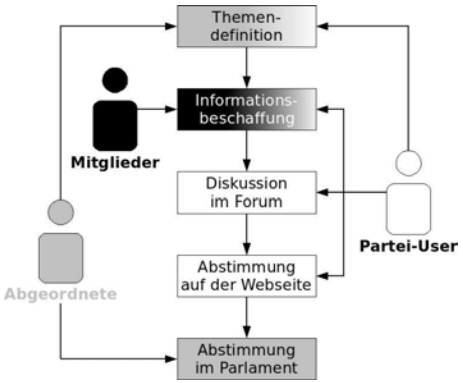
Zur Homepage der Publikation

Politische Beteiligung durch eProzesse

Stand und Perspektiven internetbasierter Informatikanwendungen in einer elektronischen Demokratie



Ingo Ibelings (Hrsg.)

BIS-Verlag
Bibliotheks- und Informationssystem der Universität Oldenburg
2008

Verlag: Bibliotheks- und Informationssystem
der Carl von Ossietzky Universität Oldenburg
(BIS) – Verlag
Postfach 2541, 26015 Oldenburg

Tel.: 0551/798 2261, Telefax: 0441/798-4040
E-Mail: verlag@bis.uni-oldenburg.de

ISBN 978-3-8142-2095-6

Vorwort

Der vorliegende Seminarband entstand im Anschluss an das Seminar „eDemokratie - Informatikanwendungen in der Politik“, das im Wintersemester 2005/06 an der Carl von Ossietzky Universität Oldenburg im Department für Informatik, Abteilung Wirtschaftsinformatik, von mir angeboten wurde. Im Rahmen des Seminars sollte insbesondere die technische Realisierbarkeit internetbasierter Informatikanwendungen in Politik und Wirtschaft untersucht werden. Des Weiteren sollte geprüft werden, inwieweit die an politischen Prozessen beteiligten Akteure einen Zugang zu den unterschiedlichen Systemen erhalten können und welche Sicherheitsaspekte zu berücksichtigen sind. Das Ergebnis ist eine breite Diskussion von den Ansätzen einer elektronischen und selbstorganisierenden Gesetzesfolgenabschätzung, über Bürgerrechte im Internet, wie sich elektronisch demokratische Parteien organisieren und welche Voraussetzungen zu erfüllen sind, um elektronische Wahlen durchzuführen.

Während der Seminararbeit wurde allerdings deutlich, dass die technischen Einsatzmöglichkeiten eine große Bedeutung innerhalb der elektronischen Demokratie haben, jedoch politik- und gesellschaftswissenschaftliche Einflussgrößen ebenso große Beachtung für politische eProzesse finden müssen. Gemeint ist hier die Fähigkeit und Bereitschaft aller Akteure, „sich in verschiedenen sozialen Gemeinschaften zu integrieren und demokratische Prozesse mitzugestalten.“ Dabei soll jeder Mensch in der Lage sein, „eine eigene gesellschaftliche Identität herauszubilden und zu vertreten. Er benötigt Kenntnisse über politische und gesellschaftliche Systeme und ihre Funktionsweisen“. Nachzulesen sind die zitierten Kernaussagen in verschiedenen Politik-Lehrplänen, die um folgenden Zusatz erweitert werden sollten: „sowie Zugang zu den vielfältigen Informatik-Anwendungen, die die politischen und gesellschaftlichen Systeme unterstützen, und Kenntnisse über deren Einsatz.“ Die politische Handlungs- und Gestaltungskompetenz innerhalb der politischen Bildung definiert sich nicht ohne Grund nur über die Inhalte und Formen, sondern auch auch über die Prozesse (mehrdimensionales Politikverständnis), die heute vielfach auch über elektronischem Wege ablaufen.

Die Ergebnisse dieser Seminararbeit sollen zu weiteren Diskussionen anregen. Bereits in vorangegangenen Seminaren wurde hierfür der Grundstein gelegt und ein Forum eingerichtet, um die zukünftigen Entwicklungen auf diesem Gebiet weiter zu beobachten und inhaltlich zu diskutieren. Sie finden das Forum unter der URL `http://www.informatik-politik.de`. Auch freue ich mich über Zuschriften an `forum@informatik-politik.de`. Ich lade Sie daher herzlich ein, mein Vorhaben mit einem aktiven Beitrag (Vortragsfolien, Referat, URL, ...) zu unterstützen.

Hiermit bedanke ich mich bei allen Seminarteilnehmern für die erfolgreiche Durchführung unseres Seminars „eDemokratie - Informatikanwendungen in der Politik.“ Auch wenn die Bearbeitung dieses Seminarbandes von allen Seminarteilnehmern nachhaltig unterstützt wurde, gebührt jedoch besonderer Dank Anke Lederer und Sönke Brummerloh, die als Editoren im Team die redaktionelle Fertigstellung koordinierten. Für die Inhalte sind die Autoren verantwortlich, die Verantwortung für evtl. noch vorhandene formale Fehler verbleibt jedoch beim Herausgeber.

Oldenburg, März 2008

Ingo Ibelings

Herausgeber

Dipl.-Hdl. Dipl.-Kfm. (FH) **Ingo Ibelings** ist Studienrat am Schulzentrum für den Sekundarbereich II an der Bördestraße in Bremen. Während des Seminars war er Lehrbeauftragter in der Abteilung Wirtschaftsinformatik an der Universität Oldenburg.

Redaktion

Dipl.-Inform. **Anke Lederer** ist Mitarbeiterin bei der BTC Business Technology Consulting AG in Oldenburg. Während des Seminars war sie Studentin der Informatik an der Universität Oldenburg.

Dipl.-Inform. **Sönke Brummerloh** ist wissenschaftlicher Mitarbeiter am Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und -Systeme (OFFIS). Während des Seminars war er Student der Informatik an der Universität Oldenburg.

Inhaltsverzeichnis

1 Ansätze für eine elektronische und selbstorganisierende Gesetzesfolgenabschätzung

Ansätze für eine elektronische und selbstorganisierende Gesetzesfolgenabschätzung

Edzard Weber

12. April 2006

1.1 Einleitung

Systematische Verfahren zur Unterstützung der Ausarbeitung von Gesetzestexten wurden bereits in den 70er Jahren diskutiert. In die praktische Politik haben sie damals keinen nachhaltigen Einzug gefunden. Indessen haben sich jedoch z. B. durch die entstandene Gesetzesdichte die Forderung nach mehr Transparenz und Mitbestimmung und durch die Europäisierung die Rahmenbedingung für die Gesetzgebung verschärft. Somit stieg auch die Notwendigkeit geeigneter Verfahren zur Beurteilung von Gesetzen an.

In den letzen Jahren konnte sich die Gesetzesfolgenabschätzung (GFA) und dabei insbesondere der Ansatz nach Böhret/Konzendorf als systematisches Verfahren zur Ausarbeitung von Gesetzestexten durchsetzen [BK00, BK01]. Ein allgemeines Ziel eines zentralen Verfahrens ist es, die bereits vorhandenen aber getrennt eingesetzten Mechanismen der Folgenabschätzung zusammenzufassen, zu verstärken, verschlanken und zu ersetzen [Kom02, S. 3]. Die Bundes-

ministerien und viele Landesministerien greifen nun auf die GFA als obligatorische Maßnahme zurück.

Die Propagierung dieses Ansatzes geschah zunächst im Rahmen der Verwaltungsmodernisierung durch die Bundesregierung [Bun03]. In mehreren wissenschaftlich betreuten Anwendungsfällen wurde die GFA auf ihre Eignung hin untersucht.

Weitgehend unberücksichtigt bei der Diskussion um den Nutzen der GFA sind die Anschlussmöglichkeiten einer breit angelegten und GFA-basierten Bürgerpartizipation im Gesetzgebungsprozess. Dieser Beitrag zeigt die eben dafür notwendigen Ansatzpunkte auf, um die GFA als eine elektronische und selbstorganisierende Form der Volksgesetzgebung einsetzen zu können.

In der vorliegenden Arbeit wird die GFA begrifflich und inhaltlich vorgestellt und bezüglich ihrer Institutionalisierung, ihres Einsatzes und Erweiterungsmöglichkeiten untersucht.

1.2 Grundlagen zur Gesetzesfolgenabschätzung

Zunächst wird der Begriff der Gesetzesfolgenabschätzung erläutert (vgl. [GM97], S. 12ff), bevor auf die mit der GFA verfolgte Absicht und auf die gegenwärtige Relevanz bzw. Institutionalisierung des Verfahrens eingegangen wird.

1.2.1 Begriffsbestimmung

Folgen und Wirkungen beschreiben jeweils einen Kausalitätszusammenhang, der einen Sachverhalt ordnet bzw. aufreiht. Während Wirkungen Zusammenhänge zielorientiert betrachten, ist der Begriff Folgen umfassender und schließt

auch ungerichtete Zusammenhänge von Handlungen oder das Ausbleiben von Handlungen ein.

Folgen können direkt oder indirekt sein. Sie sind monokausal oder multikausal. Weil die Ursachen zudem noch voneinander abhängig oder unabhängig sein können, können die Situationen, die zu einer bestimmten Folge führen, beliebig komplex sein. Weitere Kriterien von Folgen sind:

- die Absicht (beabsichtigt oder unbeabsichtigt),
- die Bewertung (positiv oder negativ),
- die Reversibilität (reversibel, partiell reversibel oder nicht reversibel),
- die Beherrschbarkeit (beherrschbar oder unbeherrschbar),
- das Ausmaß (kaum wahrnehmbar, umfangreich, extrem),
- das zeitliche Eintreten (sofort, mittelfristig, schleichend) und
- der Adressat (der Handelnde, andere Personen, (Sub-)Systeme, die Umwelt).

Der Begriff Gesetz ist ebenfalls im weitesten Sinne zu verstehen. Es sollen damit auch Rechtsverordnungen oder Verwaltungsvorschriften erfasst werden können und nicht nur die Gesetze als Ergebnis parlamentarischer Arbeit.

Somit stellen Gesetzesfolgen diejenigen Folgen dar, die sich auf Erlass, Änderung oder Unterlassung eines bestimmten Gesetzes zurückführen lassen. Durch geeignete Methoden (Analysen, Tests, Simulationen,...) sollen jene Eigenschaften möglicher Folgen bestimmt werden, um sie als fassbare und vergleichbare Größen im Gesetzgebungsprozess berücksichtigen zu können. Die Gesetzesfolgenabschätzung hat ein Vorgehensmodell anzubieten, nach dem die Eignung einer Methode festgestellt werden kann, die Ergebnisse korrekt gewichtet werden können, die Auswahl und das Zusammenwirken fachkompetenter Personen verbessert werden kann und auch der Fortbestand der GFA gerechtfertigt werden kann.

Die Gesetzesfolgenabschätzung wird in [GM97, S. 19] wie folgt definiert:

> Mit einer Gesetzesfolgenabschätzung werden die Notwendigkeit einer (Neu-)Regelung, die Wirksamkeit einer Regelung/ eines Regelungspaketes und die Folgen, die über die Wirksamkeit i.e.S. hinaus gehen, mittels eines interdisziplinären Forschungsansatzes multidimensional erfasst und bewertet.

Böhret und Konzendorf schreiben [BK01, S. 1,2]:

> Gesetzesfolgenabschätzungen sind Verfahren zur Erkundung und vergleichenden Bewertung von Folgen beabsichtigter bzw. in Kraft getretener Rechtsvorschriften. Sie dienen der expertengestützten Entwicklung von Regelungsalternativen und deren vergleichender Folgenbeurteilung, der Überprüfung nach bestimmten Kriterien wie Kosten/Nutzen, Verständlichkeit, der laufenden oder zeitpunktbezogenen Evaluierung der tatsächlich eingetretenen Wirkung geltender Rechtsvorschriften.

Die GFA stellt somit eine Obermenge zur wirkungsorientierten Gesetzgebung und der Gesetzesevaluation dar, welche sich auf die Beurteilung und Steigerung der Effektivität und Effizienz von Regelungsmaßnahmen bezüglich beabsichtigter Auswirkungen beschränkt. Leider wird dieser Differenzierung nicht ausreichend Rechnung getragen, so dass Gesetzesfolgenabschätzung und Gesetzesevaluation häufig synonym verwendet werden.

1.2.2 Intention der GFA

Die Menge aller Gesetze eines Staates beeinflusst nicht nur die allgemeine Lebensqualität sondern stellt insbesondere für die Wirtschaft einen entscheidenden Standortfaktor dar. Bedrängt von der hohen Regelungsdichte und Überregulierung wurden insbesondere von wirtschaftlichen Interessensverbänden Forderungen nach einer neuen Qualität in der Gesetzgebung laut, um den inhaltlichen Verlauf bei der Entstehung eines Gesetzes transparenter zu gestalten

und Möglichkeiten der sachlichen Einflussnahme zu institutionalisieren (vgl. [HMO+01, Bun05]).

Auch die Reduzierung der Gesetzesmenge ist ein Anliegen. In diesem Zusammenhang steht auch die Frage, ob die Gültigkeit eines Gesetzes zeitlich befristet sein soll. Insbesondere dafür ist es wichtig, eine klare Entscheidung darüber fällen zu können, ob ein Gesetz seine Wirkung erzielt hat. Eine ausschließlich rückwirkende Betrachtung hat es jedoch versäumt, bereits im Vorfeld Ursachen für Fehlregulierungen auszuschließen, wenn es darum geht, den Regelungsbedarf selbst zu bestimmen und eine konkrete Regelungsmaßnahme zu entwickeln.

Der Gesetzgebungsprozess soll in allen Stadien mit einer höheren Transparenz für den Bürger versehen sein. Informationen zum allgemeinen Vorgehen, zu Gesetzesvorhaben und Ergebnissen sollen leicht und öffentlich zugänglich sein (vgl. [Bun00b, S. 6-7],[Deu05, S. 14]). Die Gesetzgebung soll als bürgerorientierter, demokratischer Prozess den erlassenen Gesetzen höhere Akzeptanz bescheren. Es sind nicht primär die politischen Akteure, die mittels ihrer zugesprochenen Kompetenzen einem Gesetz die notwendige Legitimität verleihen. Sie liegt in der Qualität der verwendeten Verfahren im Entstehungsprozess begründet [Ism01, S. 220]. So ist die öffentliche Auseinandersetzung und Entscheidungssuche in einem parlamentarischen Verfahren größer als bei der Verabschiedung von Verordnungen als Ergebnis administrativen Handelns. Auf diese Weise legitimiert sich die stärkere Verbindlichkeit von Gesetzen. Die Folgenabschätzung soll als Kommunikationsinstrument dazu beitragen, dass interessierte und betroffene Bürger zusätzliche Informationen in den Gesetzgebungsprozess einbringen können (vgl. [Kom02, S. 3]).

Notwendig ist aber, dass jene Kommunikationsprozesse nicht nur mit ausreichender Qualität ablaufen können, sondern auch dass das erreichte Maß an Öffentlichkeit, der Zeit- und Kostenaufwand und die Qualität und die Reichweite der Gesetze in einem angemessenen Verhältnis zueinander stehen (vgl. [Deu05, S. 4]). Es gilt der Grundsatz der proportionalen Analyse, wonach die Gründlichkeit, der Umfang und somit auch die Höhe der für eine Gesetzesfol-

genabschätzung verwendeten Mittel im richtigen Verhältnis zur Bedeutung des Vorschlags und seiner wahrscheinlichen Folgen stehen [Kom02, S. 9].

1.2.3 Institutionalisierung

Institutionalisierung ist die Zuordnung von Legitimität an sozio-kulturelle Einrichtungen und Regelwerke. Die entstehenden Institutionen bilden ein kollektives Gedächtnis und die Grundlagen für das allgemeine Handeln und Denken [BK01, S. 317]. Damit die GFA vollständige, verbindliche und gewissenhafte Anwendung finden kann, muss auch sie eine bestimmte Legitimität erlangen. Böhret und Konzendorf beschreiben drei Dimensionen, über die eine Institutionalisierung der GFA stattfinden kann/muss:

Rechtliche Institutionalisierung: Festschreibung der GFA-Durchführung in Verfassung, Gesetz oder (Ver-)Ordnung, wodurch jeweils unterschiedliche Ausmaße an Verbindlichkeit und Anwendungsbreite erzielt werden.

Organisatorische Institutionalisierung: Errichtung von Stellen zur Leitung und Durchführung von GFA-Prozessen. (Zu den Funktionen dieser Stellen zählen insbesondere Koordination, Methodenpflege, Beratung, Information und Fortbildung.)

Personale Institutionalisierung: Identifikation und Einbeziehung GFA-relevanter Akteure (Methodenexperten, Fachexperten, Normadressaten, politisch Verantwortliche) und deren GFA-spezifische bzw. projektbezogene Information und Fortbildung.

Das Forschungsinstitut für öffentliche Verwaltung in Speyer hat einige Prozesse der GFA zu konkreten gesetzlichen Anliegen wissenschaftlich begleitet und dokumentiert (z. B. [GM97, BK98, Wor02, Bun02]). Ziel war es - neben der Qualitätssteigerung des gesetzgebenden Outputs - das Verfahren zur GFA hinsichtlich seiner Praktikabilität und Vollständigkeit zu überprüfen, um verfahrenstechnische Verbesserungsmöglichkeiten zu identifizieren. Weiterführende Projekte sichern die anwendungsorientierte Fortentwicklung der GFA [Deu06].

Einsatz findet die GFA nun auf Bundesebene durch Verankerung in der Gemeinsamen Geschäftsordnung der Bundesministerien [Bun00a, §44]. Gleiches gilt für die Geschäftsordnungen einiger Landesregierungen (z. B. Niedersachsen [Nie04, §38] oder Rheinland-Pfalz als Vorreiter dieser „experimentellen“ Gesetzgebung) [Brä04].

1.3 Die Module der GFA

Die Gesetzesfolgenabschätzung unterteilt sich in drei Module, die jeweils den speziellen Bedürfnissen und Gegebenheiten der Phasen einer Gesetzestexterarbeitung angepasst sind. Es liegt im Ermessen der Entscheidungsträger, welche Phasen (alle, einzelne, keine) durch eine GFA unterstützt werden soll. Die folgende Darstellung der einzelnen Module richtet sich nach dem Verfahren *Böhret/Konzendorf* [BK00, BK01].

1.3.1 Prospektive Gesetzesfolgenabschätzung

Die prospektive Gesetzesfolgenabschätzung (pGFA) kann angestoßen werden, wenn ein Regelungsbedarf identifiziert worden ist. Ihre Aufgabe liegt darin, die Notwendigkeit einer Regelung aufzuzeigen. Sie unterstützt die Entwicklung von Regelungsalternativen und unterzieht diese einer Folgenabschätzung. Die Ergebnisse werden vergleichend analysiert, so dass eine als optimal ermittelte Regelungsalternative als Empfehlung an die politisch administrative Ebene weitergereicht werden kann. Die pGFA besteht aus drei Phasen: Konzeption, Durchführung und Auswertung (vgl. Abbildung 1.1).

Konzeptionsphase

Voraussetzung ist, dass die verantwortliche, politisch administrative Ebene die Durchführung einer pGFA angeordnet hat. Danach wird zunächst das Regelungsfeld analysiert. Dies kann durch Ziel-, Problem- oder Systemanalysen geschehen, je nachdem ob eine bestimmte politische Zielvorgabe, ein konkretes Problem in der Praxis oder die Gesamtheit des Regelungsfeldes im Mittelpunkt der Betrachtung stehen soll. Im nächsten Schritt werden verschiedene Regelungsalternativen entworfen. Hier sollen verschiedene Grundideen einer möglichen Umsetzung Berücksichtigung finden (z. B. Marktsteuerung, Selbststeuerung) wie auch die Null-Alternative. Weiterhin müssen unterschiedliche Zukunftsszenarien entwickelt werden, auf die später die Regelungsalternativen angesetzt werden. Als letzter Vorbereitungsschritt gilt die Auswahl und Aufbereitung von Verfahren und Instrumenten, mit dessen Hilfe eine Folgenabschätzung für alle Permutationen der Alternativen-Szenarien-Kombination. Es sind idealer Weise mehrere Instrumente zu bestimmen, so dass sich Ergebnisverzerrungen erkennen und vermeiden lassen. Die Auswahl reicht über qualitative Instrumente/ Verfahren (Experten-Workshops, Nutzwertanalyse, Science Court-Verfahren, Effektivitäts-Kosten-Abschätzung) bis hin zu quantitativen Instrumenten (Delphi-Befragung, standardisierte Befragung) und systematisierenden Instrumenten (Computersimulation, Folgenorientierte Systemanalyse) [BK01, S. 19–21].

Durchführungsphase

Die zuvor erarbeiteten Analysen, Regelungsalternativen und Szenarien werden nun durch die zuvor ausgewählten Instrumente und Verfahren auf Vollständigkeit, Richtigkeit und Schlüssigkeit untersucht. Gegebenenfalls sind die Regelungsalternativen zu modifizieren. Ein Workshop als strukturierte Experten- und Normadressatendiskussion wird dabei als obligatorisch abverlangt. Weitere Verfahren sind optional. Die Zusammensetzung der Diskussionsrunde ist dabei von entscheidender Bedeutung. Die Normadressaten sollen vom Regelungsfeld bzw. den Regelungsalternativen oder Szenarien direkt be-

troffen sein. Die Experten sollen unabhängig sein und unterschiedlichen Denk- und Fachrichtungen angehören. Die Folgen einer jeden Regelungsalternative in Abhängigkeit eines zugrunde gelegten Zukunftsszenariums sind herzuleiten und zu erörtern. Wichtig ist eine begleitende Dokumentation aller Anmerkungen und Einschätzungen.

Auswertungsphase

In dieser Phase findet die Dokumentation des bisherigen Vorgehens statt. Gleichfalls werden die Dokumentationen und Ergebnisse der eingesetzten Verfahren und Instrumente aufbereitet und ausgewertet. Als Ergebnis dieses Schrittes soll eine begründete und dokumentierte Empfehlung für eine Regelungsalternative vorliegen. Diese wird den politisch Verantwortlichen vorgelegt, die über eine rechtsförmige Umsetzung zu entscheiden haben.

1.3.2 Begleitende Gesetzesfolgenabschätzung

Die begleitende Gesetzesfolgenabschätzung (bGFA) kann angestoßen werden, wenn ein Regelungsentwurf vorliegt. Ihre Aufgabe liegt darin, diesen nach relevanten Prüfkriterien zu analysieren, zu testen und zu optimieren. Es soll festgestellt bzw. abgeschätzt werden, ob sich die Vorlagen bewähren dürften. Die bGFA besteht ebenfalls aus den drei Phasen: Konzeption, Durchführung und Auswertung (vgl. Abbildung 1.1).

Konzeptionsphase

Eine bGFA hat durch das jeweils verantwortliche Ressort angestoßen zu werden. Eventuell bestehen auch schon formelle Vorgaben, die eine Durchführung oder Erwägung einer bGFA verlangen.

Zunächst werden Prüfkriterien bestimmt, nach welchen der Regelungsentwurf untersucht werden soll. Hierzu zählen Zielerreichbarkeit, Praktikabilität, Verteilungswirkung, Wechselwirkungen, Verträglichkeit, Verstehbarkeit und Akzeptanz. Es ist unwahrscheinlich, dass ausreichend finanzielle, personelle und zeitliche Ressourcen zur Verfügung stehen, so dass lediglich einzelne Teile eines Regelungsentwurfes einer Bearbeitung unterzogen werden können. In Abhängigkeit der bestimmten Prüfkriterien und der ausgewählten Regelungsteilen sind geeignete Verfahren und Instrumente auszuwählen. Böhret und Konzendorf sprechen Empfehlungen dafür aus, welche Verfahren und Instrumente sich bezüglich welcher Prüfkriterien am besten eignen. Hierzu zählen Nutzwertanalyse, Praxistest, Planspiel, Kostenfolgenanalyse, Kosten-Nutzen-Analyse, Leistungsflussanalyse, Interdependenzanalyse, Schnittstellenanalyse, Verständlichkeitsprüfung, Konsistenzprüfung und Akzeptanzstudie [BK01, S. 93]. Die selektierten Verfahren sind im letzten Schritt der Konzeptionsphase vorzubereiten. Dies betrifft nicht nur die räumlichen, personellen und finanziellen Voraussetzungen, sondern auch den Ablauf vorzustrukturieren, die Mitwirkenden auszuwählen und zu instruieren und gegebenenfalls Fallbeispiele vorzubereiten.

Durchführungsphase

In dieser Phase finden die ausgewählten Verfahren und Instrumente ihre Anwendung. Erfolgskritisch ist ebenfalls wieder die Zusammensetzung der Beteiligten. Die Verfahren und Instrumente können beliebig und flexibel kombiniert werden. Kein Verfahren setzt auf ein anderes auf. Sehr wohl kann es aber Synergieeffekte geben.

Auswertungsphase

Die Auswertungsphase hat die Ergebnisse und den Verlauf systematisch zu erfassen und zu dokumentieren. Insbesondere sollen auch aufgetretene Probleme oder Erkenntnisse z. B. bezüglich der Verträglichkeit verschiedener Verfahren zueinander dokumentiert und analysiert werden, so dass zukünftige Gesetzes-

folgenabschätzungen von diesem Erfahrungswissen profitieren können. Als Ergebnis soll eine Empfehlung ausgesprochen werden, ob der betrachtete Regelungsentwurf bzw. Referentenentwurf verändert, ergänzt oder beibehalten werden soll. Die letztendliche Entscheidung einer Modifikation oder Verabschiedung verbleibt bei den verantwortlichen politischen Akteuren.

1.3.3 Retrospektive Gesetzesfolgenabschätzung

Die retrospektive Gesetzesfolgenabschätzung (rGFA) kann einige Zeit nach Inkrafttreten einer Rechtsvorschrift ihren Einsatz finden. Sie hat zu ermitteln, ob die Rechtsvorschrift ihr Ziel erreicht hat, ob weitere Nebenfolgen eingetreten sind und ob ein Nachbesserungsbedarf besteht. Auch die rGFA besteht aus den drei Phasen: Konzeption, Durchführung und Auswertung (vgl. Abbildung 1.1).

Konzeptionsphase

Ein Anstoß zur rGFA kann sowohl durch die politisch-administrative Ebene selbst als auch durch Druck bestimmter gesellschaftlicher Gruppen gegeben werden. Die Überprüfung einer Vorschrift kann auch die Vorschrift selbst durch eine interne Fristensetzung vorgeschrieben werden.

Zunächst sind Prüfkriterien zu bestimmen. Diese sind in der Regel Kostenentwicklung, Kosten-Nutzen-Effekte, Akzeptanz, Praktikabilität und Nebeneffekte. Auch hier kann man sich darauf beschränken, die Prüfkriterien nur auf die auffälligsten Regelungsbereiche und Folgen anzuwenden. Für diese findet keine absolute Bewertung statt, es sei denn, dass eine offensichtliche Fehlregulierung stattgefunden hat. Vielmehr sind Verfahren für Vergleiche zwischen der vorherigen mit der durch die Rechtsvorschrift bedingten aktuellen und zukünftigen Situation vorzubereiten. Die Prüfkriterien müssen dazu operationalisiert werden. Die Ziele, die durch eine Rechtsvorschrift erreicht werden sollten, müssen eindeutig und messbar sein. Hieraus lässt sich ableiten, welche Datenbasis nötig

ist, erhoben werden muss und mit welchen Verfahren diese ausgewertet werden soll.

Durchführungsphase

Die Durchführungsphase umfasst den Vorgang der Datenerhebung. Die Daten können durch Auswertung einschlägiger und bereits von anderen Stellen gesammelter und aufbereiteter Daten gewonnen werden, so dass der Aufwand gering gehalten werden kann. Ebenfalls können qualitative Daten durch Workshops mit Experten oder den Normadressaten durchgeführt werden. Möglich ist auch die Einrichtung eines eigenen Berichtswesens, so dass die für eine Evaluation relevanten quantitativen Daten in bestimmten Zeitabständen an die GFA-durchführende Stelle übermittelt werden. Als weitere Möglichkeit ist die Feldforschung als Anwendung der empirischen Sozialforschung gegeben.

Auswertungsphase

In Abhängigkeit von den gewählten Prüfkriterien und der Vergleichsart wird die analysierte Datenbasis bestimmten Bewertungsfragen unterzogen. Das Vorgehen sowie die Analyse und Bewertungsergebnisse sind zu dokumentieren. Abschließend soll eine Empfehlung über Beibehaltung, Neufassung oder Aufhebung der betrachteten Rechtsregelung erstellt werden. Diese wird ebenfalls an die politisch verantwortlichen Akteure weitergegeben.

1.4 Elektronische Gesetzesfolgenabschätzung (eGFA)

Obwohl die Gesetzesfolgenabschätzung als Werkzeug für den Gesetzgeber im Rahmen der Verwaltungsmodernisierung konzipiert ist, bietet sie auch Poten-

ziale für den Einsatz elektronisch demokratischer und direktdemokratischer Elemente.

1.4.1 Elektronische Demokratie

Wichtige Elemente der Demokratie sind die Prozesse der politischen Willensbildung. Sie stellen eine Deformation und Aggregation individueller und kollektiver Bedürfnisse, Interessen und Meinungen dar (vgl. [Pre89], Rz. 25). Wiederum vorausgesetzt sind Prozesse der Identifikation und Artikulation von gesellschaftlichen Konflikten, welche als Gegenstand der politischen Willensbildung aufgenommen werden können. Einem solchen Demokratieverständnis wird nicht ausreichend Rechnung getragen, wenn den Bürgern lediglich Informationen und isolierte Abstimmungen angeboten werden, wenn ausschließlich die Identifikation von Mehrheiten im Vordergrund steht oder wenn erzielte Übereinkünfte in Beteiligungsverfahren ohne jede Auswirkung bleiben und lediglich eine unverbindliche Zurkenntnisnahme durch die politisch-administrative Ebene darstellen. Auch Konzepte der elektronischen Demokratie haben dieser Anforderung zu genügen [Mem00].

Elektronische Demokratie „bezeichnet Formen der politischen Partizipation unter Einsatz der Informations- und Kommunikationstechnologien [Koo06]“. Primäres Ziel ist es, dem Bürger zusätzliche, demokratische Mitbestimmungs- und Gestaltungsmöglichkeiten im politischen Diskurs zu bieten.

Partizipation bedeutet, dass an Entscheidungen, die in den Kompetenzbereich einer bestimmten Stelle fallen, noch Stellen-externe Personen oder Organe beteiligt werden. Mögliche Beteiligungsformen sind Information, Anhörung, Beratung, Mitbestimmung oder ein Vetorecht. Von der Verantwortung kann sich der Stelleninhaber jedoch nicht (vollständig) lösen [KK92, S. 158]. Im Falle der Gesetzesfolgenabschätzung geht es darum, eine optimale Anzahl und Vielfältigkeit von Experten und Normadressaten bei der Erarbeitung einer Empfehlung für die Legislative partizipieren zu lassen. Die politische Verantwortung wird vom Gesetzgeber nicht an die GFA-Beteiligten abgegeben.

Partizipation kann verschiedene Intensitäten annehmen (vgl. [Lan83, 205-206], [MOT86, 15]):

Informierende Partizipation: Lediglich Informationen werden an Normadressaten ausgegeben.

Konsultative Partizipation: Es können Vorstellungen und Meinungen gegenüber den Verantwortlichen geäußert werden, die jedoch keine Verbindlichkeit besitzen.

Repräsentative Partizipation: Es kann an der Auswahl oder Modifikation vordefinierter Alternativen teilgenommen werden. Einzelne Repräsentanten der Normadressaten können eigene Gestaltungsvorschläge einbringen.

Konsentive Partizipation: Die Beteiligung am Gestaltungs- und Auswahlprozess ist aktiv.

Selbstorganisierende Partizipation: Der Gestaltungs- und Auswahlprozess von Alternativen bzw. Empfehlungen wird von den Partizipanten selbständig betrieben.

Eine gesteigerte Transparenz des Gesetzgebungsprozesses kann bereits durch eine informierende Partizipation erzielt werden, z. B. durch die zeitnah veröffentlichte und leicht zugängliche Dokumentation zur durchgeführten GFA. Qualitätssteigerungen verspricht man sich durch die inhaltliche Beteiligung von Normadressaten mit konkurrierenden Meinungen und Experten mit tiefer und breiter Sachkenntnis. Mindestvoraussetzung ist eine konsultative Partizipation. Eine Akzeptanzsteigerung der erzielten Ergebnisse (im Sinne einer vergrößerten Legitimationsbasis) ergibt sich durch die Gesamtheit einer verfahrensgemäß und verantwortungsvoll durchgeführten GFA (vgl. 1.2.2).

1.4.2 Ansätze zur eGFA

Gewissenhaft durchgeführte, demokratische Prozesse sind komplex. Die Qualität konventioneller Verfahren kann nicht immer in elektronischen Verfahren

erreicht werden. Ein realistisches Idealbild von einer elektronischen Demokratie darf dieser deshalb nicht die Möglichkeit berauben, bewährte konventionelle Verfahren zu integrieren [Mem00]. Elektronische Demokratie soll das bestehende System verbessern und nicht verdrängen. Analog muss es auch mit der eGFA gehandhabt werden. Es darf kein Anspruch erhoben werden, jeden funktionalen Aspekt der GFA elektronisch abzubilden. Dennoch lassen sich methoden-, phasen- und modulübergreifende Vorteile besser ausnutzen. Folgende Gestaltungsbereiche gilt es zu untersuchen:

Methodenspezifische Maßnahmen: Die computergestützte Simulation wird bereits explizit vorgeschlagen. Selbstverständlich lassen sich aber nahezu alle vorgeschlagenen Methoden (z. B. Expertenbefragung, Normadressatenbefragung, Diskussionsrunden) durch ein elektronisches Verfahren realisieren. Einen elektronischen Charakter erhält die GFA dadurch aber noch nicht, weil es sich hierbei lediglich um technischen Insellösungen handelt, die per se weder Transparenz noch GFA-Effizienz erwirken (punktuelle Maßnahmen).

Modulspezifische Maßnahmen: Einzelne elektronische Verfahren, die in den verschiedenen Phasen einer GFA zum Einsatz gekommen sind, können von einem zentralen Dienst koordiniert werden. Systeme für flexible und adaptive Workflowmodelle können die zeitliche und inhaltliche Synchronisation vornehmen (verkettende Maßnahme). Einen elektronischen Charakter erhält die GFA dadurch aber noch nicht. Der GFA-Verlauf wird zwar berechenbarer und somit transparenter, aber auch das stellt eine selbstverständliche Anforderung dar und ist somit kein effektiver Zusatznutzen.

GFA-spezifische Maßnahmen: Langfristiges Nebenziel der GFA ist es, eine „Liste des Sachverstandes“ anzulegen. Einmal identifizierte Fachexperten werden darin für zukünftige, fachspezifische GFA-Durchführungen vorgemerkt. Zu überlegen wäre die Bereitstellung einer Plattform, die einzelne GFA-Durchläufe überdauert und auf der Experten auf effiziente elektronische

Weise miteinander in Kontakt treten können (vernetzende Maßnahmen). Gleiches kann auch für die Menge der Normadressaten geschehen. Bürger, die im Rahmen einer vorherigen, konkreten GFA-Durchführung an einer Konsultation oder Befragung teilgenommen haben, können auch zu zukünftigen Verfahren eingeladen werden. Um große Mengen von Normadressaten für eine Vielzahl von GFA-Durchführungen gewinnen zu können, kann es nach Kostengesichtspunkten Sinn machen, eine zentrale, verfahrensunspezifische Registrierung von Bürgern zu tätigen. Diese können dann über ein elektronisches Portal gemäß ihrem Profil als Normadressat identifiziert, zur GFA-Durchführung eingeladen und befragt werden.

Allgemeine Maßnahmen: Die Schaffung von Transparenz und Vertrauen im Gesetzgebungsprozess erfordert es, dass sich nicht die Beteiligten oder die Betroffenen, sondern auch alle anderen Bürger zu allen Fragen des Wie, Wer, Wann, Warum, Womit usw. aufklären lassen können. Dies kann durch die Schaffung von Informationsräumen geschehen, in denen nicht nur die den betrachteten Gesetzestext betreffenden Dokumente leicht zugänglich veröffentlicht werden, sondern ebenfalls alle Parameter der GFA. Dies darf allerdings nicht als punktuelle Maßnahme der GFA-Phasendokumentation betrachtet werden, sondern bedarf es für die Informationsqualität und -aufbereitung einen einheitlichen Standard, so dass verschiedenen GFA-Durchführungen bezüglich unterschiedlicher Kriterien miteinander verglichen werden können. (Bspw. ist die Veröffentlichung von Gesetzesentwürfen durch das jeweilige Bundesministerium via Internet nur optional [Bun00b, §48(3)].) Eine weitere allgemeine Maßnahme ist die Schaffung einer Partizipationskultur, die sich um eine langfristige Bindung von aktiv gewordenen Bürgern bemüht.

1.4.3 Anschlussfähigkeit einer eGFA

Die GFA bietet ein geeignetes Testfeld für elektronisch demokratische Verfahren. Diese haben in der Regel eine Vielzahl von Konflikten zu lösen und Anforderungen zu genügen, um einen tatsächlichen Anschluss in Prozessen der

Willensbildung und Entscheidungsfindung zu erzielen. Nur schwer ist eine Verbindlichkeit der Ergebnisse zu garantieren, wobei diese den eigentlichen Anreiz für eine Beteiligung durch den Bürger darstellt. Vollständige Verbindlichkeit in einem demokratischen Entscheidungsprozess kann einem elektronischen Verfahren aber nur zugesprochen werden, wenn dieses ebenfalls den demokratischen Grundsätzen genügt. Insbesondere technische und infrastrukturelle Unzulänglichkeiten wie bspw. Systemsicherheit oder Systemzugang wirken sich negativ auf die Verfahrensmerkmale Allgemeinheit, Geheimhaltung oder Gleichbehandlung aus.

Die GFA bietet hier einen großen Freiraum. Das Verfahren nach Böhret/Konzendorf ist technikunabhängig beschrieben. Jegliche Existenz verwendbarer Informations- und Kommunikationstechnik hat keinen Einfluss auf eine ordnungsgemäße Durchführbarkeit einer GFA. Sie kann also auch in der Durchführungsphase elektronische Verfahren einsetzen und dabei verfassungsrechtliche bzw. demokratietheoretische Bedenken gegenüber diesen ausklammern. Die Qualität und der Umfang der verwendeten Systeme müssen nur im Innenverhältnis der GFA gerechtfertigt sein. Im Außenverhältnis, also in der Rechtfertigung gegenüber Verfassung und Gesetzen, verstecken sich diese elektronischen Verfahren ebenso wie alle anderen im Rahmen der GFA eingesetzten Analyse- und Erhebungsverfahren hinter der ordnungsgemäßen Anwendung der GFA.

Somit entspricht die Höhe der Ergebnisverbindlichkeit elektronischer Verfahren ebenfalls nur derjenigen der GFA. Es sind lediglich Empfehlungen für die politisch Verantwortlichen. Aber eben dadurch entsteht einerseits ein Beteiligungsanreiz für Systemnutzer, weil eine tatsächliche Einbindung in den Gesetzgebungsprozess besteht. Und andererseits können neue elektronische Verfahren risikominimal, aber unter Realbedingungen eingesetzt (bzw. getestet) werden, weil Ergebnisse, die wegen Verfahrensmängel unbrauchbar sind, im Rahmen der Auswertungsphase fallengelassen oder durch die politischen Verantwortlichen als Empfehlung ignoriert werden können. Die GFA dient stets nur als Hilfe zur Entscheidungsfindung und wird niemals einen Ersatz für politische Beurteilungen darstellen [Kom02, S. 3].

Der Einsatz elektronisch demokratischer Verfahren ist im Rahmen der GFA keine politische Entscheidung mehr. Sie liegt vielmehr in den Händen der für die GFA-Durchführung beauftragten Stelle.

1.5 Selbstorganisierende GFA

Die GFA versucht die Akzeptanz, die Transparenz und die Qualität des Gesetzgebungsprozesses und dessen Ergebnis zu steigern. Dies soll und wird durch verschiedene Formen der Partizipation erreicht werden. Interessante Gestaltungsoptionen ergeben sich aus der Idee einer selbstorganisierenden GFA als höchste Form der Normadressaten-Beteiligung.

1.5.1 Organisatorische Institutionalisierung

Die Gemeinsame Geschäftsordnung der Bundesministerien regelt die Anwendung der GFA [Bun00a, §44]. Das im jeweiligen Gesetzgebungsprozess federführende Ministerium ist demnach für eine Folgenabschätzung als Bestandteil der Gesetzesbegründung verantwortlich [Bun00a, §43(1)]. Dies umfasst mindestens die Initiierung eines GFA-Prozesses; die Durchführung selbst kann aber durch andere Stellen erfolgen. Böhret/Konzendorf nennen die verschiedenen Möglichkeiten einer organisatorischen Institutionalisierung [BK01, S. 320] (nach [FH83, Unk98]). Durchführende Akteure sind nach diesen Modellen ein spezielles Rechtspflegeministerium, ein GFA-Referat, ein Gesetzeskontrollbeauftragter, der Rechnungshof, ein Parlamentsausschuss, ein Ausschussbeauftragter, wissenschaftliche Institute oder GFA-Stiftungen.

Das Modell einer GFA-Stiftung sieht vor, dass diese über ein GFA-Institut verfügt, welches für die Durchführung von GFA-Prozessen herangezogen werden kann. Ein solches Institut ist kein Organ der Exekutiven oder der Legislativen. Eine Herausforderung stellt somit der ausreichende Informationsfluss zwischen dem jeweils politisch verantwortlichem Ressort und dem Institut dar. In der Pha-

se einer prospektiven GFA wird dieser Umstand noch durch das Diskretionsbedürfnis verschärft [BK01, S. 325]. Überlegungen über die Identifizierung eines Regelungsbedürfnisses möchten politisch Verantwortliche nur bedingt Ressortextern bzw. öffentlich anstellen. Unangenehme oder unbedeutende Themen erhalten dadurch leicht eine nicht gewünschte hohe Aufmerksamkeit.

1.5.2 GFA als nicht-staatliche Dienstleistung

Bei allen Optionen der organisatorischen Institutionalisierung - mit Ausnahme der GFA-Stiftung und den wissenschaftlichen Instituten - verbleiben sowohl die GFA-Initiierung (ein Teil der politischen Verantwortung) als auch die GFA-Durchführung (die inhaltliche Verantwortung) im Bereich legislativer oder exekutiver Organe. Die Stärke der Einflussnahme durch Fachexperten oder Normadressaten wird durch diese im Zuge der GFA-Konzeptionsphasen definiert. Dies schließt eine Selbstorganisation in dem Sinne aus, dass die Normadressaten den GFA-Prozess nicht selbständig und eigenverantwortlich vorbereiten und durchführen können. Wenn die GFA-Durchführung an eine GFA-Stiftung übertragen wird, hat diese auch die GFA-Vorbereitungen zu tätigen. Sie legt fest, welche Verfahren und Instrumente in der Durchführungsphase zum Einsatz kommen und wie intensiv die Einbeziehung von Normadressaten und externen Experten sein soll. Von einer selbstorganisierenden GFA kann nun gesprochen werden, wenn die Träger der GFA-Stiftung gleichfalls die Normadressaten sind (bzw. wenn die Normadressaten eine Teilmenge der Stiftungsträger sind).

