Gang zu einem öffentlichen Wahllokal und in der Stimmabgabe im öffentlichen Raum, ein Symbolcharakter zum Ausdruck.[237] Durch die Öffentlichkeit der Wahlhandlung bringen die Wähler ihre Teilnahme und Unterstützung des politischen Systems der Demokratie zum Ausdruck. Zudem wird beim Zusammentreffen aller Bürger im Wahllokal der Gleichheitsaspekt der Wahl in einer Demokratie nach außen manifestiert. Schließlich soll der Aufwand, den ein jeder Wähler auf sich nehmen muss, um seine Stimme im Wahllokal abzugeben, beim Wähler zu einer erneuten Reflexion und Bewusstmachung über die zu treffende Wahlentscheidung führen.

Bei einer Einführung von Internetwahlen fiele das bewusste öffentliche Zusammentreffen der Wähler zur gemeinsamen Ausgestaltung der öffentlichen Angelegenheiten weg. Wenn ein jeder von jedem denkbaren Ort durch einen simplen Knopfdruck über die Regierungsbildung entscheiden kann, droht die Gefahr einer unüberlegten „junk“-Stimmabgabe,[238] der Wahlvorgang wird entritualisiert, die Öffentlichkeit und die Legitimität des Wahlaktes in Frage gestellt.[239]

2. Kosten

Mit starker Skepsis werden auch die optimistischen Kostenprognosen der „i-voting“-Befürworter beäugt. Dass deren Erwartungen hinsichtlich einer deutlichen Kosteneinsparung im Vergleich zur Papierwahl erfüllt werden, bezweifeln die Kritiker aufgrund der hohen Anschaffungsinvestitionen und Wartungskosten für die Durchführung

[236] *Bremke*, LKV 2004, S. 102, 104; *Karpen*, S. 16; *Neymanns* in Buchstein/Neymanns, S. 28; *Rüß*, MMR 2000, S. 73, 76; *Schreiber*, § 35 Rn. 9; *Will*, S. 20.
[237] *Neymanns* in Buchstein/Neymanns, S. 23, 25.
[238] *Rüß*, MMR 2000, S. 73, 76; *Will*, S. 20.
[239] *Karpen*, S. 16.

von Internetwahlen vehement.[240] Eine vorsichtige Gegenrechnung für die Einführung der neuen Wahltechnik beläuft sich auf mindestens 160 Millionen Euro für eine bundesweiten Ausstattung, in die aber weder Kosten für Reservegeräte, Server, Schulungen oder Support einkalkuliert sind.[241] Eine Amortisierung dieser Anschaffungskosten wird wenn überhaupt erst nach Jahrzehnten erreicht werden können.[242]

Völlig außen vor gelassen werden hierbei auch eventuelle Kosten, die auf den einzelnen Wähler für die Anschaffung von Smartcards zukommen würden.[243]

Insgesamt erscheint also eine Reduktion von Wahlkosten für den Staat noch nicht einmal mittelfristig realistisch.

3. „Digital divide“

Weiterhin wird die Gefahr einer Spaltung der Gesellschaft aufgrund der vorliegenden oder fehlenden Technikaffinität und -beherrschung gesehen.[244] Würde man das „Remote Internet Voting“ als ausschließliches Wahlsystem einführen, so wären all diejenigen, die nicht im Besitz des notwendigen Equipments (PC und Internetzugang auf erforderlichem Stand der Technik) sind, praktisch von der Wahl ausgeschlossen. Aber auch im Fall der gleichzeitigen Einführung des „Remote Internet Voting“ und des „Polling Place Internet Voting“ könnte die neue Wahltechnik eine Abschreckung weniger technikversierter Wähler darstellen. Bei der Einführung von Internetwahlen muss deshalb die Gefahr einer digitalen Spaltung der Gesellschaft berücksichtigt werden und es muss eine Ausgestaltung gewählt werden, die keine Bevölkerungsschicht wegen technischer Unversiertheit oder sozialer

---

[240] *Karpen*, S. 17; *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 103, *Schreiber*, § 35 Rn. 9.

[241] *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 103.

[242] *Karpen*, S. 17; s. auch die Erfahrungen in der Schweiz: Bericht des Schweizerischen Bundesrates über den vote électronique, Chancen und Risiken der Machbarkeit elektronischer Ausübung politischer Rechte, Bern 2002, S. 686; a.A. *Bremke*, LKV 2004, S. 102, 104; *Birkenmaier*, S. 51.

[243] *Birkenmaier*, S. 51; *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 105; *Rüß*, MMR 2000, S. 73, 76; zur verfassungsrechtlichen Brisanz dieser Kostenabwälzung s. *Khorrami*, S. 165.

[244] *Bremke*, LKV 2004, S. 102, 106; *Birkenmaier*, S. 111 ff.; *Karpen*, S. 17; *Rüß*, ZRP 2001, S. 518, 519; *Will*, S. 20.

Benachteiligung von der Teilnahme am demokratischen Entscheidungsprozess abhält.

4. Technische Sicherheitslücken

Schließlich weist das „Remote Internet Voting“ in technischer Hinsicht ein ganz erhebliches Gefahrenpotential auf. [245] Die denkbaren Bedrohungsszenarien dieser elektronischen Wahltechnik unterscheiden sich von den Risiken bei der herkömmlichen Wahl, aber auch von denen beim Wahlcomputer oder dem Wahlstift. Das Internetvoting zeichnet sich in technischer Hinsicht vor allem durch die Vernetzung aller Wahlkomponenten aus. Und hierin liegt gleichzeitig die hohe Attraktivität für jegliche Manipulationsversuche, da deren Reichweite aufgrund der Vernetzung um ein Vielfaches potenziert wird. Welche genauen Bedrohungen möglich sind wird im Folgenden genauer analysiert.

B. Historie

Trotz der nicht zu übersehenden Gefahren einer internetbasierten Stimmabgabetechnik, ist im In- und Ausland ein starker Trend zur diesbezüglichen Modernisierung der Wahlsysteme zu verzeichnen. Dabei haben sowohl im Bereich der privaten Wahlen als auch auf der politischen Ebene in Deutschland und vielen anderen Ländern Testwahlen und zum Teil bereits rechtsverbindliche Wahlen stattgefunden. Im Folgenden soll ein kurzer Überblick über die bisherige Praxiserfahrung mit Internetwahlen im In- und Ausland gegeben werden.

I. Nicht politische Wahlen

Als Testfeld für internetbasierte Wahlen bot sich zunächst die nicht politische Ebene an, da dort die strengen Sicherheitsanforderungen, denen öffentliche Wahlen gerecht werden müssen, nicht in letzter Konsequenz gelten.[246]

[245] *Lange* in Buchstein/Neymanns, S. 127.
[246] *Khorrami*, S. 41.

1. Deutschland

a) Sozialwahl Techniker-Krankenkasse Hamburg 1999

Zum ersten Mal in Deutschland wurde eine internetbasierte Wahl bei der Sozialwahl der Techniker-Krankenkasse in Hamburg 1999 durchgeführt.[247] Den 3,2 Millionen Versicherten wurde im Rahmen eines Planspiels die Stimmabgabe per Internet parallel zur rechtsgültigen Briefwahl anempfohlen. Hauptanliegen der von der Forschungsgruppe Internetwahlen der Universität Osnabrück entwickelten Wahlsimulation war es, das System auf Sicherheit, Anonymität und Validität der Stimmabgabe zu überprüfen und technische Problemfelder zu evaluieren.[248] Zwar waren die Sicherheitsmängel des Systems noch ganz erheblich, dennoch konnte die Simulation aufgrund der gewonnenen Erkenntnisse, zu der auch die gute Handhabbarkeit der Wahlsoftware gehörte, als Erfolg gewertet werden.[249]

b) Universitätswahlen Osnabrück 2000

Diese ersten Praxiserfahrungen stellten in der Folge die Grundlage für die weltweit erste rechtsverbindliche Internetwahl zu den Kollegialorganen der Studentenschaft der Universität Osnabrück im Februar 2000 dar.[250] Den interessierten Wahlberechtigten wurden hierbei eine mit elektronischer Signatur ausgestattete Chipkarte und das entsprechende Kartenlesegerät, sowie die Wahlsoftware ausgehändigt, woraufhin die Stimmabgabe von jedem beliebigen PC aus möglich war.[251] Zusätzlich wurden in der Universität Osnabrück Wahlterminals vorgehalten. Von den nur 156 Online-Wählern hatten etliche mit erheblichen technischen Problemen zu kämpfen. Die Wahlsoftware ließ sich mangels Kompatibilität oder auch wegen fehlender Versiertheit nicht von jedem installieren; einige digitale Signaturen blieben unlesbar und die Netzwerke der Universität fielen zeitweilig aus.[252] Aufgrund von

[247] *Lange* in Buchstein/Neymanns, S. 127, 130; *Hanßmann*, S. 52; *Khorrami*, S. 43.
[248] *Lange* in Buchstein/Neymanns, S. 127, 130.
[249] *Hanßmann*, S. 53 f.
[250] *Lange* in Buchstein/Neymanns, S. 127, 131; *Khorrami*, S. 44; *Otten* in Holznagel, S. 73, 79.
[251] *Lange* in Buchstein/Neymanns, S. 127, 131.
[252] *Lange* in Buchstein/Neymanns, S. 127, 132.

Zwischenspeicherungen der nicht übertragenen Stimmen und der fehlenden Transparenz des Systems entstand deshalb auch ein erhebliches Sicherheitsrisiko, welches zu einer aus formellen Gründen abgewiesenen Wahlanfechtung der Studierendenschaft führte.[253]

c) Daimler Chrysler AG Aktionärswahlen 2000

Als erstes Unternehmen weltweit setzte die Daimler Chrysler AG im Jahr 2000 die internetbasierte Stimmabgabe bei ihrer Hauptversammlung ein, um Aktionären, die an einem persönlichen Erscheinen gehindert waren, die Möglichkeit einzuräumen, via Internet ihre Weisungen an die Stimmrechtsvertreter des Unternehmens zu übertragen.[254] Die Legitimation der Aktionäre erfolgte mittels einer Aktionärsnummer, die dem Aktionär nach erfolgter Vollmachtserteilung und dadurch bedingter Freischaltung im Internet zugewiesen wurde, in Kombination mit einer individuellen Zugangsnummer, welche schon in den Einladungsunterlagen enthalten war.[255] Auch wegen der guten Resonanz im ersten und zweiten Jahr wurde das Angebot 2002 dahingehend erweitert, dass nunmehr auch die Vollmachtserteilung an die Stimmrechtsvertreter der Daimler Chrysler AG via Internet erfolgen konnte.

d) Personalratswahl im LDS Brandenburg 2000 und 2002

Ihren dritten Feldversuch unternahm die Forschungsgruppe Internetwahlen mit ihrem „Remote Internet Voting"-System „i-vote" im Rahmen der Personalratswahl im Landesamt für Datenverarbeitung und Statistik Brandenburg. Die im Jahr 2000 durchgeführte Simulation basierte wie die Studierendenwahlen in Osnabrück auf einem System mit einem Zertifikator, der die digitale Signatur erstellte, einem Psephor als virtueller Wahlurne und einem Validator, der die Wählerliste beinhaltete und die Auszählung vornahm.[256] Die Identifizierung der Wähler fand wiederum mit Hilfe der auf einer Chipkarte gespeicherten persönlichen

[253] *Hanßmann*, S. 55 f.
[254] *Khorrami*, S. 48.
[255] *Khorrami*, S. 48.
[256] *Otten* in Holznagel, S. 73, 79; *Will*, S. 26.

digitalen Signatur in Verbindung mit einer PIN statt.[257] Insbesondere die Aktivierung der Chipkarten mittels einer mitgelieferten Software verlief allerdings recht problematisch und führte dazu, dass etliche Wähler mit der Stimmabgabe von zu Hause scheiterten.[258]

Womöglich als Reaktion hierauf fand die rechtsverbindliche Personalratswahl in der LDS Brandenburg im Mai 2002 daraufhin ausschließlich an Computern in Online-Wahlkabinen in den Amtsgebäuden selbst statt. Die eigens für diese Wahl geschaffene Rechtsgrundlage[259] sah konkrete Vorgaben für die Durchführung der Wahl vor, welche wiederum die Identifizierung der Wähler über eine elektronische Signatur in Kombination mit einer PIN und ein Online-Wählerverzeichnis vorsah. Beim Einsatz der Chipkarten kam es erneut zu Anwendungsschwierigkeiten. Ingesamt konnte die Wahl aber als Erfolg angesehen werden.[260]

2. International – Wahlen zum ICANN-Direktorium 2000

Die bislang weltweit größte und zudem erste grenzüberschreitende „Remote Internetwahl“ war die Wahl zum Direktorium der ICANN (Internet Corporation for Assigned Names and Numbers) im Jahr 2000, bei der fünf Mitglieder des neunköpfigen Vorstands von der interessierten Öffentlichkeit übers Internet gewählt wurden.[261] Das komplexe Abstimmungsprozedere mit mehreren Wahlrunden basierte auf einer von Election.Com entwickelten Wahlsoftware und einer Verschlüsselungsroutine von ICANN. Zwar war grundsätzlich jeder Interessierte über 16 Jahren wahlberechtigt, erforderlich war aber eine Vorab-Registrierung als Mitglied mit der die Zusendung einer individuellen PIN verbunden war. Die Stimmabgabe war auf der durch das SSL-Protokoll gesicherten Webseite nach Eingabe der

[257] *Will*, S. 27.
[258] *Hanßmann*, S. 57.
[259] § 50a der Wahlordnung zum Landespersonalvertretungsgesetz Brandenburg, abrufbar unter: http://www.landesrecht.brandenburg.de/sixcms/detail.php?gsid=land_bb_bravors_01.c.14179.de#50a, (Stand: 14.06.07).
[260] *Hanßmann*, S. 59.
[261] *Brandt/Volkert*, S. 59 f.; *Khorrami*, S. 50; *Lange* in Buchstein/Neymanns, S. 127, 137; *Will*, S. 61.

Mitgliedsnummer, des Passworts und der PIN möglich.[262] Bei den zehntägigen Wahlen traten erhebliche technische und organisatorische Probleme auf, die auf die mangelnde Abstimmung des Wahlsystems von Election.Com mit der Verschlüsselungsroutine und eine organisatorische Überforderung aufgrund fehlender finanzieller und personeller Ressourcen bei gleichzeitig unerwartet hoher Wahlbeteiligung zurückzuführen war.[263] Zudem resultierte aus der Nichtbeachtung der regional unterschiedlichen Wahlpraxen eine Irritation mancher Wähler über das Registrierungserfordernis und das präferenzielle Wahlsystem.[264] Aus den ernüchternden Erfahrungen dieser Wahl zog die ICANN die Konsequenz die Wahlen zum Direktorium wegen erheblicher Zweifel an Repräsentativität, Fairness und Erschwinglichkeit des Internet-Wahlsystems vorerst nicht mehr internetbasiert durchzuführen.[265]

II. Politische Wahlen

Auch auf der politischen Ebene hat es erste Versuche gegeben, das Potential von Internetwahlen fruchtbar zu machen. Im Unterschied zu den privaten Wahlen erfordern fast alle politischen Wahlordnungen die Einhaltung der grundlegenden Wahlgrundsätze, zu denen die Einhaltung des Wahlgeheimnisses sowie die Manipulationsfreiheit gehören. Während in Deutschland deswegen nach dem Motto „Vorsicht ist besser als Nachsicht“ die Versuche noch auf niedrigster Ebene gehalten werden, wurden im Ausland wider der bekannten Risiken bereits oberste politische Organe verbindlich via Internet gewählt.

1. Deutschland

a) Wahl zum Jugendgemeinderat Fellbach im Juni 2001

Die Jugendgemeinderatswahl Fellbach im Juni 2001 stellt die erste verbindliche Internetwahl auf kommunaler Ebene in Deutschland dar.[266]

---

[262] *Will*, S. 63.
[263] *Khorrami*, S. 51.
[264] *Lange* in Buchstein/Neymanns, S. 127, 138.
[265] Vgl. *Khorrami*, S. 51.
[266] *Hanßmann*, S. 60; *Stadt Fellbach*, Jugendgemeinderatswahl 2001, abrufbar unter: http://www.fellbach.de/kommunalpolitik/Jugendgemeinderat/Dokumentation_JGRONlinewahl.PDF, (Stand: 15.06.07); *Will*, S. 28.

Die Stadt entschied sich aus Sicherheits- und Kostengründen für eine Softwarelösung, die zur Authentifizierung der Wähler nicht auf einer digitalen Signatur, sondern auf einem TAN-System basierte.[267] Die Datenübertragung wurde auch hier über das SSL-Protokoll verschlüsselt und die Anonymität der Stimmen dadurch gewährleistet, dass die Generierung der TAN von der Zusendung derselben an die Wähler entkoppelt wurde.[268] In technischer Hinsicht verlief die Wahl ohne größere Probleme und wurde somit als voller Erfolg gewertet;[269] ein Rückschluss auf die Tauglichkeit des Systems für größer angelegte Wahlen kann daraus aber wohl nicht gezogen werden.

b) Wahl zum Jugendgemeinderat Esslingen 2001

Bei der zeitnahen Jugendgemeinderatswahl in Esslingen im Juni 2001 setzten die Verantwortlichen hingegen wieder auf das „i-vote"-Wahlsystem der Forschungsgruppe Internetwahlen.[270] Die Wahl zeichnete sich vor allem dadurch aus, dass neben der Präsenzwahl auch die Stimmabgabe von vernetzten Computern in öffentlichen Einrichtungen („Polling Place Voting") ermöglicht wurde, indem den jugendlichen Wählern jeweils eine personalisierte Signaturkarte und ein entsprechendes Lesegerät überlassen wurden.[271] Die Wahl litt wiederum an den schon in den vorhergehenden „i-vote"-Projekten festgestellten technischen Problemen mit den Signaturkarten.[272]

c) Test-Landratswahl im Kreis Marburg-Biedenkopf 2001

Zu einer ersten Erprobung des „Remote Internet Voting"-Systems auf Kreisebene kam es bei der Landratswahl im Kreis Marburg-Biedenkopf im Jahr 2001, wo den Briefwählern parallel zur rechtsverbindlichen Wahl eine probeweise Stimmabgabe via Internet angeboten wurde.[273] Die federführende Projektgruppe „Elektronische Stimmabgabe im

---

[267] *Stadt Fellbach*, Jugendgemeinderatswahl 2001, S. 6.
[268] *Hanßmann*, S. 61; *Stadt Fellbach*, Jugendgemeinderatswahl 2001, S. 7 ff.
[269] *Stadt Fellbach*, Jugendgemeinderatswahl 2001, S. 20; *Will*, S. 30.
[270] *Khorrami*, S. 57; *Will*, S. 31.
[271] Jugendgemeinderatswahl 2001in Esslingen, abrufbar unter: http://www.jgrwahl.esslingen.de/online.html, (Stand: 15.06.07); *Khorrami*, S. 57.
[272] *Brandt/Volkert*, S. 57 f.; *Lange* in Buchstein/Neymanns, S. 127, 134.
[273] *Khorrami*, S. 58; *Will*, S. 34.

Internet“ (ESI) entschied sich dabei für ein PIN/TAN-basiertes System, um Hardware-Investitionen zu ersparen.[274] Besonderes Augenmerk wurde bei der erstmalig von Datenschützern begleiteten Probewahl auf die Einhaltung der Wahlrechtsgrundsätze gelegt.[275]

2. International

Während es in Deutschland also bislang nur zu den aufgezeigten zaghaften Erprobungen der Internetwahl auf unterster und – bei allem Respekt – relativ unbedeutender politischer Ebene gereicht hat, wurde die Auseinandersetzung mit internetbasierten Wahlsystemen für politische und rechtsverbindliche Wahlen im Ausland zum Teil mit viel größerer Intensität und Ernsthaftigkeit auf hoher politischer Bühne geführt und hat einige nennenswerte Resultate hervorgebracht.

a) USA

Als weltweit erste verbindliche Internetwahl auf politischer Ebene wird die Primary Election der Demokratischen Partei im März 2000 in Arizona angesehen, bei der die Kandidaten für die Präsidentschaftswahlen 2000 in den USA ermittelt wurden.[276] Neben der herkömmlichen Papierwahl stand den 821.000 registrierten Parteianhängern das Votieren via Internet an den vier Tagen vor dem Wahltag von privaten Internetzugängen, und am Wahltag selber in 124 offiziellen Wahllokalen frei.[277] Technisch basierte die Wahl auf einem System von election.com[278], welches eine Identifizierung der Wähler über eine PIN und für die sichere Übertragung der Stimmen ein Verschlüsselungssystem mit öffentlichem Schlüssel vorsah.[279] Probleme traten bei der Durchführung der Wahl zum einen mit älteren Browsern und Apple-Macintosh-Computern auf, zum anderen war sowohl die Erreichbarkeit der Webseite selber als auch des Service-Telefons wegen

[274] *Will*, S. 35.
[275] *Will*, S. 37.
[276] *Solop*, Digital Democracy Comes of Age in Arizona: Participation and Politics in the First Binding Internet Election, abrufbar unter: http://ball.tcnj.edu/pols291/readings/036015SolopFrede.pdf, (Stand: 15.06.07); *Will*, S. 46.
[277] *Lange* in Buchstein/Neymanns, S. 127, 139.
[278] http://www.election.com.
[279] *Will*, S. 47.

zu hoher Auslastung (und evt. wegen DoS-Angriffen) nicht immer gewährleistet, so dass manche Wähler nicht erfolgreich votieren konnten.[280] Dennoch konnte eine enorme Erhöhung der Wahlbeteiligung und eine hohe Akzeptanz des Internetwahlsystems verzeichnet werden.[281]

b) Estland

Die Vorreiterrolle im Bereich der Internetwahlen übernahm etwas überraschend für die internationale Expertenriege nunmehr das IT-fortschrittliche Estland: Nachdem bei der als Generalprobe konzipierten landesweiten Kommunalwahl im Oktober 2005 fast 10.000 Esten erfolgreich und ohne größere technische Probleme online votierten,[282] sahen auch die Parlamentswahlen im Frühjahr 2007 ein Nebeneinander von Präsenz- und Internetwahl vor.[283] Alle estnischen Wahlberechtigten hatten die Möglichkeit mit ihrer gültigen ID-Smartkarte, die 2002 mit einer Signaturfunktion ausgestattet worden war, und einem Kartenlesegerät von zu Hause die höchsten Volksvertreter zu wählen.[284] Technisch beruht das estnische Wahlsystem auf einer durch das Private/Public-Key-Verfahren verschlüsselten Kommunikation zwischen Wähler und Wahlamt; die Anonymität wird ähnlich wie bei der Briefwahl durch die Trennung von Signatur und Stimmzettel gewahrt.[285] Bemerkenswerte Besonderheit des Systems ist die Möglichkeit der mehrfachen Stimmabgabe, durch die dem Grundsatz der Geheimhaltung und Freiheit der Wahl in besonderer Weise Rechnung getragen werden soll. [286] Die Wähler können daher während der dem Wahltag

---

[280] *Solop*, S. 7.
[281] *Lange* in Buchstein/Neymanns, S. 127, 139; *Solop*, S. 6.
[282] *Madise*, Internet Voting in Estonia – Free and Fair Elections, S. 3, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07); *Madise/Martens* in Krimmer, S. 15 ff.
[283] *Martens*, Internet Voting in practice, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07).
[284] *Sietmann*, Heise-News vom 27.02.07, abrufbar unter: http://www.heise.de/newsticker/meldung/85921, (Stand: 15.06.07).
[285] Zum genauen technischen Ablauf: *Martens*, Internet Voting in practice, S. 7 ff., abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07); *Maaten* in Prosser/Krimmer, S. 83, 86 ff.
[286] *Madise*, Internet Voting in Estonia – Free and Fair Elections, S. 6, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07); *Maaten* in Prosser/Krimmer, S. 83, 85.

vorangehenden Internetwahlperiode mehrfach ihre online abgegebene Stimme verändern und selbst am Wahltag noch ein Papiervotum abgeben. In die Stimmauswertung fließt dennoch nur eine Stimme pro Wähler ein, und zwar das zuletzt abgegebene Online-Votum bzw., falls existent, die papierne Wahlzettel-Stimme.[287] Technische Sicherheitsbedenken, die die Diskussionen in den westlichen Demokratien beherrscht,[288] werden von den estnischen Wahlverantwortlichen in den Hintergrund geschoben, stattdessen heben sie stolz den technisch reibungslosen Ablauf und die verdreifachte Internetwahlbeteiligung (nunmehr ca. 4%) hervor.[289] Die rechtliche Grundlage für den Einsatz von einem signaturkartengestützten Internet-Wahlsystem ist in Estland nunmehr für die nationale, kommunale und europäische Ebene, sowie für Referenden geschaffen worden.[290]

c) Schweiz

In den westlichen Demokratien nimmt die Schweiz mit ihrem Projekt „vote électronique“ eine Spitzenrolle bei der Erprobung von internetbasierten Lösungen für die Ausübung politischer Rechte ein.[291] Bis 2005 fanden insgesamt fünf Internetwahlen im Rahmen von eidgenössischen Abstimmungen in den Kantonen Genf, Neuenburg und Zürich statt.[292]

Beim Pilotprojekt in Genf, das die Möglichkeit einer verbindlichen Internetwahl neben der Präsenz- und Briefwahl austesten sollte, wurde die Identifikation der Wähler über einen zugesandten, frei zu rubbelnden Code erreicht, dessen Eingabe auf der Webseite in Verbindung mit anderen Informationen den Zugang zur elektronischen Wahlurne freigab.[293] Nach Abgabe der Stimme wurde das Codewort gesperrt, so dass weder eine Korrektur der Stimmabgabe, noch ein Missbrauch mit

[287] *Madise*, Internet Voting in Estonia – Free and Fair Elections, S. 8, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07).
[288] *Sietmann*, c't 05/07, S. 42; vgl. auch *Sietmann*, c't 02/06, S. 20 f.
[289] *Martens*, Internet Voting in practice, S. 11, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07).
[290] *Khorrami*, S. 62; Gesetzestexte in estnischer Sprache: http://www. legaltext.ee.
[291] *Khorrami*, S. 64; *Will*, S. 38.
[292] *Braun/Brändli* in Krimmer, S. 27, 29 ff.
[293] *Khorrami*, S. 64 f.

einem bereits genutzten Codewort möglich war.[294] Auch bei den für die Übermittlung der Voten erforderlichen Sicherheitsstandards orientiert sich das in Genf implementierte System an den Empfehlungen des Europarates[295] und sieht eine Verschlüsselung, sowie eine zertifizierte Authentifikation vor.[296] Standortvorteil des Kantons Genf für den Pilotversuch war, dass es bereits über ein kantonales elektronisches Stimmregister verfügte,[297] und bei einem Briefwählerprozentsatz von 90 Prozent das Konzept der Distanzwahl bereits hohe Akzeptanz genoss.[298]

Bei der Erprobung der elektronischen Stimmabgabe via Internet im Kanton Neuenburg wurde ein Verfahren eingesetzt, das ähnlich wie das Telebanking mit den Faktoren Zugangscode und Passwort operierte.[299] Die Sicherheit der Stimmabgaben wurde über externe Kontrollmaßnahmen konsequent überprüft.[300]

Das ehrgeizigste Pilotprojekt[301] wird im Kanton Zürich verfolgt, wo nicht nur die elektronische Wahl vom heimischen PC, sondern auch die Stimmabgabe von mobilen Endgeräten wie Handys, PDA-Organizer und Fernsehern erreicht werden soll.[302] Anders als in den anderen Kantonen wurde hier auch die dezentrale Organisation der Gemeinden nicht völlig

---

[294] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5475, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[295] *Council of Europe*, Recommendation Rec (2004) 11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies, abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?id=778189, (Stand: 23.06.07).