Die Organisationsform einer Stiftung muss nicht zwingend sein. Prinzipiell können auch Vereine oder privatwirtschaftliche Unternehmen eine GFA durchführen. Entscheidend sind das Vertrauen der Normadressaten und der politisch Verantwortlichen auf eine korrekte Durchführung der GFA. Die Ergebnisse eines GFA-Prozesses dienen den politisch Verantwortlichen nur als Empfehlung. Die Verbindlichkeit der Ergebnisse ist also keinesfalls garantiert. Die politisch Verantwortlichen können nun als Filter fungieren und Ergebnisse von nicht ordnungsgemäß durchgeführten GFA-Prozessen ignorieren. Sie beurteilen (im Ideal- und Extremfall) nur die methodische Qualität, mit der die Normadressa-

ten die ihnen zugesprochene inhaltliche Bearbeitung einer Folgenabschätzung vollzogen haben. Die politisch Verantwortlichen betreiben im operativen Gesetzgebungsprozess lediglich ein Qualitätsmanagement. Die inhaltliche Arbeit, also das operative Problemmanagement, wird an die Normadressaten und externen Fachexperten ausgelagert. Die Kernkompetenz, das „Entscheiden“, wird dadurch nicht angegriffen. Es wird eine starke Abgrenzung zwischen Methodik und inhaltliche Gestaltung im GFA-Prozess erwirkt.

Die Filter-Funktion der politisch Verantwortlichen ermöglicht maximalen Spielraum bei der konkreten Durchführung einer GFA. Staatliche, demokratische Verfahren der Bürgerbeteiligung müssen immer dem Gleichbehandlungsgrundsatz genügen. Ein Verfahren ist nur dann legitim, wenn prinzipiell jeder Bürger eine Beteiligung wahrnehmen kann. Bei der (selbstorganisierenden) GFA können jeweils so viele Bürger bzw. Normadressaten beteiligt werden, wie es die für eine Durchführung zur Verfügung stehenden Ressourcen ermöglichen. Die Akzeptanz und die Verbindlichkeit der Ergebnisse sind von der Anzahl der Beteiligten nicht direkt abhängig. Diese liegen im Ermessen der „Qualitätsmanager“.

1.5.3 Direkte Demokratie

Seit einigen Jahren ist wieder verstärkt die Diskussion um die Einführung plebiszitärer Elemente im Gange. Die Befürworter der direkten Demokratie fordern u. a. auf Bundesebene die Verankerung von Volksgesetzgebungsverfahren in der Verfassung und auf Länderebene die Senkung von Beteiligungsquoren für das Anerkennen eines konkreten Volksgesetzgebungsverfahren.

Ebenso wie für elektronisch demokratische Verfahren bietet die GFA auch für direktdemokratische Verfahren eine Hintertür in den Gesetzgebungsprozess. Selbstverständlich kann in der Vorbereitungsphase einer GFA die Anwendung solcher Verfahren beschlossen werden. Und auch hier sind die Freiheitsgrade bei der konkreten Durchführung höher als bei rein staatlichen Angeboten. Verfassung und Gesetze machen diesen unumgängliche Vorgaben. Problematisch

ist immer der dadurch notwendige hohe finanzielle, zeitliche, organisatorische und personelle Aufwand einer Durchführung. Im Rahmen einer GFA können für eine Beteiligung der Bürger eigene Regeln aufgestellt werden, so dass konventionelle Volksgesetzgebungsverfahren aufwandsminimaler simuliert werden können. Es gibt viele Möglichkeiten der Vereinfachung: Die Beteiligungsquoren können niedriger angesetzt werden, nur bestimmte Regionen oder Bevölkerungsgruppen können als repräsentativ betrachtet und befragt werden, Nachweise über Beteiligungsberechtigung werden nicht verlangt, Fristen können verlängert werden. Die Ergebnisverbindlichkeit entspricht aber ebenfalls maximal nur derjenigen der GFA. Dies macht Bürgerbeteiligungsverfahren im Rahmen von GFA-Prozessen vergleichbar mit Volksbefragungen. Solche haben im Gegensatz zur Volksabstimmung keine rechtlich bindende Wirkung, sondern nur Empfehlungscharakter, so wie die GFA.

Nichtstaatliche (aber hoffentlich allgemeinnützige) Organisationen können es sich zur Aufgabe machen ordnungsgemäße und gewissenhafte GFA-Prozesse mit maximal möglicher Bürgerbeteiligung durchzuführen (im Sinne einer selbstorganisierenden GFA). Der Anstoß dazu kann der Gesetzgeber geben, der dann die Finanzierung zu übernehmen hat. Der Anstoß kann aber auch aus der Menge der Organisationsmitglieder bzw. aus der Menge der „Kunden“ dieser Organisation heraus entstehen. Hier wäre dann Eigenfinanzierung z. B. durch Spenden von Interessensgruppen notwendig. Leider entfällt dann auch die Gewährleistung, dass die entwickelte Empfehlung bei den politischen Akteuren Gehör findet. Entsprechend groß muss die Reputation und Stärke dieser Organisation sein. Vorteilhaft ist, dass der Kontakt mit den Bürgern bzw. den Normadressaten nur einmal organisiert werden muss und für folgende Verfahren wiederverwendet werden kann. Möglich wäre eine einmalige aufwendige Registrierung für ein elektronisches Abstimmungsverfahren. Für folgende GFA-Prozesse steht dann jedes Mal die Menge aller registrierten Anwender für eine Meinungserhebung zur Verfügung. Dies alles kann nach eigenen Regeln und Anforderungen geschehen.

1.6 Zusammenfassung

Die Gesetzesfolgenabschätzung hat in Deutschland auf Bundes- und teilweise auf Landesebene Einzug gefunden wenngleich auch vorerst nur im Rahmen von Verordnungen. Diese Form der rechtlichen Institutionalisierung ist mit relativ wenig Aufwand zu erwirken aber ebenso auch wieder rückgängig zu machen. In mehreren Gesetzesprojekten wurde die GFA auf ihre Praxistauglichkeit hin untersucht und konnte sich bewähren. Ansätze zu einer selbstorganisierenden GFA wurden hingegen noch nicht aufgegriffen. Die Initiative hierfür muss aber keineswegs von staatlichen Stellen ausgehen, was sogar seiner eigentlichen Intention widersprechen würde. Um repräsentative Ergebnisse durch eine GFA, die von unabhängiger Stelle selbstorganisiert durchgeführt worden ist, erzielen zu können, ist Verfahrenstransparenz und allgemeine Verfahrenszugänglichkeit existenziell. Große Kreise von Fachexperten und Normadressaten lassen sich zwecks Information und Partizipation aber nicht mehr ausschließlich in Präsensaktivitäten unterbringen. Für eine gewissenhafte GFA-Durchführung bedarf es somit elektronischer Verfahren, die große Teilnehmermengen koordinieren und für mehrere GFA-Projekte akquirieren können. Von einer elektronischen GFA kann nur dann gesprochen werden, wenn der Einsatz von Informations- und Kommunikationstechnologien einen emergenten Mehrwert erzeugt. Eine punktuelle „Elektronisierung“ von Funktionen ist nicht ausreichend. Vielmehr besteht der angestrebte Mehrwert durch die Vernetzung aktueller und potenzieller Akteure, die unabhängig von der Existenz einzelner konkreter GFA-Durchführungen fortbesteht.

Insbesondere für Nichtregierungsorganisationen, die sich für die verstärkte Einbeziehung der Bürger in die politischen Prozesse stark machen, stellt die selbstorganisierte GFA einen interessanten Ansatz dar. Sie kann Verfahren der Volksgesetzgebung emulieren. Diese funktionelle Nachbildung kann jedoch unter beliebig vereinfachten Zulassungsbeschränkungen stattfinden. Die Ergebnisse können aber gegenüber den politisch verantwortlichen Akteuren (ebenso wie die Ergebnisse einer Volksbefragung) nur als Empfehlung vorgebracht werden.

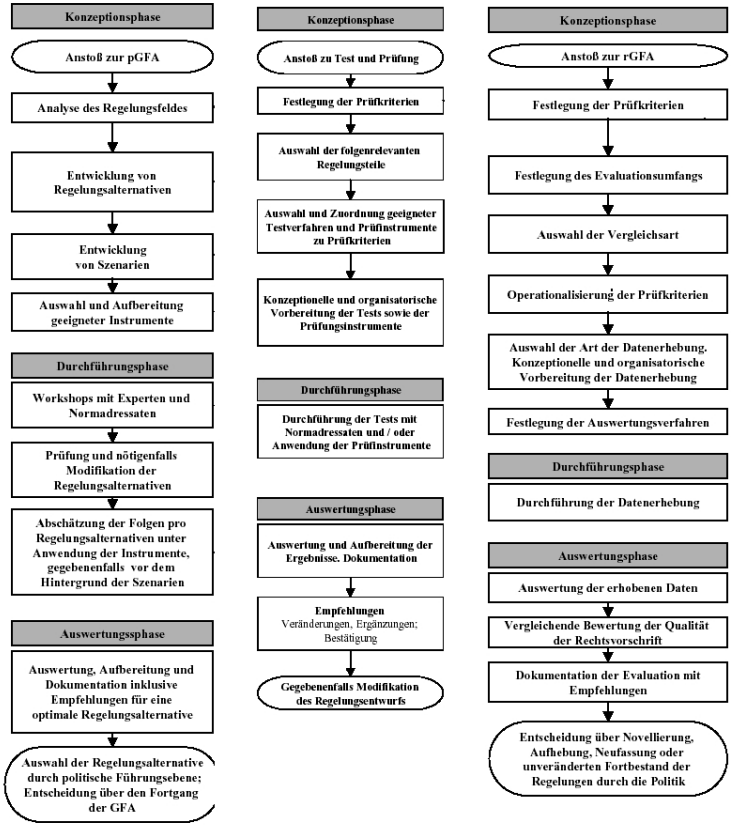


Abbildung 1.1: Prospektive, begleitende und retrospektive Gesetzesfolgenabschätzung [BK01]

Literaturverzeichnis

[BK98] BÖHRET, CARL und GÖTZ KONZENDORF: *Rechtsoptimierung mittels Gesetzesfolgenabschätzung: Waldgesetz Rheinland-Pfalz*, Band 192 der Reihe *Speyer Forschungsberichte*. Forschungsinstitut für öffentliche Verwaltung, Speyer, 1998.

[BK00] BÖHRET, CARL und GÖTZ KONZENDORF: *Moderner Staat – Moderne Verwaltung - Leitfaden zur Gesetzesfolgenabschätzung*. Bundesministerium des Innern und das Innenministerium Baden-Württemberg, Berlin, 7 2000.

[BK01] BÖHRET, CARL und GÖTZ KONZENDORF: *Handbuch Gesetzesfolgenabschätzung (GFA) - Gesetze, Verordnungen, Verwaltungsvorschriften*. Nomos Verlagsgesellschaft, Baden Baden, 2001.

[Brä04] BRÄUNLEIN, TOBIAS: *Integration der Gesetzesfolgenabschätzung ins Politisch-Administrative System der Bundesrepublik Deutschland*, Band 86 der Reihe *Beiträge zur Politikwissenschaft*. Peter Lang, Frankfurt a. M., 2004.

[Bun00a] BUNDESMINISTERIUM DES INNERN, STABSSTELLE MODERNER STAAT - MODERNE VERWALTUNG: *Gemeinsame Geschäftsordnung der Bundesministerien*. Berlin, 2000. Beschluss des Bundeskabinetts vom 26. Juli 2000.

[Bun00b] BUNDESVERWALTUNGSAMT: *Neue Gemeinsame Geschäftsordnung der Bundesministerien (GGO) - Grundlage für eine zeitgemäße Steuerung*, August 2000. INFO 1611.

[Bun02] BUNDESMINISTERIUM DES INNERN, STABSSTELLE MODERNER STAAT – MODERNE VERWALTUNG (Herausgeber): *Moderner Staat*

- Moderne Verwaltung. Abschlussbericht über den Praxistest zur Erprobung des Handbuches und es Leitfadens zur Gesetzesfolgenabschätzung an ausgewählten Vorhaben der Ressorts. Berlin, 6 2002.

[Bun03] BUNDESMINISTERIUM DES INNERN: *Moderner Staat - Moderne Verwaltung*, 2003. URL: `http://www.staat-modern.de`. (Zuletzt aufgerufen am: 01.03.2005).

[Bun05] BUNDESVERBAND DER DEUTCHEN INDUSTRIE E.V.: *Fünf Thesen zur Gesetzesfolgenabschätzung in Europa*, 2005. `http://www.bdi-online.de/download/Thesenpapier_Gesetzesfolgenabschaetzung.pdf` (Zuletzt aufgerufen am 08.02.2006).

[Deu05] DEUTSCHER BUNDESRAT: *Mitteilung der Kommission der Europäischen Gemeinschaften an den Rat und das Europäische Parlament: 'Bessere Rechtsetzung für Wachstum und Arbeitsplätze in der Europäischen Union'*. Technischer Bericht KOM(2005) 97 endg.; Ratsdok. 7797/05, Drucksache 286/05, 4 2005. Unterrichtung durch die Bundesregierung.

[Deu06] DEUTSCHES FORSCHUNGSINSTITUT FÜR ÖFFENTLICHE VERWALTUNG SPEYER: *Anwendungsorientierte Fortentwicklung der Gesetzesfolgenabschätzung*, 2006. `http://www.foev-speyer.de/projekte/projdbdetail.asp?ID=12` (Zuletzt aufgerufen am 08.02.2006).

[FH83] FRICKE, PETER und WERNER HUGGER: *Modelle zur Institutionalisierung einer Gesetzeskontrolle: Darstellung und vergleichende Bewertung*. 1983.

[GM97] GRÜN, MALEIKA K. und BENEDIKT MORSEY: *Prospektive Gesetzesfolgenabschätzung zum Problembereich Somatische Gentherapie*, Band 176 der Reihe *Speyer Forschungsberichte*. Forschungsinstitut für öffentliche Verwaltung, Speyer, 1997.

[HMO+01] HÝLLERER, MICHAEL, STEFAN MARA, MICHAEL OLIVER, GÜNTER VOITH und BARBARA ZINTER: *IV-Punktation zur Gesetzesfolgenabschätzung*. Technischer Bericht, IV - Industriellen Vereinigung, 2 2001.

[Ism01] ISMAYR, WOLFGANG: *Der Deutsche Bundestag. Der Deutsche Bundestag im politischen System der Bundesrepublik Deutschland*. Leske + Budrich, Opladen, 2. Auflage, 2001.

[KK92] KIESER, ALFRED und HERBERT KUBICEK: *Organisation*. Walter de Gruyter, Berlin, 3. Auflage, 1992.

[Kom02] KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFT: *Mitteilung der Kommission über Folgenabschätzung*. Technischer Bericht KOM(2002) 276 endg., Brüssel, 6 2002.

[Koo06] KOORDINIERUNGS- UND BERATUNGSSTELLE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK IN DER BUNDESVERWALTUNG: *Definition eDemocracy*, 2006. `http://www.kbst.bund.de/-,179s0/Glossar.htm` (Zuletzt aufgerufen am 14.02.2006).

[Lan83] LAND, F.: *Partizipation: Ihre Begründungen, Werkzeuge und Techniken*. In: MAMBREY, P. und R. OPPERMANN (Herausgeber): *Beteiligung von Betroffenen bei der Entwicklung von Informationssystemen*, Seiten 188–215. Campus Verlag, Frankfurt, 1983.

[Mem00] MEMORANDUM ELECTRONIC GOVERNMENT: *Electronic Government als Schlüssel zur Modernisierung von Staat und Verwaltung - Ein Memorandum des Fachausschusses Verwaltungsinformatik der Gesellschaft für Informatik e.V. und des Fachbereichs 1 der Informationstechnischen Gesellschaft im VDE*, September 2000.

[MOT86] MAMBREY, P., R. OPPERMANN und A. TEPPER: *Computer und Partizipation. Ergebnisse zu Gestaltungs- und Handlungspotentialen*. Westdeutscher Verlag, Opladen, 1986.

[Nie04] NIEDERSÄCHSISCHE LANDESREGIERUNG: *Gemeinsame Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen (GGO)*, 2004.

[Pre89] PREUSS, ULRICH K.: *Der Bund und die Länder*. In: WASSERMANN, RUDOLF (Herausgeber): *Kommentar zum Grundgesetz der Bundesrepublik Deutschland in zwei Bänden*, Seiten 1499–1557. Luchterhand, 2. Auflage, 1989. Reihe Alternativkommentare - Band 1.

[Unk98] UNKELBACH, INGO: *Die Institutionalisierung der Gesetzesfolgenabschätzung auf Landesebene*. Shaker, Aachen, 1998.

[Wor02] WORDELMANN, PETER: *Gesetzesfolgenabschätzung zum Entwurf eines Kinder- und Jugendhilfegesetzes des Landes Sachsen-Anhalt*, Band 227 der Reihe *Speyer Forschungsberichte*. Forschungsinstitut für öffentliche Verwaltung, Speyer, 2002.

2 Balanced E-Government - Bürgernähe vs. Verwaltungsmodernisierung

Balanced E-Government
Bürgernähe vs. Verwaltungsmodernisierung

Katja Neumann
Katja Witt

19. Dezember 2005

2.1 Einleitung

Das Internet wird wie selbstverständlich im alltäglichen Leben als Kommunikationsmittel genutzt. Die öffentliche Verwaltung ist in der Pflicht, die Bedürfnisse der Bürger zu erfüllen und hat erkannt, dass die Notwendigkeit der Modernisierung der Verwaltung mithilfe von elektronischen Hilfsmitteln, insbesondere durch das Internet besteht. Im September 2000 hat Bundeskanzler Gerhard Schröder den Startschuss für die Initiative BundOnline 2005[1] gegeben, die zum Ziel hat, bis Ende 2005 Verwaltungsprozesse der Bundesverwaltung online zu stellen. Einige seiner Ziele waren die Förderung der Zufriedenheit der Bürger mit Politik und Verwaltung, Förderung des Wirtschaftsstandorts sowie notwendigerweise die Verwaltungsmodernisierung. Der föderalistische Aufbau der Bundesrepublik Deutschland und das Recht der Selbstverwaltung von Gemeinden behindert allerdings eine Vereinheitlichung der informationstechnischen Lösungen. Auch ist das Anbieten von Diensten im Internet keine

[1] BundOnline Initiative: `http://www.wms.bundonline.bund.de/`

Universallösung für alle Bürger, da insbesondere benachteiligte sehbehinderte oder ältere Mitmenschen nur durch ein barrierefreies Internet erreicht werden können. Es gibt einige Initiativen und Projekte, die es sich zur Aufgabe gemacht haben, das Internet für alle Bürger netzwerkfähig zu gestalten[2]. In dieser Ausarbeitung soll es darum gehen, wie die oben angesprochene Bürgernähe durch ein möglichst effizientes und qualitativ hochwertiges, sowie sicheres Konzept einer Verwaltungsmodernisierung (E-Government) erreicht werden kann.

2.2 Definition und Begriffsabgrenzung

Es gibt eine Reihe von Definitionen des Begriffs des E-Governments oder auch der E-Democracy. Die nun folgende Definition ist von der Internetseite des Bundesamts für Sicherheit in der Informationstechnik und damit von einem Gremium entwickelt worden, welches sich in den letzten Jahren intensiv mit der Thematik auseinandergesetzt hat. Das Bundesamt für Sicherheit hat erstmals ein Handbuch für die Verwaltung veröffentlicht, in dem wesentliche Informationen für Leiter von Verwaltungen zusammengefasst sind:

> „Electronic Government (E-Government) bezeichnet die Nutzung des Internets und anderer elektronischer Medien zur Einbindung der Bürger und Unternehmen in das Verwaltungshandeln sowie zur Verwaltungsinternen Zusammenarbeit.“ [Bun]

Es geht hier also nicht nur um Technologien des Internets, sondern auch um herkömmliche Technologien, wie das Telefon, Fax, etc. sind hier einbezogen. Dabei geht es nicht nur um die Einbindung der Bürger und Unternehmen in den öffentlichen Publikumsverkehr, sondern auch um interne Tätigkeiten. Kernziel des E-Governments ist das Entstehen einer „digitalen Verwaltung“, deren Online-Angebot im Hinblick auf Information, Kommunikation, Dienstleistun-

[2] Barrierefreies Internet eröffnet neue Einsichten (BIENE): `http://www.biene-award.de`, Stiftung Digitale Chancen: `http://www.digitale-chancen.de`, Barrierefrei informieren und kommunizieren (BIK): `http://www.bik-online.info/`, etc.

gen und Beteiligungsmöglichkeiten auf die Bedürfnisse der Bürger und Unternehmen zugeschnitten ist [Bun].

Im Zusammenhang mit dem Begriff des E-Governments tauchen ebenfalls andere Bezeichnungen auf, die Teilgebiete von E-Government bezeichnen, sowie synonym zum E-Government verwendet werden. Den Zusammenhang zwischen diesen Begriffen verdeutlicht Abbildung 2.1.

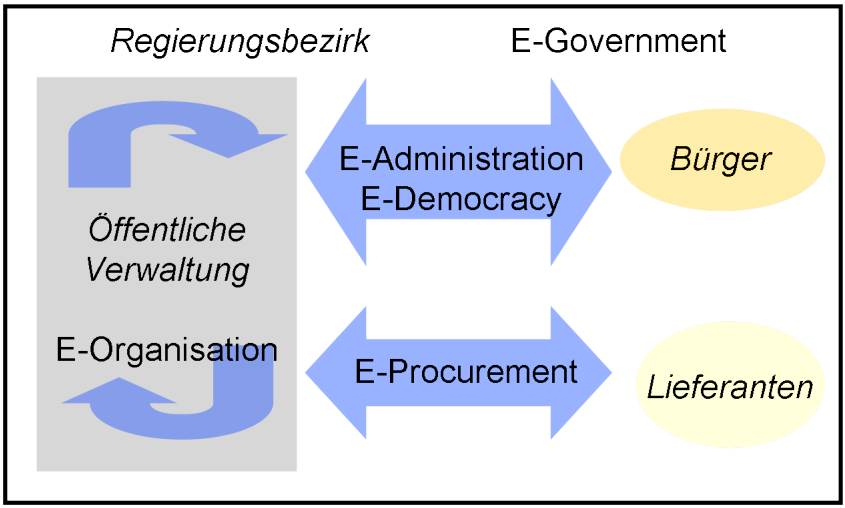


Abbildung 2.1: Begriffsabgrenzung

E-Democracy

E-Democracy wird im Allgemeinen synonym zu E-Government verwendet. Der Begriff meint im Speziellen jedoch die Tätigkeiten der Verwaltung in Hinblick auf die Beteiligung der Staatsbürger an der Regierung und ist demnach ein

Teilbereich des Oberbegriffs E-Government. E-Government setzt auf virtuelles Regieren, Service, Bürgernähe und Verwaltungsmodernisierung wobei E-Democracy Maßnahmen zusammenfasst, bei denen Internettechnologien eingesetzt werden, um Bürgern zusätzliche demokratische Mitbestimmungs- und Gestaltungsmöglichkeiten einzuräumen [Bau04]. Hier kommen Verfahren in Frage, die die Beteiligung der Bürger, also demokratische Partizipation in zum Beispiel elektronischer Form durch Internetforen, Chat, Abstimmungsfunktionalitäten ermöglichen. Durch diese Form der Bürgerbeteiligung sieht die Regierung eine neue Möglichkeit mit dem Volk zu interagieren bzw. über die Regierungsprozesse zu informieren und damit mehr Akzeptanz unter den Staatsbürgern sowie anderer Nationen herbeizuführen.

E-Administration

Wenn die öffentliche Verwaltung durch elektronische Medien bei den täglichen Verwaltungstätigkeiten unterstützt wird, die für die Pflichterfüllung gegenüber der Bürger notwendig sind, wird diese Tätigkeit der Verwaltung E-Administration genannt. Hier kommen Verfahren wie die Ermöglichung von Antragstellungen und Leistungsrechner im Internet in Frage.

E-Organisation

Die E-Organisation bezeichnet das Teilgebiet des E-Governments, welches sich mit den internen Tätigkeiten der Verwaltungsorgane beschäftigt. Hier sind Systeme inbegriffen, wie Dokumtentenmanagementsysteme, sowie herkömmliche Content Management Systeme, Wissensmanagementsysteme, Instant Messaging usw., die auch in jedem anderen Betrieb verwendet werden, um Verwaltungstätigkeiten effizienter zu gestalten.

E-Procurement

Das öffentliche Beschaffungswesen ist mit E-Procurement umschrieben. Hier werden Technologien des Online-Shoppings und Katalogsysteme eingesetzt.

2.3 Strukturwandel

Die Regierung Deutschlands ist Ende des 20. Jahrhunderts zu dem Schluss gekommen, dass der Wandel der Gesellschaft hin zu einer Informationsgesellschaft auch innerhalb der öffentlichen Verwaltung stattfinden muss, um die Akzeptanz seiner Staatsbürger zu erhalten. Diese Entwicklung haben Institutionen in ihren Studien beobachtet ([ARD], [Ber02b], [EOS02]). Die Abbildung 2.2 zeigt die Ergebnisse einer jährlichen, seit 1997 durchgeführten Studie in Deutschland. Einen weiteren, ebenfalls aus den Ergebnissen der eben erwähnten Studien stammenden, aufgefächerten Überblick zeigt die Aufteilung der Nutzer in Lebensaltern. Hier wird deutlich, dass die junge Gesellschaft sich im täglichen Umgang mit dem Internet befindet, um sich zu informieren, zu unterhalten oder zu kommunizieren (Abbildung 2.3). Aber andererseits ist ersichtlich, dass die älteren Generationen internettechnologisch aufrüsten. Der weitere Verlauf dieser Entwicklung wird die Onlinegesellschaft generationsübergreifend darstellen, da die Spitze der jungen Nutzer sich zu den älteren Nutzern verlagern wird. Damit Politik für die Staatsbürger einer Gesellschaft attraktiv, akzeptiert und erreichbar sein kann, ist es also sinnvoll, die Dienste der öffentlichen Verwaltung sowie Informationen über parteipolitische Informationen per Internet zur Verfügung zu stellen. Junge Wähler informieren sich verstärkt über das Internet und insbesondere Neuwähler gilt es für die Politik zu interessieren bzw. in die politische Willensbildung und Beteiligung einzubeziehen. In einer Informationsgesellschaft ist Wissen die Voraussetzung für eine politische Meinungsbildung. Wissensmanagementsysteme erlauben die Verwaltung sowie den Austausch von Informationen zwischen Kommunikationspartnern.

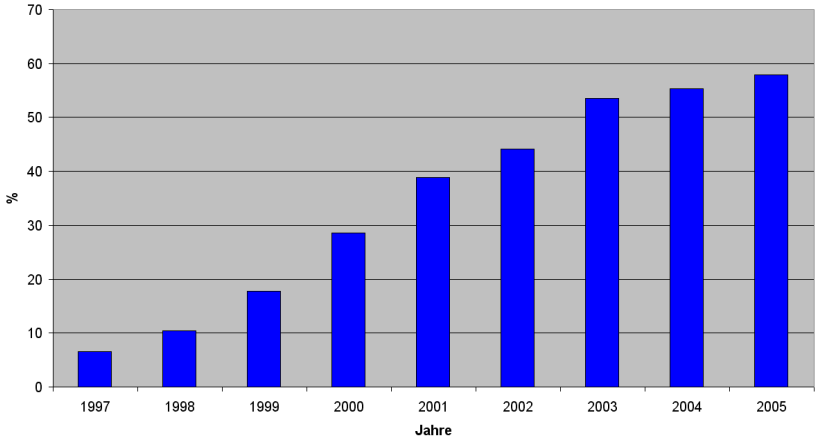


Abbildung 2.2: Prozentuale Entwicklung der Onlinenutzung, Onlinenutzer ab 14 Jahre [ARD]

Gerade Minderheiten haben erkannt, dass die Präsenz im Internet sehr viele Menschen weltweit erreichen kann. Diese Minderheiten wachsen und werden stärker. Auch kriminelle Organisationen können teilweise ungehindert ihr Publikum erreichen, weil der Rechtsstand dieses neues Mediums nicht eindeutig und international geklärt ist. Jedermann kann sich im Internet präsentieren, soweit die eigene Nation keine Zensur über Internetseiten belegt bzw. wegen strafrechtlichen Verdachtsmomenten Informationstechnologien beschlagnahmt.

Gerade die Regierung eines Landes sollte erkennen, dass diese Art der Informationsbereitstellung viele Vorteile bietet. Das Internet ist weltweit verfügbar. Die Daten können beliebig aktualisiert werden, sind somit aktueller als jede Zeitung sein kann. Je nach Internetzugang ist der Benutzer schnell und damit kostensparend in der Informationswelt unterwegs und kann bestimmte Informa-

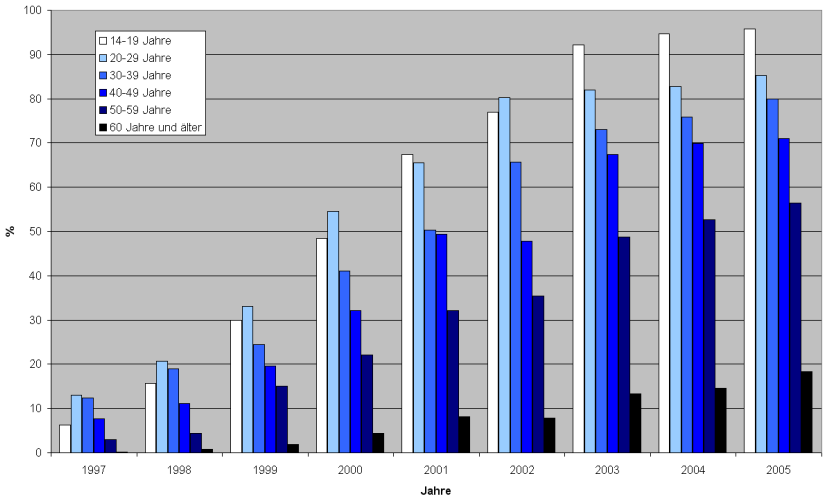


Abbildung 2.3: Altersabhängige prozentuale Entwicklung der Onlinenutzung, Onlinenutzer ab 14 Jahre [ARD]

tionen durch entsprechende Suchmaschinen finden. Das Internet scheint unendliche Kapazitäten bereitstellen zu können und ist kostengünstig. Jeder, der die entsprechende Technologie hat, kann das Internet nutzen.

Aber weil diese Technik noch relativ jung ist, werden auch informationstechnische Barrieren aufgestellt. Mitmenschen, die nicht mit diesem Medium aufgewachsen sind, haben es zunächst schwer, sich mit der Technologie auseinanderzusetzten. Darüberhinaus ist es notwendig, sich die entsprechenden Technologien erst einmal anzuschaffen. Sind diese vorhanden, steht der Benutzer einem Übermaß an Informationen gegenüber. Hier ist es notwendig sich eine entsprechende Medienkompetenz anzueignen. Außerdem ist anfangs die Navigation im Internet gewöhnungsbedürftig. Es gibt im Internet keine die Informationen be-

treffenden Qualitätskontrolle. Jeder Nutzer muss selber erkennen können, wie relevant und glaubwürdig Informationen sind.

Kritiker befürchten durch den weiterführenden Einsatz von elektronischen Hilfsmitteln die soziale Spaltung der Gesellschaft in zwei Klassen, namentlich die medienkompetenten und die nicht-medienkompetenten Bürger [Bun].

2.4 Verwaltungsmodernisierung

Das Konzept der virtuellen Regierung ist nicht ohne eine Umstrukturierung der Verwaltung möglich, soweit die betreffende Verwaltung über die reine Informationsbereitstellung über das Internet hinaus gehen möchte. Veraltete jahrelang praktizierte Verwaltungsvorgänge und -prozesse sind zu überdenken und zu modernisieren. Nicht unproblematisch ist außerdem das Rechtssystem Deutschlands, das in diversen Verwaltungsvorschriften vorschreibt, inwieweit u. a. das persönliche Erscheinen zur Beantragung eines Personalausweises oder zur einer Anhörung notwendig ist. Hier ist also der Gesetzgeber gefragt, sowie eine umfassende Anforderungsanalyse durchzuführen. Wie bereits erwähnt, wurde für die Bundesbehörden bereits ein Umstrukturierungsplan festgelegt und bis Ende 2005 sollten möglichst viele Bundesverwaltungsprozesse Online durchführbar sein. Die folgende Tabelle 2.1 beschreibt den Stand der umgesetzten Prozesse.

Dienstleistungstyp		vor 2002	2002	2003	2004	2005	insgesamt
1	Erfassen, Aufbereiten und Bereitstellen von Information	22	111	43	29	31	236
2	Beratung durchführen	1	2	1	5	5	14
3	Vorbereiten von politischen Entscheidungen bzw. Gesetzesvorhaben	0	1	1	0	1	3

...

Dienstleistungstyp		vor 2002	2002	2003	2004	2005	insgesamt
4	Zusammenarbeit mit Behörden	2	7	13	15	9	46
5	Allgemeine Antragsverfahren	2	7	8	17	16	50
6	Förderungen abwickeln	0	1	4	3	3	11
7	Beschaffungsvorhaben durchführen	3	3	9	9	4	28
8	Durchführung von Aufsichtsmaßnahmen	0	3	5	2	3	13
9	Sonstige Dienstleistungen	1	0	4	4	2	11
Dienstleistungen insgesamt		31	135	88	84	74	412
Letzte Aktualisierung: 13. Dezember 2005							

Tabelle 2.1: Fortschrittsanzeiger der Initiative BundOnline [3]

Die bereits erwähnte föderalistische und hierarchische Struktur der Bundes-, Landes- und Kommunalregierungen, erschwert eine einheitliche Umstrukturierung der Verwaltungen. Auch hat jede öffentliche Verwaltung zu unterschiedliche finanzielle Möglichkeiten sowie unterschiedlichste Standortfaktoren, um ein einheitliches Konzept umsetzen zu können. Hier sind Individuallösungen und entsprechendes Fachwissen gefragt. Gerade weil aber jede Verwaltung bisher Individuallösungen gesucht hat und sucht, und zur Zeit verschiedenste Lösungen für den selben Vorgang vorhanden sind, ist ein hohes Potential an Kostenersparnis möglich, wenn hier Kooperationen zwischen Verwaltungen gebildet werden [Bau04]. Trotz dieser skizzierten Probleme bietet E-Government insgesamt eine Chance, mithilfe neuer Medien interne und externe Prozesse, sowie das Verhältnis zum Bürger zu verbessern.

[3] Initiative BundOnline, Fortschrittsanzeiger: `http://www.wms.bundonline.bund.de/cln_027/lang_de/nn_1286/Content/60__dienstleistungen/dienstleistungen.html__nnn=true` (Stand 14.12.2005)

Für eine Gemeinde, die eine Internetseite plant, gibt es drei Qualitätstufen der Internetpräsenz. Zum einen kann die Gemeinde sich als Standort präsentieren, in dem sie digitale Informationen bereitstellt. Eine nächsthöhere Stufe wäre dann die Ermöglichung von netzbasierter Kommunikation über E-Mail-Adressen, Foren oder Chat. Die höchste Stufe stellt die Online-Transaktion dar, welche die Interaktion zwischen Bürger und Verwaltung oder Unternehmen und Verwaltung ermöglicht, um Verwaltungsprozesse zu unterstützen oder sogar komplett abzuwickeln. Die Initiative BundOnline nimmt hier eine Vorbildfunktion ein. Wie aus dem Fortschrittsanzeiger in Tabelle 2.1 ersichtlich, beziehen sich 236 (Typ 1) und damit 57% der 412 umgesetzten Dienstleistungen auf das Erfassen, Aufbereiten und Bereitstellen von Information. Hier stand die Bereitstellung von Informationen, also die erste Qualitätsstufe der Umsetzung von Bundesverwaltungsdienstleistungen zunächst im Vordergrund. Wobei natürlich die Abwicklung von Transaktionen und Kommunikation ohne Informationensbereitstellung nur eingeschränkt möglich wäre. Die zweite Stufe der Kommunikationsbereitstellung erreichen die Dienstleistungen vom Typ 2-4 mit insgesamt 63, was ungefähr 1/6 der Dienstleistungen ausmacht. Hier sind bereits Beratungswerkzeuge implementiert, wie Elternzeitrechner oder Kinderzuschlagrechner. Positiv fällt auf, dass die Transaktion bereits bei knapp 25% der umgesetzten Dienstleistungen (Typ 5-8), wie BAföG-Online, eVergabe von Beschaffungsaufträgen, ermöglicht wurde.

Die Umsetzung der virtuellen Verwaltung ist jedoch eine Investition in die Zukunft, da erst nach Jahren der Analysen und Entwicklung der Einsatz sich bei den Bürgern etablieren kann. Das höchste Einsparungspotential wird hierbei bei der Umsetzung von Verwaltungstransaktionen über das Internet, im Speziellen bei der Antragsbearbeitung erzielt werden können.

2.5 Bürgernähe

Ein Ziel, bei den bereits genannten Bemühungen elektronische Hilfsmittel einzusetzen, ist, dass mehr Bürgernähe erreicht werden soll. Eine durch das Volk

gewählte verfassungsmäßige demokratische Regierung sollte den Willen der Bevölkerung widerspiegeln. Wendet sich die Mehrheit der Bevölkerung von seiner Regierung wegen Missbilligung, Desinteresse und Ignoranz ab, entstehen Minderheitsregierungen, die nicht mehr mit dem im Grundgesetz vereinbar sind (Art.38 S.1 GG). Bürgernähe ist erforderlich, um die Akzeptanz der Bürger in Bezug auf ihre Regierung sowie die Legitimität der Regierung zu sichern. Bürgernähe wird erreicht, in dem Verwaltungsprozesse erläutert, dokumentiert und vereinfacht werden. Stellt die Verwaltung seine Prozesse dar, besteht gegenüber den Verwaltungsvorgängen Transparenz. Durch diese Transparenz wird dem Bürger das Verstehen von Vorgängen in der Verwaltung erheblich erleichtert. Bürgernähe wird außerdem unterstützt, in dem die Kommunikation und Interaktion zwischen Verwaltung und Bürgern angeregt wird. Verwaltungen haben meistens fest geregelte Öffnungszeiten. Berufstätige können diese Zeiten selten in Anspruch nehmen, da sie in der eigenen Kernarbeitszeit liegen. Durch eine Online-Präsenz könnte der Bürger die Verwaltung 24 Stunden am Tag von zu Hause aus erreichen. Doch diese Erreichbarkeit langt nicht, wenn der Bürger nicht die notwendigen Technologien zur Verfügung hat. Außerdem ist das Internet für viele deutlich schwerer zugänglich als z. B. Zeitung, Rundfunk oder Fernsehen. Eine Studie, die die Europäische Union beauftragt hat, zeigt 2002 in ihren Ergebnissen, dass kaum 50% der Bundesbürger, sowie Bürger von europäischen Mitgliedsländern einen Internetanschluss haben [EOS02]. Das heißt, dass über 50% u. a. nicht die finanziellen Mittel, sowie die Technik und das Wissen über Internettechnologien besitzen.

Nachweislich nutzen die meisten Internetnutzer das Internet für die Kommunikation untereinander, wie das Senden und Empfangen von E-Mails [EOS02]. Die Bereitstellung von behördenübergreifenden Verwaltungstransaktionen ist bisher noch kaum möglich. Welche Handlungen in Europa mit E-Government-Angeboten bisher getätigt wurden, zeigt Abbildung 2.4.

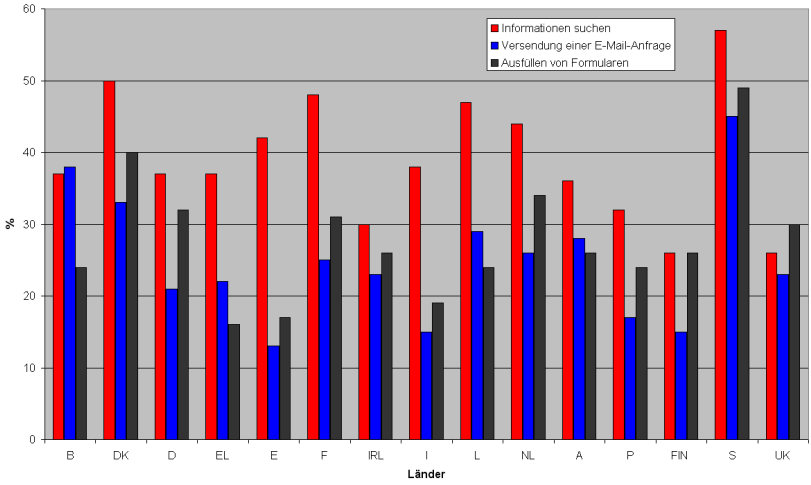


Abbildung 2.4: Nutzung von E-Government-Angeboten in der EU [EOS02]

Barrierefreies E-Government

Ein barrierefreies Internet umzusetzen bedeutet, dass der Zugang zum Internet allen Nutzern auf der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar ist (nach §6 Behindertengleichstellungsgesetz[4]). Per gesetzlicher Definition sind Menschen behindert, wenn ihre körperliche Funktion, geistige Fähigkeit oder seelische Gesundheit mit hoher Wahrscheinlichkeit länger als sechs Monate von dem für das Lebensalter typischen Zustand abweichen und daher ihre Teilhabe am Leben in der Gesellschaft beeinträchtigt ist (§3 BGG). Barrierefreie elektronische Medien unterstützen behinderte, zeitweilig eingeschränkte und ältere Menschen bei der Teilhabe am sozialen, beruflichen und kulturellen Leben.

[4] BGG

Beim Design von Webseiten wird oft nicht berücksichtigt, dass die Nutzer Einschränkungen haben könnten, weil sie sehbehindert oder blind, lese- oder konzentrationsschwach, motorisch behindert, gehörlos, älter oder ein Computerneuling sind. Es steht meistens das Design, Multimedialität und die Vielfältigkeit von Informationen im Vordergrund. Zur Unterstützung einer positiven Entwicklung in diesem Sinne hat die Bundesregierung Deutschland die Barrierefreie Informationstechnik Verordnung[5] vom 17. Juli 2002 erlassen, welche sich auf die Internetauftritte der Bundesbehörden bezieht. Nach dieser Verordnung müssen die Angebote der Bundesverwaltung bis Ende 2005 barrierefrei sein. Regierungsstellen müssen hier eine Vorbildfunktion annehmen, gerade weil die öffentliche Verwaltung bei der Umsetzung von Internetseiten bisher weniger präsent war. Auch ist bei der Erstellung von Webseiten darauf zu achten, dass die Seiten kompatibel zu Hilfsmitteln, wie zum Beispiel der Braillezeile, Großbildschirmen, Lupe-Funktionen, Sprachein- und -ausgabe sowie Tasthilfen sind. Welche Hilfsmittel prozentual bei Behinderten, die auf Hilfsmittel zurückgreifen müssen, benutzt werden, wurde von einer Umfrage, die im Auftrag des Bundesministeriums für Wirtschaft und Technologie entstand, evaluiert (Abbildung 2.5).