[296] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5476, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[297] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5474, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[298] *Khorrami*, S. 65.

[299] *Will*, S. 41; *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5479, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[300] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5482, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[301] Nunmehr ausgezeichnet mit dem Public Service Award 2007 der Vereinten Nationen, s. *Sperlich*, Heise-News vom 19.06.07, abrufbar unter: http://www.heise.de/newsticker/meldung/91412, (Stand: 20.06.07).

[302] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5485, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

aufgehoben, sondern nur für den Fall des Stimmregisters durch ein virtuelles kantonales Stimmregister, welches aus den dezentralen Einwohnermelderegistern gespeist wird, überwunden.[303]

Alle Pilotprojekte verliefen erfolgreich und ohne größere technische Zwischenfälle, so dass eine schrittweise Ausweitung des „vote électronique“ bei ständiger Anpassung der Sicherheitsmaßnahmen an die sich rasant entwickelnden Risiken angestrebt wird,[304] wobei eine bundesweite Einführung nicht innerhalb der nächsten 3 Jahre erwartet wird.

d) Großbritannien

Auch im Vereinigten Königreich Großbritannien ist nach ersten Pilot-Internetwahlen in den Jahren 2002 und 2003 und nunmehr bei den Kommunalwahlen 2007 langfristig eine elektronisch basierte General Election geplant.[305] Bei den Pilotprojekten auf Kommunalebene wurden in einzelnen Gemeinden die verschiedensten elektronischen Stimmabgabemöglichkeiten, wie z.B. über digitales Fernsehen, per SMS, und auch via Internet vom Heimcomputer und öffentlichen Wahlterminals aus, verbindlich ausgetestet.[306] Zur Erprobung des „Remote Internet Voting“ kam es in einigen Wahlbezirken der Gemeinden St. Albans, Swindon, Liverpool, Sheffield und Crewe.[307] In keiner der Gemeinden wurden Chipkarten mit digitalen Signaturen eingesetzt, stattdessen wurde die Identifizierung durch PIN und Passwörter bzw. durch eine Voter Identification Number und eine separat zugesandte PIN erreicht.[308] Insbesondere bei den Kommunalwahlen im Mai 2007 traten erhebliche technische Schwierigkeiten bei der Stimmabgabe via Internet auf, die unter anderem zu der sehr kritischen

---

[303] *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5486, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[304] *Braun/Brändli* in Krimmer, S. 27, 35; *Schweizerischer Bundesrat*, Bericht über die Pilotprojekte zum Vote Electronique, S. 5533, abrufbar unter: http://www.bk.admin.ch/themen/pore/evoting/00776/index.html?lang=de, (Stand: 15.06.04).

[305] *Khorrami*, S. 61.

[306] *Khorrami*, S. 59, 61; *Will*, S. 52 ff.

[307] *Mason*, Computer Fraud and Security 03/04, S. 6 f.

[308] *Will*, S. 53 ff.

Analyse der Open Rights Group führten.[309] Die erhoffte Erhöhung der Wahlbeteiligung konnte in den durchgeführten Pilotprojekten nicht festgestellt werden.[310]

e) Weitere Praxiserfahrungen

Auch in einigen anderen europäischen Ländern und auf EU-Ebene ist die Praktikabilität und Implementierung von Internetwahlen angetestet worden.

Nachdem das österreichische Wahlprojekt e-voting.at[311] bei den Wahlen zur Studentenvertretung an der Universität Wien im Jahr 2003 erfolgreich getestet worden war,[312] wurde das selbst entwickelte Protokoll auch bei Testwahlen von Auslands-Österreichern im letzten Jahr eingesetzt.[313] Das Protokoll sieht zur Wahrung der Anonymität der Wähler ein zweistufiges Stimmabgabeverfahren mit a) der Wähleridentifizierung über die Beantragung einer Wahlabstimmungskarte und b) der Online-Abstimmung vor.[314] Trotz einiger erkannter Verbesserungspotentiale wird diese Testwahl als sehr erfolgreich und das e-voting.at-Protokoll als zukunftsträchtig erachtet.[315]

In Frankreich zeigt sich vor allem die Gemeinde Issy-les-Moulineaux als besonders fortschrittlich und experimentierfreudig in Bezug auf Internetwahlen.[316] Bei den Stadtratswahlen im Dezember 2002 konnten die Bürger ihre Stimme ausschließlich verbindlich übers Internet abgeben. Technische Grundlage des Wahlverfahrens bildete das von der EU entwickelte Cyber-Vote-System,[317] welches durch spezielle kryptographische Verfahren die Authentifikation des Wählers und

---

[309] *Open Rights Group*, Election Report, S. 19 ff.
[310] *Mason*, Computer Fraud and Security 03/04, S. 6, 11; *Will*, S. 54.
[311] http://www.e-voting.at.
[312] *Khorrami*, S. 53; *Will*, S. 43.
[313] *Prosser/Steininger*, An Electronic Voting Test Among Austrians Abroad, abrufbar unter: http://www.e-voting.at/main.php?ID=108, (Stand: 16.06.07); *Wiener Zeitung* vom 14.10.06, Der Browser als Wahlzelle, abrufbar unter: http://www.wienerzeitung.at/DesktopDefault.aspx?TabID=3858&Alias=wzo&cob=252778, (Stand: 13.02.07).
[314] *Prosser/Steininger*, An Electronic Voting Test Among Austrians Abroad, S. 8, abrufbar unter: http://www.e-voting.at/main.php?ID=108, (Stand: 16.06.07).
[315] *Prosser/Steininger*, An Electronic Voting Test Among Austrians Abroad, S. 25, abrufbar unter: http://www.e-voting.at/main.php?ID=108, (Stand: 16.06.07).
[316] *Khorrami*, S. 60; *Will*, S. 49.
[317] http://www.eucybervote.org.

Geheimhaltung der Stimme gewährleisten soll.[318] Das Cyber-Vote-System fand auch in Schweden und Bremen weitere Testanwendungen. Aufgrund größerer technischer Schwierigkeiten, insbesondere in Form des komplizierten und zeitaufwändigen Stimmabgabeverfahrens,[319] wurde der geplante Einsatz bei der Europawahl bislang nicht verwirklicht.[320]

C. Funktionsablauf

Beim „Remote Internet Voting", d.h. bei der Internetwahl auch aus dem individuellen Bereich heraus, auf politischer Ebene kann der Wähler am Wahltag entweder jedes beliebige Wahllokal oder ein Wahlkiosk aufsuchen oder vom heimischen Computer seine Stimme abgeben. Der Wahlverlauf im Wahllokal unterscheidet sich für den Wähler im Vergleich zur Stimmabgabe am Wahlgerät nur unwesentlich, insbesondere die Benutzeroberfläche kann verschieden ausgestaltet sein. In jedem Fall müssen dem Wähler aber die Wahlvorschläge ähnlich wie auf einem herkömmlichen Wahlzettel präsentiert und die Möglichkeit der bewusst ungültigen Stimmabgabe gegeben werden. Ob die einzelnen Wahl-PCs jedoch mit anderen PCs über das offene Internet miteinander verbunden sind oder nicht, ist für den Wähler nicht ersichtlich und macht für seine Stimmabgabe organisatorisch keinen Unterschied.

Größere Abweichungen im Funktionsablauf lassen sich hingegen bei einer Wahl vom heimischen PC feststellen. Zwar unterscheiden sich die erprobten und entwickelten Internetwahl-Protokolle im Detail ganz erheblich. Dennoch kann den einzelnen Verfahren ein gemeinsames Kern-Ablaufschema entnommen werden. Der Wahl aus dem individuellen Bereich geht eine Vorab-Registrierung voraus, die zur Zuweisung der Authentifizierungsbausteine führt.[321] Während im Fall der Wahl im Wahllokal die Authentifizierung des Wählers nach dem herkömmlichen Schema verlaufen kann, also Identifizierung mit dem Personalausweis und Wahlberechtigungsprüfung anhand der

[318] Vgl. *Will*, S. 61; vgl. auch http://www.eucybervote.org/description.html, (Stand: 16.06.07).
[319] http://www.eucybervote.org/trials.html, (Stand: 16.06.07).
[320] *Khorrami*, S. 67.
[321] *Khorrami*, S. 145 ff.

Wahlbenachrichtigung und des Stimmregisters,[322] muss dieser Schritt im Fall der Wahl von beliebigen Computern aus technisch gelöst werden. Erprobt werden die Authentifizierung mittels PIN/TAN-[323], Wahlnummer/Passwort-[324] und Signaturkarten-System[325]; denkbar, aber bislang kaum erprobt, ist auch die Authentifizierung anhand biometrischer Daten[326]. Je nach Auswahl des Mittels wird der Wähler also nach der Registrierung mit Passwort/PIN/TAN/elektronischer Signatur und unter Umständen auch der nötigen Hardware in Form von Signaturkarte und Lesegerät, sowie ggf. einer Wahlsoftware ausgestattet.
Nach der Registrierung und Vorbereitung der Wahl kann der Wähler die Wahlseite über einen internetfähigen PC mittels eines Browsers aufrufen. Es folgt die vom System jeweils vorgegebene Authentifizierung und serverseitig eine Wahlberechtigungsprüfung. Bei positivem Ausgang dieser Überprüfung übermittelt der Server den virtuellen Stimmzettel, auf welchem der Wähler per Mausklick oder Tastatureingabe seine Wahlentscheidung treffen kann. Erst nach erneuter Bestätigung der Wahl wird die Stimme verschlüsselt über eine sichere Verbindung an den Wahlserver übermittelt, wo sie gespeichert und ausgewertet wird.[327] Auf dem Server wird für den jeweiligen Wähler der neue Wahlstatus vermerkt und die Stimme anonymisiert und zur Auswertung freigegeben.[328]

D. Technische Anforderungen an Internetwahlen

Die ordnungsgemäße Durchführung von Wahlen ist entscheidende Voraussetzung für die Legitimation der zu wählenden (Volks-)Vertreter. Auch bei herkömmlichen Wahlen hat die Sicherheit der Unverfälschtheit der Stimmen Priorität, um durch die Auswertung der Stimmen auch den tatsächlichen Wählerwillen ermitteln zu können. Durch die Transparenz und Öffentlichkeit des papiernen Wahlverfahrens wird die Manipulierbarkeit der herkömmlichen Wahl relativ gering gehalten und

[322] Vgl. *Kubicek/Wind* in Buchstein/Neymanns, S. 91.
[323] Z.B. http://www.election.com; für ESI: *Khorrami*, S. 153.
[324] Z.B. http://www.safevote.com.
[325] Z.B. http://www.i-vote.de
[326] *Hof* in Prosser/Krimmer, S. 63 ff.
[327] *Khorrami*, S. 157.
[328] *Khorrami*, S. 159 f.

ist nur bei Kooperation vieler einzelner Wahlhelfer denkbar. Wenn nun die Stimmabgabe und –übermittlung über das Internet, also ein offenes Netz, auf das unbegrenzt viele Personen Einfluss nehmen können, stattfindet, so erhöht sich das Bedrohungspotential nahezu spiegelbildlich zur Flexibilisierung des Wahlprozesses.[329] Bedingt durch die Struktur des Internets und die Abhängigkeit von der Technik sind die Möglichkeiten der Einflussnahme von außen auf online-übermittelte Daten vielfältig und reichen vom Aufhalten, Zerstören, Manipulieren der Daten bis hin zum Zufügung fremder Datenpakete.[330]

Im Folgenden werden deswegen zunächst einige spezifische Bedrohungen und Sicherheitsrisiken der internetbasierten Wahl vorgestellt und sodann die entwickelten Lösungen aufgezeigt.

I. Bedrohungspotentiale

Gefahren für die Sicherheit von Internetwahlen können theoretisch von jedem einigermaßen versierten Internetbenutzer ausgehen. Realistischer Weise werden aber vor allem diejenigen ein Interesse an einer Wahlmanipulation haben, die davon entweder direkt begünstigt werden (Wahlkandidaten), eine Sabotage als Druckmittel gegen den Staat nutzen wollen (Terroristen) oder das Aushebeln von Sicherheitsmaßnahmen als sportliche Herausforderung ansehen (Hacker).[331] Angriffe auf die ordnungsgemäße Durchführung der Internetwahl können an verschiedenen Risikobereichen, nämlich dem Wahlklienten, dem Wahlserver und dem Übertragungsweg, ansetzen[332] und passiv oder aktiv ausgestaltet sein, also auf das pure Auslesen oder auf die aktive Manipulation ausgerichtet sein.[333]

1. DoS-Angriffe

Eine große Gefahr stellen so genannte Denial of Service (DoS)-Angriffe auf den Wahlserver oder einen involvierten Internet-Provider dar. Ein DoS-Angriff liegt vor, wenn durch das Generieren so vieler Anfragen an

[329] Vgl. *Grimm* in Holznagel, S. 86, 89.
[330] *Krimmer/Volkamer* in Schweighofer, S. 256, 261.
[331] Vgl. *Hanßmann*, S. 70, die aber die politische Motivation völlig übersieht.
[332] *Khorrami*, S. 95.
[333] *Hanßmann*, S. 71.

den angegriffenen Server dieser derart überlastet und mit sinnlosem Datenverkehr überflutet wird, dass er für die eigentlichen Anfragen, hier also die zu übermittelnden Stimmdaten, nicht mehr erreichbar ist.[334] So könnte ein DoS-Angriff dazu führen, dass abgegebene Stimmen gar nicht oder lediglich zu spät an den Server übermittelt werden können und nicht in die Stimmauswertung einfließen.[335] Ein wirksamer Schutz gegen DoS-Angriffe ist wegen des offenen Konzepts des Internets, das gerade auf die wechselseitige Erreichbarkeit aller Nutzer untereinander ausgelegt ist, und die Schwierigkeit der Identifikation des Angreifenden nur sehr eingeschränkt möglich. Eine möglichst großzügige Serverbelastbarkeit sowie Software-Filter können den Erfolg von DoS-Angriffen verringern, stellen aber keine absolute Schutzvorrichtung dar.[336]

2. Spoofing

Die Integrität der Stimmdaten wird vor allem von „Spoofing"-Angriffen gefährdet, bei denen der Angreifer dem Wähler suggeriert, dieser wäre mit der gewünschten offiziellen Wahlseite verbunden, wobei er sich tatsächlich auf einer vom Angreifer kontrollierten Webseite befindet.[337] Diese Art von Angriff kann nicht nur zum Abfangen und Auslesen der Stimmdaten, sondern auch zur Manipulation und Zurückhaltung derselben führen, so dass hier zugleich die Erfolgsgleichheit der Stimme, das Wahlgeheimnis und die Allgemeinheit der Wahl verletzt würden.[338] Das Heimtückische des Spoofing-Angriffs ist darin begründet, dass es die Unaufmerksamkeit des Internet-Nutzers ausnutzt, dem regelmäßig nicht bewusst ist, dass seine Daten abgefangen werden. Auch wenn der Wähler sich also durch eigene Vorsicht vor dem Angriff schützen kann, indem er die Adresse des Wahlservers per Hand eingibt anstatt sich auf Links zu verlassen, wird ein Großteil der Internetnutzer regelmäßig in die Falle tappen.

[334] *Hanßmann*, S. 72.
[335] *Will*, CR 2003, S. 126, 128.
[336] *Will*, CR 2003, S. 126, 128.
[337] *Khorrami*, S. 135.
[338] *Will*, CR 2003, S. 126, 129.

3. Trojaner/Viren/Würmer

Eine andere Form der aktiven Störung der Stimmübermittlung stellt der Einsatz von Systemanomalien oder „malicious software“ dar.[339] Hierunter versteht man Programme, die Aktionen im System des PCs hervorrufen, die vom Nutzer nicht geplant, und unter Umständen auch nicht bemerkt werden, und jedenfalls nicht gewollt sind.[340] Prominenteste Beispiele sind Trojaner, Viren und Würmer. Während Viren vor allem auf die Beschädigung von Computersystemen abzielen und durch ihr destruktives Potential die Stimmabgabe unmöglich machen können,[341] stellen Würmer vor allem eine Gefahr für die Verfügbarkeit des Wahlservers oder die Funktionsfähigkeit der Internet-Provider dar, da sie einen erheblichen Datenverkehr verursachen.[342] Größte Gefahren gehen von so genannten Trojanischen Pferden aus, die als reine Spionage-Trojaner die Stimmdaten auslesen und das Wahlgeheimnis verletzen bzw. zum Stimmenkauf missbraucht werden können, und als Backdoor-Trojaner jegliche Manipulationen an den Stimmdaten von einem anderen Rechner aus ermöglichen und damit einen Angriff auf die Gleichheit und Allgemeinheit der Wahl darstellen.[343]

Obwohl ein Schutz vor „malicious software“ durch Anti-Viren-Programme grundsätzlich möglich ist, bleibt deren Effektivität deshalb sehr eingeschränkt, weil sich die Systemanomalien sehr schnell verbreiten und permanent neue Arten im Netz Verbreitung finden. Absoluten Schutz kann daher nur die totale Abschottung des PCs nach außen bieten, was aber für privat genutzte PCs unrealistisch ist.[344]

II. Lösungen

So vielfältig die Angriffsmöglichkeiten auf den Ablauf einer Internetwahl sind, so mannigfaltig wurde auch nach Gegenmaßnahmen zum Schutz der Wahlverfahren geforscht. Etlichen der ausgewählten Sicherheitsrisiken kann und wurde in den bereits erprobten

---

[339] *Hanßmann*, S. 73 ff.; *Khorrami*, S. 95 ff.; *Wilm*, Technische Anforderungen, S. 4 f.
[340] *Khorrami*, S. 96.
[341] *Hanßmann*, S. 73 f.
[342] *Khorrami*, S. 102.
[343] *Krimmer/Volkamer* in Schweighofer, S. 256, 261; *Will*, CR 2003, S. 126, 129.
[344] *Will*, CR 2003, S. 126, 129.

Wahlprotokollen auf technischer Ebene wirksam begegnet.[345] Im Folgenden werden einige technische Basiskonzepte aufgezeigt, die – wenn als Bausteine in ein Gesamtmodell eingegliedert - zur Gewährleistung einer technisch sicheren Online-Wahl beitragen können.

1. Einsatz asymmetrischer Kryptographie

Die technisch simpelste Lösung zur sicheren Gestaltung von Internetwahlen besteht darin, das Protokoll auf den Einsatz asymmetrischer Kryptographie zu stützen.[346] Bei diesem Verschlüsselungsverfahren werden zwei verschiedene Schlüssel verwandt, ein privater, der geheim gehalten werden muss, und ein öffentlicher. Die Schlüssel sind mathematisch zwar voneinander abhängig, aber die Berechnung des privaten Schlüssels aus dem öffentlichen ist nach heutigem Stand der Technik nicht möglich. Wenn bei einer Internetwahl also der Wähler seine Stimmabgabe mit dem öffentlichen Schlüssel des Wahlamtes chiffriert, so wird der Klartext in eine vermeintlich nicht interpretationsfähige Botschaft umgewandelt, die aber vom Wahlamt mittels des passenden privaten Schlüssels dechiffriert und gelesen werden kann.[347] Das Verfahren stellt also sicher, dass der Inhalt der Nachricht auf dem Übertragungsweg nicht sinnvoll ausgelesen werden kann; es ermöglicht hingegen weder die Identifizierung des Absenders noch eine Prüfung einer nachträglichen Manipulation der Wahlentscheidung.[348]

2. Verwendung einer digitalen Signatur

Letzteres kann aber durch den zusätzlichen Einsatz einer digitalen Signatur erreicht werden.[349] Auch die digitale Signatur beruht auf einem Paar elektronischer Schlüssel, die der Identifizierung ihres Eigentümers dienen.[350] Mit dem privaten Schlüssel wird der Hash-Wert des Stimm-Dokumentes verschlüsselt und als digitale Signatur an den Klartext

[345] Vgl. *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 97; *Otten* in Buchstein/Neymanns, S. 71, 75.
[346] *Hanßmann*, S. 78; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 644.
[347] *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 644.
[348] *Hanßmann*, S. 79.
[349] *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 644.
[350] *Khorrami*, S. 124.

angehangen und an den Empfänger verschickt. Dieser kann nun mit dem öffentlichen Schlüssel die digitale Signatur dechiffrieren und erhält so einen Hash-Wert, den er mit dem Hash-Wert des Originaltextes vergleichen kann. Im Fall einer Nichtübereinstimmung der Hash-Werte ist die Nachricht nachträglich manipuliert worden und die Signatur nicht echt.[351] Durch den Einsatz einer qualifizierten elektronischen Signatur, bei der die Zusammengehörigkeit von Signaturschlüsseln und einer bestimmten Person durch das Zertifikat eines – aus Sicherheitsaspekten heraus notwendigerweise auch akkreditierten – Zertifizierungsdiensteanbieters bescheinigt wird, kann der Wähler zudem authentifiziert werden.[352] Zudem wird der Gefahr einer Mehrfachwahl dadurch begegnet, dass über die eindeutige digitale Signatur der Wahlstatus eines jeden Wählers nach Registrierung der Wahlentscheidung im Wählerverzeichnis verändert werden kann.[353]

3. MIX-Modell

Einer weiteren technischen Sicherheitsanforderung an Internetwahlen, der Gewährleistung der Anonymität der Wahlentscheidung, kann aber selbst der parallele Einsatz von elektronischer Signatur und asymmetrischer Verschlüsselung nicht gerecht werden. Eine Möglichkeit der anonymen Kommunikation bei gleichzeitiger Authentifizierungsmöglichkeit des Absenders zeigte David Chaum mit seinem MIX-System auf.[354] Hierbei werden zwischen Absender und Empfänger chiffrierter Nachrichten bestenfalls mehrere so genannte MIXe geschaltet, die die eingehenden chiffrierten Dokumente sammeln, umchiffrieren und umsortieren und so die Rückverfolgbarkeit von Dokument zu Absender verhindern.[355] Das Votum wird auf diese Weise also von der Wähleridentität getrennt und dient damit der Anonymisierung der Stimmabgabe. Während mit diesem System die Sicherheitsanforderungen der Internetwahl folglich zunächst erfüllt

[351] *Hanßmann*, S. 80 f.
[352] *Hanßmann*, S. 83.
[353] *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 644 f.
[354] *Chaum*, Untraceable Electronic Mail, Return Adresses, and Digital Pseudonyms, Communication of the ACM, Vol. 24, No. 2, Februar 1981, abrufbar unter: http://world.std.com/~franl/crypto/chaum-acm-1981.html, (Stand: 19.06.07).
[355] *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 645.

werden, leidet das System beim Einsatz mehrerer MIXe unter einem recht hohen technischen Aufwand; zudem bestehen Zweifel hinsichtlich der Dauerhaftigkeit des Anonymisierungserfolges.[356]

4. Blinde Signaturen

Eine alternative Möglichkeit zur Authentifizierung des Wählers bei gleichzeitiger Anonymität des Votums bietet der Einsatz blinder Signaturen.[357] Eine blinde Signatur wird erzeugt, wenn jemand ein Dokument unterzeichnet, ohne erkennen zu können, was er unterzeichnet.[358] Im Rahmen des Stimmabgabeverfahrens könnte also der Wähler seine Wahlentscheidung mit einer nur ihm bekannten Zufallszahl multiplizieren, elektronisch signieren und dieses für Dritte nunmehr unkenntliche Dokument dem Wahlamt zur Unterzeichnung übermitteln. Das Wahlamt könnte sodann die Wahlberechtigung anhand der elektronischen Signatur überprüfen, wegen des unbekannten Blendfaktors den Inhalt aber nicht zur Kenntnis nehmen. In Verbindung mit einem Mehragentensystem bei der die Wahlberechtigungsprüfung organisatorisch von der Wahlurne und der Auswertung getrennt abläuft, wie es z.B. das Internetwahlprotokoll i-vote vorsieht,[359] könnte der Einsatz von blinden Signaturen bei Internetwahlen schlussendlich zur Wahrung der Anonymität in jedem Schritt des Wahlprotokolls führen.[360]

Diese technischen Maßnahmen stellen viel versprechende und zukunftsträchtige Ansätze zur Gewährleistung der Sicherheit von Internetwahlen dar. Dennoch werden die bislang entwickelten Konzepte weiterhin vielfach als unzureichend und dem hohen Sicherheitsniveau, das politische Internetwahlen genießen sollten, nicht entsprechend empfunden.[361] Unverkennbar sind die Sicherheitsrisiken, die bei einer internetbasierten elektronischen Wahl bestehen, aber deutlich komplexer als bei der herkömmlichen Papierwahl. Die verbleibende Ungewissheit,

---

[356] *Grimm* in Holznagel, S. 86, 92 f.; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 645.
[357] *Chaum*, Achieving Electronic Privacy, abrufbar unter: http://www.chaum.com/articles/Achieving_Electronic_Privacy.htm, (Stand: 19.06.07).
[358] *Grimm* in Holznagel, S. 86, 96; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 645.
[359] *Otten* in Holznagel, S. 73, 79 f.
[360] *Hanßmann*, S. 87 ff.; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 645.
[361] *Hanßmann*, S. 90; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 647.

ob die aufgeführten technischen Gegenmaßnahmen die möglichen Bedrohungen dauerhaft ausreichend auffangen können, muss bei der abschließenden Bewertung über die Einführung von Internetwahlen mit berücksichtigt werden.