Im E-Government-Handbuch werden die nun folgenden Gesichtspunkte erwähnt, die bei der Entwicklung zu beachten sind. Es sollten zum Beispiel keine aktiven Inhalte verwendet werden. Blinkende Inhalte verursachen bei manchen Epileptikern gesundheitliche Probleme, die zu einem Anfall herbeiführen können. Hierbei spielt die Frequenz, die Farbverwendung, der Kontrast und die Struktur eine große Rolle.

Menschen mit Lernschwäche, Sprachschwäche, geistiger Behinderung oder Gehörlosigkeit haben bei der Aufnahme bildlicher Designs oder bei Multifunktionalitäten von Seiten weniger Probleme. Hier ist eher ein besonderer Augenmerk auf die inhaltliche Gestaltung zu legen. Texte sollten also leicht verständlich und unkompliziert formuliert werden.

Motorisch behinderte Menschen benutzen als Hilfsmittel oft spezielle Tastaturen. Diese Nutzer können meistens nur schwerlich normale Computermäuse

[5] BITV

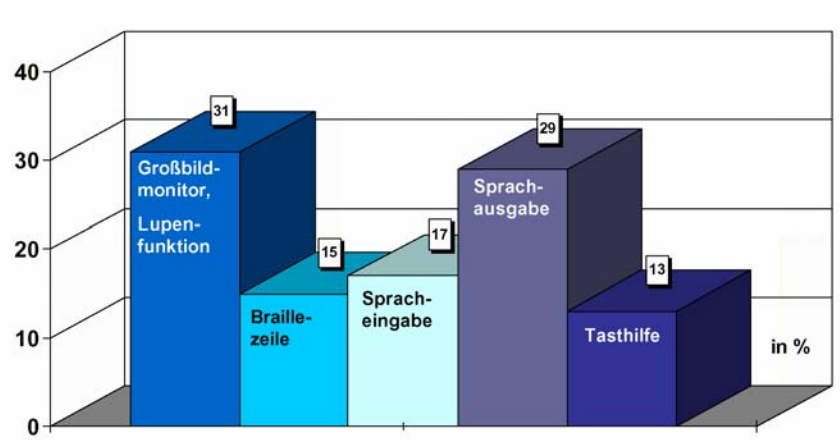


Abbildung 2.5: Hilfsmittelbedarf (30% der Studienteilnehmer brauchen Hilfsmittel) [Uni]

benutzen, da ihr Bewegungsradius eingeschränkt ist. Es ist also notwendig die Navigation in der Internetseiten per Tastatur zu ermöglichen. Andererseits sollte die Bedienbarkeit über speziellen Eingabegeräte, die beispielsweise mit Füßen, Ellenbogen oder Kopf bedient werden, gewährleistet werden. Das bedeutet für das Webdesign, dass hier u. a. die Genauigkeit der Navigation eingeschränkt sein kann. Deswegen sollten Schaltflächen nicht zu klein gestaltet werden, damit der Nutzer eine größere Angriffsfläche hat.

Besonders für blinde Mitmenschen stellt die Nutzung des Internets eine große Herausforderung dar. Schließlich können sie Inhalte nur wahrnehmen, wenn diese als Text vorliegen, die meist in Blinden- bzw. Punktschrift über eine Braillezeile ausgegeben werden. Ein spezieller Browser ermöglicht sogar die Sprachausgabe und/oder die Ausgabe als Braillezeile. Für blinde Nutzer sind durch Frames und Tabellen verschachtelte Internetseiten schlecht wahrzunehmen, da bei zu tiefer Verschachtelung für sie die logische Struktur verlorengehen kann. Bilder sollten für diese Nutzer mit einem Alternativtext versehen

werden. Es sollten also alle nicht textuellen Inhalte mit Textäquivalenten versehen werden. Das gilt insbesondere für audio- und visuelle Elemente. Leicht sehbehinderten Nutzern hilft bereits ein gut wahrnehmbares Layout oder die individuelle Einstellung von Schriftgrößen und Farbgebung.

Um die Kompatibilität von Internetseiten zu informationstechnischen Hilfsmitteln zu garantieren, sollte sich jeder Webdesigner an die Standards, insbesondere des World Wide Web Consortiums[6] halten, da Standards die Weiterentwicklung von Technologien ermöglichen und die Entwicklung von Webseiten erleichtern. Die Richtlinien der Web Accessibility Initiative vom 05. Mai 1999 [Wor99] finden sich in den im E-Government-Handbuch aufgezeigten wieder und beziehen sich auf Gesetzmäßigkeiten, die bei dem Design von barrierefreien Webseiten zu beachten sind. Diese sind im Folgenden aufgelistet:

Nr.	Richtlinie
1	Stellen Sie äquivalente Alternativen für Audio- und visuellen Inhalt bereit.
2	Verlassen Sie sich nicht auf Farbe allein.
3	Verwenden Sie Markup und Stylesheets und tun Sie dies auf korrekte Weise.
4	Verdeutlichen Sie die Verwendung natürlicher Sprache.
5	Erstellen Sie Tabellen, die geschmeidig transformieren.
6	Sorgen Sie dafür, dass Seiten, die neue Technologien verwenden, geschmeidig transformieren.
7	Sorgen Sie für eine Kontrolle des Benutzers über zeitgesteuerte Änderungen des Inhalts.
8	Sorgen Sie für direkte Zugänglichkeit eingebetteter Benutzerschnittstellen.
9	Wählen Sie ein geräteunabhängiges Design.
10	Verwenden Sie Interim-Lösungen.
11	Verwenden Sie W3C-Technologien und -Richtlinien.
12	Stellen Sie Informationen zum Kontext und zur Orientierung bereit.

...

[6] W3C: `http://www.w3c.org`

Nr.	Richtlinie
13	Stellen Sie klare Navigationsmechanismen bereit.
14	Sorgen Sie dafür, dass Dokumente klar und einfach gehalten sind.

Tabelle 2.2: Zugänglichkeitsrichtlinien für Web-Inhalte [Wor99]

Ob eine Internetseite barrierefrei ist, beurteilen in Deutschland Initiativen wie BIENE[7], die den BIENE-Award vergeben. Für diesen Zweck wurde 2005 ein Kriterienkatalog über 94 Punkte entwickelt. Diese teilen sich in die nun folgenden Oberkategorien ein:

Kritik-punkte	Oberkategorie
0	Grundvoraussetzungen: Keine parallelen Alternativ-Auftritte
1-7	Lesbarkeit / inhaltliche Erschließung: Zusammenfassungen, Wortwahl, Glossar
8-16	Variable Präsentation: Textäquivaltente für Audio- und Visuelle Elemente
17-28	Navigation: Tastatur, Shortcuts, Beschriftung, Nachvollziehbarkeit
29-33	Struktur / Aufbau des Internetangebots: Trennung von Inhalt und Layout
34-38	Kompatibilität: Standards, Umgang mit deaktivierten Elementen
39-43	Fehlerhandling und Hilfe in Formularen: Angemessenheit, Zugänglichkeit
44-45	Hilfe und Support: geografische Informationen
46-51	Komplexe Formulare: Verständlichkeit, Alternativen, Kategorisierung
52-56	Komplexe Transaktionen: Bestätigungsanfragen, Bezahlfunktionen
57-63	Shop und Warenkorb- und Bezahlfunktion: Transparenz, Bezahlfunktionen
64	Datenschutz: Information
65-66	Werbung: Erkennbarkeit, keine Pop-Ups ohne Nutzerinteraktion

...

[7] Barrierefreies Internet eröffnet neue Einsichten

Kritik-punkte	Oberkategorie
67-68	Downloads und Formularserver: Barrierefreiheit
69-70	Newsletter / Antwort-E-Mails: Standards, Textformat
71-72	Statistiken / Datentabellen: Zusammenfassungen, grafische Darstellungen
73-74	Komplexe Dokumente: Organisation, Layout, Gliederung, Aussagekraft
75-81	Multimedia / Spiele / Videos / Animationen: Beschreibungen, Äquivalente
82-87	Gebärdensprach-Filme: Wahrnehmung, Verständlichkeit, deutliche Kennzeichnung
88-93	Leichte Sprache: Angemessenheit, Wortwahl, Erklärungen, Veranschaulichungen

Tabelle 2.3: Kriterienkatalog (BIENE-Award 2005) [8]

Die Gewinner des goldenen BIENE-Awards 2005 für den Bereich E-Government, E-Demokratie sind die Internetpräsenzen des Landtages Nordrhein-Westfalen[9] und des Landesportals Baden-Württemberg[10].

2.6 Umsetzung

E-Government ist vielfach bisher nur ein Schlagwort. Sicherlich ist ein gutes E-Government für alle Bereiche wünschenswert, jedoch stellt die Umsetzung eine Aufgabe mit immensem Aufwand dar, die bisher noch von wenigen Städten und Gemeinden in Angriff genommen wurde. Jedoch wird dies zunehmend mehr.

Für die Umsetzung von gutem E-Government gibt es viele Empfehlungen und Vorschläge, im Folgenden sollen nur zwei näher behandelt werden - das E-

[8] Kriterienkatalog BIENE-Award 2005: `http://www.biene-award.de/award/kriterien/`

[9] Landtag Nordrhein-Westfalen: `http://www.landtag.nrw.de`

[10] Landesportal Baden-Württemberg: `http://www.baden-wuerttemberg.de`

Government-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik und der 10-Punkte-Plan der Bertelsmann Stiftung.

E-Government-Handbuch

Das E-Government Handbuch wurde vom Bundesamt für Sicherheit in der Informationstechnik erstellt und ist ein Nachschlagewerk zum Thema „Sicheres E-Government“. Es richtet sich an E-Government-Koordinatoren und -Teams sowie Entscheider in Bund, Ländern und Kommunen, Mitarbeiter in Forschung und Entwicklung, die an E-Government-Konzepten und -Lösungen arbeiten und an Behördenmitarbeiter und Bürger, die sich für Themen rund um E-Government interessieren. Das Handbuch gibt keine Regeln für die Umsetzung von E-Government vor, sondern soll Vorschläge und Empfehlungen geben.

Das E-Government-Handbuch wurde aus verschiedenen Gründen erstellt. Es soll „Hilfe zur Selbsthilfe bei der Einführung von E-Government in Behörden“ geben, aber auch „Grundlage der begleitenden Beratung von Bundesbehörden bei der Einführung von E-Government durch das BSI oder durch die zu bildenden Kompetenzzentren“ sein. Zudem ist es ein „Beitrag zur Standardisierung von kommerziellen Produkten für den Einsatz im E-Government durch richtungsweisende Empfehlungen innerhalb des Handbuchs“. [Bun]

Das E-Government-Handbuch ist momentan als Loseblattsammlung und als Online-Version verfügbar und wird laufend ergänzt und aktualisiert. Inhalte des Handbuches sind [Bun]:

1. Sensibilisierung
2. Grundlagen
3. Phasenplan
4. Thematische Schwerpunkte
5. Spezifikationen und Lösungen
6. Hilfsmittel

Das Handbuch gibt somit einen umfassenden Überblick über die E-Government-Umsetzung, viele Informationen beziehen sich jedoch auf die IT und die IT-Sicherheit.

Der 10-Punkte-Plan

Der 10-Punkte-Plan aus 2002 für gutes E-Government der Bertelsmann Stiftung gibt konkrete Tipps zur Umsetzung effizienten und bürgernahen E-Governments. Hierbei werden für jeden Punkt eine Beschreibung, Maßnahmen, die zur Realisierung dienen können und Beispiele angeführt. Mit der Reihenfolge der Punkte werden keine Prioritäten dargestellt, diese ist willkürlich gewählt und kann individuell angepasst werden.

Im Folgenden werden die Punkte kurz erläutert, für weitere Informationen hierzu kann das Dokument der Bertelsmann Stiftung herangezogen werden. [Ber02a]

- Prozesse gestalten
  In dieser Phase der Umsetzung müssen alle zur Disposition stehenden Abläufe und Zuständigkeiten überprüft werden. Ohne eine Überprüfung sämtlicher Prozesse kann keine Effizienzsteigerung stattfinden, da die Umgestaltung dieser entscheidend ist bei der Umsetzung von E-Government.
- Transparenz herstellen
  Die Offenlegung interner Prozesse führt zu Transparenz, wodurch Informationen erst nachvollziehbar werden. Um ein E-Government-System nutzbar zu machen, ist diese Phase unbedingt notwendig, da sie sehr zur Vertrauensbildung und Akzeptanz beim Bürger beiträgt.
- Beteiligung ermöglichen
  Beteiligung von Bürgern an staatlichen Prozessen führt zu einer veränderten Beziehung von Staat und Bürger zueinander. War der Staat vorher vor allem Versorger, wird er nun zum Dialogpartner und der Bürger kann aktiv in das Geschehen eingreifen.

- Nutzer einbinden
  Wichtig bei der Einführung und Umsetzung von E-Government ist die Befragung von Nutzern vor der Entwicklung eines konkreten Systems. Auch sollte das Nutzerverhalten kontrolliert werden. Hierdurch werden teure Fehlentwicklungen vermieden und das System wird auf den Nutzer zugeschnitten. Dies erhöht wiederum die Akzeptanz des Systems.
- Standards nutzen
  Häufig sind schon Standardlösungen für die Abwicklung von Prozessen vorhanden. Werden diese genutzt und angepasst, können die finanziellen Aufwendungen möglichst klein gehalten werden. Auch ermöglicht die Verwendung von Standards einen Austausch von Daten zwischen verschiedenen Stellen.
- Kooperationen sicherstellen
  Die kommunale Selbstverwaltung führt dazu, daß jede Gemeinde für sich an Lösungen arbeitet. Sinnvoller ist es in diesem Zusammenhang aber, Vergleiche mit anderen Gemeinden, Landkreisen und Ministerien zu ziehen und Lösungen gemeinsam zu entwickeln. Zudem sollte Kooperation auch zwischen den Verwaltungsabschnitten stattfinden.
- Finanzierung maßschneidern
  Abhängig von der finanziellen Situation, dem Umfang des Vorhabens und der Dringlichkeit der Umsetzung müssen konkrete Finanzpläne zur Umsetzung von E-Government erstellt werden. Sind diese nicht vorhanden, kann ein Projekt mit so großem Umfang schnell aufgrund fehlender Finanzkraft im Sande verlaufen.
- Service bieten
  Laut einer Untersuchung politischer Internetseiten schöpfen diese nur 20 Prozent des Service-Potenzials aus. Bürger erwarten aber vor allem Service-Angebote beim Stichpunkt E-Government. Hierauf sollte daher viel Wert gelegt werden, um die Akzeptanz und Nutzung des Systems sicherzustellen.
- Kompetenzen schaffen
  Durch die Umstrukturierung der Prozesse werden eventuell auch eine Neuordnung der Personalstruktur, teilweise auch durch Schaffung von

Kompetenzen und Zuständigkeiten nötig sein. Hierbei müssen alle Betroffenen eingebunden werden, um das Projekt nicht schon am internen Widerstand scheitern zu lassen.

- Marketing planen
  Auch Gemeinden müssen heute über Marketing nachdenken, um Bürger in der Gemeinde zu halten oder sie anzulocken. Hierbei sollte ein gutes E-Government-System durchaus als Standortvorteil gesehen und auch entsprechend beworben werden.

2.7 Probleme und Herausforderungen

Bei der Umsetzung von E-Government gibt es sicherlich viele Probleme und Herausforderungen. Die meisten Probleme sind recht offensichtlich, einige entstehen auch erst durch andere Zieldefinitionen. Prinzipiell sind zwei Arten von Konflikten zu unterscheiden, die im Folgenden dargelegt werden sollen.

Zielkonflikte

Bei Zielkonflikten handelt es sich schon im System angelegte Konflikte, bei denen sich zwei Ziele gegenseitig ausschließen und die auch nicht zu beseitigen sind. Hierfür gibt es einige Beispiele.

Partizipation und Effizienz sind solche Ziele, die sich entgegenstehen. Um Partizipation zu gewährleisten, ist ein hoher Aufwand an Zeit und Geld nötig, wobei dies sowohl für die Schaffung der Voraussetzungen für Partizipation als auch für die Umsetzung der partizipatorisch erlangten Lösungen gilt. Dies kann nie mit Effizienzverbesserungen einhergehen.

Auch Legalität und Effizienz stehen sich entgegen. Die Gewährleistung der verwaltungstechnischen Legalität erfordert ebenfalls einen immensen Aufwand.

Die festgelegte hierarchische Kontrolle bedeutet beispielsweise teure Doppelarbeit.

Nicht zuletzt stehen auch die Ressourcensicherungsinteressen der Verwaltung einer effizienten Mittelverwendung entgegen. Eine Effizienzsteigerung bedeutet notwendigerweise auch die Einsparung von Ressourcen.

Die Machtinteressen mancher Politiker sind sicher nicht mit Bürgerpartizipation vereinbar. Partizipation bedeutet auch eine Mitbestimmung durch den Bürger, wodurch der Politiker kein unumschränktes Bestimmungsrecht mehr hat, sondern weiterhin einem demokratischen Prozess unterworfen ist.

Diffusionsprobleme

Unter Diffusionsproblemen versteht man Probleme, die durch miteinander vernetzte Faktoren entstehen. Verändert man einen Faktor, wird ein anderer dadurch auch beeinträchtigt. Hier muss eine optimale Balance gefunden werden. Diffusionsprobleme entstehen auf verschiedenen Ebenen. [Win04]

- Technische Ebene
  Die Lösung der technischen Probleme bedeutet einen immensen Aufwand, der mit hohen Kosten einhergeht. Hierunter fallen die Anschaffung der IT-Ausstattung und -Zugänge sowohl bei der Verwaltung als auch beim Bürger und die Entwicklung einer Transaktionsinfrastruktur, um Ein- und Ausgänge verwalten zu können und die Abwicklung von Geschäftsprozessen zu ermöglichen. Auch die Entwicklung einer brauchbaren digitalen Signatur, einer Verschlüsselungsfunktion, eines Paymentsystems und einer Firewall gehören zu den zu lösenden technischen Problemen, die bisher nur teilweise angegangen wurden. Ein letztes Problem ist die Gewährleistung der Interoperabilität von Verfahren, damit alle Systeme untereinander kommunizieren können und so Medienbrüche wirklich beseitigt werden können.

- Organisatorische Ebene
  Ein E-Government-System kann nur dort nutzbringend eingesetzt werden, wo die Organisationsstrukturen und die zugehörigen Prozesse neu geordnet wurden. Die momentane Struktur der Verwaltung eignet sich nicht zur Umsetzung in einem solchen System.
- Wissensebene
  Neue technische Kenntnisse und zusätzliche Fachkompetenzen müssen sowohl in der Verwaltung als auch beim Bürger erworben werden. Auch muß der Bürger über ein Mindestmaß an Verwaltungskompetenz verfügen, um Prozesse selbständig online abwickeln zu können. Hierfür ist ein großes Maß an Transparenz nötig. Auch das Wissen um die Bedienung eines Computers und des Internets kann bei manchen Bürgern fehlen und muss zusätzlich erworben werden.
- Kulturelle Ebene
  Die technische Entwicklung ist der Anerkennung in der Gesellschaft immer weit voraus. Oberstes Ziel auf der kulturellen Ebene sollte die Entwicklung von Vertrauen in ein E-Government-System sein, was nicht ohne die nötigen technischen Voraussetzungen und wiederum auch der nötigen Transparenz möglich ist.
- Rechtliche Ebene
  Die rechtlichen Vorschriften für Verwaltungsaufgaben lassen es heute noch gar nicht zu, alle Prozesse durch E-Government abwickeln zu lassen. So ist es im Meldewesen zum Beispiel immer noch notwendig, persönlich unter Vorlage des Personalausweises zu erscheinen.
- Finanzielle Ebene
  Das finanzielle Problem liegt sicher auf der Hand. Die Umsetzung von E-Government kostet immer Geld, das sowohl für die technische als auch für die Wissens-, Management- und Organisationsebene gilt. Dieser Punkt beschränkt sich natürlich wiederum nicht nur auf die Verwaltungsebene. Auch beim Bürger muss Technik angeschafft werden und ein Internetanschluss vorhanden sein.
- Nutzenebene
  Wünschenswert bei einer Umsetzung von E-Government wäre eine Win-

Win-Situation. Für Bürger und Unternehmen, die die „Konsumenten“ in diesem System bilden, liegt der Gewinn auf der Hand. Es müssen keine Öffnungszeiten mehr eingehalten werden, das Erscheinen auf dem Amt ist nicht mehr notwendig und auf diese Art und Weise werden Zeit und auch Geld gespart. Für die Verwaltung kann E-Government aber immer nur ein zusätzliches Angebot bleiben und auch die traditionellen Öffnungszeiten und Prozessabwicklungen müssen weiterhin angeboten werden, so dass hier E-Government momentan nur einen zusätzlichen finanziellen und organisatorischen Aufwand bedeutet.

- Managementebene
  Für die Umsetzung von E-Government sind ein professionelles Projektmanagement und ein Business Plan unumgänglich, da ein Projekt von solch großem Umfang kein Selbstläufer sein kann.
- Konzeptionelle Ebene
  Auch ein detailliertes Konzept ist unbedingt erforderlich. Hierbei darf nie aus den Augen verloren gehen, dass die IT in diesem Fall Mittel zum Zweck ist und der Zweck daher unbedingt klar definiert sein muss.
- Politische Ebene
  Die Politik muss die Innovationsprozesse in Gang setzen und, was noch viel wichtiger ist, auch dauerhaft unterstützen. Ohne politische Unterstützung wird E-Government letztendlich zum Scheitern verurteilt sein.

Die BundOnline Projektgruppe des Bundesministeriums des Inneren führt eine Umfrage zu den Dienstleistungsangeboten von BundOnline durch. Von November 2004 bis August 2005 haben sich 124 Nutzer an der Umfrage beteiligt. Bei dieser Umfrage gaben die Bürger als größtes Hindernis für die Nutzung des Systems Unkenntnis an, auf Rang zwei war mangelndes Vertrauen in die Sicherheit des Systems angegeben.

Auch Wirtschaftsunternehmen nahmen an der Umfrage teil. Hier gestalten sich die Hindernisse teilweise anders als beim Bürger, wie Abbildung 2.7 zeigt. Auch hier wird Unkenntnis als wichtigstes Hindernis angegeben, jedoch werden auch Medienbrüche und zu heterogene Verwaltungsdienstleistungen angegeben.

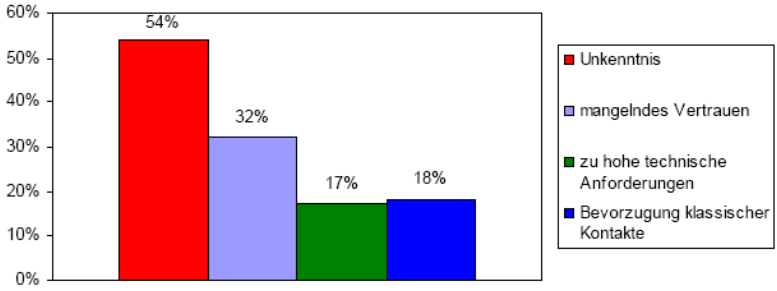


Abbildung 2.6: Hindernisse für Bürger laut Umfrage [Bun05a]

Herausforderungen

Die Herausforderungen sind im Zusammenhang mit der Umsetzung von E-Government vielfältig, jedoch nicht unlösbar. Oberstes Ziel muss die Analyse und Optimierung der Geschäftsprozesse sein. Dies allein sollte schon zu einer Effizienzsteigerung führen. Die Beseitigung der vielen Medienbrüche, die momentan bei Verwaltungsprozessen vorherrschen, erfordert eine prozessorientierte Umgestaltung, die wiederum vor allem der Effizienz zugute kommen wird. Wie schon beschrieben, erfordert die Umsetzung von E-Government trotz kommunaler Selbstverwaltung ein „Schauen über den Tellerrand“ und das Bilden von Zusammenschlüssen. Hiermit hängt auch das nötige Umdenken in der Verwaltung zusammen. Eine letzte Herausforderung stellt die Umsetzung eines „Multikanalvertriebes“ dar, um sich nicht nur auf das Internet zu stützen und somit allen Bürgern gleichermaßen den Zugang zur Verwaltung zu ermöglichen.

2.8 Vorteile

Natürlich kann es bei der Umsetzung von E-Government nicht nur Probleme und Herausforderungen geben. Es müssen auch Vorteile vorhanden sein, die

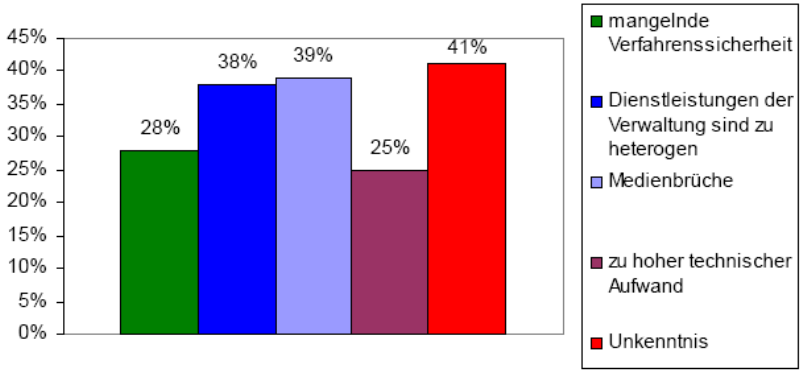


Abbildung 2.7: Hindernisse für Wirtschaft laut Umfrage [Bun05b]

vom Einsetzen eines solchen Systems erwartet werden. Derer gibt es einige. Inwieweit diese umsetzbar sind, bleibt jedoch abzuwarten.

Zuerst wird man bei der Einführung eines E-Government-Systems sicherlich immer an Kosten- und Zeiteinsparungen denken. Durch den Wegfall der persönlichen Betreuung des Bürgers können sich die Verwaltungsangestellten vermehrt den eigentlichen Verwaltungsaufgaben widmen und somit wird Zeit und letztendlich auch Kosten eingespart. Auch die Optimierung der Prozesse sollte zu Zeiteinsparungen führen. Die Kosteneinsparung wird dabei vor allem durch Einsparungen beim Personal erzielt, jedoch auch durch die Beseitigung von Medienbrüchen. Hiermit hängen natürlich Steigerung der Effektivität und der Effizienz direkt zusammen. Kosten- und Zeiteinsparungen sind aber auch für den Bürger relevant. Porto- und Fahrtkosten fallen weg und auch die Zeit, die auf Ämtern verbracht wird, reduziert sich.

Eine Verbesserung von Arbeitsbedingungen kann den Verwaltungsmitarbeitern ein E-Government-System vor allem dann bieten, wenn fragmentierte Aufgabenzuschnitte reorganisiert werden und damit die Aufgabenfelder des einzelnen Mitarbeiters wieder klar definiert und übersichtlich werden.

Die Erhöhung der Transparenz und Responsivität des politisch-administrativen Handelns liegt auf der Hand. Durch die Netzkommunikation können die Bürger in politische Prozesse stärker einbezogen werden und es kann auf geäußerte Probleme oder Anregungen viel schneller reagiert werden. Eine E-Mail ist erheblich schneller beim Empfänger als ein Brief und kann auch unmittelbar beantwortet werden. Zudem kostet diese auch weniger Zeit und Geld. Ein Beispiel von Transparenz ist in Schweden zu sehen. Dort werden jährlich die Einkommen aller Bürger und die darauf gezahlten Steuern veröffentlicht, zudem sind Grundbuch und Melderegister einsehbar. [Ber02a]

Ein erwarteter Vorteil von E-Government, ohne den ein solches System sicherlich wenig Akzeptanz finden würde, ist eine Verbesserung des Bürgerservices. Den Bedürfnissen der Bürger sollte besser Rechnung getragen werden. Schon alleine das 24-Stunden-Office einer E-Government-Lösung kann für viele Bürger, die keine Möglichkeit haben, zu den recht begrenzten Öffnungszeiten in Ämtern zu erscheinen, eine erhebliche Erleichterung bringen. Vorstellen könnte man sich aber auch eine Bündelung aller Verwaltungsaufgaben in einem Portal. Somit könnte der Bürger alle Anliegen und Aufgaben an einem Ort von zu Hause aus erledigen. Das Portal der britischen Regierung bietet einen besonderen Service, indem ein Großteil eines Umzuges online organisiert werden kann, von der Erkundung der Schul- und Immobiliensituation bis hin zu Checklisten und kommerziellen Links, die beispielsweise bei der Adressänderung helfen. [Ber02a]

Mit all diesen Vorteilen geht eine Verbesserung der Legitimität und Akzeptanz des politisch-administrativen Handelns einher. Sind alle politischen und Verwaltungsprozesse transparent und damit für den Bürger leichter einsehbar, kann dies schon zu einer größeren Akzeptanz führen. Jedoch soll mit E-Government auch die Möglichkeit der Partizipation gegeben werden, mit Hilfe dessen der Bürger stärker an der politischen Willensbildung beteiligt wird und somit politische Prozesse, an denen der Bürger beteiligt war, von ihm sicherlich auch noch stärker akzeptiert werden.

Die schon im Abschnitt Probleme und Herausforderungen genannte Umfrage zu den BundOnline Dienstleistungen ergab auch Vorteile. Vorteile, die Bürger

in dem Angebot sahen, waren vor allem der unbeschränkte und einfachere Zugang zu den Servicefunktionen sowie die Verbesserung des Services und Zeiteinsparungen. Offenbar waren Vorteile wie Transparenz und Kosteneinsparungen für diese Bürger eher zweitrangig. Dieses Ergebnis wird durch Abbildung 2.8 verdeutlicht.

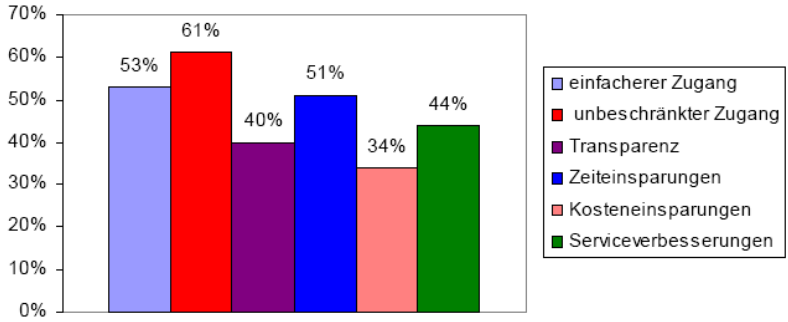


Abbildung 2.8: Vorteile für Bürger laut Umfrage [Bun05a]

Die Wirtschaft legt hier eine etwas andere Gewichtung in die genannten Vorteile. Wie in Abbildung 2.9 zu sehen, sieht die Wirtschaft die Vorteile vor allem in der Zeiteinsparung, in Serviceverbesserungen und in einer vereinfachten Orientierung und dem leichteren Zugang zu Informationen. Der unbeschränkte Zugang zu Verwaltungsdienstleistungen spielt hier eine sehr untergeordnete Rolle.

2.9 Fazit

Das Internet wird momentan von noch nicht einmal 50 Prozent aller Bundesbürger genutzt, von denen ein großer Teil zudem unter 18 Jahren alt ist und damit noch nicht an E-Government-Prozessen teilnehmen darf. Die Erreichbarkeit allein über das Internet reicht daher nicht aus, um Verwaltungsprozesse

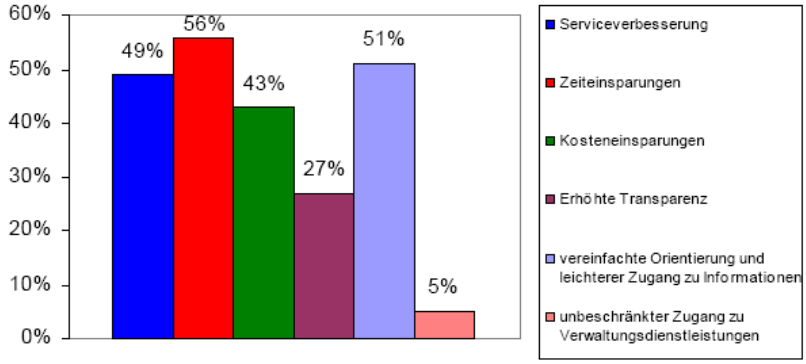


Abbildung 2.9: Vorteile für Wirtschaft laut Umfrage [Bun05b]

umfassend zu reorganisieren und anzubieten. Wichtig wären hierbei das Bereitstellen von Zugangsmöglichkeiten für ein E-Government-System auch durch den Staat, um sich nicht nur auf die privaten Internetzugänge zu verlassen. Zudem sind noch einige Barrieren für bestimmte Bürgergruppen zu überwinden. E-Government kann daher momentan nur ein zusätzliches Angebot sein und ist kein Patentrezept für die Lösung aller Probleme und Schwächen, die die momentane Verwaltungslandschaft prägen.

Zudem wird das Internet laut Umfragen und Studien vor allem für private Zwecke und als Unterhaltungs- und Kommunikationsmedium genutzt. Diese privaten Zwecke müssen gut ausgelotet und erfragt werden, um ein funktionierendes und akzeptiertes E-Government-System zu erstellen. Es werden momentan vor allem Transaktionsprozesse erwartet und die Realisierung kommunaler Dienstleistungen wie KFZ-Ummeldung, An- und Ummeldung usw. Findet diese Art der Nutzerbefragung nicht statt, wird ein eventuelles System leicht am Bürger vorbeikonzipiert werden und ist daher eine Fehlinvestition.

Die Umsetzung eines guten E-Government-Systems ist noch ein weiter Weg, auf dem viele Probleme gelöst und einige Herausforderungen gemeistert werden müssen. Dies wird Zeit und auch Geld brauchen.

Die Akzeptanz von E-Government bleibt weiterhin fraglich. Es ist bekannt, dass technische Entwicklungen der Akzeptanz in der Bevölkerung immer weit voraus sind. Solange die Sicherheit eines solchen Systems nicht gewährleistet ist, wird die Akzeptanz sicherlich ausbleiben, aber auch, wenn alle Sicherheitsaspekte gelöst sind, wird es immer Bürger geben, die solchen Systemen nicht vertrauen und es damit auch nicht akzeptieren.

Literaturverzeichnis

[ARD] ARD/ZDF-PROJEKTGRUPPE MULTIMEDIA: *ARD-Online-Studie 1997, ARD/ZDF-Online-Studien 1998-2005*. `http://www.daserste.de/service/studie.asp`. Stand 14.12.2005.

[Bau04] BAUER, ANDREAS: *E-Demokratie - neue Bürgernähe oder virtuelle Luftblase*. Aus Politik und Zeitgeschichte, Beilage zur Wochenzeitung Das Parlament, B18/2004:3–6, 2004.

[Ber02a] BERTELSMANN STIFTUNG: *10-Punkte-Plan für gutes E-Government - Ein Fahrplan zur Verwaltungsmodernisierung und Stärkung der Bürgergesellschaft*. Technischer Bericht, 2002.

[Ber02b] BERTELSMANN STIFTUNG: *Balanced E-Government: Elektronisches Regieren zwischen administrativer Effizienz und bürgernaher Demokratie (Studie)*. Technischer Bericht, 2002.

[Bun] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *E-Government-Handbuch*. `http://www.bsi.bund.de/fachthem/egov/6.htm`. Stand 17.12.2005.

[Bun05a] BUNDESMINISTERIUM DES INNERN IT-STAB STAB - PROJEKTGRUPPE BUNDONLINE: *Ergebnisse und Schlussfolgerungen der Kundenbefragung zu BundOnline- Dienstleistungsangeboten bei Bürgerinnen und Bürgern*. Technischer Bericht, 2005.

[Bun05b] BUNDESMINISTERIUM DES INNERN IT-STAB STAB - PROJEKTGRUPPE BUNDONLINE: *Ergebnisse und Schlussfolgerungen der Kundenbefragung zu BundOnline- Dienstleistungsangeboten bei der Wirtschaft*. Technischer Bericht, 2005.

[EOS02] EOS GALLUP EUROPE: *Flash Eurobarometer 135 (Studie)*. `http://www.europa.eu.int/comm/public_opinion/flash/fl135_en.pdf`, November 2002. Stand 16.12.2005.

[Uni] UNIVERSUM VERLAG FÜR BUNDESMINISTERIUM FÜR WIRTSCHAFT UND TECHNOLOGIE (STIFTUNG DIGITALE CHANCEN): *Umfrage zur Internetnutzung durch Menschen mit Behinderungen*. `http://www.digitale-chancen.de/transfer/downloads/MD248.pdf`. Stand 17.12.2005.

[Win04] WINKEL, OLAF: *Zukunftsperspektive Electronic Government*. Aus Politik und Zeitgeschichte, Beilage zur Wochenzeitung Das Parlament, B18/2004:7–15, 2004.

[Wor99] WORLD WIDE WEB CONSORTIUM: *Web Content Accessibility Guidelines 1.0 (WAI, Deutsche Übersetzung)*. `http://www.w3.org/Consortium/Offices/Germany/Trans/WAI/webinhalt.html`, Mai 1999. Stand 16.12.2005.

3 Die Bürgerrechte im Internet - Bedrohungen und Schutzmöglichkeiten

Die Bürgerrechte im Internet - Bedrohungen und Schutzmöglichkeiten

Winfried Klinker

22. Januar 2006

Das Internet gewinnt zunehmend mehr Bedeutung innerhalb der Gesellschaft und ist aus dem alltäglichen Leben vieler Menschen nicht mehr wegzudenken. In seiner Form als Nachrichtenmedium sowie durch seine umfangreichen Möglichkeiten der Partizipation und Meinungsäußerung ist es auch für das politische Leben der Bürger von Bedeutung. Daher stellt sich die Frage inwieweit die Bürgerrechte, die jeden Bürger schützen, auch im Internet zur Anwendung kommen. Die wichtigsten Bürgerrechte die im Internet von Bedeutung sind, sind das Recht auf freie Meinungsäußerung, das Fernmeldegeheimnis, die Informationsfreiheit sowie die Vereinigungsfreiheit. Da das Grundgesetz geschrieben wurde, bevor das Internet auch nur zu erträumen war, sind diese Gesetze in einigen Bereichen nicht ausreichend, um als Rechtsgrundlage alle Möglichkeiten, die das Internet bietet, abzudecken.

Durch die Technik des Internets entstehen Bedrohungen für die Bürgerrechte, wie z. B. die Zensur. Staaten, oder andere Institutionen sind eventuell in der Lage, Informationen nach ihren Vorstellungen zu filtern oder gar zu verändern. Dadurch wird es dem Benutzer und Bürger unter Umständen unmöglich, eine fundierte politische Entscheidung zu treffen und er wird in seinen Bürgerrechten verletzt. Eine andere Bedrohung ist vor allem auch die Überwachung seines

Verhaltens im Internet, durch das seine Privatsphäre und sein Persönlichkeitsrecht verletzt werden. Diese Überwachung kann durch Firmen oder anderen Institutionen erfolgen, sie kann aber auch, wie im Falle des Abhörnetzwerkes Echelon, durch Nationalstaaten erfolgen. Bei Echelon handelt es sich um ein Überwachungssystem über das nur wenige gesicherte Informationen bestehen. Es soll in der Lage sein, 90% des gesamten Internetverkehrs zu überwachen und bedroht somit nahezu jeden Internetnutzer in seinen Rechten.

Durch den dezentralen Aufbau des Internets ist es der Bundesregierung gar nicht möglich, ihre Bürger vor allen Bedrohungen durch den Missbrauch der Technik des Internets zu schützen. Daher sind diese selbst verpflichtet sich und ihre Rechte zu schützen. Um die Anonymität im Internet zu schützen können so genannte Anonymisierer und Remailer eingesetzt werden. Außerdem gibt es verschiedene Möglichkeiten wie die Zensur umgangen werden kann, solange dem Nutzer bewusst ist, dass seine Informationen zensiert werden. Des Weiteren kann sich der Bürger durch die Nutzung von kryptographischen Verfahren schützen. Durch den Einsatz von Softwarewerkzeugen kann er seinen Datenverkehr und vor allem seine E-Mail Kommunikation verschlüsseln und somit nur autorisierten Personen zukommen lassen. Außerdem kann auch die Steganographie angewendet werden, bei der Daten innerhalb von anderen Daten versteckt werden.

3.1 Einleitung

Das Internet zeichnet sich nicht nur für einen reinen technischen Wandel verantwortlich, sondern es hat auch zu einem gesellschaftlichen Wandel geführt. Als das Grundgesetz der Bundesrepublik geschrieben wurde, war an das Internet noch nicht zu denken. Dennoch liefert das Grundgesetz durch die Festlegung der allgemeinen Bürgerrechte auch die Grundlage für alle Rechtsangelegenheiten die das Internet betreffen, soweit man Bürger der Bundesrepublik Deutschland ist.

In dieser Ausarbeitung soll untersucht werden welche Rolle die Bürgerrechte in der modernen Informationsgesellschaft spielen und wie mit den Bürgerrechten innerhalb des Internets umgegangen wird. Dabei werden zunächst einmal die bedeutendsten Bürgerrechte die für die Rechtslage im Internet eine Rolle spielen aufgezeigt und sie werden in den Kontext des Internets eingeordnet. Anschließend werden Bedrohungsszenarien aufgezeigt, welche zeigen sollen wie die Bürgerrechte im Internet eingeschränkt werden können. Darauf aufbauend werden Methoden und Wege vorgestellt wie ein Bürger sich gegen diese Einschränkungen schützen kann. Zum Abschluss wird dann eine Zusammenfassung gegeben und ein Fazit gezogen wie die Bürgerrechte im Internet zur Geltung kommen und welche Möglichkeiten zum Schutz und zur Bewahrung dieser Rechte am vielversprechensten sind.

3.1.1 Grundrechte

Das Internet ermöglicht einen weltumspannenden Austausch an Information und Kommunikation. Es erscheint den meisten Menschen dabei auf dem ersten Blick wie ein Raum ohne staatliches Recht. Das Gegenteil ist jedoch der Fall: Trotz aller Anwendungsfragen und Durchsetzungsprobleme im Einzelfall gilt staatliches Recht auch für die Anbieter und Nutzer im Internet. Ausschlaggebend für die Rechtssprechung ist die Person, die in einem Land über eine Niederlassung als lokalen Bezugspunkt der dort geltenden Rechtsordnung verfügt oder deren Wirken in den Geltungsbereich der Rechtsordnung eines Landes fällt und deswegen von dieser auch erfasst wird (vgl. [Biz05]). Wer beispielsweise rechtswidrige Inhalte vom Ausland aus für Nutzer in Deutschland verfügbar macht, kann sich nach deutschem Recht strafbar machen. Es kann daher also keine Rede davon sein, dass das Internet ein rechtsfreier Raum sei.

Die Grundrechte des Grundgesetzes (vgl. [Was05]) gelten also für Anbieter und Nutzer von Information und Kommunikation im Internet. Staatliche Reglementierungen des Internets müssen sich demnach an die Grundgesetze halten und dürfen die Bürgerrechte des Nutzers auch im Internet nicht verletzen.

Die Grundrechte verhalten sich zu den medialen Formen ihrer Ausübung neutral. Das heißt sie schützen jede Form der Freiheitsausübung, auch in elektronischen Netzen. Die Grundrechte sollen die Freiheit der Menschen schützen, nicht aber bestimmte Lebensformen bevorzugen, weshalb sich ihre Schutzgehalte mit dem Wandel von Technik und Lebensformen weiterentwickeln müssen. Das bedeutet das die Grundrechte grundsätzlich auch einem Wandel unterzogen seien müssen und das sie sich an neue technische und kulturelle Entwicklungen anzupassen haben.

Im Folgenden sollen die wichtigsten Grundrechte die für den Kontext des Internets von Bedeutung sind kurz dargestellt werden.

Recht auf freie Meinungsäußerung

> Art. 5 GG
>
> 1. Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten (. . .)
>
> 2. Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutz der Jugend und in dem Recht der persönlichen Ehre.

Das Grundrecht auf Schutz der Meinungsäußerungsfreiheit soll sicherstellen, dass jeder frei das sagen kann, was er denkt, ohne dass er hierfür Gründe anführen muss. Das Grundrecht ist eine Voraussetzung für die Meinungsbildung und die mediale Form der Äußerung ist für das Grundrecht nicht von Belang. Es gilt für jeden Nutzer, der sich im Internet äußert und darstellt und es macht keinen Unterschied für den grundrechtlichen Schutz gegen staatliche Eingriffe, ob sich der Nutzer in öffentlichen oder geschlossenen Foren und Gruppen des Internets äußert. Die Freiheit der Meinungsäußerung gilt auch für die private Kommunikation. Dieses Recht kann nur eingeschränkt werden wenn z. B. der Jugendschutz gefährdet wird.

Fernmeldegeheimnis

> Art. 10 Abs. 1 GG
> Das Briefgeheimnis sowie das Post-und Fernmeldegeheimnis sind unverletzlich.

Das Fernmeldegeheimnis hat eine lange Tradition und wurde zunächst nur in das Verfassungsrecht geschrieben. Im Zuge der Einführung des Grundgesetzes wurde es in dieses übernommen. Im digitalen Zeitalter ist Schutzgegenstand des Fernmeldegeheimnisses die Vertraulichkeit der elektronisch vermittelten Kommunikation. Es schützt die Inhalte und Verbindungsdaten aus der und über die Kommunikation der Teilnehmer einschließlich der erfolglosen Verbindungsversuche. Als individuelles Recht auf Schutz der Vertraulichkeit umfasst es auch das Recht des Einzelnen, seine Nachrichten unabhängig von Dienstleistern der Telekommunikation und staatlichen Vorgaben selbst zu ver- und entschlüsseln.

Informationsfreiheit

> Art. 5 Abs. 1 Satz 1 GG [Informationsfreiheit]
>
> 1. Jeder hat das Recht, (. . .) sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.

Als Grundrecht schützt die Informationsfreiheit des Einzelnen den ungehinderten Zugang zu allgemein zugänglichen Informationen. Allerdings vermittelt dieses Recht keinen Anspruch auf Informationen, die der Staat unter Verschluss hält, sondern nur einen Anspruch auf ungehinderte Information aus bereits „allgemein zugänglichen“ Quellen. In Verbindung mit dem Gleichheitssatz (Art. 3 Abs. 1 GG) besteht aber ein Anspruch gegen den Staat, zumindest auch die Informationen zur Verfügung gestellt zu bekommen, die Dritten bereits zur Verfügung gestellt worden sind.

Vereinigungsfreiheit

Art. 9 Abs. 1 Satz 1 GG

1. Alle Deutschen haben das Recht, Vereine und Gesellschaften zu bilden.

Bedeutung kann im Internet auch das Grundrecht auf die Bildung von Vereinen und Gesellschaften gewinnen, das allerdings nur ein Deutschen vorbehaltenes Recht ist. Zu denken ist an virtuelle Vereine, die sich als geschlossene Benutzergruppe zu einem bestimmten Zweck bilden und betätigen. Entsprechendes gilt für die Gründung einer Vereinigung zu wirtschaftlichen Zwecken. Als Folge dieses Grundrechts wird beispielsweise zu prüfen sein, ob und unter welchen Voraussetzungen das geltende Vereinsrecht virtuelle Mitgliederversammlungen zulassen muss. Im Gesellschaftsrecht hat die Entwicklung virtueller Hauptversammlungen bereits begonnen.

Fraglich ist, ob das Grundrecht der Versammlungsfreiheit für elektronische Kommunikation Bedeutung haben kann. Dieses Grundrecht soll die Versammlung von Personen zu Zwecken gemeinsamer Kommunikation ermöglichen. In der Tradition politischer Demonstrationen zielt dieses Grundrecht auf eine reale Versammlung von Personen. Ein Schutz virtueller Versammlungen durch das Grundrecht ist jedoch nicht ausgeschlossen. Denkbar ist eine Konstellation, in der sich Netzbürger virtuell in einem Forum zu einem bestimmten Zweck einloggen, um auf diese Weise „versammelt“ ihre Meinung zu äußern. Allerdings entfaltet die Versammlungsfreiheit nur Schutzwirkungen, wenn die Versammlung „friedlich und ohne Waffen“ erfolgt. Die gemeinschaftliche Blockade einer Webseite wäre unter dieser Voraussetzung beispielsweise keine grundrechtlich geschützte Versammlung. Im Übrigen kommt die Meinungsäußerungsfreiheit auch ohne Anwendung der Versammlungsfreiheit zur Anwendung, natürlich in den Schranken der zum Schutz der Rechte Dritter geltenden Gesetze.

3.2 Bedrohung der Bürgerrechte

Im Folgenden sollen Bedrohungen aufgeführt werden, die durch das Internet entstehen oder genutzt werden können, welche die Grundrechte eines Bürgers einschränken können.

3.2.1 Zensur

Da es sich bei dem Internet auch um ein Nachrichtenmedium handelt und es ein offenes Forum für alle Bürger bietet, besteht grundsätzlich die Gefahr, dass es zu Zensur seitens des Staates oder auch anderer Organisationen kommen kann. Zensur bedeutet Informationen oder andere durch Medien vermittelte Inhalte zu kontrollieren, zu unterdrücken oder im eigenen Sinn zu steuern. Dabei werden vor allem Nachrichten, künstlerische Äußerungen und Meinungsäußerungen zum Gegenstand der Zensur. Sie dient überwiegend dem Ziel, das Geistesleben in politischer, sittlicher oder religiöser Hinsicht zu kontrollieren (vgl. [Die05]).

Die Zensur wird meist durch die folgenden technischen Methoden bewerkstelligt:

- Per DNS-Server geblockte URL's
  Dabei werden bestimmte URL's blockiert so das der Client diese nicht mehr aufrufen kann.
- Zwangsproxy / Transparenter Proxy
  Der Nutzer wird über einen Proxyserver mit dem Internet verbunden. Dies kann auch transparent geschehen, das bedeutet, dass der Nutzer sich dessen nicht bewusst ist. Dieser Proxy Server filtert dann die aufgerufenen Webseiten oder leitet den Nutzer auf andere Webseiten um.
- Wortfilter
  Durch den Wortfilter werden die von Nutzer aufgerufenen Webseiten ge-

parst und falls sie Wörter enthalten die als zensiert markiert sind, wird die entsprechende Webseite blockiert.

- Portsperren
  Es werden bestimmte Ports gesperrt, so dass die entsprechenden Services die diese Ports nutzen, wie z. B. Newsgroups, nicht mehr zugänglich sind.

Daraus, dass im Internet keine Staatsgrenzen existieren, ergibt sich eine hohe Komplexität rechtlicher Fragen, da Unvereinbarkeiten zwischen Rechtssystemen nicht lösbar sind. Regierungen und staatliche Organe können durch das Sperren von Webseiten, die in ihrem Rechtsbereich liegen, auch die Bürger anderer Staaten von diesen Informationen abhalten, jedoch können sie nicht verhindern, dass die Bürger sich Zugang zu illegalen Informationen verschaffen, die im Ausland liegen.

In Deutschland sind zum Beispiel die Verherrlichung der NS-Kriegsverbrechen oder auch die Verleugnung des Holocausts verboten. Auf US-Servern hingegen können diese Dinge ungestraft verbreitet werden, da sie im US-Recht von der Meinungsfreiheit abgedeckt werden.

Die Meinungsunterdrückung ist im Internet oftmals leichter zu realisieren als dies in anderen Medien der Fall ist. Obwohl es technisch schwierig ist, die gesamte Bandbreite der Angebote im Internet zu zensieren, ist es vor allem in autoritär regierten Staaten möglich, dies leicht zu erreichen. Diese Staaten sind meist zentralistisch organisiert und aufgrund ihrer schwächeren Wirtschaftskraft gibt es meist nur wenige technische Verbindungen zum Ausland, die sich daher auch leicht kontrollieren lassen. Dabei wird der Zugang zum Internet über so genannte Proxy Server hergestellt die von der Regierung nicht erwünschte Seiten sperren und so den Nutzer daran hindern sich aus unabhängigen Nachrichtenquellen zu informieren oder seine Meinung in Foren zu äußern.

Ein Beispiel für eine derart praktizierte Zensur im Internet ist China. In China erfolgt der Anschluss des gesamten Landes an das Internet über 8 zentrale Knotenpunkte. Diese werden von der Regierung betrieben und stellen den einzigen Weg zu ausländischen Adressen her. Dadurch ist die Regierung in der Lage Inhalte zu zensieren und an dieser Stelle zu blockieren.

Aber auch viele andere Länder schränken den Zugriff auf das Internet ein, dies ist nicht immer nur in autoritär regierten Staaten der Fall. Es gibt sie z. B. auch in Deutschland. Im Februar 2004 zensierte der Internetdienstanbieter Freenet.de Webseiten, die sich kritisch zu dem Unternehmen äußerten, indem er einen Teil der Nutzer seines Dienstes, die versuchten, die unternehmenskritischen Seiten aufzurufen, auf andere Webseiten umlenkte. Technisch wurde dies durch einen transparenten Proxy realisiert der für den Kunden des Unternehmens nicht zu erkennen war. Für den Kunden war es nicht möglich die betreffenden Webseiten aufzurufen, was gegen die zuvor aufgeführten Rechte des Grundgesetzes verstößt. Freenet begründete die Zensur mit Markenrechtsverletzungen auf den gesperrten Seiten, beseitigte die Sperre aber nach Protesten.

Ein anderer Weg der Zensur besteht darin, mit juristischen Mitteln kritische Informationen zu unterbinden. Ein Beispiel hierfür ist z. B. die Sekte Scientology, die versucht gerichtlich gegen Webseiten vorzugehen die sich kritisch gegen die Sekte äußern und diese vom Netz zu nehmen. Aber auch Suchmaschinen wie Google haben und nutzen die Möglichkeiten zur Zensur. Ohne die Aufnahme einer Webseite in den Index einer Suchmaschine können Webseiten vom Benutzer auch nur schwer gefunden werden. Die Suchmaschinenbetreiber haben somit grundsätzlich einen großen Einfluss auf die Inhalte, da sie zumindest technisch sehr leicht in der Lage sind, von ihnen unerwünschte Seiten wie z. B. die Angebote von Konkurrenzunternehmen aus ihrem Index zu entfernen.

3.2.2 Überwachung

Eine weitere Bedrohung für die Rechte der Bürger die ebenfalls zusammen mit der Zensur einhergeht ist die Überwachung bzw. Ausspionierung der Bürger. Anders als bei der Zensur wird der Bürger nicht aktiv an der Partizipation gehindert aber er wird in seinen Persönlichkeitsrechten eingeschränkt. Außerdem wird durch die Überwachung der Internetaktivitäten eines Nutzers auch das Fernmeldegeheimnis verletzt.

Vor allem Unternehmen setzen spezielle Software, so genannte Spyware, ein welche das Nutzungsverhalten des Bürgers ohne sein Wissen analysieren. Die Spyware zeichnet dabei Webseiten auf die der Nutzer besucht und versucht zusammen mit dem auf dem Computer gespeicherten Daten ein Profil des Nutzers zu erstellen (vgl. [Gol05]). Dies wird meist für Werbezwecke genutzt, das heißt das die Werbung speziell auf die Bedürfnisse des Kunden anpasst werden soll, so das diese effektiver ist. Außerdem wird durch Spyware untersucht ob Lizenzverstöße oder das Urheberrecht verletzt wurden.

3.2.3 Echelon

Echelon ist der Name eines Spionagenetzes das von den Staaten USA, Großbritannien, Kanada, Australien und Neuseeland betrieben wird (UKUSA Allianz) [Bun05]. Anders als Spyware ist es mit diesem Netz auch möglich weitere Kommunikationswege wie z. B. Telefone abzuhören. Das Wissen über Echelon ist begrenzt, da es als geheim eingestuft ist, seine Existenz ist aber mittlerweile bewiesen.
Zunächst war Echelon nur dazu gedacht, die militärische und diplomatische Kommunikation der Sowjetunion und ihrer Verbündeten abzuhören, jedoch wird es heute, nach dem Ende des Kalten Krieges, zur Suche nach terroristischen Verschwörungen, Aufdeckungen im Bereich Drogenhandel und als politischer und diplomatischer Nachrichtendienst benutzt. Kritiker behaupten außerdem, dass dieses System hauptsächlich der Wirtschaftsspionage diene.

Ein Beispiel für die Wirtschaftsspionage ist der Fall Enercon (siehe [Rav05]). Der deutsche Windenergieanlagenhersteller Enercon GmbH hatte den neuen, preiswerten Windkraftanlagentyp E-40 entwickelt, der auch für den amerikanischen Exportmarkt von Bedeutung war. Wie sich durch eine Recherche des Plusminus-Magazins der ARD und einer Sendung am 14. April 1998 herausstellte, hatte die NSA durch Echelon die Daten und Konferenzen, die per Satellit und Telefonleitungen zwischen dem Forschungslabor und der Fabrikationsanlage Enercons übertragen wurden, abgehört, Forschungsdaten und die Sicherheits- und Zugangscodes der E-40 abgefangen und damit ein Agenten-

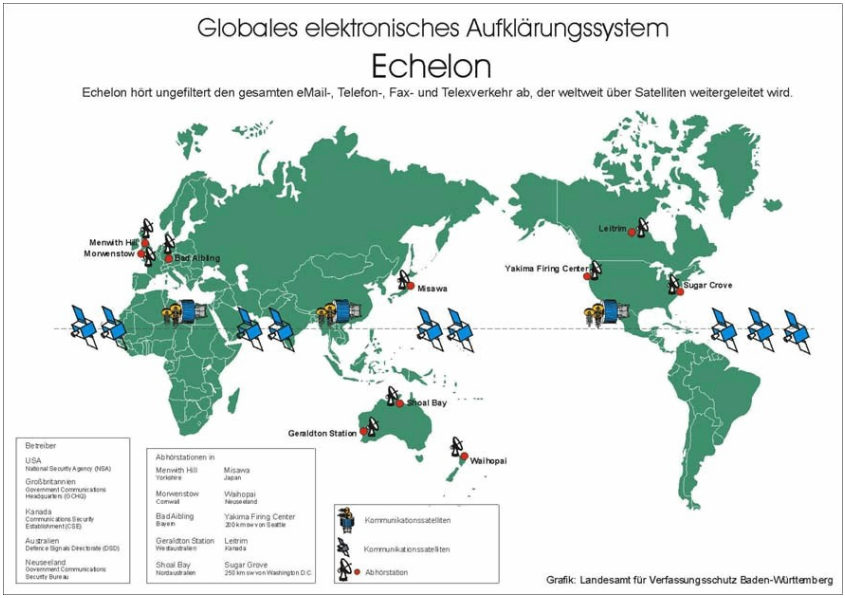


Abbildung 3.1: Echelon Weltkarte

team ausgestattet. Das Agententeam konnte mit Hilfe der Daten die Sicherheitssperren einer E-40 Anlage ausschalten und so die eigentlichen Betriebsmechanismen analysieren und fotografieren. Die gewonnenen Erkenntnisse gab die NSA an die amerikanische Konkurrenzfirma Kenetech weiter, die daraufhin flugs die Neuentwicklung Enercons als eigenes Patent anmeldete und Enercon daraufhin gerichtlich untersagte, die darauf basierenden Produkte auf dem US-Markt zu vertreiben. Für Enercon ergab sich aufgrund des Echelonangriffs ein Verlust in Höhe von 100 Millionen DM.

Das Echelonsystem ist einfach im Aufbau. Alle Mitglieder der englischsprachigen Allianz sind Teil der nachrichtendienstlichen Allianz UKUSA, deren Wurzeln bis zum Zweiten Weltkrieg zurückreichen. Diese Staaten stellten Abhörsta-

tionen und Weltraumsatelliten auf, um Satelliten-, Mikrowellen-, Mobilfunk- und Glasfaserkabel- Kommunikation abzuhorchen. Die eingefangenen Signale werden durch eine Reihe Supercomputer verarbeitet, die dazu programmiert wurden, Zieladressen, Wörter, Sätze oder sogar individuelle Stimmen zu erkennen. Dabei soll es mittlerweile sogar möglich sein, nach ganzen Sachverhalten zu suchen und nicht nur nach einzelnen Schlagwörtern. Das Echelon-System unterliegt der Verwaltung der National Security Agency (NSA) der USA.

Die neue geheimdienstliche Priorität ist die Wirtschaftsspionage, wodurch die Mitglieder der Allianz, allen voran die USA, einen erheblichen wirtschaftlichen Vorteil haben. Das Internet ist hierbei eine wahre Goldgrube für die Geheimdienste, denn die allermeisten Datenpakete passieren das Netz unchiffriert. Es gibt Schätzungen, nach denen die Geheimdienste generell etwa 40% ihrer Informationen „offenen Quellen“ entnehmen (und diese dann geschickt verknüpfen und auswerten). Dazu zählt auch Traffic Analysis, wobei die Verkehrsdaten des Internet untersucht werden um ein Profil der Nutzer zu erstellen. Zurzeit ist es dabei anscheinend aber noch nicht möglich den Inhalt all dieser Daten zu analysieren, aber alleine durch die Rahmenpackete mit ihren Metadaten wie Uhrzeit usw., lassen sich bereits vielfältige Informationen gewinnen.

Das Echelon System soll über ca. 120 Landstationen verfügen, eine davon wird in Deutschland, in Bad Aibling (Bayern) betrieben. Das System überwacht die Kommunikation zwischen Bodenstationen und ihren Satelliten sowie alle wichtigen Unterseekabel. Dadurch soll es in der Lage sein, ca. 90% des weltweiten Internetverkehrs zu überwachen (vgl. [Wik05]). Hinzu kommt die Überwachung eines Großteils des mobilen Verkehrs.

3.3 Schutz

Wie zuvor gezeigt wurde gibt es durchaus ernstzunehmende Bedrohungen für die Bürgerrechte durch den technologischen Wandel und die Möglichkeiten des Internets, die durch den Staat oder andere Organisationen ausgenutzt werden können. Daher sollen an dieser Stelle Möglichkeiten aufgezeigt werden, wie

sich Bürger gegen diese Eingriffe schützen können und was dabei zu beachten ist. Hierbei handelt es sich allen voran um technische Methoden. Andere Wege zum Schutz seiner Rechte wie juristische Mittel werden an dieser Stelle außen vor gelassen.

Grundsätzlich sollte man als Nutzer des Internets über eine Firewall auf seinem Rechner verfügen die schädlichen Datenverkehr aus dem Internet blocken kann. Außerdem sollte ein aktueller Virenscanner installiert sein der in regelmäßigen Abständen aktualisiert werden sollte. Des Weiteren ist der Einsatz von Anti-Spyware Produkten sinnvoll, welche Spyware Programme auf dem Rechner aufspüren und diese löschen. Somit ist gewährleistet, dass keine ungewollten Informationen nach außen dringen können.

3.3.1 Anonymisierer

Ein Anonymizer ist ein System, das Benutzern hilft, ihre Anonymität im Internet, vor allem im World Wide Web, zu wahren. Anonymizer sollen dabei helfen Datenschutz und Datensicherheit beim Surfen zu bewahren. Ein Anonymizer wird als ein so genannter Proxy zwischen Benutzer und Zielrechner geschaltet. Da nun der Proxy anstelle des Benutzers mit dem Zielcomputer kommuniziert, kann die Verbindung zum ursprünglichen Nutzer nicht ohne weiteres zurückverfolgt werden. Dazu ist es allerdings nötig, dass es sich um einen anonymen Proxy handelt und nicht um einen regulären Proxy, der per Header mitteilt, dass die Anfrage von einem Proxy kommt und welcher Client anfragt. Üblicherweise wird der Datenstrom zwischen Nutzer und Anonymizer verschlüsselt, um ein Abhören der Verbindung zwischen Nutzer und Proxy zu verhindern. Dabei wird vorausgesetzt, dass möglichst viele Nutzer denselben Proxy gleichzeitig nutzen, damit einzelne Verbindungen nicht zu bestimmten Nutzern zugeordnet werden können. Viele bekannte Anonymizer setzen auf das SSL oder SOCKS Protokoll und können daher mit einer Vielzahl von Anwendungen verwendet werden, nicht nur beim normalen Websurfen.

Bei Systemen mit nur einem Proxyserver hängt die Sicherheit von der Vertrauenswürdigkeit des Proxyrechners ab: Wird dieser korrumpiert, oder arbeitet er gar absichtlich gegen den Nutzer, so ist das ganze System gebrochen. Moderne Anonymizer setzen daher auf mehrere hintereinander geschaltete Proxys, so genannte Mix-Kaskaden. Hier werden die Daten mehrfach verschlüsselt und durch mehrere Rechner geleitet, wobei pro Rechner eine Verschlüsselung entschlüsselt wird. Erst am Ende der Mix-Kaskade werden die Daten lesbar. Da die Verbindungsdaten verschiedener Benutzer an jedem Glied der Kaskade neu gemischt werden, ist eine eindeutige Zuordnung jedoch unmöglich. Nur ein Angreifer, der alle Rechner in einer Mix-Kaskade kontrolliert, kann den Datenverkehr überwachen. Selbst wenn nur ein einziger Mix unversehrt bleibt, bleibt das Gesamtsystem sicher.

Ein bekanntes deutsches Produkt ist der Java Anon Proxy (JAP) der TU Dresden [Tec05]. Der JAP funktioniert, da er in der Programmiersprache Java geschrieben wurde, auf nahezu allen Plattformen.

3.3.2 Remailer

Um anonyme E-Mails versenden zu können oder anonym Usenet-Postings zu erstellen, benutzt man so genannte Remailer. Diese funktionieren ähnlich wie ein Proxy, nur das sie für den E-Mail Verkehr angewendet werden. Eine Nachricht wird von dem Remailer weiterversendet, so dass dieser als Absender auftaucht, wobei der Remailer den Proxy darstellt. Es wurden verschiedene Technologien entwickelt, um Remailer-Dienste zu realisieren. Die momentan im Internet anzutreffenden Remailer-Dienste verwenden entweder das Cypherpunk- oder das Mixmaster-Protokoll. Während ersteres einen reinen Weiterleitungsdienst definiert, der durch Verschlüsselungssysteme zusätzlich abgesichert werden muss, etabliert Mixmaster von Haus aus ein hochsicheres Remailer-Netz. Eine Mischform der beiden Remailer-Typen stellen sog. Hybrid-Remailer dar. Diese Remailer Clients bieten aufgrund der Verschlüsselung ausreichend Sicherheit und ermöglichen somit ein sicheres und anonymes Senden von Nachrichten.

Neben den lokal installierten Remailer Clients gibt es eine Reihe von Remailer Clients, die in webbasierter Form angesprochen werden. Generell sind Remailer Clients auf dem heimischen Rechner den webbasierten Remailer Clients vorzuziehen, da meistens die Nachricht schon als Klartext eingegeben und über HTTP übertragen wird. Außerdem werden auf dem Webserver die Zugriffe in Logfiles festgehalten und vom Browser Identifikationsmerkmale übertragen. Werden webbasierte Remailer Clients verwendet, sollten mindestens anonymisierende Proxy zwischen Browser und WWW-Remailer Client geschaltet werden. Besser sind aber Proxys und WWW-Remailer Clients, die SSL Verschlüsselung anbieten.

3.3.3 Umgehung der Zensur

Um der Zensur im Internet zu entgehen gibt es einige Möglichkeiten, die jedoch nicht immer ausreichend sein können. In vielen Fällen ist der Nutzer gegen Zensur machtlos, in einigen Fällen merkt er sogar noch nicht einmal das Informationen zensiert wurden. Aus technischer Sicht hat der Benutzer folgende Möglichkeiten (vgl. [Fre05]) eine Zensur zu umgehen:

- Nutzung eines nicht zensierten DNS Servers
  Wenn die Zensur auf Basis eines Zensierenden DNS Servers besteht, ist es möglich diesen zu ersetzen. Der Nutzer ist nicht auf den DNS Server seines Providers angewiesen und kann selbstständig einen anderen DNS Server nutzen. Es gibt im Internet Listen mit DNS Server die nicht zensieren.
- IP statt URL nutzen
  Wenn die IP einer gesperrten Seite bekannt ist (z. B. durch die Veröffentlichung dieser auf einer nicht zensierten Seite) kann auch die IP direkt für den Aufruf der Webseite genutzt werden. Somit wird ebenfalls die Zensur auf Basis von DNS Servern umgangen.
- Spiegeln von Webseiten
  Oftmals werden Seiten, von denen bekannt ist das sie in einigen Ländern zensiert sind, gespiegelt, das heißt sie werden auf einem anderen Server

unter einer anderen Adresse ebenfalls angeboten. Nutzer können somit auf diese gespiegelten Seiten zugreifen bis diese ebenfalls zensiert werden.

Wenn die Zensur über Wortfilter realisiert ist, gibt es keine Möglichkeit diese so einfach überwinden und der Nutzer ist von seiner Position am Ende der Informationskette machtlos.

3.3.4 Einsatz von Kryptographie

Um sich vor Überwachung zu schützen, sowie zum Schutz der Privatsphäre allgemein, sollte jedwede Kommunikation durch Kryptographie gesichert werden. Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen und befasst sich damit, die Kommunikation an sich zu verschleiern und vor allem damit, den Inhalt von Nachrichten für Dritte unzugänglich zu machen. Die moderne Kryptographie hat vier Hauptziele:

1. Vertraulichkeit der Nachricht: Nur der gewünschte Empfänger sollte in der Lage sein, den Inhalt einer verschlüsselten Nachricht zu lesen. Weiterhin sollte es nicht möglich sein, Information über den Nachrichteninhalt zu erlangen (beispielsweise eine statistische Verteilung bestimmter Zeichen).
2. Datenintegrität der Nachricht: Der Empfänger sollte in der Lage sein festzustellen, ob die Nachricht seit ihrer Übertragung verändert wurde.
3. Authentifizierung: Der Empfänger sollte den Absender eindeutig identifizieren können. Weiterhin sollte es überprüfbar sein, ob die Nachricht tatsächlich von diesem Absender stammt.
4. Verbindlichkeit: Der Absender sollte nicht in der Lage sein zu bestreiten, dass er die Nachricht gesendet hat.

Nicht alle kryptographischen Systeme und Algorithmen erreichen alle oben genannten Ziele. Manche Ziele sind nicht praktikabel (oder notwendig) in gewis-

sen Umgebungen und benötigen hoch entwickelte und rechenintensive Algorithmen.

Man unterscheidet in der Kryptographie zwischen symmetrischen und asymmetrischen Verfahren. Bei symmetrischen Verfahren wird zum Ver- und Entschlüsseln derselbe Schlüssel verwendet. Daher muss der Schlüssel zwischen den Kommunikationspartnern über einen sicheren Weg ausgetauscht werden, wie beispielsweise einem vertrauenswürdigen Kurier oder dem direkten Treffen der Kommunikationspartner. Dies lässt sich bei der Kommunikation im Internet nicht bewerkstelligen, da die einzelnen Kommunikationspartner räumlich meist weit entfernt sind und sich untereinander nicht kennen. Außerdem ist dieses

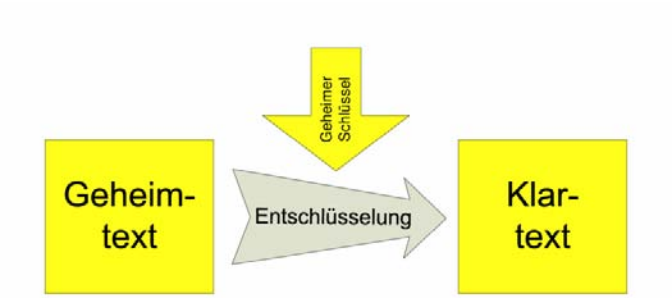


Abbildung 3.2: Entschlüsselung (Asymmetrisches und Symmetrisches Verfahren)

System bei der hohen Frequenz der Kommunikation nicht praktikabel. Zudem wird ein jeweils neuer Schlüssel für jeden Kommunikationspartner benötigt, wenn die anderen Teilnehmer nicht in der Lage sein sollten die Nachrichten zu entschlüsseln. Dieses System der symmetrischen Verschlüsslung wird daher auch als Private Key Kryptographie oder Shared Secret bezeichnet. Es kann daher nur eingesetzt werden, wenn die Anzahl der an der Kommunikation beteiligten Personen gering ist und zwischen ihnen ein sicherer Weg zum Austausch

des Schlüssels besteht. In Abbildung 3.2 ist die Verschlüsselung mithilfe eines symmetrischen Schlüssels dargestellt.

Beim asymmetrischen Verfahren, der so genannten Public Key Kryptographie wird ein Paar zusammenpassender Schlüssel eingesetzt. Der eine ist ein öffentlicher Schlüssel, der zum Verschlüsseln benutzt wird. Der andere ist ein privater Schlüssel, der geheim gehalten werden muss und zur Entschlüsselung eingesetzt wird. Mit dieser Methode wird nur ein einziges Schlüsselpaar für jeden Empfänger benötigt, da der Besitz des öffentlichen Schlüssels die Sicherheit des privaten Schlüssels nicht aufs Spiel setzt. Im Allgemeinen ist ein solches System nicht umkehrbar, d. h. eine Nachricht, welche mit dem privaten Schlüssel verschlüsselt wurde, kann nicht mit dem öffentlichen Schlüssel entschlüsselt werden. Abbildung 3.3 stellt den Verschlüsselungsvorgang mithilfe eines öf-

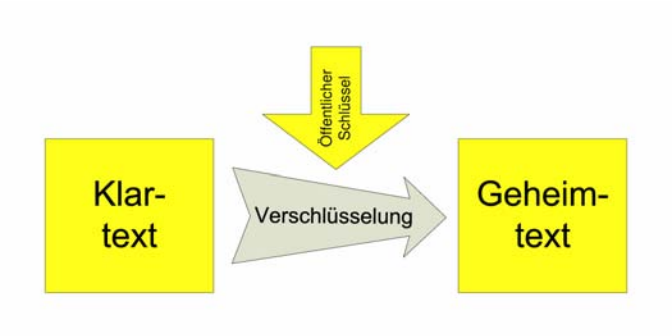


Abbildung 3.3: Verchlüsselung mit dem asymmetrischen Verfahren

fentlichen Schlüssels dar. Die Entschlüsselung erfolgt wie bereits in Abbildung 3.2 dargestellt mit dem privaten Schlüssel, genau wie beim symmetrischen Verfahren.

Für den privaten Einsatz gibt es zahlreiche Verschlüsselungsprogramme die unter anderem dabei helfen die eigene E-Mail Kommunikation abzusichern. Einige wichtige Programm für sicheren Datenverkehr sind im Folgenden aufgelistet:

- GnuPG
  GnuPG ein Programm, mit dem man auch lokal auf der eigenen Festplatte alle Dateien verschlüsseln kann. Besondere Bedeutung hat GnuPG aber für den verschlüsselten Austausch von E-Mails, Instant Messaging Chats und Kurznachrichten. Darüber hinaus kann man mit GnuPG Texte in Klarform (Faxe, E-Mails) oder Programme mit einer digitalen Signatur versehen, um auch im elektronischen Bereich, in dem eine handschriftliche Unterschrift nicht möglich ist, die Überprüfung der Authentizität elektronisch vorliegender Texte und Daten zu ermöglichen.
- Quicksilver
  Quicksilver ist ein freier Remailer-Client für Windows zur Benutzung von Mixmaster und Cypherpunk Remailern, der zudem die Verschlüsselung erlaubt.
- SFTP
  SFTP ist die Abkürzung für „Secure File Transfer Program“, einem interaktiven Dateitransferprogramm ähnlich FTP, mit dem der User vor dem eigentlichen Transfer Verzeichnisse und deren Inhalt auf dem Server einsehen und Kommandos auf dem Server ausführen kann.

3.3.5 Einsatz von Steganographie

Neben der reinen Verschlüsselung von Daten gibt es eine zweite Methode, um unautorisierten Datenzugriff zu vermeiden - die Steganographie. Über steganographische Algorithmen ist es möglich, die Bits einer Datei zwischen den Bits einer Bild- oder Tondatei zu verstecken. Äußerlich betrachtet ergibt sich zwischen der Rohdatei und der steganographisch behandelten Bild- oder Tondatei bei guten steganographischen Programmen kein erkennbarer Unterschied.

Das Wort „Steganographie“ kommt aus dem Griechischen und heißt übersetzt „verborgenes Schreiben“. Die Sicherheit einer geheimen steganographischen Botschaft liegt darin, dass dem Angreifer die Existenz einer solchen nicht auffällt. Im Gegensatz zur Kryptographie, bei der eine Botschaft verschlüsselt wird, versucht die Steganographie, eine Botschaft dadurch vor dem Zugang

Unbefugter zu schützen, dass für den nicht eingeweihten Betrachter nicht erkennbar ist, dass eine versteckte Botschaft überhaupt vorhanden ist.

Durch eine Kombination beider Techniken wird somit eine größere Sicherheit gewährleistet. Mithilfe der Steganographie kann man sich eventuell vor Überwachung schützen und seine Privatsphäre absichern. Selbst das Echelon System ist vermutlich nicht ohne genauere Hinweise in der Lage, Informationen die z. B. in einem Bild innerhalb einer E-Mail verborgen sind, zu finden.

Die Folgende Liste enthält einige Beispiele von Programmen, die für die Steganographie verwendet werden können:

- F5
- Camouflage
- MP3Stego
- Masker 5.0

Die Programme können von [Sei05] heruntergeladen werden. Diese sind leicht zu bedienen und erlauben das Verstecken von Informationen in verschiedenen Datendateien (je nach Programm unterschiedlich), wie z. B. Jpeg Bildern und mp3's.

3.4 Fazit

Das Internet ist kein rechtsfreier Raum, es gelten die Rechte des Landes des jeweiligen Nutzers. Dadurch ergibt sich, das in Deutschland bei allen Handlungen im Internet die Bürgerrechte die im Grundgesetz festgelegt sind zur Anwendung kommen. Diese Freiheitsrechte lassen sich im virtuellen Raum durch technische Maßnahmen leichter einschränken als das im normalen Leben der Fall ist. Die Überwachung von Personen und das Eindringen und Verletzten ihrer Privatsphäre kann dabei enorme Ausmaße annehmen. Viele Nutzer sind sich ihrer Rechte nicht immer bewusst. Einige Einschränkungen wie z. B. die Zen-

sur, sind nicht ohne weiteres als solche zu erkennen, da sie durch technische Maßnahmen, wie die Nutzung eines transparenten Proxy, verschleiert werden. Durch Spyware wird vor allem durch Unternehmen versucht gezielt ein Profil des Nutzers zu erstellen und dieses meist für Werbezwecke zu nutzen. Viele dieser Programme sind nicht mit den Gesetzen des Grundgesetzes vereinbar, da sie z. B. das Fernmeldegeheimnis brechen.

Die Bürgerrechte werden aber auch von anderen Regierungen bedroht, wie am Beispiel des Überwachungs- und Spionagenetzwerkes Echelon zu sehen ist. Dabei wird ein Großteil der weltweiten Kommunikation überwacht und die gewonnenen Informationen werden oftmals zur Wirtschaftsspionage eingesetzt. Die Regierung der Bundesrepublik schützt ihre Bürger nicht aktiv und ist im gewissen Maße auch an der Überwachung und Spionage beteiligt.

Daher liegt es in der Verantwortung der Bürger, selber für die Durchsetzung ihrer Rechte zu sorgen. Zu einem gewissen Grad kann dies schon durch den Einsatz einfacher Mittel wie Anonymisierer und Remailern erreicht werden. Es gibt heute bereits eine Vielzahl von freien und somit auch kostenlosen Programmen, die zur Verschlüsselung der eigenen Kommunikation eingesetzt werden können. Durch diese leicht zu implementierenden Maßnahmen wird es zumindest schwieriger für Außenstehende, seien es Regierungen, Unternehmen oder Privatpersonen, die eigene Privatsphäre zu verletzen.

Literaturverzeichnis

[Biz05] BIZER, JOHANN: *Grundrechte im Netz - Von der freien Meinungsäußerung bis zum Recht auf Eigentum*. http://www.bpb.de/files/FPQOF9.pdf, Oktober 2005.

[Bun05] BUNDESZENTRALE FÜR POLITISCHE BILDUNG: *Echelon*. http://www.bpb.de/popup/popup_druckversion.html?guid=U3P11A, Oktober 2005.

[Die05] DIETRICH, MANUEL: *Zensurmethoden*. http://www.datenreise.de/de/censorship/zensurmethoden.php#freeDNS, Oktober 2005.

[Fre05] FREERK: *HOWTO: Internetzensur umgehen*. http://www.zensur.freerk.com/index-de.htm, Oktober 2005.

[Gol05] GOLTZSCH, PATRIK: *Anonymität im Internet*. http://www.bpb.de/files/D9AWDO.pdf, Oktober 2005.

[Rav05] RAVEN, KAI: *Echelon - Das globale Abhörnetzwerk*. http://kai.iks-jena.de/miniwahr/echelon-index.html, Oktober 2005.

[Sei05] SEIBOLD, MICHAEL: *Cipherbox*. http://www.cipherbox.de/down-stegano.html, Oktober 2005.

[Tec05] TECHNISCHE UNIVERSITÄT DRESDEN: *JAP - Anonymity and Privacy*. http://anon.inf.tu-dresden.de/index.html, Januar 2005.

[Was05] WASSERMANN, RUDOLF: *Das Grundgesetz - Anspruch und Verpflichtung*. http://www.bpb.de/files/I6VE0P.pdf, Oktober 2005.

[Wik05] WIKIPEDIA: *Echelon*. `http://de.wikipedia.org/wiki/Echelon`, Oktober 2005.

4 Elektronische Demokratische Parteien - am Beispiel der VVVD

Elektronische Demokratische Parteien - am Beispiel der VVVD

Anke Lederer
Hauke Tschirner

2. Februar 2006

4.1 Einleitung

Elektronische demokratische Parteien beschreiten einen völlig neuen Weg in der heutigen Parteienlandschaft. Sie besitzen weder ein politisches Programm noch irgendeine politische Richtung wie es bisher bei Parteien üblich ist. Programm sowie Richtung der Partei werden ausschließlich vom Volk bestimmt und gelenkt. Mittels exakter mathematischer Abbildung des Volkswillens ins Parlament wird ein direktdemokratischer Einfluss auf Entscheidungen im Parlament hergestellt. Durch den Einsatz des Internets gibt es dabei nahezu keine räumlichen und zeitlichen Barrieren mehr, so dass theoretisch jeder Bürger bzw. jede Bürgerin mitwirken kann.

Die nachfolgende Ausarbeitung beschäftigt sich mit dem Konzept von elektronischen demokratischen Parteien und stellt diese Art Partei anhand der ersten und bisher einzigen elektronischen demokratischen Partei Deutschlands, der VIRTUELLEN VOLKSVERTRETER DEUTSCHLANDS E.V. (VVVD), vor. Wie

sind sie definiert? Wie sind sie motiviert? Wie funktionieren sie? Welche Vor- und Nachteile bieten sie? Ein Interview mit dem amtierenden Generalsekretär der VVVD gewährt dabei u. a. Anworten auf diese Fragen und tiefere Einblicke in das Konzept und die praktische Umsetzung einer elektronischen demokratischen Partei.

4.2 Definition

Elektronische demokratische Parteien zu definieren ist schwierig, da es zum aktuellen Zeitpunkt lediglich eine dieser Art gibt. In einer Veröffentlichung von einem der Gründungsmitglieder der VVVD ist jedoch nachfolgende Definition zu finden [GWU05].

Eine elektronische demokratische Partei ist eine Partei nach Artikel 21 des Grundgesetzes. Damit muss sie demokratischen Grundsätzen entsprechen und an der politischen Willensbildung des Volkes mitwirken.

Sie besitzt kein politisches Programm oder eine festgelegte politische Richtung. Die politische Richtung wird durch das Volk vorgegeben und ggf. immer wieder neu definiert. Damit ist sie als direktdemokratisch einzustufen.

Eine elektronische demokratische Partei ist lediglich ein Serviceanbieter für den Bürger und bietet nur eine elektronische Plattform (z. B. mit politischen Informationen, Diskussionsforen u.ä.) zur politischen Willensbildung und Entscheidungsfindung an. Sie bietet also nur die Methoden und die Technologie zur Entscheidungsfindung an, der Inhalt wird durch die Bevölkerung bestimmt.

Sie besitzt kein spezialisiertes Wissen oder hat eigene Experten zu bestimmten politischen Themenbereichen (z. B. Experten für das Steuerrecht). Das benötigte Spezialwissen ist außerhalb der Partei angesiedelt.

Nicht-Mitglieder werden explizit mit eingebunden.

4.3 Motivation

Die Motivation, die hinter den elektronischen demokratischen Parteien steht, wird schon aus der Definition heraus deutlich: Bürger sollen mehr in politische Entscheidungsprozesse eingebunden werden bzw. überhaupt erst direkteren Zugang bekommen. Man geht davon aus, dass die Bürger politisch interessiert, informiert und mündig genug sind, ihre Interessen selbst zu vertreten und dass somit der basisdemokratische Ansatz gerechtfertigt ist. Durch diese Art der Einbindung erhofft man sich eine Verminderung der Politikverdrossenheit.

Ein weiterer wichtiger Motivationsgrund ist das sogenannte Ostrogorski-Paradoxon. Das Ostrogorski-Paradoxon zeigt auf, dass der Volkswillen durch die Wahl von Parteien bzw. Parteiprogrammen nur schlecht abgebildet wird. Dies lässt sich am einfachsten an einem Beispiel erklären. Als Referenz dient Tabelle 4.1.