E. Rechtliche Zulässigkeit in Deutschland

Dass die Implementierung eines Internetwahlsystems auf einige erhebliche technische Schwierigkeiten, bestenfalls Herausforderungen, stößt, die es schrittweise anzugehen gilt, ist von Experten weltweit erkannt worden. Die Frage aber, ob die Einführung von Wahlen über das Internet rechtlich überhaupt zulässig ist, ist auf nationaler Ebene zu beantworten, da die rechtlichen Anforderungen vom jeweiligen Wahlrecht aufgestellt werden.[362] Der folgende Abschnitt analysiert deswegen die rechtliche Vereinbarkeit von zunächst politischen und schließlich privaten Wahlen mit den gesetzlichen Vorgaben in Deutschland.

I. Politische Wahlen

Grundlage des deutschen Wahlrechts stellen die verfassungsrechtlichen Wahlgrundsätze in Art. 38 I 1 GG dar, die unmittelbar zwar lediglich für die Wahlen zum deutschen Bundestag gelten,[363] über Art. 28 I 2 GG aber auch verbindliche Anwendung bei den Volksvertreterwahlen auf Landes-, Kreis- und Kommunalebene finden.[364]

Einfachgesetzlich konkretisiert und ausgestaltet sind die verfassungsrechtlichen Wahlgrundsätze im Bundeswahlgesetz und der Bundeswahlordnung. Die Internetwahl muss sich bezüglich ihrer rechtlichen Zulässigkeit nur dann direkt an den Grundsätzen des Art. 38 I 1 GG messen lassen, wenn sie sich keinem der in den §§ 34-36 BWG zugelassenen Wahlverfahren zuordnen lässt. Die einzig in Betracht zu

---

[362] *Hanßmann*, S. 92; auf europäischer Ebene existieren aber die Empfehlungen des Europarates: *Council of Europe*, Recommendation Rec (2004) 11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies, abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?id=778189, (Stand: 23.06.07).

[363] *BVerfGE* 3, S. 383, 390 f.

[364] *BVerfGE* 11, S. 266, 272.

ziehende Qualifikation als „Stimmabgabe mit einem Wahlgerät“ i.S.d. § 35 BWG, scheidet aber schon deshalb aus, weil es sich bei den für die Internetwahl eingesetzten PCs nicht um Wahlgeräte i.S.d. Norm handelt.[365] Ursprünglich schloss § 35 I BWG noch ausdrücklich solche Geräte, die kein selbständiges Zählwerk haben, um die abgegebenen Wahlentscheidung zu erfassen, vom Anwendungsbereich der Norm aus. [366] Aber auch nach der Gesetzesänderung ist aus dem Gesamtreglement von § 35 BWG und der BWahlGV zu entnehmen, dass das „Remote Internet Voting“ nicht unter den Begriff der „Wahl mit Stimmabgabegeräten“ fallen soll, weil eine Vernetzung der Geräte mit Internettechnologie von der BWahlGV nicht vorgesehen ist.[367]

Im Übrigen sind auch die sehr detaillierten Regelungen der BWahlGV zu den stationären Wahlgeräten nicht für das Konzept der Internetwahl vom individuellen Computer nutzbar.[368]

Folglich muss sich die Internetwahl an den verfassungsrechtlichen Wahlgrundsätzen messen und auf ihre rechtliche Zulässigkeit überprüfen lassen.

1. Wahlrechtsgrundsätze

Nach Art. 38 I 1 GG müssen die parlamentarischen Volksvertreter in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl durch das Volk bestimmt werden. Diese Wahlrechtsgrundsätze stellen auch den Maßstab für eine zu implementierende Internetwahl dar. Im Folgenden wird untersucht, ob eine Wahl, die sich auf die Internettechnologie stützt, überhaupt mit dem Verfassungsrecht vereinbar ist und welche Ausgestaltung das Wahlverfahren einfachgesetzlich gegebenenfalls finden muss.

a) Allgemeinheit der Wahl

Der Grundsatz der allgemeinen Wahl soll dem gesamten Volk die Möglichkeit der verantwortlichen politischen Mitbestimmung in formal

[365] *Bremke*, LKV 2004, S. 102, 106; *Hanßmann*, S. 52; *Holznagel/Hanßmann* in Holznagel, S. 55, 58; *Karpen*, S. 34; *Khorrami*, S. 72; *Rüß*, ZRP 2001, S. 518 ff.
[366] *Schreiber*, § 35 Rn. 1.
[367] Vgl. §§ 10 I Nr. 3, 12, 13, 14 I, III BWahlGV; *Schreiber*, § 35 Rn. 1.
[368] *Bremke*, LKV 2004, S. 102, 106; *Hanßmann*, S. 99; *Holznagel/Hanßmann* in Holznagel, S. 55, 58; *Karpen*, S. 34; *Rüß*, ZRP 2001, S. 518 ff.

möglichst gleicher Weise gewährleisten.[369] Durch Art. 38 I 1 GG wird dem Gesetzgeber der Ausschluss bestimmter Bevölkerungsgruppen von der Wahl aufgrund wirtschaftlicher, politischer oder sozialer Differenzierungsmerkmale untersagt.[370]

Die Einführung von Internetwahlen gefährdet diesen Allgemeinheitsgrundsatz in unterschiedlicher Hinsicht.

Eine Wahl ausschließlich über individuelle internetfähige Computer schlösse all diejenigen von der Stimmabgabe aus, die über keinen solchen Computer verfügen. Hierin läge ein klarer Verstoß gegen den Grundsatz der allgemeinen Wahl.[371] Selbst wenn das rein internetbasierte Wahlsystem auch die elektronische Wahl im Wahllokal („Polling Place Internet Voting") und an Wahlkiosken vorsähe und grundsätzlich jedem Bürger die Wahl ermöglichte, so würde dennoch die abrupte Umstellung der Wahltechnik zu einer verfassungswidrigen digitalen Spaltung der Gesellschaft führen, da große Teile der Bevölkerung von der Technik vor einer Stimmabgabe abgeschreckt werden könnten.[372]

Führt man die Internetwahl allerdings als eine die bestehenden Wahlmöglichkeiten von Präsenz- und Briefwahl ergänzende Maßnahme ein, so könnte sie sich regelrecht als Unterstützung der Allgemeinheit der Wahl darstellen, indem sie zu einer erhöhten Wahlbeteiligung, insbesondere unter Jungwählern, führt[373] und für Sehbehinderte und Blinde sogar eine Stimmabgabevereinfachung darstellt.[374] Allerdings begegnet auch die ergänzende Einführung der Internetwahl rechtlichen Bedenken. Der Wahlgrundsatz der Allgemeinheit beinhaltet auch das Gebot einer möglichst gleichförmigen Ausübung des Wahlaktes. Dem wird der Gesetzgeber bislang durch die gesetzlich angeordnete Regel der Stimmabgabe im Wahllokal gerecht,[375] während die Briefwahl zwar als verfassungsgemäß, aber auch als ausdrücklicher Ausnahmefall und nur

[369] *Jarass/Pieroth*, Art. 38 Rn. 5; *Schreiber*, § 1 Rn. 7.
[370] *BVerfGE* 58, S. 202, 205.
[371] *Birkenmaier*, S. 113; *Karpen*, S. 21; *Khorrami*, S. 75; *Will*, CR 2003, S. 126, 127; *Will*, S. 154.
[372] *Holznagel/Hanßmann* in Holznagel, S. 55, 60; *Khorrami*, S. 75.
[373] *Bremke*, LKV 2004, S. 102, 107; *Karpen*, S. 21; *Will*, S. 154.
[374] *Rüß*, ZRP 2001, S. 518, 519.
[375] *Tauss* in Kubicek, S. 285, 289; *Schreiber*, § 36, Rn. 4.

unter im Gesetz abschließend aufgeführten Voraussetzungen[376] als zulässig anerkannt ist.[377] Da schon die momentane extensive Praxis der Briefwahl verfassungsrechtlichen Bedenken begegnen muss,[378] ist die Einführung von Internetfernwahlen jedenfalls auch nur unter den Zulassungsvoraussetzungen für Briefwahlen, also Antrag, Verhinderungsgrund und eidesstattliche Erklärung, rechtlich haltbar.[379]
Während die Internetwahl diesen Anforderungen in technischer Hinsicht gerecht werden kann,[380] stellen die bislang nicht beherrschbaren Risiken der Wahlbehinderung durch DoS-Angriffe und intendierte oder zufällige Systemausfälle die Einhaltung des Allgemeinheitsgrundsatzes in organisatorischer Hinsicht in Frage.[381] Würden größere Wählerkreise aufgrund einer Unerreichbarkeit des Wahlservers faktisch von der Stimmabgabe ausgeschlossen, wäre die Allgemeinheit der Wahl nicht gegeben. Dieses Problem kann auch nicht dadurch gelöst werden, dass die Internetfernwahl lediglich im Vorfeld des Wahltages ausgetragen wird, so dass bei einem technischen Ausfall noch die Wahl im Wahllokal am Wahltag selbst bestünde, weil die Teilnahme an der Internetfernwahl ja gerade in der Verhinderung am Wahltag selbst begründet liegt.
Mit Blick auf den momentanen Stand der Technik erscheint also eine Internetfernwahl als Alternative zur Briefwahl nicht mit dem Allgemeinheitsgrundsatz zu vereinbaren.

b) Unmittelbarkeit der Wahl

Bezüglich des Grundsatzes der Unmittelbarkeit der Wahl, wonach zwischen Wähler und zu Wählendem keine weitere Instanz, z.B. Wahlmänner, treten darf, bestehen bei der Wahl über ein internetbasiertes System keine Probleme.[382] Für Menschen mit Behinderungen wird durch die Internetwahl womöglich sogar ein Mehr an Unmittelbarkeit, i.S.v.

---

[376] § 25 BWO.
[377] *BVerfGE* 59, S. 119, 125.
[378] *Birkenmaier*, S. 108; *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 100; *Tauss*, S. 285, 289; *Will*, S. 156.
[379] *Birkenmaier*, S. 113; *Karpen*, S. 21; *Khorrami*, S. 76: *Rüß*, MMR 2000, S. 73, 75; *Will*, CR 2003, S. 126, 130; kritisch: *Schreiber*, § 35 Rn. 9.
[380] *Birkenmaier*, S. 113 f.; *Khorrami*, S. 76.
[381] *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 97; *Will*, S. 154.
[382] *Birkenmaier*, S. 57 f.; *Bremke*, LKV 2004, S. 102, 107; *Holznagel/Hanßmann* in Holznagel, S. 55, 63; *Karpen*, S. 22 f.; *Rüß*, ZRP 2001, S. 518, 528; *Will*, S. 157 f.