Man nehme zwei Parteien, X und Y, welche zu drei konkreten Fragen eine bestimmte Ansicht haben. Nun nehme man vier verschiedene Wählergruppen, welche jeweils einen bestimmten Prozentsatz der Bevölkerung vertreten (hinter dem Namen der Gruppe in Prozent angegeben). Jede Wählergruppe vertritt nun die eigene Meinung. Wählergruppe A stimmt z. B. in Frage 1 mit der Partei X überein, während sie mit den anderen beiden Fragen eher mit Partei Y übereinstimmt. Da diese Wählergruppe in $\frac{2}{3}$ der Fragen mit Partei Y übereinstimmt, wählt sie diese auch mit großer Wahrscheinlichkeit. Dies ist in der rechten Spalte mit dem Titel Wahlverhalten vermerkt. Wenn man nach diesem Prinzip vorgeht, wählen drei von den vier Wählergruppen die Partei Y, und eine der Gruppen die Partei X. Dabei erhält Partei Y 60% und X 40% der Stimmen aufgrund der Aufteilung der Bevölkerung in die jeweiligen Gruppen. Partei Y würde die Wahl gewinnen.

Wenn man sich jetzt jedoch anschaut, wie die Bevölkerung abgestimmt hätte wenn sie jede Frage einzeln hätte auswählen können, sieht die Sache schon anders aus. Bei allen Fragen stimmen jeweils zwei Wählergruppen mit der Partei X überein. Da diese beiden Wählergruppen zusammen jeweils immer 60%

der Bevölkerung stellen (Wählergruppe D, die ja einen größeren Anteil an der Bevölkerung stellt als die drei anderen Gruppen ist, ist immer mit von der Partie), würde bei einer Wahl zu den jeweiligen Einzelfragen Partei X bei jeder einzelnen Frage immer 60% der Wählerstimmen auf sich vereinen und somit schlussendlich gewinnen.

	Frage 1	Frage 2	Frage 3	Wahlverhalten	
Gruppe A (20%)	X	Y	Y	Y	} 60%
Gruppe B (20%)	Y	X	Y	Y	
Gruppe C (20%)	Y	Y	X	Y	
Gruppe D (40%)	X	X	X	X	} 40%
Einzelabstimmung	X (60%)	X (60%)	X (60%)		

Tabelle 4.1: Ostrogorski-Paradoxon

Diese Diskrepanz zwischen dem mehrheitlichen Willen des Volkes (Partei X gewinnt) und dem oben aufgeführten, fast zwangsläufig auftretenden Wahlverhalten (Partei Y gewinnt) dient als Motivation und auch als Ideengeber für das Konzept elektronischer demokratischer Parteien.

4.4 VVVD

Die im September 2001 in Oldenburg gegründete VVVD (Virtuelle Volksvertreter Deutschlands, `http://www.vvvd.de`) ist die erste und bisher einzige elektronische demokratische Partei Deutschlands. Sie nimmt damit eine Vorreiterrolle ein und sieht sich dabei selbst als Prototyp für zukünftige elektronische demokratische Parteien.

Abbildung 4.1 gibt einen Eindruck von der Webseite dieser Partei. Auf der Webseite kann man sich zur Zeit über das Konzept der Partei und Artikel, die über die Partei in der Presse veröffentlicht wurden, informieren. Es sind dort aber

Abbildung 4.1: Bildschirmfoto der VVVD-Webseite

auch Informationen zu Gesetzestexten und Verweise zu relevanten politischen Webseiten vorhanden.

Die Idee hinter der Partei ist, dass gut informierte und politisch interessierte Bürger die politische Arbeit der Partei verrichten, um so den Volkswillen besser in Entscheidungen im Parlament einfließen zu lassen. Dabei kann sich praktisch jeder wahlberechtigte Bürger beteiligen. Insbesondere der bei konventionelle Parteien oft undurchsichtige Entscheidungsfindungsprozess wird durch die direkte Beteiligung und Einbeziehung des Volkes transparenter. Die Partei will den Prozess der politischen Willensbildung und die Entscheidungsfindung durch die Bereitstellung von relevantem Informationsmaterial und einer elektronischen Plattform für den Austausch und die Entscheidungsfindung der Bürger unterstützen.

Die Organisationsstruktur der Partei ist konventionell (das bedeutet, dass z. B. Versammlungen stattfinden) um den Anforderungen des Parteiengesetzes und des Bürgerlichen Gesetzbuches gerecht zu werden. Auf diese Art und Weise kann die Partei direktdemokratische Elemente mit einbringen, ohne dass Gesetze erweitert oder geändert werden müssten.

Es wird zunächst auf den Aufbau der Partei eingegangen, insbesondere die Aufteilung der unterschiedlichen Rollen innerhalb der Partei ist hierbei von Interesse, da sie für das Verständnis entscheidend ist. Danach wird der Ablauf des Meinungsbildungs- und Entscheidungsfindungsprozesses erläutert, wie ihn sich die Partei vorstellt. Zum Schluss werden die Aufgaben und Anforderungen, welche die Partei für sich selbst sieht, näher erörtert.

4.4.1 Aufbau

Bei konventionellen Parteien sind politische Arbeit und parteiliche Verwaltungsarbeit miteinander verknüpft. Bei der VVVD hingegen findet eine Unterteilung in parteilicher Verwaltungsarbeit, politischer Arbeit und Gewichtung der politischen Arbeit statt. Damit haben z. B. die politisch aktiven Personen die Möglichkeit, politisch freier zu agieren, ohne sich um die Verwaltungsarbeit kümmern zu müssen.

Diese Trennung der verschiedenen Bereiche wird durch den Aufbau der VVVD deutlich. Die VVVD gliedert sich in mehrere Personengruppen, die sich z. T. überschneiden können. Abbildung 4.2 gibt eine Übersicht.

Bevölkerung sind alle Menschen, die in der Bundesrepublik Deutschland leben. Aus ihr rekrutieren sich alle anderen unten aufgeführten Personengruppen.

Mitglieder sind technisch, administrativ und redaktionell tätig. Sie kümmern sich z. B. um die Wartung des Webservers oder die redaktionelle Betreuung der Webseiteninhalte. Sie haben darüber hinaus die Aufgabe, den Verwaltungsapparat zu unterhalten und zu pflegen. Sie sind nicht poli-

tisch tätig. Mitglieder der Partei dürfen in keiner anderen Partei Mitglied sein.

Partei-User sind die politisch aktiven Personen, sie diskutieren und entscheiden über politische Themen und können auch selber Anträge oder Gesetzesvorschläge einbringen. Der Name dieser Personengruppe ist von der VVVD geprägt worden. Partei-User können Mitglied der Partei sein, müssen es aber nicht zwingend (schraffierte Fläche in Abbildung 4.2). Eine Mitgliedschaft in anderen ggf. konkurrierenden Parteien ist ebenfalls möglich sofern sie nicht Mitglied der VVVD sind. Diese Personen müssen das Wahlrecht besitzen und authentifiziert sein.

Abgeordnete sind eine Untermenge der Mitglieder. Sie sind die Vertreter der Partei im Parlament. Ihr Abstimmungsverhalten wird durch die Arbeit der Partei-User bestimmt.

Wähler sind das ganze Volk mit Wahlberechtigung (nicht in der Grafik vorhanden). Sie gewichten durch ihr Wahlverhalten, wie stark der direktdemokratische Einfluss der Partei im Parlament sein soll.

Nachfolgend werden insbesondere die Rollen der Partei-User, der Mitglieder und der Abgeordneten betrachtet, da sie die Hauptakteure sind.

4.4.2 Meinungsbildungs- und Entscheidungsfindungsprozess

Der Meinungsbildungs- und Entscheidungsfindungsprozess der VVVD ist von zentraler Bedeutung für die Umsetzung des Parteikonzepts. Er ist es, der elektronische demokratische Parteien von konventionellen Parteien unterscheidet. In Abbildung 4.3 ist er zum leichteren Verständnis graphisch dargestellt.

Zunächst muss ein Thema definiert werden, über welches diskutiert, beraten und schlussendlich abgestimmt werden soll. Dies kann von den Partei-Usern selbst oder aber durch die Abgeordneten, z. B. weil demnächst im Parlament eine bestimmte Abstimmung stattfindet, erfolgen. Die Mitglieder erarbeiten nun

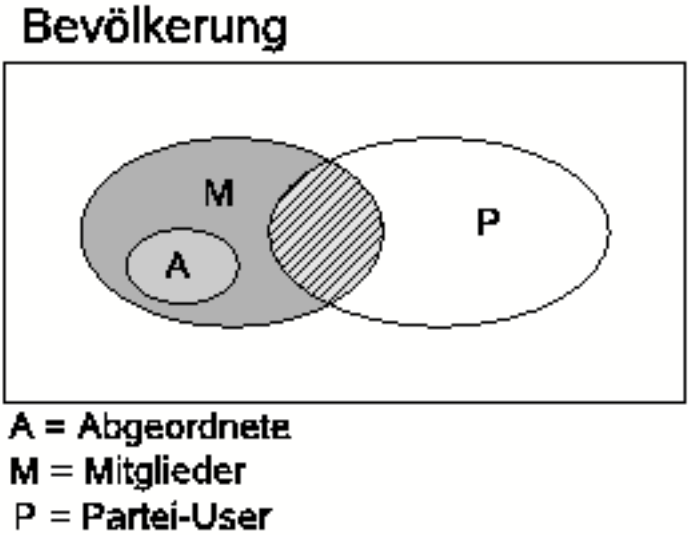


Abbildung 4.2: Übersicht der Personengruppen

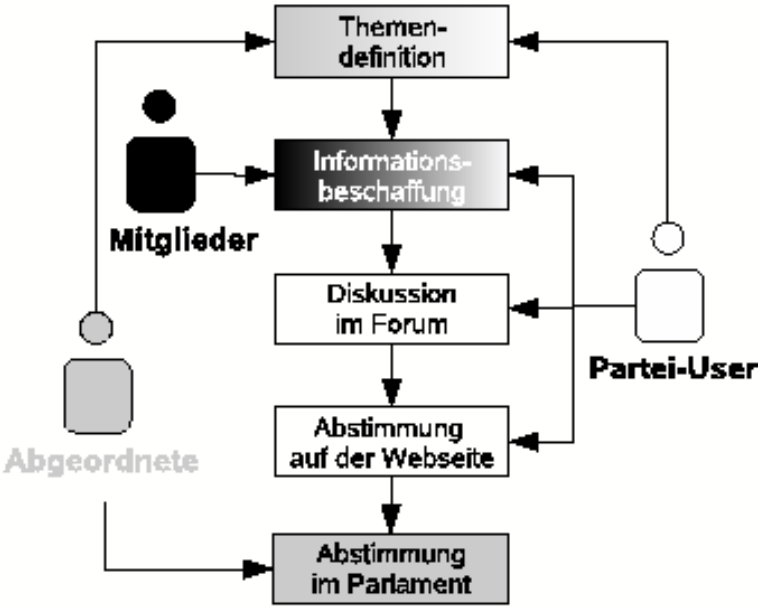


Abbildung 4.3: Abstimmungsablauf

redaktionelle Inhalte zu dem konkreten Thema, insofern noch nicht vorhanden, und ermöglichen den Partei-Usern den Zugriff auf diese Inhalte. Dabei ist es oberste Pflicht der Mitglieder, ausgewogene und/oder politisch neutrale Informationen bereitzustellen, um die Partei-User nicht auf diese Weise zu beeinflussen.

Ein Partei-User informiert sich nun über das konkrete Abstimmungsthema und diskutiert darüber mit anderen Partei-Usern. Es findet dabei an dieser Stelle eine Meinungsbildung durch den Austausch mit anderen politisch interessierten Menschen statt.

Ab einem bestimmten Zeitpunkt in einem bestimmten Zeitraum findet eine Abstimmung zu dem diskutierten Thema statt. Dieser Zeitpunkt und Zeitraum muss rechtzeitig bekannt gegeben werden und entsprechend groß gewählt werden, um nicht Gefahr zu laufen dadurch Partei-User ihr Stimmrecht - willentlich oder nicht - zu entziehen. Nach dem Ende der Abstimmung ist der Entscheidungsfindungsprozess abgeschlossen.

Das Ergebnis der Abstimmung wird nun an die Abgeordneten kommuniziert. Diese sind nun angehalten, dieses Abstimmungsergebnis mathematisch exakt im Parlament abzubilden. Wenn also 70% der Partei-User für eine bestimmte Sache und 30% dagegen sind, so sollen 7 von 10 Abgeordneten dafür und 3 von 10 dagegen stimmen. Welcher Abgeordnete dafür und welcher dagegen stimmt, sollen die Abgeordneten unter sich klären. So soll der Wille des Volkes direktdemokratisch ins Parlament fließen.

Die Formulierung „angehalten“ lässt schon erahnen, dass die Abgeordneten zwar die Aufgabe aber keinerlei Verpflichtung haben, das Abstimmungsergebnis der Partei-User mathematisch exakt abzubilden. Sie unterliegen der sogenannten Gewissensfreiheit, wie sie in Artikel 38 des Grundgesetzes vermerkt ist. Dies wirft einige Probleme auf, welche später behandelt werden.

4.4.3 Aufgaben

Die Aufgaben der VVVD ergeben sich aus der Definition von elektronischen demokratischen Parteien. Die Partei hat die Aufgabe Informationsmaterial und eine elektronische Plattform für den Meinungsbildungsprozess bereitzustellen. Ebenso müssen für eine Entscheidungsfindung Möglichkeiten zum abstimmen über ein definiertes Thema vorhanden sein.

Die VVVD hat darüber hinaus noch weitere Aufgaben für sich definiert. Sie sieht sich selbst als Prototyp und nimmt dies zum Anlass, ihr Konzept möglichst klar und strukturiert darzulegen, um anderen, zukünftigen Parteien den Einstieg zu erleichtern und um als Referenzmodell zu dienen. Daher soll darauf geachtet werden, keine kurzfristigen politischen Eingeständnisse zu machen, da diese langfristig den Referenzcharakter verderben könnten.

Durch die Neuartigkeit und vor allem durch die hohen technischen Anforderungen an die Sicherheit soll die Partei als Lehr- und Lernplattform dienen und so Interessierten die Möglichkeit bieten, die realen Anforderungen an E-Voting- und E-Partizipations-Systemen kennenzulernen und ggf. neue Konzepte und Lösungen zu erarbeiten und zu erproben.

Eine weitere wichtige Aufgabe besteht darin, dass die Partei Schulungsmaßnahmen für die Partei-User durchführen muss. Partei-User sollten zumindestens Grundlagen über die verwendeten technischen Systeme, das Gesetz und die Politik allgemein besitzen, um auch wirklich effektiv und effizient politisch agieren zu können. Angedacht sind Kurse mit unterschiedlichen Schwerpunkten, so z. B. das politische System der Bundesrepublik Deutschland, Internettechnologien und Datenschutz, um nur einige zu nennen. Ebenso möchte die Partei Aufklärungsarbeit zum Thema Sicherheit von technischen Abstimmungs- und Beteiligungssystemen für alle Bürger anbieten.

4.4.4 Anforderungen

Für eine erfolgreiche Umsetzung des Konzepts der VVVD sind einige Anforderungen zu beachten. Die ökonomischen Anforderungen müssen erfüllt sein, um die Partei langfristig etablieren zu können. Eine wichtige Rolle spielen die technischen Anforderungen. Ohne ihre Erfüllung ist eine Umsetzung des Konzepts nicht möglich. Die persönlichen Anforderungen sollten zumindestens Großteils erfüllt sein, da ansonsten das Konzept ad absurdum geführt wird.

Ökonomische Anforderungen

Die Ausgaben der Partei sollen möglichst minimiert werden. So sollen Partei-User für die anfallenden Registrierungskosten selber aufkommen, dabei sollen diese Kosten ebenfalls minimiert werden. Mittel- und langfristig sollen zusätzliche externe Finanzquellen in Form von z. B. Werbung erschlossen werden.

Technische Anforderungen

Die technischen Anforderungen sind durch das Konzept der VVVD schon recht klar umrissen. Es werden Systeme benötigt, die den Meinungsbildungs- und den Entscheidungsfindungsprozess in Form von z. B. Foren und Abstimmungen unterstützen. Diese Systeme müssen hohe Anforderungen erfüllen in Bezug auf Sicherheit bei den Abstimmungen (z. B. darf keine Mehrfachabstimmung einer Person möglich sein) und im Bereich des Datenschutzes (z. B. müssen persönliche Daten von Personen wie z. B. Partei-Users, geschützt sein). Diese Systeme sollten mit wachsender Anzahl von Partei-Usern skalierbar sein.

Zum jetzigen Zeitpunkt existieren noch keine geeigneten Systeme, um diese Aufgabe zu bewältigen. Es werden ebenso Systeme benötigt, die die administrative Arbeit der Partei (Kommunikation, Mitgliederbetreuung, Selbstdarstellung, etc.) unterstützen, hierfür sind bereits Systeme bekannt und werden z. T.

auch schon eingesetzt (z. B. ist die Selbstdarstellung in Form einer Webseite bereits realisiert).

Persönliche Anforderungen

Es werden auch bestimmte persönliche Anforderungen an Parteimitglieder gestellt. So sollten diese z. B. ein Interesse an direkter Demokratie haben, und da die Partei keine eigene politische Meinung als solche vertritt, sollten sich auch die Mitglieder in der Öffentlichkeit politisch möglichst neutral verhalten. Die redaktionelle Tätigkeit der Mitglieder sollte dabei ebenfalls politisch neutral und ausgewogen durchgeführt werden.

Insbesondere sollten Mitglieder eine gewisse Akzeptanz gegenüber politisch Andersdenkenden mitbringen und sich auch darüber im Klaren sein und akzeptieren, dass Abstimmungen bzw. die politische Richtung der Partei ggf. konträr zur eigenen Meinung erfolgen kann. Dies alles gilt besonders für Mitglieder, die als Abgeordnete tätig werden wollen.

4.5 Grenzen der elektronischen Partizipation

Als wesentliche Bestandteile einer medialen Aufbereitung innerhalb der Vorstellung einer elektronischen Demokratie können die sechs Domänen Technik, Recht, Organisation, Kultur und Politik identifiziert werden. Diese sollten technischen und sozio-kulturellen Anforderungen genügen um ein weites Anwendungsspektrum zu finden [vgl. GWU05, S.2]. Im Rahmen der elektronischen demokratischen Parteien bedeutet dies, dass sie, um für die breite Öffentlichkeit nutzbar zu sein, in den oben genannten Bereichen gesellschaftlichen Anforderungen entsprechen müssen. Das Konzept der elektronischen demokratischen Parteien betrachtet allerdings nur einen Teilausschnitt des Konzeptes der elektronischen Demokratie. Demnach sind die Anforderungen an Systeme der elektronischen Demokratie nur begrenzt auf diese anwendbar. Die genannten

Bereiche oder Domänen bilden jedoch im Folgenden einen Bestandteil der Betrachtung von Vor- und Nachteilen elektronischer demokratischer Parteien.

4.6 Vorteile elektronischer demokratischer Parteien

Die vorgestellten Vorteile, die durch den zuvor definierten Ansatz der elektronischen demokratischen Parteien entstehen, basieren auf den Angaben aus [GWU05]. Entsprechend werden sie anhand ihrer Perspektive in Vorteile aus technischen, organisatorischen, ökonomischen, kulturellen, rechtlichen und politischen Gesichtspunkten unterteilt [vgl. GWU05, S.6]. Dabei wird im Wesentlichen auf Vergleiche zu konventionellen Parteien zurückgegriffen.

4.6.1 Technische Vorteile

Die Vorteile aus einer technischen Perspektive entstehen durch die Tatsache, dass die genutzte Software bzw. der Systemzugang durch eine Partei und nicht durch den Staat reguliert wird. Technisch fehlerhafte Systeme werden durch Mechanismen des Marktes durch funktionsfähige Systeme ersetzt [vgl. GWU05, S.6]. Dies setzt allerdings eine Konkurrenzsituation zwischen Parteien voraus, welche vergleichbare Systeme nutzen.

Entgegen einem Konzept eines staatlich regulierten Systems muss ein durch Parteien wie etwa eine elektronische demokratische Partei reguliertes System nicht jedem Bürger zugänglich sein [vgl. GWU05, S.7], da eine politische Konkurrenz die Möglichkeit ausschließt, dass man ein bestimmtes System nutzen muss. Dies hat den Vorteil, dass es einer elektronisch demokratischen Partei Freiheiten in dem Aufbau der Infrastruktur ihres Systems lässt [vgl. GWU05, S.7].

4.6.2 Organisatorische Vorteile

Die organisatorischen Vorteile entstehen dadurch, dass der organisatorische Teil der elektronischen demokratischen Parteien von der Entscheidungsfindung entkoppelt ist [vgl. GWU05, S.7]. Entgegen konventionellen Parteien ist der Entscheidungsfindungsprozess innerhalb einer elektronischen demokratischen Partei sehr transparent. Diskussionen die zur Entscheidungsfindung beitragen können nachvollzogen werden, indem man entsprechende Foreneinträge liest, ebenso wie der Entscheidungsprozess selbst, indem die Abstimmungsergebnisse betrachtet werden.

Durch die direkte und auf einzelne politische Fragen beschränkte Abstimmung durch die Bürger wird eine Deformierung der Wählerentscheidungen, wie zuvor mit dem Ostrogorski-Paradoxon vorgestellt, vermieden [vgl. GWU05, S.7].

Volksreferenden können weniger umständlich als durch konventionelle politische Konzepte abgebildet werden. Dazu können auch virtuelle Abstimmungen, entgegen Abstimmungen konventioneller Parteien, relativ kurzfristig abgehalten werden [vgl. GWU05, S.7].

Eine elektronische demokratische Partei benötigt keine große Parteibasis an Mitgliedern. Wenige Mitglieder reichen aus, da diese im Wesentlichen für die Instandhaltung des Systems zuständig sind.

4.6.3 Ökonomische Vorteile

Die Finanzierung einer elektronischen demokratischen Partei begrenzt sich im Wesentlichen auf die Schaffung und Instandhaltung eines Systems zur Nutzung ihrer Konzepte. Dabei sollte eine elektronische demokratische Partei nur in das momentan benötigte System investieren und nicht in zukünftige oder ideale Systeme. Die benötigte Qualität eines solchen Systems ergibt sich dabei allein aus den Anforderungen der Benutzer des Systems [vgl. GWU05, S.7]. Den

Staat selbst fallen keine Kosten bei der Nutzung von elektronischen demokratischen Parteien an.

Durch die theoretische Unabhängigkeit bzw. Neutralität der Abgeordneten einer elektronischen demokratischen Partei wird eine Bestechung oder Erpressung dieser Abgeordneten unmöglich. Ein Einfluss durch Lobbyisten ist zudem völlig nutzlos. Dies bewirkt wiederum, dass eine elektronische demokratische Partei attraktiv für die Wähler wird [vgl. GWU05, S.7].

Kostspielige Parteiversammlungen können durch die geringe Zahl der Mitglieder minimiert werden.

4.6.4 Kulturelle Vorteile

Für die Abstimmungen innerhalb einer elektronischen demokratischen Partei sind die Bürger selbst verantwortlich. Die Abgeordneten bilden nur die Ergebnisse der Abstimmungen ab. Dadurch besitzen sie die „größtmögliche Legitimationsbasis“ [GWU05, S.7].

Jeder der an der Abstimmung teilnehmen möchte kann dies auch tun. Einzige Voraussetzung zur Teilnahme ist die Wahlzulassung und eine Anmeldung als Partei-User [vgl. GWU05, S.8]. Eine Mitgliedschaft in der Partei wird nicht verlangt. Mit der Zeit wird sogar erwartet, dass eine Menge von Bürgern an den Abstimmungen teilnehmen, welche eine repräsentative Menge der Gesamtbevölkerung abbilden [vgl. GWU05, S.7]. In diesem Fall wären die gefällten Entscheidungen als repräsentativ für die Gesamtbevölkerung zu bewerten.

Die Meinung der Partei-User wird dabei nicht verfälscht. Die einzige Korrektur der Entscheidung der Partei-User wird rein mathematisch, durch Rundung der Ergebnisse, ausfallen.

Ein „digital divide“, also eine gesellschaftliche Spaltung die dadurch ausgelöst wird, dass einige Personen Zugang zum Internet haben und andere nicht, wird durch elektronische demokratische Parteien vermieden. Dies wird dadurch be-

gründet, dass jeder Bürger die Möglichkeit besitzt seine Zustimmung zu den Entscheidungen der elektronischen demokratischen Parteien in der Wahl, in der diese aufgestellt sind, abzugeben und dadurch letztlich doch noch an der Entscheidung teilzunehmen.

Die Partei selbst hat kein Programm und keine Tradition. Keine Entscheidungen werden dadurch aufgrund unausgesprochener Konventionen getroffen. Die Partei versteht sich selbst nur als „provider of services“ [GWU05, S.7].

4.6.5 Rechtliche Vorteile

Für die Nutzung der Konzepte einer elektronischen demokratischen Partei ist keine Verfassungs- oder Gesetzesänderung notwendig. Dies gilt sowohl auf staatlicher, als auch auf föderaler, als auch auf kommunaler Ebene [vgl. GWU05, S.8]. Nach dem Parteiengesetz gilt auch eine elektronische demokratische Partei als politische Partei.

4.6.6 Politische Vorteile

Der Wille der Bevölkerung zur Nutzung der vorgestellten Konzepte einer elektronischen demokratischen Partei ist Voraussetzung und Maß der Gewichtung einer elektronischen demokratischen Partei. Dieser Wille wird in einer konkreten Wahl abgebildet und kann gemessen werden.

Elektronische demokratische Parteien bilden den Willen der Bürger entsprechend einem Volksreferendum ab, besitzen allerdings zudem die Vorteile konventioneller Parteien, etwa in der Entscheidungsfähigkeit [vgl. GWU05, S.8].

Grundlage der Abstimmung bilden die zugrundeliegenden Informationen, welche etwa von konventionellen Parteien häufig subjektiv gefärbt präsentiert werden. Eine elektronische demokratische Partei sollte Informationen neutral auf-

bereitet präsentieren. Dadurch wird es jedem Bürger ermöglicht sich zuerst eine eigene Meinung zu bilden.

4.7 Nachteile elektronischer demokratischer Parteien

Die im Folgenden vorgestellten Nachteile, die bei der Nutzung von elektronischen demokratischen Parteien entstehen, stammen ebenfalls aus [GWU05]. Sie werden den Vorteilen entsprechend ebenfalls in Nachteile aus technischen, organisatorischen, ökonomischen, kulturellen, rechtlichen und politischen Gesichtspunkten unterteilt [vgl. GWU05, S.8]. In [GWU05] werden sie allerdings nicht als Nachteile sondern als Zweifel bezeichnet. Sie sind dabei abhängig von der Zustimmung der Partei durch die Bürger. D.h. je mehr Personen eine elektronische demokratische Partei wählen, desto stärker fallen die Nachteile ins Gewicht [vgl. GWU05, S.8].

4.7.1 Technische Nachteile

Es ist anzunehmen, dass das Konzept der elektronische demokratische Parteien nicht sofort Konkurrenz im Bereich der Bürgerpartizipation bekommt. In einer solchen konkurrenzlosen Situation ist die Notwendigkeit zur Haltung eines Qualitätsstandards für die Anwendungssoftware nicht gegeben. Demnach kann in dieser Situation die Softwarequalität leiden [vgl. GWU05, S.8].

Zudem ist ein System welches konzeptionell auf die Arbeit über das World Wide Web ausgelegt ist anfällig für Fehler, etwa durch Überlastung des Servers oder durch Sicherheitslücken. Ein solcher Ausfall würde die gegebenen Voraussetzung einer freien Partizipation einschränken.

4.7.2 Organisatorische Nachteile

Eine elektronische demokratische Partei hat keine Führungskraft. Die Menge der Entscheidungen, die in einer solchen Position zu treffen sind, würde die Partei-User überfordern [vgl. GWU05, S.8]. Um dies zu bewältigen müsste eine elektronische demokratische Partei zum Konzept der Politikpakete zurückkommen, damit aber einen großen Teil ihres Gesamtkonzeptes aufgeben.

4.7.3 Ökonomische Nachteile

Elektronischen demokratischen Parteien mangelt es an einem vergleichbaren Standard um die finanziellen Grenzen konkret einschätzen zu können. Deshalb ist auch eine Abschätzung der finanziellen Anforderungen bisher nur zu prognostizeren.

Finanzielle Mittel müssen zuerst in die Wählerwerbung investiert werden, da das System nutzlos ist wenn die Partei nicht gewählt wurde [vgl. GWU05, S.9]. In diesem Fall hätten die Entscheidungen der Partei-User nämlich keinerlei politisches Gewicht.

4.7.4 Kulturelle Nachteile

Unter Umständen kann eine elektronische demokratische Partei in der Öffentlichkeit nur als Spiel oder „Maus-Click-Demokratie“ verstanden, also nicht ernst genommen werden [vgl. GWU05, S.8]. Dies ist im Wesentlichen vom Zuspruch durch Partei-User abhängig.

Zudem besteht die Gefahr das Partei-User uninformiert über ein Thema abstimmen. Die Informierung ist allerdings nicht als Notwendigkeit zur Teilnahme an einer Abstimmung festgelegt. Demnach können auch äußere Einflüsse, wie der Einfluss der Medien eine gewichtige Rolle bei der Entscheidungsfindung der

Partei-User bilden. Die Gefahr ist, dass dies zu Entscheidungen führt welche wenig durchdacht und nicht von allen Seiten betrachtet sind.

Ein weiteres Problem ist es, dass die persönlichen Daten, die ein Partei-User bei seiner Anmeldung angeben muss, bei der Partei liegen. Daher muss ein Partei-User darauf vertrauen, dass die Partei diese Daten vertraulich behandelt und nicht etwa weiterverkauft [vgl. GWU05, S.8].

4.7.5 Rechtliche Nachteile

Die rechtlichen Nachteile ergeben sich als Ergebnis der vorgestellten organisatorischen Nachteile. Demnach ist eine elektronische demokratische Partei nicht fähig in einer staatlichen Führungsposition zu arbeiten. Die Fähigkeit zur Ausfüllung einer solchen Führungsposition ist aber in Deutschland eine formale Spezifikation zur Zulassung zu staatlich getriebenen Abstimmungen [vgl. GWU05, S.8]

4.7.6 Politische Nachteile

Die notwendige 5-Prozent-Hürde muss durch eine elektronische demokratische Partei selbstständig, also ohne fremde Hilfe, gemeistert werden. Dies betrifft sowohl finanzielle Mittel als auch die Organisation von Wahlwerbung. Zu dem Zweck einer schnellen Wählerfindung müssen Mittel und Zeit, die zuvor zur Systemerhaltung genutzt wurden, aufgebracht werden. Darunter kann die Qualität und damit die Attraktivität des Systems leiden.

4.8 Ergebnisse des Interviews mit der VVVD

Am 21.12.2005 führten die Autoren dieses Beitrages ein Interview mit dem Generalsekretär und stellvertretendem Vorsitzenden der VVVD: Mathias Usler. Es stellten sich die Fragen nach der Grundidee hinter dem Konzept der elektronischen demokratischen Parteien nach dem momentanen Status der VVVD und nach den zukünftigen Aussichten der VVVD. Zusätzlich wurden einige Probleme und mögliche Lösungsansätze im Laufe des Interviews diskutiert. Die Ergebnisse des Interviews werden im Folgenden vorgestellt. Die genannten Konzepte beziehen sich auf die Antworten des Generalsekretärs der VVVD.

4.8.1 Die Grundidee

Das Konzept der elektronischen demokratischen Parteien basiert auf der Fragestellung wie sich Bürger heutzutage mittels elektronischer Medien über politische Themen informieren. Als negativen Trend der letzten Zeit sieht die VVVD in diesem Zusammenhang Wahl-o-maten und Politiker-Weblogs. Diese seien stark subjektiv gefärbt und daher nicht für eine neutrale Auseinandersetzung mit politischen Themen geeignet. Ein positiver Trend ist jedoch auch zu erkennen. Immer häufiger werden politische Themen in sogenannten „Communities“ diskutiert. Eine Diskussion in Onlineforen ist dazu zumeist das Mittel der Wahl. Auf dieser offenen Kommunikation basiert das Konzept der elektronischen demokratischen Parteien.

Einzelthemen sollen neutral diskutiert und über diese soll, nach Ablauf einer bestimmten Frist, entschieden werden. Dabei liegt der Schwerpunkt des Konzeptes auf der Neutralität der Partei und auf der Entscheidungsfindung auf detaillierter Ebene entgegen der konventionellen Politikpakete.

Wesentlich ist auch der Einsatz einer elektronischen Wahlsoftware zur Abstimmung der diskutierten Themen über das Internet. Als Standard und insbesondere als Sicherheitsstandard stellt sich die VVVD vor, dass sie jedem Partei-User eine CD mit dem Betriebssystem Knoppix zukommen lässt.

4.8.2 Der aktuelle Status der VVVD

Die VVVD umfasst zum aktuellen Zeitpunkt (Stand: 21.12.2005) 85 Mitglieder und keine Partei-User. Mitglieder rekrutieren sich dabei bisher zumeist aus links-orientierten bis links-extremen Schichten.

Partei-User sollen erst angeworben werden, wenn ein lauffähiges System vorhanden ist. Eine lauffähiges Version der elektronischen Wahlsoftware befindet sich noch in der Entwicklung, ist also noch nicht vorhanden.

Die VVVD besitzt mehrere Landesverbände in Deutschland. Sie ist gesetzlich als politische Partei anerkannt und gleichberechtigt. Eine Wahlzulassung besitzt sie jedoch noch nicht.

4.8.3 Die Zukunft der VVVD

Absicht der VVVD ist es, in naher Zukunft eine lauffähige Version der elektronischen Wahlsoftware fertigzustellen um daraufhin Partei-User aufzunehmen.

Zusätzlich sollen in nächster Zeit, etwa in Bremen im Jahr 2006, 300 Unterschriften für die Wahlzulassung der VVVD gesammelt werden.

4.8.4 Probleme mit Lösungsansätzen

Die Autoren dieses Beitrages wollten im Laufe des Interviews bewusst einige Probleme ansprechen, die sie selbst innerhalb des Konzeptes der elektronischen demokratischen Parteien sehen. Für einige Probleme besitzt die VVVD konkrete Lösungskonzepte.

So war eine Frage, ob eine Mitgliederwerbung, bzw. eine Werbung für Aktivität in der VVVD, allein über die Website der VVVD genügen würde. Dies

sollte, nach Angaben der VVVD genügen. Eine Erweiterung der Werbung für die VVVD ist bisher nicht vorgesehen.

Der Umgang mit rechts- oder linksextremen Teilnehmer in der Diskussion und Abstimmung politischer Entscheidungen ist bisher weitgehend ungeklärt. Ein Konzept wäre z. B. eine Einschränkung der Auswahlmöglichkeiten in einer Abstimmung, welche extreme Positionen ausblendet. Eine Gefahr davon ist allerdings das Abrücken von der grundsätzlich definierten Meinungsfreiheit der Partei-User. Die Bestimmung, die VVVD sei eine demokratische Partei, ist allerdings auch ein Grundsatz der VVVD. Dieser Grundsatz schließt prinzipiell eine nichtdemokratische Politik aus und lässt damit, in einem gewissen Rahmen, die Beschränkung der Abstimmungsoptionen zu.

Teilnehmer, die die Diskussion stören oder das System nur aus Freude an der Verfälschung der Abstimmungsergebnisse nutzen, sollen bereits durch die notwendige Anmeldung mit persönlichen Daten von der Teilnahme abgeschreckt werden. Der Einsatz einer elektronischen Wahlsoftware soll sie zusätzlich abschrecken.

Eine interessante Frage ist auch die nach der Finanzierung der VVVD. Im Moment finanziert sie sich durch private Spenden. Langfristig sollen zur Instandhaltung des Systems Gebühren von 1 Euro pro Jahr für aktive Mitglieder verlangt werden. Ein Mitglied ist nicht verpflichtet diese Gebühr zu verrichten. Wenn er sie nicht zahlt, so ruht seine Mitgliedschaft. Will ein Mitglied wieder aktiv werden, so erreicht er diesen Status wieder durch die Nachzahlung der verfehlten Gebühren. Die Kosten der Instandhaltung des Systems sind zudem, nach der Prognose der VVVD, die einzigen wesentlichen Kosten die auf sie zukommt. Die Finanzierung des politischen Konzeptes der VVVD sei also ausreichend.

Ein wichtiger zukünftiger Gesichtspunkt der Finanzierung ist die erste Wählerwerbung im Fall einer Wahlzulassung. Diese finanzielle Hürde soll durch Vorfinanzierung bestritten werden.

Die Neutralität der Abgeordneten der VVVD bezüglich der gefällten Entscheidungen der Partei-User ist ein weiteres Problem, welches im Laufe des Interviews angesprochen wurde. Diese steht der im Grundgesetz verankerten Gewissensfreiheit einer jeden Person gegenüber. Ein Zwang zur Abstimmung entgegen der eigenen Meinung der Abgeordneten gibt es, nach Angaben der VVVD, auch bei den konventionellen Parteien. Dort sei es der Fraktionszwang. Eine Abweichung von der Abstimmung der Partei-User sei zudem möglich und auch zumeist, aufgrund von geheimen Abstimmungen, nicht nachvollziehbar.

Im optimalen Fall sollten Personen ohne konkrete politische Meinung als Abgeordnete der VVVD arbeiten.

4.8.5 Probleme ohne Lösungsansätze

Es bestehen auch einige Probleme, welche zuvor bereits angesprochen wurden, für die keine konkreten Lösungsansätze durch die VVVD existieren. Im Verlaufe des Interviews wurden die folgenden Probleme ohne Lösungsansätze identifiziert.

Gefährlich sei es, wenn eine elektronische demokratische Partei mehr Personen abbildet als sie Meinungen von Partei-Usern vertritt. Dies würde dazu führen, dass man eine ungleiche Abbildung der politischen Meinung der Bevölkerung vertritt und damit dem Konzept direkter Demokratie nicht mehr entspricht. Daher sei eine parlamentarische Vertretung von mehr als 10 Prozent als gefährlich einzuschätzen. Die VVVD schätzt ihr Maximalpotential allerdings auch auf 5 Prozent.

Gefährlich sei es zudem, wenn eine einzelne Person oder eine Gruppe von Personen die Meinungsführerschaft in der politischen Diskussion der VVVD übernimmt. Diese Person oder Personengruppe könnte etwa eine Vertrauensbasis für sich aufbauen und damit eine Anhängerschaft anderer Partei-User nach sich ziehen. In folgenden Diskussionen würde dann etwa seiner Meinung gefolgt ohne diese zu hinterfragen.

Ungelöst ist zudem das Problem, wie man etwa Ausschussarbeit mit den Mitteln der VVVD bewältigen kann. Dies knüpft an das zuvor besprochende Problem der nicht bestehenden Führungskraft der elektronischen demokratischen Parteien an.

4.9 Zusammenfassung

Die Absicht der Autoren war es mit diesem Beitrag einen Einblick in das Konzept der elektronischen demokratischen Parteien und in konkrete Umsetzungskonzepte durch die bisher einzige elektronische demokratische Partei, die VVVD, zu geben.

Es wurde beschrieben aus welchem Grund ein solches Konzept die Meinung der Bürger differenzierter als die konventionelle Politik abbilden kann. Die Stärken einer elektronischen demokratischen Partei wurden dargestellt, sie umfassen im Wesentlichen Vorteile aus einem kulturellen Blickwinkel. So wird der Wandel von einer Gesellschaft in der der Bürger seine politische Verantwortung in dem Moment abgibt, in dem er bei der Wahl seine Stimme abgibt, hin zu einer Gesellschaft ganzheitlicher politischer Beteiligung der Bürger propagiert. Dabei wird an keiner Stelle die Bereitschaft der Gesellschaft zu einer solchen Beteiligung hinterfragt. Man muss sich ernsthaft fragen, ob viele Bürger bereit sind sich über jedes aktuelle politische Thema zu informieren und über jedes politische Thema abzustimmen. Wesentlich ist dabei auch die Frage inwiefern man einem großen Teil der Bevölkerung eine Kompetenz in der Entscheidung über politische Fragen zumisst.

Ein solches Konzept birgt einige Gefahren in sich. So wird der Einfluss der Öffentlichkeit bzw. der Medien anscheinend von dem Konzept der elektronischen demokratischen Parteien unterschätzt. Das öffentliche Meinungsbild wird aber sehr stark durch die Medien geprägt. Aber vielleicht erreichen elektronische demokratische Parteien gerade an dieser Stelle auf Dauer einen Kulturwandel. Dadurch, dass die Parteien Informationen zu relevanten politischen Themen bereitstellen, ermöglichen sie den Menschen den leichteren Zugang zu diesen In-

formationen fern ab der traditionellen Medien. Dadurch könnte der Einfluss der Medien auf das Meinungsbild verringert werden. Es bleibt abzuwarten, inwiefern diese Erwartung tatsächlich zutrifft.

Die vorgestellten Nachteile und Probleme der elektronischen demokratischen Parteien haben eindeutig die Grenzen des Konzeptes gezeigt. Elektronische demokratische Parteien haben ein Maximalpotential, welches sie nicht überschreiten sollten, aus Gründen des eigenen Verständnisses und aus Gründen der nicht vorhandenen Handlungskompetenz ab einer bestimmten Menge von Aufgaben.

Über die praktische Umsetzung durch die VVVD lässt sich zu diesem Zeitpunkt wenig sagen. Diese Partei befindet sich noch in einem Anfangsstadium.

Zusammenfassend kann man sagen, dass elektronische demokratische Parteien einen interessanten Ansatz für die Einbringung direktdemokratischer Elemente in die bestehenden Verfassung bieten. Durch die Neuartigkeit dieser Parteien gibt es jedoch noch keinerlei Erfahrung mit ihrer konkreten Realisierung, so dass anzunehmen ist, dass das Weiterentwicklungspotenzial dieses Parteienkonzeptes noch verhältnismäßig groß ist. Es bleiben zudem noch viele Fragen und Probleme ungeklärt, so dass abzuwarten ist, wie diese in Zukunft beantwortet bzw. gelöst werden können.

Literaturverzeichnis

[GWU05] GRONAU, N., E. WEBER und M. USLAR: *Institutionalization of a general electronic democracy through eletronic democratic parties - a general concept with focus on Germany*. 2005.

[Vir] VIRTUELLE VOLKSVERTRETER DEUTSCHLANDS E.V.: *Statut 2001*. `http://www.vvvd.de/statut`. letzter Zugriff 09.01.2006.

[Web03] WEBER, E.: *Arbeitsbericht der VVVD: 2/03 - Leitbild und Erläuterungen einer elektronisch demokratischen Partei: Anwendungsfall VVVD*. 2003. letzter Zugriff 09.01.2006.