Höchstpersönlichkeit, dadurch erreicht, dass diese keine Hilfs- oder Vertrauenspersonen zur Stimmabgabe mehr in Anspruch nehmen müssen.[383]

c) Freiheit der Wahl

Nach dem Grundsatz der Freiheit der Wahl müssen die Wähler in ihrer Wahlentscheidung frei von jeglichem politischen, wirtschaftlichen oder sozialen Zwang oder sonstigem rechtswidrigem Einfluss von außen bleiben.[384]

Genau wie bei der Briefwahl wird bei der Internetwahl aus dem individuellen Bereich heraus die Wahlentscheidung der Beeinflussungsmöglichkeit durch andere Personen im Haushalt und Umfeld ausgesetzt, wodurch der Freiheitsgrundsatz gefährdet wird. Auch aus diesem Grund müssen an die Internetfernwahl die gleichen engen Voraussetzungen wie an die Briefwahl gestellt werden, wodurch der Ausnahmecharakter der Distanzwahl verdeutlicht werden soll.[385]

Das Erfordernis der eidesstattlichen Versicherung bei der Briefwahl kann parallel bei der Internetwahl über das System der digitalen Signatur technisch erfüllt werden.[386]

Eine alternative Möglichkeit die Freiheit der Stimmabgabeentscheidung zu gewährleisten besteht darin eine Mehrfachwahl zuzulassen, bei der lediglich die letztabgegebene Stimme in die Auszählung eingeht.[387] Dieser Weg wurde bereits bei den Internetwahlen in Estland verfolgt, wo zudem einer eventuell abgegebenen Papierstimme absolute Priorität vor einer elektronisch abgegebenen Stimme eingeräumt wurde.[388]

Im Übrigen muss die Stimmabgabe am vernetzten Computer frei von jeglicher Wahlbeeinflussung auf dem Bildschirm durch Pop-Up-Fenster mit beeinflussendem Inhalt, Werbemitteilungen oder Wahlpropaganda

---

[383] *Bremke*, LKV 2004, S. 102, 107.
[384] *Schreiber*, § 1 Rn. 13a.
[385] *Khorrami*, S. 79 f.; *Rüß* in Buchstein/Neymanns, S. 39, 43 f.; *Rüß*, ZRP 2001, S. 518, 520; *Will*, S. 156.
[386] *Khorrami*, S. 80; *Rüß* in Buchstein/Neymanns, S. 39, 44.
[387] *Skagestein/Haug/Nødtvedt/Rossebø* in Krimmer, S. 107, 109; *Volkamer/Grimm* in Krimmer, S. 97, 101 f.; *Will*, S. 156.
[388] *Madise*, Internet Voting in Estonia – Free and Fair Elections, S. 6, abrufbar unter: http://www.vvk.ee/engindex.html, (Stand: 15.06.07); *Maaten* in Prosser/Krimmer, S. 83, 85.

bleiben.[389] Technisch ist eine solche Beeinflussung für die Browser auf heimischen Computern zwar nicht gänzlich auszuschließen, durch Aufklärung der Wähler über wirksame Verhaltensmaßnahmen kann sie aber stark minimiert werden.

Schließlich beinhaltet der Grundsatz der freien Wahl auch das Recht auf eine bewusst ungültige Stimmabgabe.[390] Technisch kann dies in Form eines eigenen Felds „Ungültige Stimmabgabe“ oder vorzugswürdig, weil nicht zur Ungültigkeitswahl animierend,[391] durch ein sich im Fall der ungültigen Stimmabgabe öffnendes Hinweisfenster, welches eine Korrektur- oder Bestätigungsmöglichkeit vorsieht, ausgestaltet werden.[392]

Bei Einhaltung der angeführten Anforderungen kann also durch spezielle Ausgestaltung ein Internetwahlverfahren geschaffen werden, das mit dem Grundsatz der freien Wahl zu vereinbaren ist.

d) Gleichheit der Wahl

Der ebenso in Art. 38 I 1 GG verbürgte Gleichheitsgrundsatz beinhaltet einerseits in aktiver Hinsicht die Gewährleistung gleichen Zähl- und Erfolgswerts der Stimmen und in passiver Hinsicht die Chancengleichheit für jeden Wahlbewerber.[393]

Letztere Anforderung bedeutet in Bezug auf die Internetwahl, dass die Parteien und Kandidaten wie auf dem traditionellen Papierwahlzettel anzuordnen und auf dem elektronischen Stimmzettel gleichermaßen einfach zu erreichen sein müssen.[394] Da bereits die Notwendigkeit des Scrollens wegen zu großer Stimmzettel-Dimensionen eine Benachteiligung darstellen würde, [395] erscheint der Einsatz von

[389] *Birkenmaier*, S. 58 f.; *Bremke*, LKV 2004, S. 102, 107; *Rüß*, ZRP 2001, S. 518, 520; *Rüß*, MMR 2000, S. 73, 74; *Will*, S. 156.
[390] *Bremke*, LKV 2004, S. 102, 107; *Karpen*, S. 23; *Rüß*, MMR 2000, S. 73, 74; *Schreiber*, § 1 Rn. 13a.
[391] *Bremke*, LKV 2004, S. 102, 107; *Karpen*, S. 24; Will, S. 156.
[392] *Karpen*, S. 24; *Khorrami*, S. 80; *Will*, S. 156.
[393] *Karpen*, S. 25.
[394] *Bremke*, LKV 2004, S. 102, 107; *Schwarz* in Schweighofer, S. 263, 268; *Will*, CR 2003, S. 126, 132.
[395] *Birkenmaier*, S. 62; *Will*, CR 2003, S. 126, 130; *Will*, S. 155.

Mobiltelefonen zur Stimmabgabe unter verfassungsrechtlichen Gesichtspunkten mehr als fraglich.[396]

Die Gewährleistung, dass jede elektronisch abgegebene und übers Internet übermittelte Stimme gleiche Auswirkungen auf das Endergebnis hat, ist nur dann erreicht, wenn eine mehrfache Wahl ausgeschlossen werden kann.[397] Dies setzt zum einen eine zuverlässige Identifizierung des Wählers voraus, so dass niemand an seiner statt wählen kann, und zum anderen eine Registrierung der abgegebenen Stimme, um eine mehrfache Stimmabgabe auszuschließen.[398] Technisch lässt sich diese sichere Identifizierung wie oben dargestellt z.B. durch eine qualifizierte elektronische Signatur erreichen;[399] den Ausschluss einer Doppelwahl im privaten Umfeld muss der Wähler durch die Abgabe einer Versicherung an Eides statt ebenfalls mittels einer qualifizierten elektronischen Signatur erklären.[400]

Ein Verstoß gegen den Grundsatz der gleichen Wahl würde auch in jeder Veränderung der ursprünglich abgegebenen Stimme liegen.[401] Die Gefahr der Manipulation besteht für die Wahlentscheidung sowohl auf dem Übertragungsweg (durch Spoofing, Trojaner) als auch bei der Stimmauszählung und –auswertung, bei der eine manipulierende Software zum Einsatz kommen kann.[402] Dass die Manipulationsfreiheit der Stimmübermittlung nur bis zu einem gewissen Grad und - realistisch betrachtet - nicht ausreichend gewährleistet werden kann, weil technische Gegenmaßnahmen insbesondere vom Internetnutzer selbst eingeleitet werden müssten, wurde bereits erläutert.[403] Das manipulationsfreie Funktionieren der Auswertungssoftware sicherzustellen, wirft hingegen noch größere Probleme auf, da hier die Gefahr insbesondere von Innentätern droht. Um dieser Bedrohung erfolgreich entgegen zu wirken, müssen die Offenlegung des Programmcodes und auch eine

[396] *Birkenmaier*, S. 63.
[397] *Bremke*, LKV 2004, S. 102, 107; *Rüß*, ZRP 2001, S. 518, 520; *Will*, CR 2003, S. 126, 131; *Will*, S. 155.
[398] *Karpen*, S. 26; *Khorrami*, S. 82; *Will*, S. 155.
[399] *Birkenmaier*, S. 69 ff.; *Rüß*, ZRP 2001, S. 518, 520; *Will*, S. 155.
[400] *Will*, CR 2003, S. 126, 131.
[401] *Will*, CR 2003, S. 126, 132.
[402] *Khorrami*, S. 83 f.
[403] S. oben unter Kapitel 4 D. I.

kontinuierliche Kontrolle der Software im Rahmen eines Zertifizierungssystems gefordert werden.[404] Wie schwierig es jedoch ist die Software-Entwickler von diesem Ansatz zu überzeugen, zeichnet sich momentan bei der Debatte um die Sicherheit der Wahlcomputer ab, bei der die Verantwortlichen weiterhin auf das Konzept „security by obscurity" setzen.[405]

e) Geheimheit der Wahl

Im Zusammenspiel mit den Grundsätzen der allgemeinen und unmittelbaren Wahl ist die Einhaltung des Geheimheitsgrundsatzes unabdingbare Voraussetzung für die Freiheit der Wahlentscheidung eines jeden Wählers in der Demokratie.[406] Die Geheimheit der Wahl setzt voraus, dass die Stimmabgabe des Wählers keinem anderen bekannt werden darf.[407] Das Wahlsystem muss also derart ausgestaltet sein, dass der Wähler seine Wahlentscheidung unbeobachtet im Verborgenen treffen kann, die Stimme während der Übermittlung nicht auslesbar ist und bei der Wahlauswertung ein Rückschluss auf die Identität des Wählers ausgeschlossen ist. Die Geheimheit der Stimmabgabe steht nicht zur Disposition, sondern ist obligatorisch, so dass der Wähler dazu verpflichtet ist, die vom Staat ergriffenen Maßnahmen zur Gewährleistung der Geheimhaltung in Anspruch zu nehmen.[408] Ausnahmen von der obligatorischen Geheimhaltung sind nur in den engen gesetzlichen Grenzen, die im Gegenzug - wie z.B. die Briefwahl - der Allgemeinheit der Wahl dienen sollen, zugelassen.[409] Es wird inzwischen angezweifelt, dass dieser Ausnahmecharakter der Briefwahl bei stark angestiegener Anzahl von Briefwählern überhaupt noch gewahrt ist.[410] Umso kritischer muss unter verfassungsrechtlichen Gesichtspunkten das Konzept der Distanzwahl per Internet betrachtet werden, welches vorsätzlich zu noch mehr Stimmabgaben aus dem heimischen Bereich animiert und damit den obligatorischen

[404] *Buchsbaum* in Schweighofer, S. 278, 284; *Will*, CR 2003, S. 126, 132; *Will*, S. 155.
[405] Vgl. oben Kapitel 2 C II. 1.d) aa).
[406] *Khorrami*, S. 84.
[407] *Birkenmaier*, S. 86; *Karpen*, S. 27; *Will*, S. 157.
[408] *Birkenmaier*, S. 87; *Karpen*, S. 27; *Khorrami*, S. 85.
[409] *Karpen*, S. 28 f.
[410] *Buchstein* in Buchstein/Neymanns, S. 51, 61; *Will*, S. 156.

Geheimhaltungsgrundsatz verletzt.[411] Da eine Rechtfertigung bei der bestehenden Rechtslage nicht denkbar erscheint, wird das Konzept der Geheimhaltungspflicht teilweise insgesamt in Frage gestellt.[412] Eine nähere Auseinandersetzung mit dieser Kritik würde den Rahmen der vorliegenden Arbeit jedoch sprengen.

Zur Sicherheit der Stimmübertragung können die bereits angeführten Gegenmaßnahmen, wie insbesondere die komplexe Kryptographie, elektronische Signaturen, blinde Beglaubigungssysteme und eine organisatorische informationelle Gewaltenteilung beitragen.[413] Obwohl die Anonymisierung bei gleichzeitiger zuverlässiger Identifikation des Wählers auf technischem Wege erreicht werden kann,[414] ist ein absoluter technischer Schutz dennoch bislang nicht zu gewährleisten und die Gefahren durch Spoofing, Trojaner und Viren stehen der Einhaltung des Geheimhaltungsgrundsatzes entgegen. Aufgefangen werden könnten diese Bedrohungen von dem in Estland verfolgten Konzept der wiederholten Stimmabgabemöglichkeit.[415]

Weitere Beachtung muss unter dem Gesichtspunkt der Geheimhaltung auch der Ausgestaltung der Wahlkreise geschenkt werden. Bei Neu-Einführung einer ergänzenden Internetfernwahlmöglichkeit ist nicht in jedem Wahlkreis mit einer so hohen Wahlbeteiligung via Internet zu rechnen, dass ein Rückschluss auf die digitalen Wähler ausgeschlossen ist. Hier muss also gegebenenfalls eine Anpassung der Wahlbezirke erfolgen.[416]

Schließlich muss die Geheimhaltung der Wahlentscheidungen nicht nur während des laufenden Wahlprozesses gewährleistet werden können, sondern vielmehr nachhaltig weit über die Wahl hinaus.[417] Dass die bislang in den Internetwahlprotokollen vorgesehenen

---

[411] *Birkenmaier*, S. 110; *Buchstein* in Buchstein/Neymanns, S. 51, 65; *Holznagel/Hanßmann* in Holznagel, S. 55, 63; *Schreiber*, § 35 Rn. 9; Karpen in *Sietmann*, c't 01/06, S. 80 ff.

[412] *Buchstein* in Buchstein/Neymanns, S. 51, 65 ff.; *Karpen*, S. 29.

[413] Vgl. *Karpen*, S. 29; *Ullmann/Koob/Kelter*, DuD 2001, S. 643, 644 ff.

[414] *Birkenmaier*, S. 104; *Bremke*, LKV 2004, S. 102, 104 f.; *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 96; *Rüß* in Buchstein/Neymanns, S. 39, 46 f.

[415] *Volkamer/Grimm* in Krimmer, S. 97, 101 f.; *Skagestein/Haug/Nødtvedt/Rossebø* in Krimmer, S. 107, 109 f.

[416] *Karpen*, S. 30 f.; *Rüß* in Buchstein/Neymanns, S. 39, 46 f.

[417] *Krimmer/Volkamer* in Schweighofer, S. 256, 261.

Anonymisierungsverfahren, welche auf einen besonders hohen Rechenaufwand zur Dekryptierung aufbauen,[418] zu einer dauerhaften Geheimhaltung führen, ist bei der rasanten technologischen Entwicklung zweifelhaft. Einen denkbaren Lösungsansatz bietet hier der von der Forschungsgruppe Industrielle Software der TU Wien entwickelte „Vote Scrambling Algorithm“, der zu einer Veränderung der Stimmen dergestalt führt, dass sie unabhängig von der eigentlichen Stimmverteilung einer Gleichverteilung unterliegen.[419]

Aufgrund bislang fehlender technischer Lösungen zur absoluten Manipulationssicherheit und wegen des Verstoßes gegen die obligatorische Geheimhaltung, sind Internetwahlen nicht mit dem Geheimhaltungsgrundsatz des Art. 38 I 1 GG vereinbar.

f) Öffentlichkeit der Wahl

Neben den Wahlrechtsgrundsätzen des Art. 38 I 1 GG, müssen sich Internetwahlen auch an ungeschriebenen Grundsätzen, allen voran an dem Grundsatz der Öffentlichkeit der Wahl, messen lassen. Dieser wird aus dem Demokratie- und Rechtsstaatsprinzip abgeleitet[420] und besagt, dass alle Phasen des Wahlverlaufs der Kontrolle durch die Öffentlichkeit zugängig sein müssen, so dass diese sich über den ordnungsgemäßen Wahlverlauf selbst vergewissern kann.[421]

Ähnlich wie bei den Wahlcomputern wird die derartig angestrebte Schaffung von Transparenz und Nachvollziehbarkeit durch das „Remote Internet Voting“-System stark in Frage gestellt. Internetdistanzwahlen lassen sich nur durch ein hoch komplexes technisches Protokoll verwirklichen, welches sich vom durchschnittlich versierten Wähler in keiner Weise nachvollziehen, geschweige denn auf Sicherheitslücken oder Abweichungen überprüfen lässt. Es droht folglich die Erodierung des Öffentlichkeitsprinzips dadurch, dass das reibungslose und manipulationsfreie Funktionieren des Wahlsystems, von Stimmabgabe bis Stimmauswertung, nur von Experten und den Systemherstellern

[418] Vgl. *Forschungsgruppe Internetwahlen*, i-vote Report, S. 23.
[419] *Fischer/Zuser* in Schweighofer, S. 286 ff.
[420] *Bremke*, LKV 2004, S. 102, 107; *Karpen*, S. 31.
[421] *Hanßmann*, S. 184.

kontrolliert werden kann.[422] Zur Einhaltung des Grundsatzes der öffentlichen Wahl muss aber die Verantwortung für den korrekten Wahlverlauf beim Wahlvorstand liegen und der Wahlöffentlichkeit die Überwachung der Stimmauswertung möglich sein. Hierzu könnten die Schaffung eines papiernen Belegs oder eines digitalen Speichers sowie der Einsatz von Kontrollinstanzen einen wichtigen Beitrag leisten.[423] Denkbare Gegenmaßnahmen liegen hierbei in der Zertifizierung der Wahlsoftware durch z.B. die PTB oder das BSI[424], besser noch die Offenlegung des Programmcodes der Wahlsoftware.[425]

Auch in sozio-kultureller Hinsicht birgt die internetbasierte Wahl aus dem individuellen Bereich heraus die Gefahr, dass die Identifikation des Wählers mit dem Staat verloren geht.[426] Die Tatsache, dass der Wähler bequem von zu Hause aus seine Stimme abgeben kann ohne den Gang zum öffentlichen Wahllokal auf sich nehmen zu müssen, nimmt dem Wahlverlauf seine symbolisch-rituelle Funktion und trivialisiert die Stimmentscheidung.[427]

g) Weitere ungeschriebene Verfassungsgrundsätze

Ebenso bestehen im Hinblick auf andere ungeschriebene Verfassungsgrundsätze Bedenken bezüglich der Einführung des „Remote Internet Voting".

Schon aus dem Grundsatz der Kostenfreiheit der Wahl für die Wähler ergibt sich, dass eine Umstellung des Wahlsystems auf eine ausschließliche internetgestützte Distanzwahl nicht verfassungsgemäß wäre, da der Staat ansonsten jeden Bürger mit einem internetfähigen Computer ausstatten müsste. Aber auch bei der Ausgestaltung als zusätzliches Angebot neben Präsenz- und Briefwahl, bzw. als Kiosk

[422] *Hanßmann*, S. 188; *Karpen*, S. 32; *Otten* in Buchstein/Neymanns, S. 71, 86; *Will*, S. 153.
[423] *Bremke*, MMR 2004, S.IX, XII; *Hanßmann*, S. 188 f.; *Otten* in Buchstein/Neymanns, S. 71, 86.
[424] *Bremke*, LKV 2004, S. 102, 108.
[425] *CalTech/MIT*, S. 46; *Grimm* in Holznagel, S. 86, 101; *Rüß*, ZRP 2001, S. 518, 519; *Will*, CR 2003, S. 126, 132; *Will*, S. 155.
[426] *Bremke*, LKV 2004, S. 102, 108; *Karpen*, S. 31.
[427] *Bremke*, LKV 2004, S. 102, 108; *Karpen*, S. 31.

Voting stellt sich die Frage, wer die Anschaffungskosten für die Signaturkarten und Kartenlesegeräte übernimmt.[428]

Weiterhin steht die technische Komplexität des Internetwahlsystems in krassem Gegensatz zur Verständlichkeit und Einfachheit der Präsenzwahl. Die Internetwahl verlangt den Wählern computertechnische Grundkenntnisse ab und könnte mit dieser Anforderung zu einer problematischen Spaltung der Gesellschaft führen.[429]

Schließlich leidet die Internetwahl auch unter dem Problem des Mangels an Gleichzeitigkeit der Stimmabgabe, welches schon bei der Briefwahl besteht und kritisiert wird.

2. Zusammenfassung

Eine verfassungskonforme Durchführung von Internetwahlen ist bei bestehender Rechtslage und unter Berücksichtigung der bisher entwickelten technischen Lösungen, nicht möglich. Den Bedrohungspotentialen, die sich aus der Übertragung der Stimmen über das offene Internet von nicht unter staatlicher Kontrolle stehenden Endgeräten ergeben, kann bislang nicht zufrieden stellend mit entsprechenden Gegenmaßnahmen begegnet werden, so dass die Grundsätze der Allgemeinheit, der Gleichheit und der Geheimheit der Wahl nicht gewährleistet sind. Ebenso fehlt es an einer Kontrollmöglichkeit der Öffentlichkeit über den ordnungsgemäßen Wahlverlauf, weil die technische Komplexität die Systemüberprüfung Spezialisten vorbehält. Damit ist auch der Grundsatz der Öffentlichkeit verletzt.

II. Private Wahlen

Die Tatsache dass die Durchführung von Internetwahlen auf oberster politischer Ebene beim derzeitigen Stand der Technik verfassungsrechtlich unzulässig ist, führt zu der Frage, ob dies vorerst jeglichen verbindlichen Einsatz internetbasierter Wahlsysteme zur Folge hat, oder ob außerhalb der Parlamentswahlen mögliche Einsatzfelder denkbar sind, in denen nicht die gleichen rechtlichen Bedenken greifen.

[428] *Karpen*, S. 33; *Kubicek/Wind* in Buchstein/Neymanns, S. 91, 105.
[429] *Karpen*, S. 33.

Attraktives Potential haben hier insbesondere Stimmabgaben in kleinen Gremien wie z.B. bei Wahlen zu Selbstverwaltungsorganen von Hochschulen, Personal- oder Betriebsratswahlen, Aktionärs- und Vereinswahlen, gezeigt.[430] Für diese nicht politischen Wahlen gelten die Wahlrechtsgrundsätze aus Art. 38 I 1 GG nicht zwangsläufig und auch nicht immer umfassend.[431] Abweichungen und Einschränkungen sind je nach Wahlkontext vor allem in Bezug auf das Prinzip der Allgemeinheit und der Gleichheit der Wahl möglich,[432] welche gegebenenfalls zu Gunsten eines überragenden Differenzierungsgrundes weichen. Auch ist eine geheime Stimmabgabe nicht notwendigerweise für jede Wahl vorgeschrieben;[433] wohingegen eine begründete Einschränkung der Freiheit der Wahl in keiner Wahlumgebung ersichtlich ist.[434]

In einem demokratischen Staat müssen die Grundsätze des Art. 38 I 1 GG aber dennoch als maßgebliche Orientierungspunkte und ungeschriebene Verfassungsgrundsätze auch im privaten Umfeld bei Stimmabgabeprozessen beachtet werden und sind oft auch einfachgesetzlich bzw. per Verordnung oder Satzung vorgeschrieben.[435]

In die Bewertung der Zulässigkeit einer Abweichung von Art. 38 I 1 GG muss deswegen immer eine Verhältnismäßigkeitsprüfung einfließen, die die Intensität der Abweichung, den betroffenen Sach- und Beteiligtenbereich und die die Wahlverfahrensmaßstäbe bestimmende Institution berücksichtigt.[436]

Rechtliche Rahmenbedingungen für den Einsatz von Internetwahlsystemen wurden z.B. durch eine Gesetzesänderung des AktG geschaffen, welches nunmehr die Stimmabgabe von abwesenden Aktionären bei der Hauptversammlung erleichtert.[437] Den Vorteil der online-Vollmachtserteilung für Stimmrechtsvertreter konnten die Aktionäre der DaimlerChrysler AG bereits auskosten.[438]

---

[430] *Holznagel/Hanßmann* in Holznagel, S. 55, 65.
[431] *Karpen*, S. 42 ff.; *Jarass/Pieroth*, Art. 38 Rn. 2a; *Will*, S. 159.
[432] BVerfGE 41, S. 1, 13 f.
[433] Vgl. für die Aktionärswahlen: § 118 AktG.
[434] *Karpen*, S. 42.
[435] *Holznagel/Hanßmann* in Holznagel, S. 55, 65; *Will*, S. 159.
[436] *Karpen*, S. 43; vgl. auch *Jarass/Pieroth*, Art. 38 Rn. 2a.
[437] *Holznagel/Hanßmann* in Holznagel, S. 55, 65; *Noack* in Hoeren/Sieber, Kapitel 21.2, Rn. 87 ff.
[438] Vgl. *Neymanns/Buchstein* in Buchstein/Neymanns, S. 7, 17.

Die Durchführung von Internetwahlen auf dieser Ebene begegnet auch beim heutigen Stand der Technik nicht annähernd den gleichen Bedenken wie der Einsatz bei Parlamentswahlen. In Symbolik, demokratischer Brisanz und Beteiligungsumfeld bleiben die privaten Wahlen weit hinter den Parlamentswahlen zurück und erfordern somit auch andere, niedrigere Sicherheitsanforderungen. So können z.B. unternehmensinterne Personal- oder Betriebsratswahlen auf einem technischen Niveau sicher ausgestaltet werden, welches den Anforderungen an Parlamentswahlen keinesfalls gerecht werden würde.[439]

Ebenso liegt in der Durchführung der Sozialwahlen in Deutschland in Form von - die bislang praktizierte Briefwahl ergänzenden - Internetwahlen kein Verstoß gegen die obligatorische Geltung des Geheimhaltungsgrundsatzes. Der Präsenzwahl aus Geheimhaltungserwägungen den obligatorischen Vorrang einzuräumen, steht in diesem Fall außer Verhältnis zur Bedeutung des zu wählenden Gremiums und der geringen Wahrscheinlichkeit einer Wahlbeeinflussung.[440]

Da die privaten Wahlen aber gemeinhin als technisches und sozio-kulturelles Testfeld für die angestrebten internetbasierten Parlamentswahlen angesehen werden, kann es auch in diesem Bereich nicht erstrebenswert sein, lediglich ein Mindestsicherheitsniveau einzuhalten. Um den Selbstverwaltungs-Gremien und Unternehmen die Erprobung von Internetwahlen zu erleichtern, hat die PTB einen Katalog mit Sicherheitsanforderungen für Online-Wahlsysteme bei nicht-parlamentarischen Wahlen als Orientierungshilfe entworfen.[441] Hierauf aufbauend will die Gesellschaft für Informatik in Zusammenarbeit mit dem BSI und der PTB bis 2008 ein Common Criteria-Schutzprofil

[439] *Otten* in Buchstein/Neymanns, S. 71, 84.
[440] *Birkenmaier*, S. 121 f.
[441] *Hartmann/Meißner/Richter*, Anforderungskatalog; abrufbar unter: http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf, (Stand: 22.06.07); *Meißner/Hartmann/Richter* in Prosser/Krimmer, S. 101 ff.

entwerfen, das zu einem international vereinheitlichten Schutzniveau führen soll.[442]

[442] http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGGrimm/Projects/cc_profile, (Stand: 22.06.07); *Grimm/Krimmer/Meißner/Reinhard/Volkamer/Weinand/Helbach.*, Security Requirements, S. 15 ff.; *Grimm/Krimmer/Meißner/Reinhard/Volkamer/ Weinand/Helbach* in Krimmer, S. 203, 209.