5 Elektronische Wahlen im internationalen Vergleich

Elektronische Wahlen im internationalen Vergleich

Sönke Brummerloh
Mareike Wagner

10. Februar 2006

Im Oktober 2005 war der Presse zu entnehmen, dass es bei der landesweiten Kommunalwahl in Estland die Möglichkeit gab, über das Internet von privaten Computern aus zu wählen. Im Gegensatz zu diesem modernen Verfahren wird in Deutschland in den meisten Wahlkreisen noch per Kreuz auf Papier abgestimmt. Allerdings werden seit 1999 vermehrt unvernetzte elektronische Wahlmaschinen statt Wahlbögen eingesetzt. Ob Deutschland sich in Bezug zu anderen Ländern in Sachen Onlinewahlen im Rückstand befindet, oder ob das Einführen von elektronischen Wahlmaschinen der richtige Weg ist, wird in diesem Seminarbeitrag beurteilt. Dazu wird zunächst eine kurze Einführung in elektronische Wahlmaschinen und Onlinewahlen gegeben. Nachdem Vor- und Nachteile dieser Systeme aufgezeigt wurden, wird der Status diverser Länder in Bezug auf elektronische Wahlmaschinen und Onlinewahlen betrachtet. Deutschland wird genauer behandelt, andere Länder werden kurz umrissen. Am Ende wird ein Fazit gezogen, ob sich Deutschland im Rückstand befindet, und wie die Entwicklung der Wahlen in Deutschland am besten voranschreiten sollte.

5.1 Einleitung

Wer die Pressemeldungen Ende 2005 im Bereich der elektronischen Wahlen verfolgt hat, konnte erfahren, dass in Estland im Oktober eine landesweite Kommunalwahl über das Internet durchgeführt wurde und in der Schweiz angefangen wurde per Handy zu wählen. Über die Entwicklung in Deutschland war nur zu lesen, dass die Anzahl der Wahlbezirke, in denen elektronische Wahlmaschinen eingesetzt wurden, bei der Bundestagswahl 2005 auf ca. 2100 Bezirke angewachsen ist.

Beim Lesen dieser Meldung kann der Eindruck entstehen, dass Deutschland veraltet und wenig fortschrittlich in Bezug auf elektronische Wahlen ist. Ob dem wirklich so ist und wie Deutschland gegenüber anderen Ländern dasteht, wird in dieser Ausarbeitung untersucht. Dazu wird die aktuelle Entwicklung elektronischer Wahlen weltweit vorgestellt.

In Kapitel 5.2 wird zunächst eine Einführung in das Thema elektronische Wahlen gegeben. Dazu werden Begriffe wie „elektronische Wahl“ und „Onlinewahl“ definiert (Kapitel 5.2.1), elektronische Wahlen in Kategorien und Szenarien eingeteilt (Kapitel 5.2.2) und abschließend Vor- und Nachteile aufgezeigt. Auf Basis dieser Grundlagen schließt sich in Kapitel 5.3 der internationale Vergleich an. Zunächst wird in Kapitel 5.3.1 die Situation in Deutschland vorgestellt. Danach wird ein großer Überblick über andere Länder gegeben.

Zum Schluss wird in Kapitel 5.4 beurteilt, wie Deutschland im Gegensatz zu anderen Ländern dasteht und ob der Einsatz von elektronischen Wahlmaschinen der richtige Weg ist.

5.2 Grundlagen

In diesem Kapitel werden die Grundlagen zum Verständnis und Einschätzen von elektronischen Wahlen vermittelt. Dazu werden in Kapitel 5.2.1 wichti-

ge Begriffe definiert. In Kapitel 5.2.2 folgt eine Einteilung von elektronischen Wahlen in zwei Kategorien und vier Szenarien. Im Anschluss werden Vorteile elektronischer Wahlen (Kapitel 5.2.3), sowie Probleme mit Wahlmaschinen (Kapitel 5.2.4) und Gefahren von Onlinewahlen (Kapitel 5.2.5) angesprochen.

5.2.1 Definitionen

Im Folgenden werden die Begriffe „elektronische Wahl“ (Kapitel 5.2.1), „elektronische Wahlmaschinen“ (Kapitel 5.2.1) und „Onlinewahl“ (Kapitel 5.2.1) verwendet. Deshalb wird in diesem Kapitel definiert, was darunter zu verstehen ist.

Elektronische Wahl

Unter elektronischen Wahlen sind Wahlen zu verstehen, bei denen mit Hilfe elektronischer Geräte gewählt wird. Elektronische Geräte können z. B. spezielle elektronische Wahlmaschinen (siehe Kapitel 5.2.1) sein, aber auch normale Computer und Handys, wie sie im Alltag zu finden sind. Synonym zum Begriff „elektronische Wahl“ wird oft auch der Begriff „e-Voting“ verwendet(vgl. [Bir04, S. 47f]).

Elektronische Wahlmaschinen

Elektronische Wahlmaschinen sind elektronische Geräte, mit denen gewählt werden kann. Hierbei handelt es sich um Geräte, die nur zur Stimmenabgabe genutzt werden können und die Stimmen elektronisch zählen. Bei einigen Geräten wird für jeden Wähler ein Beleg mit den Angaben, wie gewählt wurde, ausgedruckt. Wenn dieser Ausdruck zusätzlich in eine Urne geworfen und später per Hand ausgezählt wird, ist es möglich zu überprüfen, ob die Maschi-

ne richtig gezählt hat oder ob unerlaubte Manipulationen durchgeführt wurden (vgl. [Bir04, S. 49f]).

Weltweit werden unterschiedliche Wahlmaschinen eingesetzt. In Europa sind vor allem elektronische Wahlmaschinen der niederländischen Firma N.V. Nederlandsche Apparatenfabriek (Nedap) (vgl. [Ned]) im Einsatz. Bei diesen Maschinen entspricht die Darstellung auf dem Bildschirm den gewohnten Papierbögen. Die Maschinen von Diebold Election Systems (vgl. [Die]), dem größten Hersteller für elektronische Wahlmaschinen in den USA, sind deutlich leistungsfähiger und aufwändiger gestaltet, allerdings sollen diese Wahlmaschinen eine Reihe von Sicherheitslücken haben (vgl. [Bla] und [Jon]). Die elektronischen Wahlmaschinen, die in Indien (vgl. [EVM]) eingesetzt werden, sind dagegen möglichst einfach gehalten, und die Wahlmöglichkeiten werden durch Bilder zusätzlich zu den Namen der Kandidaten gekennzeichnet. Dadurch soll Menschen, die nicht lesen können, trotzdem die Wahl ermöglicht werden.

Neben elektronischen Wahlmaschinen existieren auch mechanische Wahlmaschinen, die wie in den USA z. B. die Stimmenabgabe in Lochkarten stanzen. Mechanische Wahlmaschinen werden in dieser Ausarbeitung nicht weiter behandelt.

Onlinewahl

Unter Onlinewahlen werden alle elektronischen Wahlen verstanden, bei denen die Stimmen über ein Netz zum Auszählungsserver[1] geschickt werden. Das kann z. B. von einer elektronischen Wahlmaschine, die in einem Wahllokal steht und mit dem Server des Wahlkreises verbunden ist, geschehen. Denkbar wäre aber auch, von einem privaten Computer über das Internet oder per Handy die Stimme an den Auszählungsserver zu schicken (vgl. [Bir04, S. 47f]).

[1] Ein Server ist ein Computer, der über ein Netz (z. B. das Internet) erreichbar ist und bestimmte Dienste (z. B. das Empfangen und Auswerten von Wahlstimmen) bereitstellt.

Wenn von Onlinewahlen gesprochen wird, sind oft Wahlen von privaten Computern oder Handys gemeint, obwohl eigentlich auch vernetzte elektronische Wahlmaschinen eine Form der Onlinewahl darstellen. In dieser Ausarbeitung wird unter Onlinewahlen sowohl die Wahl von elektronischen Wahlmaschinen, als auch die Wahl von privaten Computern und Handys verstanden.

Elektronische Stimmenauszählung

Unter elektronischer Stimmenauszählung wird das Auswerten von Papierwahlzetteln mit einer elektronischen Maschine verstanden. Nach einer Wahl werden bei diesem Verfahren die einzelnen Stimmen nicht mehr von Menschen gezählt, sondern von Maschinen. Dadurch sollen ein schnelleres Auszählen und weniger Auszählungsfehler erzielt werden. Weitverbreitet ist die elektronische Stimmenauszählung nicht, da die meisten Länder bei einer Modernisierung des Wahlverfahrens direkt zu elektronischen Wahlmaschinen wechseln und nicht den Zwischenschritt über Maschinen zur elektronische Stimmenauszählung zu gehen.

5.2.2 Kategorien elektronischer Wahlen

Elektronische Wahlen lassen sich unterteilen in unvernetzte und vernetzte Wahlen. Bei den vernetzten Wahlen sind vier mögliche Szenarien denkbar (siehe Kapitel 5.2.2).

Unvernetzte Wahlen

Wenn elektronische Wahlen von unvernetzten Geräten aus durchgeführt werden sollen, dann geschieht dies über elektronische Wahlmaschinen in Wahllokalen. Die Stimmen werden dann auf einem Speichermedium in der elektronischen Wahlmaschine gespeichert. Zum Auszählen wird das Speichermedium aus der

elektronischen Wahlmaschine entnommen und in die Zählmaschine gesetzt. Die Zählmaschine addiert dann die Stimmen aller Speichermedien und präsentiert das Auszählungsergebnis.

Vernetzte Wahlen

Bei vernetzten Wahlen, bzw. Onlinewahlen, sind vier mögliche Szenarien denkbar (vgl. [BN02, S. 26ff]):

1. Vernetzte elektronische Wahlmaschinen stehen in Wahllokalen.
2. Vernetzte elektronische Wahlmaschinen stehen in öffentlichen Einrichtungen.
3. Gewählt wird von einem beliebigen Computer über das Internet.
4. Gewählt wird von einem beliebigen Handy.

Elektronische Wahlmaschinen im Wahllokal Die sicherste Onlinewahl ist die vom Wahllokal aus. Hier würden die Stimmen, wie bei der unvernetzten elektronischen Wahl, über elektronische Wahlmaschinen abgegeben. Die Stimme würde zu Auszählungszwecken nach ihrer Abgabe an den Auszählungsserver geschickt und mit allen anderen Stimmen verrechnet. Für den Wähler würde sich im Vergleich zur unvernetzten elektronischen Wahl also nichts ändern. Die Änderungen würden im Hintergrund geschehen und nur die Aufgaben der Wahlhelfer etwas verändern.

Elektronische Wahlmaschinen in öffentlichen Einrichtungen Bei Wahlen mit elektronischen Wahlmaschinen könnten Wahlmaschinen auch in öffentlichen Einrichtungen, wie z. B. Bibliotheken, Banken und Einkaufszentren, aufgestellt werden. Die Wähler müssten sich dann der Maschine gegenüber mit einer Chipkarte oder Ähnlichem ausweisen, um ihre Stimme abgeben zu können. Der Vorteil bei diesem Vorgehen wäre, dass die Wähler kein Wahllokal

aufsuchen müssten, um ihre Stimme abzugeben. Sie könnten vielmehr während ihres gewohnten Tagesablaufs an einer beliebigen elektronischen Wahlmaschine wählen. Bei diesem Vorgehen müsste allerdings sichergestellt werden, dass die Stimmen nicht einzelnen Personen zuordbar sind. Das Problem ist nämlich, dass sich die Wähler der Maschine gegenüber zwar ausweisen müssen, ihre Stimme aber anonym abgespeichert werden muss.

Computer Wenn von einem beliebigen privaten Computer aus gewählt werden könnte, dann wären die Wähler noch freier in ihrer Wahl des Wahlortes. Am Wahltag könnte von zu Hause aus gewählt werden und der Weg zum Wahllokal müsste nicht mehr angetreten werden. Außerdem könnte wirklich von überall gewählt werden: Selbst wenn einige Wähler während der Wahl im Ausland wären, könnten sie ihre Stimme abgeben. Alles, was sie bräuchten, wäre ein Computer mit Internetverbindung. Hier liegt allerdings ein Problem dieser Onlinewahlform: Nicht alle Menschen besitzen einen Computer oder einen Internetanschluss. Solange nicht gewährleistet ist, dass Computer mit Internetverbindung flächendeckend verfügbar sind, kann die Wahl von privaten Computern aus nur ein Zusatzangebot sein, es sei, denn in Wahllokalen werden ebenfalls Computer mit Internetverbindung aufgestellt. Ein anderes Problem ist, dass sich der Wähler eindeutig identifizieren muss, um wählen zu dürfen. Trotzdem darf seine abgegebene Stimme ihm nicht mehr zuordbar sein.

Handy Wenn von privaten Computern aus gewählt werden kann, dann ist es gedanklich nur noch ein kleiner Schritt, ganz mobil über Handy zu wählen. Damit könnte die Stimme von überall und jederzeit abgegeben werden, indem eine SMS mit der getroffenen Wahl an den Wahlserver geschickt wird.

Allerdings gelten die Probleme, die bei der Wahl von Computern genannt wurden, auch für Wahlen per Handy: Nicht alle Wähler besitzen Handys und die Stimmen dürfen nicht mehr den Wählern zuordbar sein, obwohl sich diese identifizieren müssten.

5.2.3 Vorteile elektronischer Wahlen

Durch den Einsatz von elektronischen Wahlen erhoffen sich deren Befürworter folgende Vorteile (vgl. [BN02, S. 28ff] und [Bir04, S. 51ff]):

- Weniger Fehler
- Geringere Kosten
- Die Möglichkeit zu wählen, von wo man möchte
- Schnellere Ergebnisspräsentation
- Prestigegewinn
- Erhöhte Wahlbeteiligung

Es werden weniger Fehler beim Zusammenzählen der Stimmen auftreten, weil ein Computer beim Zählen normalerweise keine Fehler macht, ein Mensch verzählt sich viel schneller. Auch andere mögliche menschliche Fehler, wie z. B. das falsche Ausfüllen eines Wahlbogens, der dadurch unbeabsichtigt ungültig wird, könnten verhindert werden, indem der Wähler auf seine Fehler aufmerksam gemacht wird. Die Möglichkeit, ungültig zu wählen, muss natürlich auch weiterhin gegeben sein (siehe Kapitel 5.3.1). Allerdings werden durch den Einsatz von Maschinen auch neue Fehler hinzukommen, wie z. B. defekte Wahlmaschinen, überlastete Server und Bedienungsfehler.

Jede Wahl, die mit Wahlbögen durchgeführt wird, erzeugt hohe Kosten. So müssen in Deutschland Wahlbenachrichtigungen gedruckt und verschickt werden, Wahlbögen gedruckt und an die Wahlbezirke verteilt werden, Wahllokale gemietet werden usw. Durch elektronische Wahlmaschinen müssten keine Wahlbögen mehr gedruckt werden und durch die Beschleunigung des Wahlvorganges im Wahllokal könnten mehrere Wahlbezirke zusammengelegt werden. Allerdings müssen die elektronischen Wahlmaschinen gekauft oder geleast werden, und wenn sie gekauft wurden, müssen sie gewartet werden. Dadurch entstehen wieder neue Kosten. Bei Wahlen von privaten Computern und Handys müssten zwar keine Wahlbögen gedruckt und Wahllokale gemietet werden, aber es müssten Server zum Empfangen der Stimmen gekauft und Software

zum Durchführen von Wahlen gekauft oder entwickelt werden. Auch dadurch entstehen hohe Kosten.

Wenn Onlinewahlen durchgeführt werden, wäre es möglich, von überall zu wählen. Selbst bei vernetzten Wahlmaschinen gäbe es diese Möglichkeit. Würde z. B. ein Bayer an der Nordsee während einer Wahl Urlaub machen, dann könnte er ein Wahllokal an der Nordsee aufsuchen, sich dort identifizieren und würde den Wahlbogen seines Wahlkreises auf dem Bildschirm angezeigt bekommen. Er bräuchte also, wie es zur Zeit nötig wäre, keine Briefwahl zu beantragen. Wenn Computer die Auszählung der Stimmen vornehmen, dann würde das vollständige endgültige Wahlergebnis einige Minuten nach Wahlende vorliegen. Das stundenlange Auszählen würde also wegfallen. Was seine Vor- und Nachteile hat, denn manche Menschen empfinden das Spektakel nach Wahlende, wo mal die eine Partei vorne liegt, dann die andere, als äußerst spannend und unterhaltsam.

Es wird gesagt, dass elektronische Wahlen modern seien. Das bedeutet: Wer elektronische Wahlen einsetzt, zeigt, dass er modern und zukunftsorientiert ist. Solange dies nicht zu Lasten der Bevölkerung und seiner Sicherheit geht, ist das eine gute Möglichkeit für ein Land zu zeigen, wie modern es ist, und dadurch einen Prestigegewinn zu erzielen.

Ein Punkt, der oft angeführt wird, ist, dass elektronische Wahlen die Wahlbeteiligung, besonders bei jüngeren Wählern, steigern. Bisherige elektronische Wahlen konnten dies allerdings nicht, bzw. nicht in dem erwarteten Maß, bestätigen.

5.2.4 Probleme mit elektronischen Wahlmaschinen

Wie im Text oben bereits angedeutet wurde, gibt es in Bezug auf elektronische Wahlmaschinen auch eine Reihe von Problemen, die beachtet werden müssen (vgl. [Bir04, S. 49f]). Diese sind im Besonderen:

- Anschaffungspreis

- Instandhaltungskosten
- Schulungen
- Nachweisbarkeit der Stimmen
- Sicherheit der Maschine

Wenn Wahlmaschinen eingesetzt werden sollen, dann müssen diese vorher gekauft oder geleast werden. Dadurch entstehen nicht unerhebliche Kosten. Wenn elektronische Wahlmaschinen gekauft wurden, dann müssen sie gewartet werden, um nicht in ihrer Funktionalität beeinträchtigt zu werden. Auch dies verursacht weitere Kosten.

Wahlen mit Papierbögen und Stift sind leicht zu verstehen, der Umgang mit Maschinen und Computern ist dagegen für viele Menschen ein großes Problem. Es müssten also Schulungen durchgeführt werden, um den Wahlhelfern die Wahlmaschinen zu erklären und um sie zu befähigen, den Wählern den Wahlvorgang erklären zu können. Durch diese Schulungen würden ebenfalls Kosten entstehen.

Ein Problem beim elektronischen Speichern der Stimmen ist, dass nicht nachgewiesen werden kann, dass der Computer richtig gezählt und niemand die Anzahl der Stimmen manipuliert hat. Als mögliche Lösung wird vorgeschlagen, für jede Stimme einen Ausdruck zu erzeugen und in die Wahlurne zu werfen. Dadurch könnte nachgezählt werden, ob das vom Computer präsentierte Ergebnis wirklich richtig ist. Diese Sicherung würde allerdings zu Kosten führen, die eigentlich eingespart werden sollten.

Ein anderes Problem ist die Sicherheit der elektronischen Wahlmaschine. Es muss sichergestellt sein, dass die Wahlmaschinen richtig arbeiten und nicht ausfallen. Außerdem muss gewährleistet sein, dass die Maschinen nicht ohne erheblichen Aufwand manipuliert werden können. Wo hier die Grenzen gesetzt werden, ist von Land zu Land unterschiedlich: So werden die elektronischen Wahlmaschinen der Firma Nedap, die in Deutschland eingesetzt werden, in Irland auf Grund von Sicherheitsbedenken nicht eingesetzt (vgl. [Com04] und [Com05]). Aus den USA gibt es Berichte zu bemerkten Manipulationsversu-

chen und Ausfällen bei den elektronischen Wahlmaschinen (vgl. [Ulb04]), die den Wahlablauf störten.

5.2.5 Gefahren bei Onlinewahlen

Bei Onlineverfahren gibt es auch eine Reihe von Problemen und Gefahren (vgl. [Bir04, S. 79ff] und [BN02, S. 102ff]):

- Viren, Würmer, Trojanische Pferde
- Unsichere Übertragungsnetze
- Unsichere Server
- (Distributed) Denial of Service Angriffe
- Wahlverfahren nur für Fachleute verständlich

Wenn mit einem privaten Computer oder von einem Handy aus gewählt wird, so besteht immer die Gefahr, dass sich auf diesen Geräten problematische Software, wie z. B. Viren, Würmer, Trojanische Pferde und Spyware, befindet. Diese könnte die Eingaben des Wählers behindern oder eingegebene Daten ausspionieren. Über Trojanische Pferde wäre es sogar möglich, die Eingabe des Nutzers so zu ändern, dass anders als beabsichtigt gewählt würde. Die Problematik von Trojanischen Pferden und Spyware betrifft allerdings nur Computer und noch nicht die Handys. Um einen sicheren Computer zu gewährleisten, könnten an alle Wähler spezielle CDs verteilt werden, von denen ein eigenes Wahlbetriebssystem gestartet werden könnte. Auf diese Weise kann ein sicherer Computer gewährleistet werden. Allerdings könnten viele Wähler mit einer Boot-CD überfordert sein. Außerdem entstehen durch Millionen von CDs, die an die Wähler verteilt werden, Kosten.

Neben möglichen unsicheren Computern und Handys ist auch das Übertragungsnetz zum Wahlserver unsicher. In unsicheren Netzen ist es möglich, dass Nachrichten verloren gehen, mitgelesen oder manipuliert werden. Mit geeig-

neten Techniken aus dem Bereich der Kryptographie[2] kann das Mitlesen und Manipulieren sicher verhindert werden.

Die Wahlserver müssen natürlich auch vor Manipulation abgesichert sein. Da die Sicherheit von Servern nie zu 100% gewährleistet werden kann, liegt auf der Serverseite immer ein geringes Restrisiko.

Ein anderes Problem ist die Verfügbarkeit der Wahlserver. Diese kann nicht sichergestellt werden, denn wer die Wahl stören möchte, kann dies mit entsprechendem Aufwand tun. Ein erfolgsversprechender Angriff ist der (Distributed) Denial of Service Angriff (DoS bzw. DDoS). Beim DoS werden von einem Computer (beim DDoS von mehreren Computern) ununterbrochen Anfragen an einen Server geschickt. Dadurch ist der Server völlig ausgelastet, so dass die eigentlichen sinnvollen Nachrichten (z. B. die abgegebenen Stimmen) den Server nicht mehr erreichen können. Mit Hilfe von alternativen Servern, die angesprochen werden, wenn der eigentliche Server nicht erreichbar ist, lässt sich das Problem der DoS Angriffe weitestgehend abfangen. Durch alternative Server entstehen allerdings wieder weitere Kosten.

Für die meisten Probleme und Gefahren, die bei Onlinewahlen auftreten, gibt es zwar Lösungen, diese verkomplizieren die Wahl bzw. das Wahlsystem aber in einem Maße, dass nur noch Experten den ganzen Ablauf verstehen können. Die normalen Wähler, die sich kaum mit Computern und dem Internet auskennen, werden das ganze System nicht mehr in seinen Einzelheiten verstehen können.

5.3 Internationaler Vergleich

In diesem Kapitel wird der aktuelle Stand elektronischer Wahlen in mehreren Ländern betrachtet. Deutschland (Kapitel 5.3.1) wird genauer betrachtet, andere Länder werden nur kurz beschrieben.

[2] Die Kryptographie beschäftigt sich mit Methoden zum Ver- und Entschlüsseln von Daten mit Hilfe bestimmter Schlüssel. Mit der im Bereich der elektronischen Wahl eingesetzten asymmetrischen Verschlüsselung, wird mit einem anderen Schlüssel verschlüsselt als entschlüsselt.

5.3.1 Deutschland

Es wird auf den aktuellen Stand elektronischer Wahlen in Deutschland eingegangen. Dazu wird zunächst in Kapitel 5.3.1 auf Probleme eingegangen, die durch die Gesetzgebung, bzw. das Grundgesetz, in Bezug auf elektronische Wahlen entstehen. In Kapitel 5.3.1 wird erläutert, wieso die Probleme, die nicht durch eine Gesetzesänderung des Grundgesetzes gelöst werden können. Danach folgt in Kapitel 5.3.1 die bisherige Entwicklung von elektronischen Wahlen in Deutschland. In Kapitel 5.3.1 wird die bisherige Entwicklung bewertet und in Kapitel 5.3.1 ein Ausblick in die nahe Zukunft gegeben.

Sind elektronische Wahlen mit dem Grundgesetz vereinbar?

In Artikel 38 des deutschen Grundgesetzes (vgl. [GG]) steht in Absatz 1:

> Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt. Sie sind Vertreter des ganzen Volkes, an Aufträge und Weisungen nicht gebunden und nur ihrem Gewissen unterworfen.

Was unter einer allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahl zu verstehen ist und wie dies in Bezug zur elektronischen Wahl umgesetzt werden kann, wird im Folgenden beschrieben (vgl. [BN02, S. 42ff] und [Bir04, S. 56ff]).

Allgemein Eine Wahl muss allgemein sein, das bedeutet, dass allen Staatsbürgern die Möglichkeit zum Wählen gegeben sein muss und ebenso muss gesichert sein, dass sie gewählt werden können. Durch die verwendeten Wahlmethoden darf also kein Staatsbürger von der Wahl ausgeschlossen werden. Würde nur per Computer über das Internet oder per Handy gewählt, dann wären viele Wähler von der Wahl ausgeschlossen, weil Computer, Internetanschlüsse und Handys nicht allen Wählern zugänglich sind, bzw. diese nicht in erforderlichem

Maße damit umgehen können. Eine Wahl nur über Computer oder Handy ist zur Zeit also nicht zulässig. Denkbar wäre aber die Wahl mit solchen Geräten zusätzlich, also ähnlich der Briefwahl, anzubieten.

Was keine Probleme in Bezug zum Grundsatz der Allgemeinheit erzeugt, ist das Ersetzen der Papierwahlbögen in den Wahllokalen durch unvernetzte oder vernetzte elektronische Wahlmaschinen, wenn diese Wahlmaschinen vom Bundesministerium des Innern (BMI) (vgl. [BMI]) zugelassen wurden und entsprechend der Bundeswahlgeräteverordnung (BWahlGV) (vgl. [BWa]) eingesetzt werden.

Fazit: Der Grundsatz der Allgemeinheit einer Wahl kann bei elektronischen Wahlen eingehalten werden, wenn auch mit Einschränkungen.

Unmittelbar Eine Wahl muss unmittelbar sein, das bedeutet, dass die Wahl nicht von Dritten, wie z. B. Wahlmännern abhängen darf. Es darf zwischen den Wählern und den Wahlbewerbern keine weitere Instanz geben, die nach eigenem Ermessen die Wahlbewerber wählt. Die abgegebenen Stimmen der Wähler müssen also direkt in die Kandidatenwahl fließen.

Elektronische Wahlen hängen nicht von einer zwischengeschalteten Instanz ab, sondern ermöglichen, wie bei den bisherigen Wahlen, eine direkte Auszählung der Stimmen.

Fazit: Bei elektronischen Wahlen bleiben die Wahlen auch weiterhin unmittelbar.

Frei Eine Wahl muss frei sein, das bedeutet, dass der Wahlprozess frei von jeglichem öffentlichen und privaten Druck erfolgen muss. Der Stimmzettel muss unbeeinflusst und persönlich ausgefüllt werden. Dabei steht es dem Wähler auch frei, nicht oder ungültig zu wählen. In Bezug auf elektronische Wahlen bedeutet das, dass keine Werbung eingeblendet werden darf. Erlaubt wäre es aber, weiterführende Informationen zu allen Parteien anzubieten, wenn diese

für alle Parteien zur Verfügung stehen. Denkbar wären z. B. Links auf die Homepages der Parteien.

Wichtig bei elektronischen Wahlen ist, dass immer explizite die Möglichkeit gegeben sein muss, ungültig zu wählen. Das kann durch eine zusätzliche Wahloption geschehen oder durch eine ungültige Auswahl von Kandidaten. Bei einer ungültigen Auswahl sollte die Maschine den Wähler darauf aufmerksam machen, dass die Wahl ungültig ist und die Möglichkeit zur Korrektur geben. Wenn der Wähler seine Stimmen nicht korrigieren, sondern ungültig stimmen möchte, dann muss diese Möglichkeit zur Auswahl gegeben sein. Dass ein Wähler frei von äußerem Druck wählen kann, wird durch die Aufsicht in den Wahllokalen gewährleistet. Außerhalb des Wahllokales kann nicht gewährleistet werden, dass kein Druck auf Wähler ausgeübt wird. Aus diesem Grund ist die Briefwahl auch nur für Ausnahmefälle gedacht. Genauso müsste die Onlinewahl von privaten Geräten eine Ausnahme bleiben. Bei der Briefwahl wird per Unterschrift bestätigt, dass ohne äußeren Druck gestimmt wurde. Bei der Onlinewahl müsste etwas Vergleichbares, wie z. B. digitale Unterschriften, verwendet werden.

Für die Wahl mit elektronischen Wahlmaschinen in einem Wahllokal ist weiterhin gewährleistet, dass kein äußerer Druck auf den Wähler ausgeübt wird.

Fazit: Wahlmaschinen im Wahllokal gefährden den Grundsatz der freien Wahl nicht. Wahlen mit einem privaten Computer oder Handy stellen eine Gefährdung des Grundsatzes dar, die mit einer digitalen Unterschrift etwas gemildert werden könnte.

Gleich Eine Wahl muss gleich sein, das bedeutet zum einen, dass alle Wahlvorschläge, bzw. Kandidaten, gleich behandelt und ihnen damit die gleiche Chance eingeräumt werden müssen. Zum anderen bedeutet es, dass alle abgegebenen Stimmen gleich gewichtet werden müssen. Es darf also keine Stimmen geben, die mehr zählen als andere, und es dürfen nicht unterschiedlich viele Stimmen pro Wähler abgegeben werden, indem z. B. zweimal gewählt wird.

In Bezug auf elektronische Wahlen ist die Chancengleichheit der Kandidaten ein Problem, denn alle Kandidaten müssten auf einen Blick zu sehen sein. Dies wäre schon nicht mehr gewährleistet, wenn in einem Fenster die Bildlaufleiste verwendet werden müsste, um einige Kandidaten zu sehen. Um das zu lösen, könnte eine Menüstruktur verwendet werden, in der z. B. erst die Partei ausgewählt wird, worauf dann die Kandidaten der Partei angezeigt werden würden. Diese Art der Darstellung führt aber dazu, dass ein im Wahllokal verwendeter Wahlbogen anders aussieht als die Menüstruktur auf einem Bildschirm. Das könnte zu einer Ungleichheit zwischen den verschiedenen angebotenen Wahlmethoden führen und gegen die gleiche Wahl verstoßen. Aus diesem Grund sehen Oberflächen der Wahlmaschinen genauso, bzw. fast genauso, aus wie die entsprechend verwendeten Papierbögen. Die Auswahl bestimmter Parteien und Kandidaten geschieht dann, ähnlich wie bei vielen Bankautomaten, über Knöpfe an den Seiten.

Die Gleichheit der Stimme muss bei elektronischen Wahlen gewährleistet werden. Dazu muss zum einen sichergestellt werden, dass bei mehreren alternativen Wahlmöglichkeiten, nicht mehrfach abgestimmt werden kann. Um das zu gewährleisten, muss sich der Wähler gegenüber dem Wahlsystem ausweisen, so dass seine Stimme als abgegeben betrachtet werden kann. Für diese abgegebene Stimme muss sichergestellt werden, dass sie nicht manipuliert werden kann. Könnte sie unbemerkt verändert werden, würde das bedeuten, dass jemand unerlaubt mehrfach wählen könnte.

Fazit: Die Gleichheit der Wahl kann ohne größere Probleme bei Wahlmaschinen gewährleistet werden. Bei einer Wahl über Computer oder Handy, besteht die Gefahr, dass der Grundsatz der gleichen Wahl verletzt wird.

Geheim Eine Wahl muss geheim sein, das bedeutet, dass nur der Wähler weiß, wen er gewählt hat. Dazu muss der Wähler seine Stimme im Verborgenen, also unbeobachtet abgeben. Nur durch die Geheimhaltung kann eine freie Wahl gewährleistet werden, denn durch eine geheime Wahl braucht niemand Konsequenzen auf Grund seiner abgegebenen Stimme befürchten. Im Wahllokal ist die geheime Wahl gewährleistet, aber außerhalb des Wahllokales bei ei-

ner Wahl mit privatem Computer oder Handy kann das nicht gewährleistet werden. Mit einer Wahlmaschine kann die geheime Wahl, wie mit Wahlbögen aus Papier, gewährleistet werden, solange die Maschine keine Töne beim Drücken der Knöpfe erzeugt, mit deren Hilfe auf die gewählten Kandidaten geschlossen werden kann.

Bei Onlinewahlen über private Computer und Handys kann nicht gewährleistet werden, dass niemand mitbekommt, wie der Wähler seine Stimme abgegeben hat, weil jemand einen Blick auf den Bildschirm werfen konnte. Der Grundsatz der geheimen Wahl ist also nicht gewährleistet werden.

Bei der Briefwahl ist der Grundsatz der geheimen Wahl allerdings auch nicht gewährleistet. Begründet wird die Zulassung der Briefwahl damit, dass durch die Briefwahl die allgemeine Wahl gewährleistet wird, denn Personen, die sonst nicht an einer Wahl teilnehmen könnten, können durch die Briefwahl trotzdem ihre Stimme abgeben. Außerdem muss der Wahlberechtigte selber die Briefwahl unter Angabe von Gründen beantragt und sich per Unterschrift verpflichtet haben, den Stimmzettel unbeobachtet auszufüllen. Eine ähnliche Regelung könnte auch für Wahlen mit Computer und Handy gefunden werden.

Dann bleibt aber trotzdem noch das Problem, dass sich der Wähler eindeutig identifizieren muss, obwohl es nicht möglich sein darf, ihm seine Stimme wieder zuzuordnen. Eine oft verwendete Lösung ist, die Verwendung mehrerer Server und geschickter Verschlüsselung und Signierung der Stimme (siehe Kapitel 5.3.1). Dadurch wird ein ähnlicher Mechanismus wie bei der Briefwahl, bei der zwei Umschläge verwendet werden, geschaffen.

Fazit: Wahlmaschinen gefährden den Grundsatz der geheimen Wahl normalerweise nicht. Bei Onlinewahlen mit privatem Computer und Handy wird der Grundsatz der geheimen Wahl verletzt. Deshalb sind diese Formen der elektronischen Wahl zur Zeit ähnlich der Briefwahl nur in Ausnahmefällen einsetzbar.

Können die Wahlgrundsätze geändert werden?

Aus Kapitel 5.3.1 kann entnommen werden, dass die Grundsätze der deutschen Wahl die Stimmenabgabe außerhalb eines Wahllokales eigentlich verbieten. Deshalb könnte vorgeschlagen werden, dass Grundgesetz zu ändern (vgl. [Bir04, S. 114ff]).

Auf Grund schlechter Erfahrungen in Deutschland in den 30er Jahren des 20. Jahrhunderts wurde nach dem zweiten Weltkrieg eine Klausel in das Grundgesetz eingebaut, die verbietet, bestimmte Teile zu ändern. Diese Klausel ist Artikel 79 Absatz 3:

> Eine Änderung dieses Grundgesetzes, durch welche die Gliederung des Bundes in Länder, die grundsätzliche Mitwirkung der Länder bei der Gesetzgebung oder die in den Artikeln 1 und 20 niedergelegten Grundsätze berührt werden, ist unzulässig.

Artikel 38 in dem die Wahlgrundsätze niedergelegt sind, wird in Artikel 79 zwar nicht direkt erwähnt, aber in Artikel 20 Absatz 2 steht, dass die Staatsgewalt vom Volk durch Wahlen ausgeübt wird:

> Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.

Da sich Artikel 38 mit Wahlen beschäftigt und es in Artikel 20 Absatz 2 um Wahlen geht, darf Artikel 38 Absatz 3 nicht geändert werden. Eine Änderung von Artikel 38 würde nämlich die Grundsätze von Artikel 20 Absatz 2 berühren.

Eine Änderung des Grundgesetzes, um Onlinewahlen flächendeckend mit privaten Geräten zu ermöglichen, ist also nicht möglich. Abgesehen davon würde ein Streichen z. B. vom Grundsatz der geheimen Wahl die Demokratie unterlaufen und (außen)politisch ungeschickt sein, da er gegen Artikel 21 Absatz 3 der allgemeinen Erklärung der Menschenrechte (vgl. [Men]) verstoßen könnte:

> Der Wille des Volkes bildet die Grundlage für die Autorität der öffentlichen Gewalt; dieser Wille muß durch regelmäßige, unverfälschte, allgemeine und gleiche Wahlen mit geheimer Stimmabgabe oder in einem gleichwertigen freien Wahlverfahren zum Ausdruck kommen.

Bisherige Entwicklung

Auf Grund der Rechtslage (siehe Kapitel 5.3.1 und 5.3.1) wird in Deutschland vor allem auf elektronische Wahlmaschinen gesetzt. Onlinewahlen über private Computer wurden nur in kleinem nicht-parlamentarischen Rahmen untersucht und getestet.

Elektronische Wahlmaschinen Die gesetzliche Grundlage für elektronische Wahlmaschinen wurde Anfang 1999 durch eine Änderung der Bundeswahlgeräteverordnung (BwahlGV) (http://bundesrecht.juris.de/bwahlgv/) geschaffen. Im Mai 1999 folgte dann eine Bauartzulassung des BMI für Geräte der niederländischen Firma Nedap. Getestet wurden die elektronischen Wahlmaschinen mit der Bezeichnung NEDAP ESD1 durch die Physikalisch-Technische Bundesanstalt (PTB) (siehe [PTB]).

Im Juni 1999 wurden dann das erste Mal elektronische Wahlmaschinen in Köln eingesetzt. Bei der Bundestagswahl am 22.09.2002 gab es bereits in ca. 1400 Bezirken elektronische Wahlmaschinen. Bei der Bundestagswahl am 18.09.2005 wurden dann bereits in ca. 2100 Wahlbezirken elektronische Wahlmaschinen eingesetzt. Mittlerweile sind auch Wahlmaschinen mit der Bezeichnung NEDAP ESD2 in Deutschland zugelassen (vgl. [Sie05]).

Dass elektronische Wahlmaschinen noch nicht weiter verbreitet sind, liegt zum Teil daran, dass sie nicht ohne Weiteres bei Kommunalwahlen eingesetzt werden können. Für Bundestagswahlen gilt die BwahlGV, aber auf kommunaler Ebene existieren nur für Brandenburg, Hessen, Nordrhein-Westfalen,

Rheinland-Pfalz und Sachsen-Anhalt entsprechende Regelungen, um bei Landtags- und Kommunalwahlen elektronische Wahlmaschinen einzusetzen. Deshalb wurden auch nur in diesen Bundesländern elektronische Wahlmaschinen während der Bundestagswahlen eingesetzt (vgl. [Sie05]).

i-vote Das System i-vote entstand aus dem vom Bundesministerium für Wirtschaft und Arbeit (BMWA) geförderten Projekt „Wählen im Internet“, das durch die Forschungsgruppe Internetwahlen an der Universität Osnabrück durchgeführt wurde.

Bei i-vote handelt es sich um ein Onlinewahl-System, das mit Hilfe von Signaturkarten und PINs arbeitet. Um die im Grundgesetz festgelegten Wahlgrundsätze so gut wie möglich zu gewährleisten, werden drei sich gegenseitig kontrollierende Instanzen eingesetzt. Die drei Instanzen sind:

- Der Zertifikatsaussteller
- Der Wahlamtsserver
- Die Wahlurne

Der Zertifikatsaussteller stellt die elektronische Signatur für den Wähler aus und garantiert damit die Personenechtheit von diesem. Der Wahlamtsserver prüft, ob der Wähler wahlberechtigt ist, und die Wahlurne überprüft die Einmaligkeit der abgegebenen Stimme. Durch diese Gewaltenteilung soll gewährleistet werden, dass der Wähler sich eindeutig identifizieren und nur einmal wählen, aber trotzdem seine abgegebene Stimme ihm nicht mehr zugeordnet werden kann.

Die elektronische Signatur mit anderen Personen bezogenen Daten befindet sich auf einer Chipkarte. Neben der Chipkarte muss sich der Wähler noch zusätzlich mit einer PIN ausweisen.

Wenn ein Wähler mit dem i-vote-System wählen möchte, muss er sich zunächst registrieren, um eine elektronische Signatur zu bekommen. Zur Wahl ruft er die Web-Seite der Wahl auf und identifiziert sich dort gegenüber dem Wahlamtsserver. Dieser verwaltet das Wählerverzeichnis und kann daher feststellen, ob der

Wähler zur Wahl zugelassen ist und ob er bereits gewählt hat. Wenn der Wähler noch wählen darf, wird ihm der elektronische Stimmzettel präsentiert und ein Vermerk im Wahlregister vorgenommen, der angibt, dass der Wähler einen Stimmzettel erhalten hat. Der Wähler kann nun seine Wahlentscheidung vornehmen. Daraufhin kann die Stimme mit dem öffentlichen Schlüssel der Wahlurne verschlüsselt und anschließend mit der Signatur des Wählers signiert werden. Danach wird die Stimme an den Wahlamtsserver geschickt. Dieser prüft die Gültigkeit des Signaturzertifikates des Wählers und entfernt die Signatur von der verschlüsselten Stimme. Stattdessen wird die Stimme mit der Signatur des Wahlamtsservers versehen. Der Wahlamtsserver weiß nur, dass der Wähler gewählt hat, da er aber nicht den geheimen Schlüssel der Wahlurne zum Entschlüsseln der Stimme besitzt, kann er nicht feststellen, wie gewählt wurde. Die Stimme mit der neuen Signatur wird an die Wahlurne gesendet und dort mehrfach gespeichert. Auf diese Weise soll verhindert werden, dass Stimmen durch Datenfehler verloren gehen können. Sobald die Speicherung vorgenommen wurde, wird der Status des Wählers auf dem Wahlamtsserver auf „hat gewählt“ gesetzt und eine Meldung an den Wähler geschickt, dass seine Stimme erfolgreich gespeichert wurde. Nach Wahlende werden alle Stimmen entschlüsselt und gezählt (vgl. [DCC02]).

Das i-vote-System verwendet zwei getrennte Server: Einen für den Wahlamtsserver und einen für den Urnenserver. Der größte Teil der i-vote -Software ist in Java implementiert. Für die Verschlüsselung werden in C/C++ implementierte kryptographische Bibliotheken über das Java Native Interface (JNI) angesprochen. Der Source-Code des i-vote-Systems wurde bisher nicht veröffentlicht (vgl. [DCC02] und [Wil04]).

Am 02.02.2000 wurde die erste weltweit rechtsgültige Onlinewahl bei der Studierendenparlamentswahl an der Universität Osnabrück durchgeführt. Für die Wahl hatten sich 406 Teilnehmer registriert und eine Signaturkarte erhalten. Abgestimmt werden konnte über in der Universität aufgestellte Computer mit Kartenlesegeräten oder auch von beliebigen anderen Computern, sofern ein Lesegerät angeschlossen war. Da diese Lesegeräte wenig verbreitet sind, wurden zusätzlich Kartenlesegeräte ausgeteilt. Von den registrierten Wählern wählten nur 156 per Onlinewahl. Grund dafür waren vermutlich eine Reihe von Proble-

men, die auftraten, wie z. B. dass Kartenlesegeräte zu manchen Computersystemen inkompatibel waren und dass manche Karten nicht lesbar waren. Außerdem brach das Universitätsnetz über längere Zeiträume zusammen (vgl. [BN02, S. 131f]).