Kapitel 5: Fazit und Ausblick

Angetrieben von vor allem ökonomischen und medienpolitischen Interessen sind vielfältige technische Lösungen entworfen worden, die die mühsame Handauszählung von Papierstimmzetteln entbehrlich und die Wahlauswertung in Sekundenschnelle per Knopfdruck Realität werden lassen können. Die elektronische Wahl ist technisch machbar. Dass aber nicht alles, was technisch realisierbar ist, auch umgesetzt werden soll oder gar darf, zeigt die Intensität der inzwischen auch öffentlichen Diskussion über elektronische Wahlsysteme. [443] In Deutschland steht das Wahlsystem an einem Scheideweg. Erste Einsätze von Wahlcomputern und Wahlstift haben auf politischer Ebene stattgefunden; die Internetwahl ist in privaten Gremien ausgetestet worden. Der Ruf nach Modernisierung auf der einen Seite begegnet einem lautstarken Veto der Kritiker auf der anderen Seite.
Abschließend soll ein kurzes Fazit und ein Ausblick bezüglich der drei ausgewählten elektronischen Wahlsysteme gegeben werden.

A. Wahlcomputer

Einen nunmehr schweren Stand hat das System der Wahlgeräte, nachdem es anlässlich der Wahldesaster in Florida und dem Nedap-Hack in den Niederlanden einen schweren Imageverlust hinnehmen musste. Die öffentliche Sorge und Kritik geht z.T. so weit, dass nicht bloß eine Verbesserung der Technologie der Wahlgeräte gefordert wird, sondern gar die Abschaffung von § 35 BWG verlangt wird.[444] Andere bleiben in ihrer Kritik moderater und wollen noch nicht gänzlich von dieser elektronischen Technik Abstand nehmen. Einig sind sich die kritischen Experten dahingehend, dass sowohl auf rechtlicher als auch auf technisch-organisatorischer Ebene starke Veränderungen am System vorzunehmen sind, bevor eine flächendeckende Einführung von politischen Wahlen an Wahlcomputern überhaupt diskutabel ist. Den großen Risiken der Manipulationen durch Außentäter muss eine

[443] *Birkenmaier*, S. 120 ff.; *Karpen*, S. 53 ff.; *Neymanns* in Buchstein/Neymanns, S. 34 ff.
[444] Abrufbar unter: http://itc.napier.ac.uk/e-Petition/bundestag/view_petition.asp?PetitionID=294 (Stand: 06.03.07).

konsequente Sicherheitsumgebung entgegengestellt werden, zu der die lückenlos sichere Aufbewahrung der Geräte vor und während der Wahl ebenso gehört wie eine ernsthafte Absicherung des Geräteinneren vor unerlaubten Zugriffen von außen. Als zwingend erforderliche Maßnahme, um dem wesentlichen Defizit des Wahlcomputers zu begegnen, der mangelnden Transparenz und Nachvollziehbarkeit der Systemtechnologie und der Ordnungsmäßigkeit der Stimmauswertung, wird die Ausstattung mit einem Papieraudit vorgebracht.[445] Andere fordern auch die Offenlegung des Quellcodes, um die Systemoperabilität und damit die Kontrolle einem breiteren Kreis als lediglich den Herstellern zugänglich zu machen.[446] Schließlich wäre eine Zertifizierung der Software durch das BSI mit regelmäßiger Überprüfung sehr wünschenswert, ähnlich wie sie für das „Digitale Wahlstift"-System eingeleitet wurde.

Doch trotz allem noch vorhandenen technischen und organisatorischen Verbesserungspotential erscheint es dennoch bedenklich, in der Stimmabgabe an stationären Wahlcomputern das Wahlsystem der Zukunft zu sehen. Die Bedrohungsszenarien sind mannigfaltig und selbst wenn eine technische Lösung dieser Sicherheitslücken gefunden werden sollten, so würde dies zu einer noch komplexeren Systemstruktur führen, die dem Transparenz- und Nachvollziehbarkeitsgebot immer weniger gerecht werden könnte. Zudem bleibt es sehr zweifelhaft, ob das System einen der im Vergleich zur Papierzettelwahl erhöhten Manipulationsattraktivität adäquaten Sicherheitsstandard je erreichen kann, um wenigstens das bestehende Sicherheitsniveau beizubehalten. Die Gegenüberstellung von technischem, organisatorischem und finanziellem Aufwand mit dem Nutzen, den eine Stimmabgabe per Wahlcomputer mit sich bringt, zeigt damit eine große Unverhältnismäßigkeit auf, die eine Umstellung von der herkömmlichen Wahl auf die Wahl an Wahlcomputern wie den Nedap-Geräten nicht erstrebenswert erscheinen lässt.

---

[445] *Sietmann*, c't Hintergrund vom 21.02.07, abrufbar unter: http://www.heise.de/ct/hintergrund/meldung/85615, (Stand: 06.03.07); *STS*, Recommendations, S. 13 f.

[446] *Karpen*, S. 36.

Für den Einsatz bei privaten Wahlen würde das erreichbare Sicherheitsniveau des Wahlgeräte-Systems zwar mitunter ausreichen, der dortigen Verwendung steht aber der hohe finanzielle Aufwand, insbesondere im Vergleich zur kostengünstigeren Alternative der Internetwahl, entgegen.

Noch bevor das Wahlgeräte-System den Durchbruch in Deutschland schaffen konnte, scheint es aus sicherheitstechnischen und verfassungsrechtlichen Unzulänglichkeiten bereits als Wahlsystem der Zukunft ausgeschieden zu sein.

B. Wahlstift

Leider hält auch das so augenscheinlich hoffnungsvolle „Digitale Wahlstift“-System nicht, was es zu versprechen scheint, nämlich die Vorteile von elektronischer und herkömmlicher Wahl miteinander zu vereinen.

Zwar haben die Verantwortlichen bezüglich der technischen Ausgestaltung und rechtlichen Absicherung des Systems einen zukunftsträchtigen Weg eingeschlagen, indem sie zusammen mit dem BSI ein Common Criteria Schutzprofil entwerfen. Dies ist im Hinblick auf eine Erhöhung der Sicherheitsanforderungen zu befürworten und dient auch einer tieferen Vertrauensschaffung bei den Wählern. Die Systemausgestaltung des „Digitalen Wahlstifts“ an sich bietet die Möglichkeit die physische Manipulierbarkeit auf ein Minimum zu beschränken und vereinfacht damit die Einhaltung des Geheimheitsgrundsatzes.

Dennoch kann auch der „Digitale Wahlstift“ das größte Problem der elektronischen Wahlsysteme nicht aus der Welt schaffen: Durch die Parallelität von digitaler Stimme und papiernem Wahlzettel wird zwar eine höhere Belegfunktion als z.B. beim Wahlcomputer erreicht. Weil aber im Ernstfall der vermuteten Wahlfälschung und der daraus resultierenden Nachzählung der Stimmen eine Entscheidung zu Gunsten einer der beiden Stimmaufzeichnungsmethoden fallen muss, wird entweder der erstrebte Kosten- und Organisationsvorteil (bei Priorisierung der Papierwahlzettel) leer laufen oder die Einhaltung des Öffentlichkeitsprinzips (bei Priorisierung der digitalen Stimmen)

geopfert werden. Die Tendenz Hamburgs, als bislang einzig ernsthaftem Aspiranten auf Einsatz des „Digitalen Wahlstift"-Systems, die elektronischen Stimmdatensätze als verbindliches Ergebnis anzuerkennen, nährt die Befürchtung, dass hier ökonomische Interessen über verfassungsrechtliche Prinzipien gestellt werden.
Auch das Digitale Wahlstift System sollte aus diesen Erwägungen heraus auf der Ebene parlamentarischer Wahlen auch in Zukunft nicht zum Einsatz kommen.

C. „Remote Internet Voting"

Unter momentaner Gesetzeslage völlig chancenlos stellt sich ein Einsatz des „Remote Internet Voting"-Systems bei politischen Wahlen dar.
Die subjektive Bequemlichkeit, die durch die Stimmabgabe vom heimischen PC gewonnen würde, kann bei den bestehenden enormen Sicherheitsrisiken mit nichts gerechtfertigt werden. Von der Verfassung ausgeschlossen ist nicht nur ein internetbasiertes Wahlsystem ausschließlich aus dem individuellen Bereich heraus, welches eine digitale Spaltung der Gesellschaft und damit einen Verstoß vor allem gegen den Grundsatz der Allgemeinheit der Wahl konstituieren würde. Auch ein ergänzender Einsatz von Internetwahlen zu Präsenz-/Briefwahl oder Wahlgerätewahl begegnet zu vielen verfassungsrechtlichen Bedenken. Selbst wenn eine Internetwahlverordnung mit umfassenden technischen Sicherheitsanforderungen als Pendant zur Wahlgeräteverordnung geschaffen und erlassen würde,[447] so zeichnet sich nicht ab, dass technische Lösungen gefunden werden, die die Erfolgswahrscheinlichkeit internetbedingter Angriffe so weit minimieren könnten, dass ein ausreichendes Sicherheitsniveau erreicht und die Wahlrechtsgrundsätze des Art. 38 I 1 GG eingehalten werden könnten. Die Offenheit des Internets in Verbindung mit den nicht kontrollierbaren heimischen PCs addiert sich zu einem extrem manipulationsanfälligen Konstrukt, welches die hohen Anforderungen, die an ein Stimmabgabesystem bei politischen Wahlen gestellt werden muss, nicht zu erfüllen vermag.

[447] *Bremke*, LKV 2004, S. 102, 108.

Die gleichen Sicherheitsrisiken bestehen in abgeschwächter Form auch dann, wenn ein „Kiosk"- oder „Polling Place Internet Voting"-System etabliert wird. Hier erscheint zudem zweifelhaft, dass die Kosten für die Ausstattung aller Wahllokale, Wartung und Schulungen noch im Verhältnis zum Gewinn in Form von Flexibilität und Schnelligkeit des Wahlverlaufs stehen.[448]

Sinnvolle und gewinnbringende Einsatzmöglichkeiten für Internetwahlen bestehen hingegen in weniger sicherheitssensiblen Bereichen.[449] Bei Wahlen von Selbstverwaltungsgremien, Vereinen, Personal- und Betriebsräten oder Aktionärsversammlungen gelten die Wahlrechtsgrundsätze nicht in der gleichen Schärfe wie bei parlamentarischen Wahlen. Den entsprechenden Sicherheitsanforderungen können die bestehenden technischen Wahlprotokolle deswegen mitunter gerecht werden, auch aufgrund des wesentlich überschaubareren Wählerkreises sowie einer geringeren Bedrohungswahrscheinlichkeit. Das Interesse an einer Rationalisierung und Vereinfachung des Stimmabgabeverfahrens steht bei privaten Wahlen mithin den Risiken einer Manipulation in einem angemessenen Verhältnis gegenüber.

Die Internetwahlen im privaten Bereich allerdings als Pilotprojekte für einen späteren Einsatz auf politischer Ebene anzusehen, ist meines Erachtens eine Verkennung der Lage. Konzeptionell unterscheiden sich diese Verwendungsbereiche zu sehr, als dass sich technische Lösungen, die für den Einsatz bei kleinen Wählergruppen ausreichen, auf eine bundesweite Anwendung bei Parlamentswahlen übertragen ließen, ohne die verfassungsrechtlichen Wahlgrundsätze zur Disposition zu stellen. Die Zukunft von Internetwahlen kann folglich nur im Bereich nicht-parlamentarischer Wahlen liegen.

D. Schlussbemerkung

Per Knopfdruck von jedem beliebigen Ort die Politik von Morgen zu bestimmen – es klingt verlockend, doch erstrebenswert ist die Einführung der elektronischen Wahl zum jetzigen Zeitpunkt nicht.

[448] *Will*, CR 2003, S. 126, 133.
[449] *Will*, CR 2003, S. 126, 133.

Keine der bislang in Deutschland angedachten und getesteten elektronischen Wahlkonzepte kann das Sicherheitsniveau halten, welches die Wahl mit Stift und papiernem Wahlzettel bislang gewährleistet. Auch die herkömmliche Wahl ist nicht immun gegenüber Wahlmanipulationen, doch stehen Aufwand und Manipulationserfolg in solch einem schlechten Verhältnis zueinander, dass eine Wahlfälschung in hohem Grad unattraktiv ist. Dieses Gleichgewicht würde durch eine Technisierung des Wahlsystems empfindlich gestört werden. Die elektronischen Wahlsysteme mögen zwar zunächst einmal durch ihre Komplexität eventuelle Manipulationsversuche erschweren. Entscheidend ist aber, dass die Systemsicherheit nicht absolut ist und aufgrund der komplexen Technologie jeder Angriff zu einer viel umfassenderen und zudem nur schwer oder gar nicht aufdeckbaren Wahlfälschung führen kann.

Der Verlust der Transparenz des Wahlverlaufs und damit einhergehend auch der Kontrollmöglichkeit für die breite Öffentlichkeit unterläuft zudem wesentliche Grundprinzipien des demokratischen Staates und kann nicht gebilligt werden.

Sollen die verfassungsrechtlichen Grundsätze nicht geopfert und das Vertrauen der Bürger in eine demokratisch-legitimierte Regierung nicht herausgefordert werden, so wird die Stimmabgabe auch in Zukunft mit Stift und Papier in der Wahlurne stattfinden müssen.