Weitere Wahlen mit i-vote waren z. B. die im Juni 2000 durchgeführte Testwahl zur Personalratswahl beim Landesbetrieb für Datenverarbeitung und Statistik Brandenburg und die im Juli 2001 rechtsgültige Jugendgemeinderatswahl in Esslingen. Zu beiden Wahlen wurde das System i-vote zwar verbessert, aber Probleme mit den Kartenlesegeräten und den Signaturkarten traten weiterhin auf (vgl. [BN02, S. 133f]).

W.I.E.N. - Wählen in elektronischen Netzen Das Projekt „W.I.E.N. - Wählen in elektronischen Netzwerken“ ist das Nachfolgeprojekt von „Wählen im Internet“ und wurde ebenfalls vom BMWA gefördert. Gestartet wurde W.I.E.N im Jahre 2002 mit dem Ziel, verschiedene Typen von Onlinewahlen zu entwickeln und zu testen. Dies sollte für kleinere, nicht-parlamentarische Wahlen, wie z. B. bei Betriebsrats-, Aktionärs-, Personalrats- und Sozialwahlen, geschehen. Verwendet wird dazu das i-vote System, das an die organisatorische Gestaltung, an rechtliche Fragen und die Akzeptanz bei den Wählern angepasst werden sollte. Erklärtes Ziel von W.I.E.N. war es, ein erprobtes Wahlverfahren für alle Formen der Onlinewahl bereitzustellen (vgl. [Was]).

Das Projekt W.I.E.N. wurde von einem Konsortium durchgeführt, dessen Mitglieder das T-Systems CDS, die Forschungsgruppe Internetwahlen der Universität Osnabrück und der Landesbetrieb für Datenverarbeitung und Statistik (LDS) Brandenburg waren (vgl. [Was]).

Im Jahre 2002 wurden durch die Projektgruppe W.I.E.N. zwei rechtsgültige Onlinewahlen mit i-vote durchgeführt: Die erste Wahl vom 6. bis 8. Mai 2002 war die Betriebsratswahl im Unternehmen T-Systems CSM. Damit ist, nach der Projektgruppe W.I.E.N., T-Systems CSM das erste Unternehmen in Deutschland, das eine bundesweite, rechtsgültige Betriebsratswahl elektronisch durchgeführt hat. Bei dieser Betriebsratswahl konnten 7000 Mitarbeiter aus sieben Nieder-

lassungen mit insgesamt 15 Wahlorten von ihrem Arbeitsplatz oder von einem Wahllokal aus die Onlinewahl ausführen. Alternativ konnte auch per Papierwahlbogen gewählt werden. In den meisten Betrieben stimmten 70% bis 90% der WählerInnen im Wahllokal per Onlinewahl ab, in Magdeburg wurde im Wahllokal sogar zu 100% online gewählt. Größere Probleme gab es bei dieser Wahl angeblich nicht (vgl. [DCC02]).

Die zweite Wahl vom 24. bis 31. Mai 2002 war, laut der Projektgruppe W.I.E.N., die erste weltweit rechtsverbindliche Online-Personalratswahl. Sie wurde im LDS Brandenburg in Potsdam mit 538 Mitarbeitern durchgeführt. Von diesen Wahlberechtigten wählten 72% über Computer an vier Wahlorten. Die Wahl verlief ohne größere Probleme, aber bei der Auszählung wurde festgestellt, dass mehr Stimmen abgegeben worden waren, als sich Wähler registriert hatten. Der Grund für diesen Fehler konnte nicht festgestellt werden, deshalb wird vermutet, dass die Abweichung auf Bedienungsfehler des Wahlvorstandes zurückzuführen ist (vgl. [LDS02]).

Online-Wahlsystem Polyas Das web-basierte Online-Wahlsystem Polyas (vgl. [Pol]) wird von der Micromata Objects GmbH (siehe [Mica]) entwickelt. Polyas existiert bereits seit 1996 und wurde nach dem 1985 verstorbenen Mathematiker George Pólya benannt (vgl. [Micc]). Zielgruppe für Polyas sind Vereine und Verbände, die eine Onlinewahl über private Computer durchführen möchten. Die Micromata Objects GmbH stellt dabei nicht nur die Software, sondern auch die Wahlserver zur Verfügung. Außerdem werden weitere Services, wie das Wählerverzeichnis anzulegen, sowie die Wahlunterlagen zu erstellen und zu verteilen, angeboten. Ähnlich wie i-vote arbeitet Polyas mit einem getrennten Wahlamts- und Urnenserver. Die Identifikation des Wählers gegenüber dem Wahlamtsserver erfolgt aber nicht über eine Signaturkarte, sondern nur über eine PIN und eine TAN. Wenn die PIN und TAN an den Wahlamtsserver übermittelt und geprüft wurden, schickt dieser einen Wahlschlüssel an den Wähler zurück, mit dem dieser seine Stimme verschlüsseln und an den Urnenserver schicken kann (vgl. [Micb]).

Eingesetzt wurde Polyas bereits in mehreren größeren Wahlen:

- Die erste große Wahl fand 1996 in Finnland statt. Damals gaben 64.000 Jugendliche mit Polyas bei der Youth Election ihre Stimme ab.
- Im Jahre 2002 fand parallel zur Bundestagwahl in fast allen Bundestagswahlkreisen eine Jugendwahl mit insgesamt 72.000 Wählern statt.
- Die erste rechtsgültige Vereinswahl wurde 2003 mit Polyas durchgeführt. Damals wurde der Vorstand der „Initiative D21“ (vgl. [D21]) gewählt. Im Jahre 2005 wurde erneut der Vorstand über Polyas gewählt.
- Im Herbst 2004 wählten über 20.000 Mitglieder der „Gesellschaft für Informatik“ (siehe [GI]) über Polyas das Präsidium.

Automatisches Wahlabwicklungssystem Seit der Bundestagswahl 2002 wird in Deutschland ein System zur automatischen Wahlabwicklung eingesetzt. Das sogenannte IVU-System wurde von der IVU Traffic Technologies AG (siehe [IVU]) in Zusammenarbeit mit dem Statistischen Bundesamt entwickelt und steuert den gesamten Wahlprozess nach der Auszählung der Stimmen. Am Wahlabend werden von den 16 Landeswahlleitern die Ergebnisse der Auszählung erfasst und über verschlüsselte Verbindungen zu den Servern in Wiesbaden geschickt. Dort wird die vollständige Sitzeverteilung für den neuen Bundestag berechnet. Aktuelle Hochrechnungen werden ebenfalls vom System aufbereitet. Außer bei den Bundestagswahlen wurde das IVU-System 2004 auch bei Wahlen zum EU-Parlament und bei Wahlen auf Landesebene (z. B. im Saarland) eingesetzt (vgl. [Hen04] und [IVU05]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	seit 1999
Onlinewahlen	✔	2000
Wahlen per Handy	✘	

Tabelle 5.1: Übersicht eingesetzter Technologien in Deutschland

Probleme und Kritik

Es hat sich gezeigt, dass Kosten gespart werden können, indem die Anzahl der Wahlbezirke und Wahlhelfer reduziert wird. In Köln wurde die Anzahl der Wahlbezirke um ca. 30% und die Anzahl der Wahlhelfer um ca. 50% verringert. Diese starke Reduzierung ist möglich, weil vor allem die Auszählung der Stimmen kaum noch einen Zeitaufwand bedeutet. Es wird einfach der Zählspeicher aus der Wahlmaschine genommen und in die Zählmaschine gesetzt. Durch diese Arbeitserleichterung kann die Anzahl der Wahlhelfer auf ein Minimum herabgesetzt werden, wodurch sich die starke Reduzierung der Wahlhelfer erklären lässt (vgl. [Sie05]).

Die elektronischen Wahlmaschinen der Firma Nedap wurden allerdings von Irland als unsicher eingestuft und deshalb zur Wahl 2005 nicht eingesetzt (vgl. [Com04] und [Com05]). Die Prüfberichte der PTB für die Bauartzulassung in Deutschland wurde nicht der Allgemeinheit zugänglich gemacht, was vermuten lässt, dass die Wahlmaschinen tatsächlich nicht so sicher sind, wie sie sein sollten. Bisher ist allerdings noch nicht von Manipulationen bzw. Manipulationsversuchen während einer der letzten drei Bundestagswahlen berichtet worden, was wiederum für die Wahlmaschinen der Firma Nedap spricht.

Kritisiert werden kann aber, dass die Geräte der Firma Nedap keine Papierausdrucke erzeugen, über die das Ergebnis der Wahlmaschine überprüft werden könnte. Ein anderes Problem ist, dass es einige Wähler gab, die die Wahlmaschinen zunächst nicht richtig bedienten. Dies lässt sich zumindest zum Teil darauf zurückführen, dass die elektronischen Wahlmaschinen noch neu und ungewohnt sind. Zum anderen sind die Maschinen natürlich nicht so intuitiv zu bedienen, wie ein Blatt Papier, auf dem mit einem Stift nur zwei Kreuze gemacht zu werden brauchen.

Im Fall von i-vote zeigte sich, dass die fehlende flächendeckende Verwendung von Chipkartenlesegeräten ein Problem ist: Die zur Wahl verteilten Lesegeräte funktionierten nicht an jedem Computer. Würde jeder Bürger mit einer Chipkarte für digitale Signaturen ausgestattet und wären Chiplesegeräte weiter verbreitet, dann wären die Probleme in diesem Bereich sehr viel geringer.

Ausblick in die Zukunft

Für die nahe Zukunft kann davon ausgegangen werden, dass in mehr Wahlbezirken elektronische Wahlmaschinen eingesetzt werden. Außerdem werden mit Sicherheit auch Landtags- und Kommunalwahlen mit Wahlmaschinen durchgeführt werden.

Da die Wahlergebnisse bereits über das Internet an den zentralen Wahlserver geschickt werden, könnte in Zukunft auch eine direkte Vernetzung der elektronischen Wahlmaschinen mit dem Wahlserver geschehen, natürlich nur unter der Voraussetzung, dass Wahlmaschinen eingesetzt werden, die eine solche Vernetzung zulassen, was bei den aktuell eingesetzten Geräten der Firma Nedap nicht der Fall ist. Die Abgabe der Stimme wird mit Sicherheit auch weiterhin in Wahllokalen stattfinden, weil die Wähler sich den bisherigen elektronischen Wahlmaschinen nicht per Chipkarte ausweisen können. Ein Aufstellen der Wahlmaschinen an öffentlichen Plätzen macht aus diesem Grund keinen Sinn, zumal dann eine freie und geheime Wahl nicht mehr sichergestellt werden kann.

Parlamentarische Wahlen von einem beliebigen Computer über das Internet oder einem Handy bleiben auf Grund von Sicherheitsbedenken und rechtlichen Einschränkungen zur Zeit noch ein fernes Ziel.

5.3.2 Australien

Australien verwendet, seit die gesetzlichen Grundlagen für den Einsatz von elektronischen Wahlen im Dezember 2000 geschaffen wurden, sowohl dieses als auch elektronische Stimmauszählung. Beide Verfahren wurden erstmals bei den parlamentarischen Wahlen im Oktober 2001 eingesetzt und auch bei der Wahl vom Oktober 2004 fanden diese wieder Anwendung (vgl. [Elea]).

Das e-Voting-System besteht aus Wahl-Terminals, die mit dem in jedem Wahllokal befindlichen Server vernetzt sind. Keine der Stimmen werden über öffentliche Netzwerke wie z. B. das Internet übermittelt (vgl. [Elea]).

Personen, die ihre Stimmen abgeben möchten, werden zunächst durch Offizielle von der Wählerliste gestrichen, um zu gewährleisten, dass jede Person nur einmal wählt. Sie werden dann vor die Entscheidung gestellt, entweder auf elektronischem Wege oder wie bisher auf Papier abzustimmen. Bei der elektronischen Stimmabgabe erhalten die Wähler einen eindeutigen Barcode, der aus einem zufällig geordneten Stapel für die eingeschriebene Wählerschaft entnommen wird. Dieser identifiziert nicht den Wähler, sondern nur die Wählerschaft (electorate) und das Wahllokal. Außerdem enthält er eine digitale Signatur, um Fälschungen vorzubeugen (vgl. [Eleb]).

Die Stimmabgabe erfolgt an den elektronischen Wahlmaschinen, bei denen der Wähler als erstes die Möglichkeit der Sprachauswahl hat. Durch Einscannen des Barcodes wird die Wahl begonnen und dem Wähler der elektronische Stimmzettel auf dem Bildschirm präsentiert. Mit Hilfe von einigen Knöpfen kann dieser dann durch die einzelnen Parteien und Kandidaten navigieren und für einzelne abstimmen. Die Wahl wird durch ein erneutes Einlesen des Barcodes bestätigt, wobei eine Stimme nur dann akzeptiert wird, wenn es derselbe Barcode war, mit dem die Wahl auch begonnen wurde. Hierbei ist es auch möglich, eine ungültige Stimme abzugeben, indem vorher kein Kandidat ausgewählt wurde. Nach der Wahl wird der Barcode vom System als bereits verwendet erkannt, so dass mit diesem keine weitere Abstimmung möglich ist (vgl. [Eleb]).

Das e-Voting-System steht für die Wähler drei Wochen vor dem eigentlichen Wahltag in sog. pre-poll voting centres und am Wahltag in einer begrenzten Anzahl in Wahllokalen zur Verfügung. Wähler haben die Möglichkeit zu entscheiden, ob sie elektronisch oder wie bisher auf Papier abstimmen möchten. Bietet das Wahllokal keine elektronische Abstimmungsmöglichkeit an, so können die Wähler dort nur auf Papier wählen (vgl. [Elea]).

Die elektronische Stimmauszählung erfasst sowohl die auf Papier als auch die elektronisch abgegebenen Stimmen. Dazu werden die auf Papier abgegebenen Stimmen von zwei unabhängigen Anwendern eingegeben, vom System elektronisch auf Fehler überprüft und gegebenenfalls manuell korrigiert. Diese Stimmen werden dann mit den elektronisch abgegebenen Stimmen kombiniert ([Elea]).

Elektr. Stimmauszählung	✔	Seit 10/2001
Elektr. Wahlmaschinen	✔	Seit 10/2001
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.2: Übersicht eingesetzter Technologien in Australien

Die Software, die die elektronische Abstimmung und Stimmauszählung ermöglicht – EVACS (electronic voting and counting system) genannt – wurde unter Linux entwickelt, um sicher zu stellen, dass diese offen ist und an dem Wahlprozess beteiligten Personen wie z. B. Wahlhelfern oder Kandidaten zugänglich gemacht werden kann ([Elea]).

5.3.3 Belgien

Belgien hat von den hier erwähnten Ländern eine der längsten Erfahrungen mit elektronischen Wahlmaschinen. Die ersten Versuche fanden bereits 1991 statt, bevor der Einsatz dieser Wahlmaschinen 1994 dann gesetzlich zugelassen wurde. Seitdem hat sich elektronisches Wählen im Land stark verbreitet, z. B. wurde es in den Jahren 1999 und 2000 für Kommunal- sowie Parlamentswahlen in weiten Teilen Belgiens eingesetzt. Inzwischen sind weitere Gemeinden mit Wahlmaschinen ausgestattet worden und laut [Bel04b] wird erwartet, dass in diesem Jahr alle Wahlberechtigten elektronisch abstimmen können.

Die in Belgien verwendeten Wahlmaschinen, die u. a. auch bei den Wahlen im Mai 2003 sowie bei der europäischen und den regionalen Wahlen am 13.06.2004 zum Einsatz kamen, bestehen aus Computern mit Kartenlesern, Bildschirmen und einem optischen Stift. Wahlsimulationen in verschiedenen Sprachen stehen unter der URL `http://elections2004.belgium.be/fr/automated\_voting.html` zur Verfügung. Wähler, die sich vorab mit dem System und dem Verlauf der Stimmabgabe vertraut machen wollten,

denen dafür aber die Simulation nicht genügte, konnten die Wahlmaschinen einige Tage vor der Wahl selbst ausprobieren. Das System ermöglicht jedoch nicht, die einmal abgegebene Stimme nachträglich zu ändern (vgl. [Bel04b]).

Die Wahlmaschinen standen 2003 und 2004 ausschließlich in Wahllokalen zur Verfügung. An anderen öffentlichen Einrichtungen konnten keine Stimmen abgegeben werden. Im Vergleich zu 2003 konnten bei den Wahlen 2004 die Wahllokale, auch wenn einige technische Probleme auftraten, rechtzeitig schließen. Dies war 2003 auf Grund von Verzögerungen, die durch eine zu geringe Anzahl an bereitgestellten Wahlmaschinen, eine Reihe von Computerfehlern oder Stromausfällen, die Komplexität des System sowie die Unkenntnis der meisten Wähler verursacht wurden ([Bel04b]).

Der Quellcode von der Digivote und Jites Wahlsoftware, die in den belgischen Wahlmaschinen eingesetzt wird, wurde nach der Wahl am 13.06.2004 vom belgischen Innenministerium veröffentlicht, um die Transparenz der Wahlprozesse zu gewährleisten (vgl. [Bel04a]).

Kritik wurde zum einen hinsichtlich der verwendeten Software, zum anderen bzgl. der Kontrolle des e-Votings/e-Votingprozesses geäußert. Das Unternehmen aFront, spezialisiert auf den Bereich der Datenkonvertierung sowie des Nachbaus (reverse engineering), hat nach Veröffentlichung des Digivote Quellcodes diesen analysiert und dabei herausgefunden, dass die Anonymität des Wahlprozesses gefährdet sei. Der Analyse zur Folge sind hierfür zwei Hauptfehler verantwortlich, die auf denselben Fehler – der Annahme, dass die Zufallsfunktion tatsächlich eine zufällige Zahl zurückliefert, was laut aFront nicht der Fall sei – zurückzuführen. Hierdurch sei es möglich, die Reihenfolge der Stimmabgaben in fast allen Fällen von dem Inhalt der Datei wiederherzustellen (vgl. [Bel04a]).

Die Freie Universität Brüssel hingegen kritisiert in einem Bericht u. a. , dass der gesamte e-Votingprozess in Belgien nicht transparent sei, da dieser von zwei Unternehmen kontrolliert würde. Hinsichtlich dieses Themas wurde auch von Pour Eva, einer Gruppe von Bürgern, Kritik geäußert. Laut dieser Gruppe kann ein Wahlsystem nur vertrauenswürdig sein, wenn dieses von den Bürgern selbst

kontrolliert werde und nicht von privaten Unternehmen betrieben würde (vgl. [Bel04b]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Seit 1991
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.3: Übersicht eingesetzter Technologien in Belgien

5.3.4 Brasilien

Brasilien setzt, nachdem 1996 erstmals einige Bezirke elektronische Wahlmaschinen eingeführt haben, diese seit 2000 landesweit ein.

In Brasilien kommt ein einheitliches Wahlmaschinensystem zum Einsatz, dass aus tragbaren elektronischen Wahlmaschinen ohne Touchscreen besteht, die für den Fall eines Stromausfalles mit Batterien ausgestattet sind. An einigen Wahlmaschinen sind Drucker angebracht, die einen prüffähigen Ausdruck erzeugen. Dieser kann nach Stimmabgabe durch eine Glasscheibe geschützt vom Wähler angesehen werden, bevor er in einem fest an der Maschine angebrachten versiegelten Plastikbeutel gesammelt wird. Vor der Wahl wird die verwendete Software ins Internet gestellt und die Wahlmaschinen mit den entsprechenden Wahldaten bestückt. Diese sind auf Disketten gespeichert, die auf der Rückseite der Maschinen eingelegt und dort mit manipulationsnachweisendem Klebeband versiegelt werden (vgl. [Mir04]).

Die eingesetzten Wahlmaschinen stammen von dem Unternehmen Diebold Election Systems, das die brasilianischen Firmen Unisys und ProComp übernommen hat, deren Maschinen in den USA von Computerfachleuten bzgl. der Möglichkeit der Verfälschung von Wahlergebnissen (tampering) kritisiert werden. Die in Brasilien eingesetzten Wahlmaschinen besitzen im Gegensatz zu

den in den USA verwendeten keine Touchscreen und sind daher billiger in der Anschaffung (vgl. [Mir04]).

Bei der Präsidentenwahl 2003 konnte die Bevölkerung in (Bus-)Bahnhöfen und Banken ihre Stimme abgeben, wo die tragbaren elektronischen Wahlmaschinen für die Durchführung der Wahl aufgestellt worden sind. In jedem Bezirk war eine Liste mit Nummer und den jeweils zugehörigen aufgestellten Kandidaten erhältlich. Zur Abstimmung gaben die Wähler die Zahl für den Kandidaten ihrer Wahl ein, woraufhin der Name und ein Bild dieser Person erschien. Durch Betätigen eines grünes Knopfes wurde die Wahl bestätigt und konnte im Nachhinein nicht mehr geändert werden (vgl. [Mir04]).

Der Einsatz der Wahlmaschinen bei der Präsidentenwahl 2003 stellte sich jedoch als nicht fehlerfrei heraus, denn menschliche, Hardware- und Softwarefehler haben dazu geführt, dass Ergebnisse bei einer Handvoll von Fällen gestrichen werden mussten (vgl. [Mir04]).

In Brasilien wurde im Oktober 2003 ein Gesetz verabschiedet, dass ausgedruckte e-Voting-Belege abschafft. Regierungsbeauftragten zu Folge würde Brasilien hierdurch etwa 100 Millionen Dollar sparen. Ein weiterer Vorteil sei laut Pressesprecher Paulo Cesar Camarao, dass druckerlose Maschinen den Wahlprozess beschleunigen würden, denn 2003 haben Drucker die Wahl in einigen Gemeinden z. B. um 12 Stunden verzögert. Außerdem würden diese aufgrund des brasilianischen tropischen und subtropischen Klimas häufig technische Probleme erleiden. Von Kritikern wurde dieser Schritt jedoch als Rückschlag bzgl. der Wahltransparenz bezeichnet, da es keine ausgedruckten Belege zum eventuellen späteren manuellen Auszählen mehr gibt und die Wähler der Möglichkeit beraubt werden, ihre Stimme nach Abgabe zu überprüfen (vgl. [Mir04]).

Vorgesehen war, nachdem Anwälte im Jahr 2001 forderten, die Wahlmaschinen mit Druckern auszustatten, an etwa 12000 der eingesetzten Maschinen Drucker anzubringen, so dass die Wähler ihre Stimmen nach der Abgabe auf einem Beleg überprüfen können. Bei der Präsidentenwahl 2003 wurden aber nur in etwa 3% aller Bezirke Drucker verwendet (vgl. [Mir04]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Erstmal 1996, seit 2000 landesweit
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.4: Übersicht eingesetzter Technologien in Brasilien

5.3.5 Estland

Estland hat 2005 sowohl Tests mit Wahlen über das Internet in der Hauptstadt Tallinn als auch landesweit durchgeführt.

Die Stadt Tallinn sowie das estnische nationale Wahlkomitee organisierten im Januar 2005 eine Volksbefragung, bei der die Wähler, Einwohner Tallinns, die Möglichkeit hatten, ihre Stimme online abzugeben. Für die Stimmabgabe über das Internet benötigen die Wähler ID-Karten, von denen über 700000 Stück in drei Jahren ausgegeben wurden. In Tallinn findet diese weite Verbreitung, da sie dort auch als e-Ticket im öffentlichen Verkehr eingesetzt wird (vgl. [Est]).

Anhand des auf jeder ID-Karte vorhandenen Authentifizierungszertifikats kann das Internetvotingsystem die Wähler authentifizieren und anhand einer Liste überprüfen, ob die Personen für die Wahl zugelassen sind oder nicht. Handelt es sich bei den Personen um für die Wahl registrierte Wähler, werden diesen die zur Verfügung stehenden Wahlmöglichkeiten angezeigt. Nach Abgabe der jeweiligen Stimmen werden diese mit dem öffentlichen Schlüssel des Systems verschlüsselt und mit der persönlichen digitalen Signatur des jeweiligen Wählers unter Verwendung der ID-Karte versehen. Damit die Anonymität der Wähler gewährleistet bleibt, wird die digitale Signatur von den übermittelten Stimmabgaben vor der Auszählung entfernt. Ein Wähler kann bei diesem System wiederholt seine Stimme abgeben, für die Auswertung wird jedoch nur die zuletzt abgegebene berücksichtigt. Durch das Systemdesign und die strikt überwachten Prozeduren wird gewährleistet, dass alle Eigenschaften einer demokratischen

Wahl wie Anonymität, freier Wille und eine Stimmabgabe pro Person gewährleistet sind (vgl. [Est]).

Bei den Lokalwahlen im Oktober 2005 wurde dieses Linux-basierte System mit einigen Modifikationen dann landesweit zu Testzwecken eingesetzt. Die Wähler konnten ihre Stimmen über das Internet in einer dreitägigen Phase vom 10. bis zum 12. Oktober vor dem eigentlichen Wahltag am 16.10.2005 abgeben. Die Wähler benötigten hierfür mit dem Internet verbundene Computer mit Kartenlesegeräten, um auf die Wahlwebseite gelangen und sich über ihre elektronischen ID-Karten am System identifizieren zu können. Nach Authentifizierung durch jeweils einen PIN-Code konnten die Wähler schließlich ihre Stimme über ein verschlüsseltes System abgeben, durch einen weiteren PIN-Code ihre Wahl bestätigen und mit ihrer digitalen Signatur versehen (vgl. [Est05]).

Bei den Wahlen im Oktober wurden aufgrund der eingeschränkten Verbreitung von Kartenlesern in der Bevölkerung öffentlich zugängliche Computer u. a. in Banken, in Staats- und Gemeindeämtern und in Telekommunikationsunternehmen aufgestellt.
Durch diese Maßnahme sollte sichergestellt werden, dass das Internetvotingsystem für die etwa 800000 der eine Million Wahlberechtigten, die bereits eine ID-Karte besitzen, zugänglich war. Trotz der Verfügbarkeit des Systems wurden nur 9287 Stimmen online abgegeben. Dies entspricht 1% aller sowie 7% der im voraus abgegebenen Stimmen. Ungeachtet/Obgleich der geringen Beteiligung wurde der Versuch von Wahloffiziellen als Erfolg angesehen, da von keinen technischen oder Sicherheitsproblemen berichtet wurde. Der erfolgreiche Test könnte die Regierung deshalb dazu bewegen, Internetwahl optional aber gesetzlich bindend für die Wahlen 2007 einzusetzen (vgl. [Est05]).

Kritik an dem System kam von dem estnischen Präsidenten Arnold Rüütel, der die Möglichkeit der Änderung einer Stimme durch wiederholtes Wählen über das Internet als Verstoß gegen die Gleichheit der Wähler ansieht, da Personen, die weiterhin auf Papier wählen, ihre Stimme nach Abgabe nicht mehr ändern können (vgl. [Est05]). Das Verfassungsgericht in Tallinn hingegen war nicht dieser Auffassung, da jeder Wähler auch weiterhin nur eine Stimme hat. Diese

Entscheidung vom 01.09.2005 ermöglichte erst den Einsatz des Wahlsystems für eine landesweite politische Wahl (vgl. [Lem05]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✘	
Onlinewahlen	✔	10/2005 landesweiter Test
Wahlen per Handy	✘	

Tabelle 5.5: Übersicht eingesetzter Technologien in Estland

5.3.6 EU

In der Europäischen Union startete am 1. September 1999 das Projekt CyberVote (siehe. [Cyba]). Dieses Projekt wurde von einem Konsortium unter der Leitung der European Aeronautic Defence and Space Company (EADS) (siehe [EAD]) geleitet. Aus Deutschland war die Freie Hansestadt Bremen (siehe [Sta]) Mitglied des Konsortiums. Ziel von CyberVote war es, einen Prototyp für ein Onlinewahl-System zum Einsatz bei staatlichen Volksvertreterwahlen zu erstellen. Dafür stand bis zum 1. März 2003 ein Budget von 3,2 Millionen Euro zur Verfügung. Offiziell beendet wurde das Projekt aber erst im Juli 2003. (vgl. [Cybb])

Da die Stadt Bremen an CyberVote beteiligt war, wurde ein Prototyp des CyberVote-Systems vom 13. bis 15. Januar 2003 bei Wahlen in der Universität Bremen zu Testzwecken eingesetzt. Für die Wahl wurden die Stimmen über einen bereitgestellten und von den Wahlhelfern überwachten Computer durchgeführt. Signiert wurde die Stimme mit Hilfe einer zuvor registrierten Signaturkarte. Obwohl sich fast 300 Personen registriert hatten, stimmten nur 47 Personen über das CyberVote-System ab. Allerdings lag die gesamte Wahlbeteiligung auch nur bei unter 10% (vgl. [Cybc]).

Neben der Wahl an der Universität Bremen wurde noch eine Testwahl in Stockholm in Schweden mit 226 Wahlteilnehmern und eine Testwahl in Issy les Moulineaux in Frankreich mit 860 Teilnehmern durchgeführt. Die Wahl in Schweden wurde vom 27. bis 31. Januar 2003 von Wahlkiosken aus durchgeführt. Bei Interesse konnte die Stimme auch über einen Nokia Communicator (Nokia ist Mitglied im CyberVote Konsortium) abgegeben werden. Die Wahl in Frankreich fand am 11. Dezember 2002 statt und konnte von einem der zehn Wahlkioske oder von einem privaten Computer aus durchgeführt werden (vgl. [Cybc]).

Am 13. Oktober 2004 wurde das CyberVote-System noch einmal in Paris, Bordeaux, Grenoble, Nizza und Alençon in Frankreich eingesetzt. Über den drei Wochen dauernden Wahlzeitraum nahmen bei dieser Onlinewahl 340.000 Wähler teil.

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✘	
Onlinewahlen	✔	getestet
Wahlen per Handy	✔	in Schweden getestet

Tabelle 5.6: Übersicht EU-weiter Projekte

5.3.7 Frankreich

In Frankreich dürfen elektronische Wahlmaschinen für gesetzlich bindende politische Wahlen eingesetzt werden, nachdem am 18.03.2004 eine Verordnung von der Regierung verabschiedet wurde, die es zuerst 33, später dann 20 weiteren, Gemeinden erlaubt, Wahlmaschinen einzusetzen (vgl. [Fra05b]).

Elektronische Wahlmaschinen wurden in Frankreich erstmal während der Europäischen Wahlen am 13.06.2004 in 18 Gemeinden und bei den Regionalwahlen

im März 2004 von sechs Städten getestet, darunter auch die erste gesetzlich bindende Wahl in Brest. Bei beiden Gelegenheiten wurde von keinen großen technischen Problemen berichtet (vgl. [Fra05b]). Bei der Volksabstimmung am 20.05.2005 zur EU-Verfassung wurden in etwa 60 Gemeinden elektronische Wahlmaschinen verwendet, wobei die Stimmabgabe in einigen Gemeinden gesetzlich bindend und in anderen nur optional war (vgl. [Fra05a]).

Bei der Volksabstimmung 2005 durften drei der vier vom Innenministerium anerkannten Arten von Wahlmaschinen eingesetzt werden. Zu diesen zählen nach [Fra05b] die Wahlmaschinen von Nedap 2.07 (durch France Election vertrieben), iVotronic (durch RDI-Concortium Univote vertrieben) und Point&Vote (gebaut und vertrieben durch das spanische Unternehmen Indra), die bereits bei den Wahlen 2004 getestet worden sind. Am 08.03.2005 wurde dann die vierte Art von Wahlmaschinen (Nedap ESF1) vom Innenministerium anerkannt, die bei der Volksabstimmung aber nicht zur Anwendung kam. Trotz dieser Auswahl an Wahlmaschinen setzten ungefähr drei Viertel der Kommunen die Nedap Powervote Maschinen ein (vgl. [Fra05a]).

Zusätzlich zu den Wahlmaschinen wurde bei der Volksabstimmung 2005 E-Poll, ein elektronisches System für vernetzte Wahlen (remote voting), von einigen Einwohnern von Issy-les-Moulineaux getestet. Im Unterschied zu den anderen eingesetzten Maschinen identifizieren die Maschinen von E-Poll die Wähler anhand von sog. smart cards. Durch eine Vernetzung dieser Maschinen ist es einerseits außerdem möglich, dass Wähler in irgendeinem Wahllokal ihre Stimme abgeben können und andererseits können die Ergebnisse der einzelnen Wahllokale einfach zusammengefasst werden ([Fra05a]).

Ursprünglich wurde das E-Poll Konzept zwischen September 2000 und November 2002 als ein IST Forschungsprojekt unter dem Fifth Framework Programme for Research and Development der EU entwickelt und wird seitdem als ein eTEN Projekt weitergeführt. Ziel dieses Projektes ist es, ein vollständiges e-voting System zu entwickeln, dass einfach an die unterschiedlichen Gesetzgebungen in europäischen Ländern angepasst werden kann (vgl. [Fra05a]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Erste bindende Wahl 2004 in Brest
Onlinewahlen	✔	Test bei Volksabstimmung 2005
Wahlen per Handy	✘	

Tabelle 5.7: Übersicht eingesetzter Technologien in Frankreich

5.3.8 Großbritannien

Großbritannien hat von 2002 bis 2003 Versuche mit e-Voting durchgeführt, weitere für die Wahlen 2004 und 2005 geplante Tests wurden jedoch auf Anraten der Wahlkommission abgesagt. Auch die für die Lokalwahlen im Mai 2006 angesetzten e-Voting Versuche wurden von der Regierung abgesagt (vgl. [GBC05]).

Des Weiteren wird in Großbritannien elektrische Stimmauszählung eingesetzt. Erste Versuche fanden während der Bürgermeister- und London Assembly Wahlen 2000 in London statt, bei der ein paar organisatorische und kleinere technische Probleme in einigen Auszählungsstellen eine optimale Leistung dieser Technologie verhindert haben. Die Auszählungsergebnisse lagen dennoch zur Mittagszeit nach dem Wahltag vor. Der Einsatz elektrischer Stimmauszählung in London bei der Wahl im Juni 2004 dagegen lief reibungslos ohne berichtete technische Probleme ab. Die Auszählung der Stimmzettel für die Lokal-, Europa- und Bürgermeisterwahlen endete bereits am selben Abend (vgl. [GBE04]).

Für die elektronische Stimmauszählung in London wurden ungefähr 300 Scanner in 14 Auszählungseinrichtungen eingesetzt, die es erlaubten, fast sechs Millionen Stimmzettel von drei verschiedenen Wahlsystemen (für die Lokal-, Europa- und Bürgermeisterwahl) innerhalb von einigen Stunden zu zählen. Das System wertet die Stimmzettel aus und speichert elektronische Bilder von den

Stimmzetteln, bei denen es Zweifel an der Absicht des Wählers gab, um sie für anschließende Entscheidungen den Wahlhelfern zu präsentieren ([GBE04]).

Bisher wurde die elektronische Stimmauszählung nur in London eingesetzt, auch wenn im März 2004 das Büro des stellvertretenden Premierministers dem Testeinsatz der elektronischen Stimmauszählung zugestimmt haben. Aufgrund von zeitlichen Engpässen konnte diese Technologie zur Wahl 2004 nur in London verwendet werden ([GBE04]).

Elektr. Stimmauszählung	✔	2000 erste Versuche, 2004 nur in London
Elektr. Wahlmaschinen	✘	Tests in 2002/03, weitere abgesagt
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.8: Übersicht eingesetzter Technologien in Großbritannien

5.3.9 Indien

Indien führte 1998 erste Tests mit elektronischen Wahlmaschinen in 16 Wahlkreisen bei drei Landtagswahlen durch. Zur Bundes- und Landtagswahl 2004 wurden die Wahlmaschinen landesweit zu Testzwecken eingesetzt (vgl. [Ind04a]).

Die verwendeten elektronischen Wahlmaschinen wurden von dem Wahlkomitee in Zusammenarbeit mit zwei staatseigenen Unternehmen, Bharat Electronics und Electronics Corporation of India, entwickelt. Sie bestehen jeweils aus zwei Einheiten, die durch ein Kabel miteinander verbunden sind. Zum einen gibt es die Steuerungseinheit, die von den Wahlhelfern bedient wird, und eine Einheit, die sich in der Wahlkabine befindet und die Stimmabgaben der Wähler entgegennimmt (vgl. [Ind04a]).

Die Einheit, die die Wähler zum Abstimmen nutzen, besitzt eine Reihe von Knöpfen, neben denen sich jeweils der Name und das Symbol eines Kandidaten oder einer Partei auf Papierstreifen notiert befinden, so dass sich die Knöpfe bei verschiedenen Wahlen unterschiedlichen Kandidaten zuweisen lassen. Die verwendete Software ist auf einem Mikroprozessor eingebettet oder in diesen fest einprogrammiert. Bei dem Versuch, eine Maschine aufzubrechen, schaltet sich diese automatisch aus. Auch können Wahlhelfer die Maschinen bei Problemen per Knopfdruck abschalten (vgl. [Wei04]).

Die Wähler können, nachdem sie eine ID-Karte aus Papier vorgelegt haben, durch Druck auf den entsprechenden Knopf für einen Kandidaten abstimmen. Eine leuchtende rote Lampe und ein akustisches Signal geben an, dass die Stimme registriert worden ist. Die Wahlmaschinen sind so programmiert, dass sie nur eine Stimme jede fünf Sekunden annehmen. Es erfolgt jedoch kein Ausdruck der abgegebenen Stimmen (vgl. [Wei04]).

Nach Abgabe aller Stimmen, werden die Wahlmaschinen solange unter Verschluss gehalten, bis die Auszählung beginnt. Wahlhelfer rufen dabei die Anzahl der abgegebenen Stimmen für jeden Kandidaten von den Maschinen ab, die dann in einer Auszählungsstelle anhand einer Strichliste authentifiziert werden (vgl. [Ind04b]).

Für die Wahlen 2004 wurden elektronische Wahlmaschinen in knapp 200000 Wahlkabinen aufgestellt. Es gab einige Berichte, nach denen es bei der Durchführung der Wahl zu ein paar Problemen kam, z. B. war eine Maschine blockiert und konnte nicht ersetzt werden, so dass Wähler ihre Stimmen nicht abgeben konnten, und es gab Berichte von einer Wahlmanipulation (vote tampering), von fehlerhaften Starts (faulty starts) und von Verwirrung auf Seiten der Wähler (vgl [Ind04b]).

Indiens oberstes Gericht hat entschieden, bzgl. einer Klage eines Informatikers keine Entscheidung zu treffen, besorgt, dass die Wahlmaschinen nicht so manipulationssicher sein könnten, wie die Regierung dies behauptete. Frederick Noronha erklärte, dass ein Missbrauch der Maschinen nur deshalb möglich sei, da der Quellcode von den beiden Herstellern der Wahlmaschinen nicht der Öffent-

lichkeit zugänglich gemacht wurde und somit nur einige Offizielle verstehen würden, wie die Maschinen funktionieren (vgl. [Wei04]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	1998 erste Tests, 2004 landesweit
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.9: Übersicht eingesetzter Technologien in Indien

5.3.10 Irland

In Irland sollten zu den Lokal- und Europawahlen im Juni 2004 elektronische Wahlmaschinen eingesetzt werden. Aufgrund eines Zwischenberichts der Commission on Electronic Voting wurde der Einsatz der Wahlmaschinen von der Regierung im April 2004 abgelehnt (vgl. [Irl05]).

Bei den Wahlmaschinen, die in Irland zur Lokal- und Europawahl 2004 zum Einsatz kommen sollten, handelt es sich um Nedap/Powervote Maschinen. Die 6200 Maschinen fanden in Irland bisher aber bei keiner gesetzlich bindenden Wahl Anwendung (vgl. [Irl05]). Die unabhängige Commission on Electronic Voting, die das Nedap/Powervote System getestet hat, empfiehlt in ihrem Zwischenbericht vom 30.04.2004 (vgl. [Com04]) den Einsatz dieser Wahlmaschinen nicht. Zu den angeführten Gründen, die zu dieser Einschätzung der Commission führten, gehören laut [Irl04]:

- Unzureichende Systemprüfungen: Die bisher durchgeführten Tests können die Zuverlässigkeit des System nicht belegen.
- Zeitmangel für Softwaretests: Aufgrund des Zeitmangels bis zu den Wahlen im Juni 2004 konnte die endgültige Version der Software nicht vollständig getestet werden.

- Kein Zugang zum Quellcode: Das Komitee erhielt keinen Zugang zu dem vollständigen Quellcode.
- Richtigkeit kann nicht bestätigt werden: Da die endgültige Version der Software bisher unbekannt ist, ist es unmöglich, die Fehlerfreiheit dieser zu bestätigen.
- Bedenken bzgl. Geheimhaltung: Das Komitee hat des Weiteren Bedenken hinsichtlich des Wahlgeheimnisses (z. B. könnte es für einen Insider möglich sein, die Zufälligkeit der Methode herauszufinden, die für die Speicherung der Stimmen genutzt wird).

In dem Zwischenbericht werden auch Handlungsempfehlungen genannt, die es dem Komitee erlauben sollen, sich von der Richtigkeit des Systems und der Geheimhaltung von Stimmen zu überzeugen. Erwähnt werden nach [Irl04] u. a. :

- Es sollte sich auf eine endgültige Version der Software sowie zugehörige Hardware- und Softwarekomponenten geeinigt werden, die bei Wahlen eingesetzt werden soll.
- Es sollte eine unabhängige Überprüfung sowie ein Test des endgültigen Quellcodes durchgeführt werden. Nachfolgende Änderungen an der Software machen einen weiteren vollständigen Systemtest erforderlich.
- Es sollte ein unabhängiger end-to-end Test des Systems durchgeführt werden.
- Es sollte ein unabhängiger paraller Systemtest möglichst in einem echten Wahlkontext durchgeführt werden.
- Eine anerkannte Institution sollte die Tauglichkeit jeder neuen Version des gesamten Systems für den Einsatz bei Wahlen testen und zertifizieren.

Trotz der Kritik möchte die Regierung das System bei zukünftigen Wahlen einsetzen (vgl. [Irl05]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✘	Ablehnung von Wahlmaschinen 2004
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.10: Übersicht eingesetzter Technologien in Irland

5.3.11 Italien

Italien setzt weder elektronische Stimmauszählung noch elektronische Wahlmaschinen gesetzlich bindend ein, jedoch wurden mit beiden Technologien Experimente durchgeführt.

Elektronische Stimmauszählung wurde sowohl bei der Wahl zum Europaparlament im Juni 2004 wie auch bei den Regionalwahlen in Ligurien im April 2005 zu Testzwecken eingesetzt. Bei der Wahl 2004 erstreckte sich der Einsatz der elektronischen Stimmauszählung über ganz Italien und fand neben der traditionellen Auszählung per Hand in annähernd 1500 Wahlbezirken statt. Ziel dieses Versuches, bei dem ungefähr eine Million Stimmen aus 49 Städten gezählt wurden, war es, den elektronischen Wahlprozess sowie die elektronische Übertragung der Wahlergebnisse zu testen. In jedem Wahllokal wurden die Stimmzettel gescannt und die gewonnenen Daten auf einem lokalen Computer gespeichert. Diese Ergebnisse wurden dann elektronisch in eine nationale Zentrale übertragen. Der gesamte Versuch wurde von Innovazione Italia, einem im Oktober 2003 gegründeten staatseigenen Unternehmen, koordiniert (vgl. [Ita04]).

Die elektronische Stimmauszählung bei den Regionalwahlen in Ligurien vom April 2005 umfasste erstmals eine ganze italienische Region (1796 Wahlbezirke in 235 Gemeinden). Hierfür wurde eine umfangreiche technische Architektur in Ligurien geschaffen, die u. a. aus einem Netzwerk von lokalen IT-Systemen für die Erfassung, die Speicherung und die Übertragung von Prüfdaten sowie einem zentralen System für die Zusammenführung und Analyse dieser Daten bestand.

Die Ergebnisse der elektronischen Stimmauszählung wurden verschlüsselt und elektronisch an die zuständigen Behörden übermittelt. Dieser Versuch wurde vom Innenministerium, dem Department für Innovation und Technologien, dem Vorsitz des Regierungspräsidiums von Ligurien und der staatseigenen Firma Innovazione Italia koordiniert (vgl. [Ita05]).

Elektronische Wahlmaschinen wurden bei der Wahl zum Europaparlament 2004 in Vigevano in Norditalien eingesetzt, bei denen über 4000 registrierte Wähler die Möglichkeit hatten, diese zu testen. Die verwendeten Wahlmaschinen stammen von AccuPoll, einem US-amerikanischen Unternehmen. Diese sind mit Touchscreens ausgestattet und stellen ausgedruckte Belege der abgegebenen Stimmen bereit, so dass Wähler ihre Stimmabgabe überprüfen können und eine manuelle Auszählung der Stimmen im Nachhinein ermöglicht werden kann (vgl. [Ita04]).

Elektr. Stimmauszählung	✔	Tests in 2004 und 2005
Elektr. Wahlmaschinen	✔	Tests in 2004
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.11: Übersicht eingesetzter Technologien in Italien

5.3.12 Japan

Japan setzte erstmals bei Lokalwahlen in Niimi, etwa 500 Kilometer südwestlich von Tokio, im Juni 2002 elektronische Wahlmaschinen ein (vgl. [Ass02]).

Die verwendeten Wahlmaschinen identifizieren die Wähler anhand von eingesteckten Plastikkarten in der Größe von Kreditkarten. Auf dem Touchscreen der Maschinen erscheinen dann die Namen der Kandidaten, aus denen der Wähler durch Drücken des Entsprechenden seinen Favoriten auswählen kann (vgl. [Ass02]).

Bei der Lokalwahl in Niimi wurden 15000 Stimmen in 43 Wahllokalen auf elektronischem Wege abgegeben. Die Ergebnisse der Wahl wurden 40 Minuten nach Beginn der Auszählung der elektronischen Stimmzettel, die 90% der abgegebenen Stimmen umfassten, bekanntgegeben. Die übrigen etwa 2000 Stimmzettel auf Papier wurden manuell ausgezählt (vgl. [Ass02]).

Die Wahl verlief – abgesehen von einer anfänglichen Maschinenstörung, die die Ausstellung von Wahlkarten für etwa 15 Personen verzögerte – reibungslos (vgl. [Ass02]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Erstmals 2002
Onlinewahlen	✘	
Wahlen per Handy	✘	

Tabelle 5.12: Übersicht eingesetzter Technologien in Japan

5.3.13 Kanada

Kanada hat in dem Staat Ontario im November 2003 zu den Gemeindewahlen die erste vollständig elektronische Wahl in Nordamerika durchgeführt.

Die etwa 100000 registrierten Wähler aus 12 Gemeinden im Osten Ontarios konnten vom 5. bis zum 10. November 2003 ihre Stimme über das Internet oder per Tonwahltelefon abgeben. Die Möglichkeit, wie bisher auf Papier zu wählen, stand für die Wähler dieser Gemeinden nicht mehr zur Verfügung. Um den Wählern die Stimmabgabe elektronisch zu ermöglichen, erhielten diese Wähleridentifiaktionsnummern und Passwörter (vgl. [Kan03]).

Das eingesetzte System, das unter Linux betrieben wird, stammt von dem kanadischen Unternehmen CanVote. Nach Aussage dessen Vorsitzenden, Joe Church, bietet das System Sicherheit und Flexibilität. Des Weiteren wies er

daraufhin, dass für die Stimmabgabe eine 128-bit Verschlüsselung verwendet werde, wie sie z. B. auch bei Banken zum Einsatz kommt. Außerdem erhöhe das System die Zugänglichkeit für behinderte Wähler durch den Einsatz akustischer Webbrowser und Braille-fähiger Technologie. Zusätzlich erwähnte Church, dass durch die Verwendung des Systems die Wahlbeteiligung in einigen Orten auf 55% (im Vergleich zu 25 bis 30% bei normalen Gemeindewahlen) angestiegen sei (vgl. [Lym03]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✘	
Onlinewahlen	✔	2003 in Ontario
Wahlen per Handy	✘	

Tabelle 5.13: Übersicht eingesetzter Technologien in Kanada

5.3.14 Niederlande

In den Niederlanden werden seit langer Zeit elektronische Wahlmaschinen gesetzlich bindend eingesetzt. Zusätzlich führte Holland 2004 einen Test mit Onlinewahlen durch.

Bei den, in den Niederlanden verwendeten, elektronischen Wahlmaschinen handelt es sich um Nedap Powervote Maschinen. Zuletzt wurden diese bei der Volksabstimmung über die europäische Verfassung am 01.06.2005 eingesetzt. Die Mehrheit der Wähler benutzen dabei die Wahlmaschinen, die in den Niederlanden weite Verbreitung gefunden haben. Mit Ausnahme von Amsterdam, Arnheim und einigen kleinen Ortschaften waren die Wahlmaschinen allgegenwärtig. Berichte von Problemen gab es bei dieser Wahl nicht (vgl. [Fra05a]).

Bei der Wahl zum Europaparlament 2004 wurde in den Niederlanden erstmals die Wahl über das Internet für im Ausland lebende Bürger getestet. Etwa 5000

Wähler gaben ihre Stimmen online über das System ab, das Bestandteil eines größeren Fernwahlprogramms (remote voting programm) ist, dass auch eine telefonbasierte Lösung (telephon-based voice solution) umfasst (vgl. [Nie04]).

Die niederländische Regierung hat am 21.06.2004 den Quellcode von der Software, die für die Wahl über das Internet verwendet wurde, unter der URL http://www.ososs.nl/index.jsp öffentlich zur Verfügung gestellt. Der Quellcode steht unter der General Public License (GPL), die es ermöglicht, dass Interessierte diesen auf Sicherheitsverstöße/Sicherheit hin untersuchen können. Dieser Schritt der Regierung kann als Antwort auf die Kritik u. a. von Seiten der Organisation Electronic-highway Platform Nederland (EPN) angesehen werden. Kritisiert wurde dabei z. B. die Wahl eines geschützten Softwarepakets anstatt von Open Source Software, die es erlauben würde, die öffentliche Kontrolle über das System zu vergrößern. Von der Veröffentlichung des Quellcodes bleibt die Software in den Nedap Powervote Maschinen ausgenommen (vgl. [Nie04]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Letzter gesetzlich bindender Einsatz 2005
Onlinewahlen	✔	Erster Test 2004
Wahlen per Handy	✘	

Tabelle 5.14: Übersicht eingesetzter Technologien in den Niederlanden

5.3.15 Portugal

Portugal hat sowohl Tests mit elektronischen Wahlmaschinen als auch mit Wahlen über das Internet durchgeführt.

Elektronische Wahlmaschinen wurden bei der Europawahl im Juni 2004 sowie bei der Wahl im Februar 2005 getestet. Bei der Europawahl 2004 konnten Wähler ihre Stimme in neun Gemeinden innerhalb Portugals, die aufgrund von

bestimmten Kriterien wie der geographischen Lage, der Größe und der traditionellen politischen Präferenzen ausgewählt worden sind, nach der gesetzlich bindenden Stimmabgabe auf Papier optional an elektronischen Wahlmaschinen wählen. Abhängig von der Gemeinde standen den Wählern hierbei drei unterschiedliche Arten von Systemen zur Verfügung: eine Wahlmaschine mit Touchscreen, ein System mit einem Leuchtstift und eine Lösung beruhend auf elektronischen Karten. An der Wahl beteiligten sich von den 128060 in den neun Gemeinden registrierten Wählern 50562. Von diesen testeten 9390 die Möglichkeit, elektronisch zu wählen (vgl. [Por04]).

Bei der Wahl im Februar 2005 wurden elektronische Wahlmaschinen in den fünf Gemeinden getestet, in denen der portugiesische Präsident und die Vorsitzenden der fünf größten politischen Parteien für die Stimmabgabe registriert waren. Insgesamt konnten etwa 40000 registrierte Wähler die Möglichkeit nutzen, ihre Stimme optional elektronisch abzugeben. Das Ziel dieses Versuchs bestand darin, den Einsatz von elektronischen Technologien während des gesamten Wahlvorgangs von der Identifikation und Authentifizierung der Wähler bis hin zum Zählen der abgegebenen Stimmen zu testen. Die Versuche wurden von etlichen portugiesischen und ausländischen Unternehmen wie Multicert, PT Corporate, Unisys, Indra und Election Systems & Software geleitet (vgl. [Por05]).

Onlinewahlen für portugiesische im Ausland lebende Bürger, die traditionell ihre Stimme per Briefwahl abgeben können, wurden erstmals während der Wahl im Februar 2005 getestet. Jeder der 150000 zur Wahl aus dem Ausland registrierten Portugiesen erhielt einen Zugangscode per Post, der es ihnen ermöglichte, ihre Stimme über eine sichere Internetplattform nichtbindend abzugeben. Dieser Pilotversuch wurde organisiert von der Portuguese Agency for the Knowledge Society (UMIC), dem technischen Sekretariat für Wahl(prozess)angelegenheiten (Technical Secretariat for Electoral Process Issues) (STAPE) in Zusammenarbeit mit dem nationalen Wahlkomitee (National Electoral Commission) und dem Außenministerium (vgl. [Por05]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Tests in 2004 und 2005
Onlinewahlen	✔	Erster Test 2005
Wahlen per Handy	✘	

Tabelle 5.15: Übersicht eingesetzter Technologien in Portugal

5.3.16 Schweiz

In der Schweiz wurden in den drei Kantonen Genf, Neuchâtel und Zürich jeweils Wahlen über das Internet eingesetzt. In Zürich gab es für die Wähler außerdem die Möglichkeit per Mobiltelefon bzw. SMS abzustimmen.

Im Kanton Genf wurde den Bürgern vom 14. bis zum 19. Januar 2003 erstmals zusätzlich die Möglichkeit angeboten, bei einer lokalen Volksabstimmung im Genfer Außenbezirk Anières über das Internet abzustimmen (vgl. [Sch03b]). Der zweite Einsatz vom 17. bis zum 29. November 2003 erfolgte ebenfalls bei einem lokalen Volksentscheid im Genfer Vorort Cologny, an dem sich 28,9% der Wähler online beteiligten. 23% dieser Personen waren dabei älter als 60 Jahre (vgl. [Sch03a]).

Die Möglichkeit der Onlinewahl bei einer Volksabstimmung auf Bundesebene wurde den Wählern im Kanton Genf drei Wochen lang bis zum 26.09.2004 in den vier Gemeinden Anières, Cologny, Carouge und Meyrin angeboten. 2723 Personen (etwa 22% der Wähler) beteiligten sich dabei über das Internet, ohne dass Störungen der Onlinewahl aufgetreten sind (vgl. [Sch04a]). Die zweite Verwendung der Onlinewahl für einen Volksentscheid auf Bundesebene fand im November 2004 statt, bei dem 3755 Wähler aus acht Gemeinden des Kantons Genf ihre Stimme elektronisch abgaben (vgl. [Sch04b]).

Damit sich die registrierten Wähler an der Abstimmung beteiligen konnten, wurde ihnen zunächst auf Karten von ihrer Kommune mitgeteilt, welche Mög-

lichkeiten der Stimmabgabe sie haben (elektronisch, postalisch oder in Person). Auf diesen Karten befand sich außerdem ein manipulationssicherer persönlicher Einweg-ID- sowie ein PIN-Code, mit denen es den Wählern ermöglicht wurde, sich sicher von jedem mit dem Internet verbundenen Computer an dem e-Votingsystem anzumelden (vgl. [Sch04b]).

Eingesetzt wurde bei diesen Volksentscheiden eine Software, die von dem Staatszentrum für Informationstechnologien (State's Centre of Information Technologies – CTI) in Zusammenarbeit mit Hewlett Packard und dem in Genf ansässigen Online-Sicherheitsunternehmen Wisekey entwickelt wurde. Die für die Wahlen verwendete Internetanwendung ist Eigentum des Kantons Genf, der Quellcode ist jedoch öffentlich zugänglich und wurde von Experten geprüft (vgl. [Sch04b]). Eine Simulation der Wahl über das Internet kann unter der URL http://www.geneve.ch/ge-vote/demo-en/votation.html durchgeführt werden.

Im Kanton Neuchâtel (Neuenburg) wurde 2005 die Wahl über das Internet bei drei Abstimmungen verwendet. Als System kam dabei jeweils Guichet unique zum Einsatz. An der ersten Abstimmung, die am 25.09.2005 stattfand, gaben von den 1732 am System registrierten Wählern 1178 (1,85% der insgesamt abgegebenen Stimmen) ihre Stimme über das Internet ab. Zum zweiten Mal wurde das System bei der Vorrunde zu den Nachwahlen des Staatsrates am 30.10.2005 mit einer Onlinewahlbeteiligung von 1194 Personen (2,6% aller abgegebenen Stimmen) von insgesamt 2209 registrierten. An der dritten Abstimmung vom 27.11.2005 nahmen 1345 Wähler (2,5% der abgegebenen Stimmen) von 2442 registrierten Personen online teil. Bei jeder dieser Wahlen wurden alle über das Internet abgegebenen Stimmen als gültig befunden (vgl. [Cha05]).

Das im Kanton Zürich eingesetzte e-Votingsystem, das die Wahl über das Internet sowie über Handy (SMS) zulässt, wurde zum ersten Mal am 10.12.2004 bei den Studierendenratswahlen an der Universität von Zürich erfolgreich verwendet. Bei dieser Wahl stimmten 93,2% aller teilgenommenen Studenten auf elektronischem Wege ab. Die meisten gaben dabei ihre Stimmen über das Internet ab, während nur etwa ein Fünftel die Möglichkeit des SMS-Versandes nutzten. Für die Abstimmung erhielten die Wahlberechtigten auf einem Stimmrechtsausweis die Zugangscodes, die für Wahl über das Internet oder per SMS

benötigt wurden. Um zu verhindern, dass Wähler ihre Stimmen doppelt abgaben, wurde an der Universität flächendeckend die elektronische Überwachung eingesetzt. Auf die kostenintensivere Variante mit dem Sicherheitssiegel, das auf jedem Stimmrechtsausweis vorhanden ist, konnte daher verzichtet werden. Der Einsatz des Systems erfolgte unter Zusammenarbeit des e-Voting-Teams im Statistischen Amt des Kantons Zürich, der Unisys (Schweiz) AG und des Studierendenrates (vgl. [Kom04]).

Politisch wurde das e-Votingsystem des Kantons Zürich (eine Simulation ist unter der URL http://evotingdemo.zh.ch/Demo2Internet.htm zu erreichen) am 30.10.2005 in der Stadt Bülach eingesetzt. Auch hier hatten die Wähler die Möglichkeit, per Internet oder SMS ihre Stimmen abzugeben. 455 Personen nutzten dabei das Handy und 1006 Wähler das Internet. Insgesamt gingen 3919 Stimmen ein. Zu Problemen kam es bei dieser Abstimmung nur in Bezug auf die Lesbarkeit von versiegelten PIN Codes, die nur schwach auf die Wahlunterlagen gedruckt worden sind. Die Beschädigung dieses Siegels hatte in knapp hundert Fällen eine Überprüfung auf eine eventuell bereits geleistete elektronische Abstimmung zur Folge, dreimal war dies der Fall (vgl. [Her05]).

Die in den drei Kantonen durchgeführten e-Voting-Projekte werden von der Schweizer Bundeskanzlei finanziell unterstützt und koordiniert. Eine Entscheidung über den landesweiten Einsatz von Onlinewahlen könnten die Bundesbehörden 2007 treffen (vgl. [Sch04b]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✘	
Onlinewahlen	✔	Erstmals seit 01/2003 im Kanton Genf
Wahlen per Handy	✔	Seit 10/2005 im Kanton Zürich

Tabelle 5.16: Übersicht eingesetzter Technologien in der Schweiz

5.3.17 Spanien

Spanien setzte bisher keine elektronischen Technologien bei Wahlen gesetzlich bindend ein. Getestet wurden jedoch unterschiedliche Systeme, zu denen die elektronische Stimmauszählung, elektronische Wahlmaschinen, Onlinewahlen und Wahlen per Mobiltelefon bzw. SMS gehören.

Elektronische Stimmauszählung wurde bei den Wahlen zum Parlament von Katalonien im November 2003 in fünf Gemeinden getestet. Das eingesetzte System wurde von dem spanischen Unternehmen Demotek entwickelt. Es besitzt einen ultravioletten optischen Leser (ultra-violet optical reader), der die speziellen Stimmzettel von den beteiligten 1555 Wählern einlesen konnte (vgl. [Spa03]).

Elektronische Wahlmaschinen wurden ebenfalls bei den Wahlen zum Parlament von Katalonien 2003 zu Testzwecken eingesetzt. Die verwendeten Wahlmaschinen stammten von dem spanischen Unternehmen Indra und waren mit Touchscreens ausgestattet. An diesen Maschinen gaben 1592 Wähler aus fünf Gemeinden ihre Stimme elektronisch ab (vgl. [Spa03]).

Bei den Wahlen zum Parlament von Katalonien 2003 wurde außerdem die Wahl über das Internet getestet. Das zugehörige System wurde dem Unternehmen Scytl, einem Ableger eines spanischen universitären kryptographischen Forschungslabors, bereitgestellt. Der Test richtete sich an 23234 im Ausland lebende Wahlberechtigte, denen eine Benutzerkennung und ein Passwort ausgehändigt wurden. An der Onlinewahl beteiligten sich jedoch nur 730 Personen (vgl. [Spa03]).

Weitere Tests von Wahlen über das Internet fanden während der Parlamentswahl im März 2004 statt. In der Gemeinde von Jun, nahe Grenada, haben 400 Personen von mit dem Internet verbundenen Computern ihre Stimme abgegeben. In drei Wahllokalen in Zamora und Lugo standen Internetwahlmaschinen bereit, die von 274 Wählern ausprobiert wurden. Jede Person, die sich an dem Test beteiligen wollte, erhielt vorher eine Karte mit einem digitalen Zertifikat. Nach der erfolgreichen Identifikation der Wähler konnten diese über eine In-

ternetplattform abstimmen. Das System wurde von der spanischen Firma Indra entwickelt, die internationale Beobachter aus 27 europäischen und lateinamerikanischen Ländern u. a. Frankreich, Großbritannien, Polen, Argentinien und Mexiko zu den Wahlen eingeladen hatte (vgl. [Spa04]).

Im Februar 2005 hatten über zwei Millionen Wähler in 52 Gemeinden die Möglichkeit, sich an dem größten Test für Onlinewahlen zu beteiligen. Für den Test, der vom 1. bis 18. Februar vor der gesetzlich bindenden Volksabstimmung zur europäischen Verfassung stattfand, wurde das System der Firma Indra eingesetzt. Die 10543 Wähler (etwa 0,54% der Wahlberechtigten), die ihre Stimme online abgaben, konnten dies unter Verwendung einer Smart card und eines PIN Codes von jedem mit dem Internet verbundenen Computer tun (vgl. [Spa05]).

Kritik zu dem Versuch kam von der unabhängigen Gruppe E-Voting Observatory, die in einem Bericht vom 21.02.2005 darauf hingewiesen haben, dass das verwendete Internetwahlsystem Sicherheitsmängel, die von Schwachstellen in der Wahlanwendung bis hin zu Nichtbeachtung von Sicherheitsstandards für die Wähleridentifikation reichen, aufweisen würde. Diese Beschuldigungen seien dadurch bewiesen, dass Mitglieder des E-Voting Observatory den Server mit den Abstimmungsergebnissen gehackt hätten. Da die Gruppe keine Erlaubnis erhielt, das System zu prüfen, könnten nach ihrer Aussage auch weitere Probleme vorhanden sein (vgl. [Spa05]).

Als Reaktion auf diese Kritik wiesen das Innenministerium und das Unternehmen Indra die Vorwürfe zurück. Nach ihrer Aussage war es nicht möglich, von außen auf den Server zuzugreifen. Auch wäre es unmöglich gewesen, ohne Smart card und PIN Code eine Stimme abzugeben. Das System habe perfekt funktioniert (vgl. [Spa05]).

Bei der Parlamentswahl im März 2004 konnten die Wähler zu Testzwecken die Möglichkeit nutzen, per Mobiltelefon bzw. SMS abzustimmen. In der Gemeinde Jun nahmen 197 Wähler diese Gelegenheit war (vgl. [Spa04]).

Elektr. Stimmauszählung	✔	Test 2003
Elektr. Wahlmaschinen	✔	Tests 2003 und 2004
Onlinewahlen	✔	Tests 2003, 2004 und 2005
Wahlen per Handy	✔	Tests per SMS 2004

Tabelle 5.17: Übersicht eingesetzter Technologien in Spanien

5.3.18 USA

Die USA bzw. das US Verteidigungsministerium haben den geplanten Einsatz eines Internetvoting-Systems für die Präsidentschaftswahlen 2004 aus Sicherheitsgründen abgesagt. Elektronische Wahlmaschinen wurden bei diesen wie auch bei anderen Wahlen zuvor verwendet.

In den USA wurde bereits im Oktober 1996 eine Art elektronischer Wahlmaschinen der Firma I-Mark Systems – 1997 durch das Unternehmen Global Election Systems aufgekauft, welches wiederum von der Diebold Corporation 2001 erworben wurde – von der FEC/NASED (Federal Election Commission/National Association of State Election Directors) zertifiziert. Im Mai 1997 folgte die Zertifizierung des Nachfolgemodells, einer portablen Version mit Flachbildschirm (vgl. [Jon]).

Nach den während den Präsidentschaftswahlen 2000 aufgetauchten Problemen, war die allgemein verbreite Ansicht, dass veraltete Wahlmethoden durch neue Technologie ersetzt werden sollten, um das Vertrauen in das US Wahlsystem wiederherzustellen. Seitdem wurden elektronische Wahlmaschinen, ausgestattet mit Touchscreens, in vielen Bundesstaaten aufgestellt. Im Gegensatz zu den Präsidentschaftswahlen 2000, bei denen etwa 12% der Wähler ihre Stimme elektronisch abgaben, waren es bei den Wahlen 2004 fast ein Drittel der Wahlberechtigten (vgl. [USA04c]).

Neben diesen beiden Wahlen wurden elektronische Wahlmaschinen auch bei den Vorwahlen der Demokratischen Partei am 02.02.2004 in 10 Bundesstaaten eingesetzt. Wie auch bei den später im selben Jahr stattgefundenen Präsidentschaftswahlen gab es dabei einige Schwierigkeiten. Aufgrund von technischen Problemen musste in einigen Bezirken Marylands und Georgias auf Papierstimmzettel zurückgegriffen werden. Außerdem gab es teilweise „eingefrorene“ Bildschirme, fehlerhaft arbeitende Wahlmaschinen und nicht-startende Software. Für die meisten Störungen wurden menschliches Versagen und nicht angemessen geschulte Wahlhelfer verantwortlich gemacht (vgl. [USA04b]).

Von Diebold hergestellte elektronische Wahlmaschinen, von denen es in den USA Anfang 2004 etwa 33000 gab, wurden des Öfteren kritisiert. Laut einiger Experten seien diese anfällig für Angriffe von Hackern sowie für Manipulationen von Insidern (vgl. [USA04b]).

Das Internetvoting-System SERVE (Secure Electronic Registration and Voting Experiment) wurde vom US Verteidigungsministerium entwickelt, um Militärangehörigen und im Ausland lebenden Bürgern die Beteiligung an Wahlen zu ermöglichen. Das System sollte bis zu 100000 Stimmabgaben dieser Personen aus 50 Landkreisen in sieben Staaten für die Präsidentenwahl 2004 ermöglichen. Schließlich sollte SERVE für alle im Ausland lebenden Amerikaner sowie für militärisches Personal und deren Angehörige für Wahlen zugänglich sein (vgl. [USA04a]).

Die Verwendung dieses Systems für die Präsidentschaftswahlen 2004 wurde vom US Verteidigungsministerium abgesagt, nachdem ein offizieller Bericht einer beratenden Expertengruppe vom Federal Voting Assistence Program, die die Aufgabe hatte, SERVE zu evaluieren, zu dem Schluss kam, dass SERVE Sicherheitslücken beinhalte. Durch diese könnten die Privatsphäre der Wähler gefährdet sein und Stimmen nachträglich geändert werden. Da diese Schadensanfälligkeiten dem Internet selbst anhaften würden und daher nicht eliminiert werden könnten, empfehlen die Verfasser des Berichts, Internetvoting solange nicht zu verwenden, bis das Internet sowie die Infrastruktur der heimischen Computer umstrukturiert wurde oder neue Sicherheitstechniken entwickelt wur-

den. (vgl. [USA04a]). Der Bericht, der am 21.01.2004 veröffentlicht wurde, ist unter der URL http://www.servesecurityreport.org/paper.pdf zugänglich.

Trotz der Entscheidung, SERVE nicht einzusetzen, werden laut US Verteidigungsministerium die Bestrebungen weitergehen, um im Ausland lebenden Amerikanern die Möglichkeit zu bieten, das System zu einem späteren Zeitpunkt nutzen zu können (vgl. [USA04a]).

Elektr. Stimmauszählung	✘	
Elektr. Wahlmaschinen	✔	Einsatz Wahlen 2000 und 2004
Onlinewahlen	✘	Internetvoting für Wahlen 2004 abgelehnt
Wahlen per Handy	✘	

Tabelle 5.18: Übersicht eingesetzter Technologien in den USA

5.4 Fazit

In dieser Ausarbeitung wurden zunächst elektronische Wahlen als Wahlen, die mit elektronischen Geräten durchgeführt werden, definiert (siehe Kapitel 5.2.1). Nachdem elektronische Wahlen in unvernetzte und vernetzte Wahlen eingeteilt (siehe Kapitel 5.2.2), sowie Vor- und Nachteile elektronischer Wahlen erläutert wurden, wurde in Kapitel 5.3 die internationale Entwicklung in Bezug auf elektronische Wahlen beschrieben. Dabei konnte festgestellt werden, dass zwei Formen von elektronischen Wahlen vermehrt eingesetzt bzw. getestet wurden. Am häufigsten werden unvernetzte elektronische Wahlmaschinen verwendet. Diese werden in einigen Ländern nur in wenigen Gebieten, in anderen Ländern nahezu flächendeckend verwendet. Ebenfalls eine große Beachtung finden elektronische Wahlen, die von einem beliebigen Computer aus, über das Internet durchgeführt werden können. In diesem Bereich wurden weltweit viele Tests durchgeführt, aber nur wenige Länder haben bindende parlamentarische

Wahlen auf diese Weise durchgeführt. Das Problem bei Wahlen von beliebigen Computern aus, ist dass die in den verschiedenen Ländern geltenden Wahlgrundsätze verletzt werden können. Diese Problematik wurde am Beispiel von Deutschland in Kapitel 5.3.1 vorgestellt. Auf Grund von anderen gesetzlichen Vorgaben wurden im nicht-parlamentarischen Raum, z. B. in Vereinen und Unternehmen, allerdings schon bindende Wahlen von beliebigen Computern aus durchgeführt.

Neben der Einführung in das Thema elektronischer Wahlen und einer Beschreibung der internationalen Entwicklung in diesem Gebiet, sollte festgestellt werden, wie der Stand der Entwicklung in Deutschland im Vergleich zu anderen Ländern ist. Festgestellt werden kann, dass die Entwicklung in Deutschland weiter fortgeschritten ist als in vielen anderen Ländern. So wurden in Deutschland bereits bindende unvernetzte und vernetzte elektronische Wahlen durchgeführt. In vielen Ländern wurden dagegen bisher nur Tests durchgeführt. Das am weitesten entwickelte Land in Bezug auf elektronische Wahlen ist Deutschland mit Sicherheit aber nicht, denn im Gegensatz zu Deutschland gibt es Länder, wie z. B. Belgien, Brasilien und Indien, die elektronische Wahlmaschinen nahezu flächendeckend einsetzen. Im Bereich der vernetzten elektronischen Wahlen ist die Entwicklung vermutlich in Estland und der Schweiz am weitesten vorangeschritten. Estland hat die nötigen Grundlagen geschaffen, um die nächsten Wahlen landesweit über das Internet durchführen zu können und in der Schweiz wird bereits über das Internet und teilweise über Mobiltelefone abgestimmt.

Im Bereich von Wahlen über beliebige Computer oder Mobiltelefone, sollte zwar weiterhin geforscht werden, um nicht den Anschluss zu verlieren, aber ein baldiger Einsatz im parlamentarischen Rahmen in Deutschland muss zur Zeit noch als zu unsicher und daher als unrealistisch eingestuft werden. Außerdem stehen diese Formen elektronischer Wahl in Konflikt mit dem Grundgesetz. Es erscheint also sinnvoll zunächst die Erfahrungen anderer Länder und Erfahrungen im nicht-parlamentarischen Raum zu sammeln, um Vor- und Nachteile im praktischen Einsatz abschätzen zu können. Wenn in Deutschland vermehrt elektronische Wahlen durchgeführt werden sollen, dann sollte dies über elektronische Wahlmaschinen geschehen. Auf diese Weise können Konflikte mit

dem Grundgesetz vermieden und trotzdem einige Vorteile, wie das Senken der Wahlkosten, erzielt werden.

Literaturverzeichnis

[Ass02] ASSOCIATED PRESS: *Japan's First Electronic Voting Introduced in Local Election*. http://www.govtech.net/magazine/channel_story.php/16989, Juni 2002. Letzter Zugriff: 04.02.2006.

[Bel04a] *Belgian Government publishes source code of e-voting software*. http://europa.eu.int/idabc/en/document/3141/332, Juli 2004. Letzter Zugriff: 26.01.2006.

[Bel04b] *E-elections 2004: Belgium's e-voting operations considered successful*. http://europa.eu.int/idabc/en/document/2634/358, Juni 2004. Letzter Zugriff: 26.01.2006.

[Bir04] BIRKENMAIER, PHILIPP: *E-Democracy - Der Wandel der Demokratie durch das Internet*. Doktorarbeit, TU Dresden, 2004.

[Bla] *BlackBoxVoting*. http://www.blackboxvoting.org. Letzter Zugriff: 09.02.2006.

[BMI] *Bundesministerium des Innern (BMI)*. http://www.bmi.bund.de. Letzter Zugriff: 09.02.2006.

[BN02] BUCHSTEIN, HUBERTUS und HARALD NEYMANNS: *Online-Wahlen*. Leske + Budrich, 2002.

[BWa] *Bundeswahlgeräteverordnung (BWahlGV)*. http://bundesrecht.juris.de/bwahlgv. Letzter Zugriff: 09.02.2006.

[Cha05] CHANCELLERIE D'ÉTAT, BUREAU DE LA COMMUNICATION: *1345 électrices et électeurs neuchâtelois ont participé au dernier essai pilote de vote électronique*. http://www2.ne.ch/vote/

Civisme/commvoteinternet27nov052005.pdf, November 2005. Letzter Zugriff: 04.02.2006.

[Com04] COMMISSION ON ELECTRONIC VOTING: *INTERIM REPORT on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*. http://www.cev.ie/htm/report/V02.pdf, 2004. Letzter Zugriff: 09.02.2006.

[Com05] COMMISSION ON ELECTRONIC VOTING: *Request for Proposals - Review of Physical Security*. http://www.cev.ie/htm/tenders/pdf/rfp_physicalsecurity_feb2005.pdf, 2005. Letzter Zugriff: 09.02.2006.

[Cyba] *CyberVote*. http://www.eucybervote.org. Letzter Zugriff: 09.02.2006.

[Cybb] CYBERVOTE: *Project Description*. http://www.eucybervote.org/description.html. Letzter Zugriff: 09.02.2006.

[Cybc] CYBERVOTE: *The Trials*. http://www.eucybervote.org/trials.html. Letzter Zugriff: 09.02.2006.

[D21] *Initiative D21*. http://www.initiatived21.de. Letzter Zugriff: 09.02.2006.

[DCC02] DIEHL, KLAUS, OLIVER CAUSSE und EVA CORIGLIANO: *Onlinewahlen T-Systems CSM - Abschlussbericht der elektronischen Wahlen zum Betriebsrat bei der T-Systems CSM im Mai 2002*. http://www.forschungsprojekt-wien.de/pdf/t_systems.pdf, 2002. Letzter Zugriff: 09.02.2006.

[Die] *Diebold Election Systems*. http://www.diebold.com. Letzter Zugriff: 09.02.2006.

[EAD] *European Aeronautic Defence and Space Company (EADS)*. http://www.eads.net. Letzter Zugriff: 09.02.2006.

[Elea] ELECTIONS ACT: *Electronic voting and counting*. http://www.elections.act.gov.au/Elecvote.html. Letzter Zugriff: 22.01.2006.

[Eleb] ELECTIONS ACT: *The electronic voting process*. http://www.elections.act.gov.au/EvoteTR.html. Letzter Zugriff: 22.01.2006.

[Est] *E-voting pilot in Tallilnn*. http://www.vvk.ee/english/pilot_jan05.html. Letzter Zugriff: 06.02.2006.

[Est05] *About 1% of votes cast online in Estonian local elections*. http://europa.eu.int/idabc/en/document/4999/591, Oktober 2005. Letzter Zugriff: 06.02.2006.

[EVM] *Electronic Voting Machine*. http://www.eci.gov.in/EVM/index.htm. Letzter Zugriff: 09.02.2006.

[For02] FORSCHUNGSGRUPPE INTERNETWAHLEN: *i-voteReport - Chancen, Möglichkeiten und Gefahren der Internetwahl - Kurzfassung*. http://www.wahlkreis300.net/fgiw/uploader/data/Kurzfassung.pdf, 2002. Letzter Zugriff: 09.02.2006.

[Fra05a] *E-voting used in French and Dutch referendums*. http://europa.eu.int/idabc/en/document/4353/358, Juni 2005. Letzter Zugriff: 04.02.2006.

[Fra05b] *France to test e-voting during European Constitution referendum*. http://europa.eu.int/idabc/en/document/4178/358, April 2005. Letzter Zugriff: 04.02.2006.

[GBC05] *UK e-voting pilots cancelled again*. http://europa.eu.int/idabc/en/docu-ment/4644/358, September 2005. Letzter Zugriff: 04.02.2006.

[GBE04] *E-elections 2004: Successful e-counting operations in London*. http://europa.eu.int/idabc/en/document/2636/358, Juni 2004. Letzer Zugriff: 04.02.2006.

[GG] *GRUNDGESETZ (GG) für die Bundesrepublik Deutschland*. http://www.datenschutz-berlin.de/recht/de/gg. Letzter Zugriff: 09.02.2006.

[GI] *Gesellschaft für Informatik*. http://www.gi-ev.de. Letzter Zugriff: 09.02.2006.

[Hen04] HENGHUBER, GERD: *Automatisches Wahlsystem bei Wahlen im Saarland und bei der Europawahl*. http://www.ivu.de/index.cfm?pageid=25&subpage=69&year=2004&articleid=278, März 2004. Letzter Zugriff: 09.02.2006.

[Her05] HERRMANNSTORFER, MATTHIAS: *Erste elektronische Wahl per SMS in der Schweiz erfolgreich*. http://www.heise.de/newsticker/meldung/65566, Oktober 2005. Letzter Zugriff: 04.02.2006.

[Ind04a] *675 million Indian citizens to vote electronically in forthcoming elections*. http://europa.eu.int/idabc/en/document/2243/348, März 2004. Letzter Zugriff: 04.02.2006.

[Ind04b] *India does mass e-vote*. http://www.kablenet.com/kd.nsf/Frontpage/A109B59D2C4BCBA380256E9400373E62?OpenDocument, Mai 2004. Letzer Zugriff: 04.02.2006.

[Irl04] *Irish Government cancels e-voting plans for June 2004 elections*. http://europa.eu.int/idabc/en/document/2520/338, Mai 2004. Letzer Zugriff: 04.02.2006.

[Irl05] *Renewed criticism throws doubts on the future of e-voting in Ireland*. http://europa.eu.int/idabc/en/document/3860/358, Februar 2005. Letzer Zugriff: 04.02.2006.

[Ita04] *E-elections 2004: Italian authorities satisfied with e-counting pilot*. http://europa.eu.int/idabc/en/document/2637/339, Juni 2004. Letzer Zugriff: 04.02.2006.

[Ita05] *E-counting successfully tested in Italy's regional elections*. http://europa.eu.int/idabc/en/document/4080/358, April 2005. Letzer Zugriff: 04.02.2006.

[IVU] *IVU Traffic Technologies AG*. http://www.ivu.de. Letzter Zugriff: 09.02.2006.

[IVU05] IVU: *IVU-System ermittelt Endergebnis*. http://www.ivu.de/index.cfm?pageid=25&subpage=67&year=

2005&articleid=1103, September 2005. Letzter Zugriff: 09.02.2006.

[Jon] JONES, DOUGLAS W.: *The Case of the Diebold FTP Site*. http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html. Letzter Zugriff: 09.02.2006.

[Kan03] *Linux-based Internet voting system successfully used in Canada*. http://europa.eu.int/idabc/en/document/1800/469, November 2003. Letzter Zugriff: 04.02.2006.

[Kom04] KOMMUNIKATIONSABTEILUNG DES REGIERUNGSRATES DES KANTONS ZÜRICH: *Erfolgreiches e-Voting an den Studierendenratswahlen der Universität Zürich*. http://www.statistik.zh.ch/produkte/evoting/mm_stura_wahlen_nachher.pdf, Dezember 2004. Letzter Zugriff: 04.02.2006.

[LDS02] LDS BRANDENBURG: *Abschlussbericht zur Online-Wahl Mai 2002 im LDS Brandenburg*. http://www.forschungsprojekt-wien.de/pdf/lds.pdf, 2002. Letzter Zugriff: 09.02.2006.

[Lem05] LEMKE, JAKOB: *Demokratie per Internet - Esten können elektronisch wählen*. http://www.heise.de/newsticker/meldung/64672, Oktober 2005. Letzter Zugriff: 06.02.2006.

[Lym03] LYMAN, JAY: *Canada Marks First Internet Election in North America*. http://www.technewsworld.com/story/32098.html, Oktober 2003. Letzter Zugriff: 04.02.2006.

[Men] *Die Allgemeine Erklärung der Menschenrechte*. http://www.unhchr.ch/udhr/lang/ger.htm. Letzter Zugriff: 09.02.2006.

[Mica] *Micromata Objects GmbH*. http://www.micromata.de/produkte/polyas.jsp. Letzter Zugriff: 09.02.2006.

[Micb] MICROMATA: *Online-Wahlen für Verbände und Vereine*. http://www.micromata.de/produkte/documents/

polyas_broschuere_72dpi.pdf. Letzter Zugriff: 09.02.2006.

[Micc] MICROMATA: *POLYAS Glossar*. http://www.micromata.de/produkte/documents/Polyas_Glossar.pdf. Letzter Zugriff: 09.02.2006.

[Mir04] MIRA, LESLIE M.: *For Brazil Voters, Machines Rule*. http://www.wired.com/news/business/0,1367,61654,00.html?tw=wn_story_page_prev2, Januar 2004. Letzter Zugriff: 01.02.2006.

[Ned] *N.V. Nederlandsche Apparatenfabriek (Nedap)*. http://www.election.nl/bizx_html/IVS-GB. Letzter Zugriff: 09.02.2006.

[Nie04] *Source code of Dutch Internet voting software made public*. http://europa.eu.int/idabc/en/document/2652/341, Juni 2004. Letzter Zugriff: 04.02.2006.

[Pol] *Polyas*. http://www.polyas.de. Letzter Zugriff: 09.02.2006.

[Por04] *E-elections 2004: Portuguese e-voting pilot "encouraging"*. http://europa.eu.int/idabc/en/document/2633/342, Juni 2004. Letzter Zugriff: 04.02.2006.

[Por05] *Tests of electronic voting held during Portuguese general election*. http://europa.eu.int/idabc/en/document/3922/358, Februar 2005. Letzter Zugriff: 04.02.2006.

[PTB] *Physikalisch-Technische Bundesanstalt (PTB)*. http://www.ptb.de. Letzter Zugriff: 09.02.2006.

[Rüß00] RÜSS, OLIVER RENÉ: *Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen*. http://www.wahlkreis300.net/fgiw/uploader/data/ruess.pdf, 2000. Letzter Zugriff: 09.02.2006.

[Sch03a] *Successful test paves the way for e-voting in Switzerland but criticism remains*. http://europa.eu.int/idabc/en/document/1845/347, November 2003. Letzter Zugriff: 04.02.2006.

[Sch03b] *Swiss citizens cast their vote electronically for the first time*. http://europa.eu.int/idabc/en/document/836/347, Januar 2003. Letzter Zugriff: 04.02.2006.

[Sch04a] *Internet referendum successfully held in Switzerland*. http://europa.eu.int/idabc/en/document/3311/347, September 2004. Letzter Zugriff: 04.02.2006.

[Sch04b] *Second successful use of Internet voting during Swiss federal referendum*. http://europa.eu.int/idabc/en/document/3607/358, Dezember 2004. Letzter Zugriff: 04.02.2006.

[Sie05] SIETMANN, RICHARD: *Dreimal drücken? fertig? - E-Voting-Großeinsatz bei der Bundestagswahl*. http://www.heise.de/ct/05/19/054, 2005. Letzter Zugriff: 09.02.2006.

[Spa03] *E-voting systems successfully tested in Catalan elections*. http://europa.eu.int/idabc/en/document/1806/343, November 2003. Letzter Zugriff: 04.02.2006.

[Spa04] *Electronic voting successfully tested in Spain*. http://europa.eu.int/idabc/en/document/2287/343, März 2004. Letzter Zugriff: 04.02.2006.

[Spa05] *Spain's Internet voting pilot sparks controversy*. http://europa.eu.int/idabc/en/document/3923/358, Februar 2005. Letzter Zugriff: 04.02.2006.

[Sta] *Statistisches Landesamt Bremen*. http://www.bremen.de/info/statistik. Letzter Zugriff: 09.02.2006.

[Ulb04] ULBER, PETER: *Wahlmaschinen wählen nicht: Pannen mit elektronischen Wahlhelfern*. http://www.dergrossebruder.org/times/20041103000000.html, November 2004. Letzter Zugriff: 09.02.2006.

[USA04a] *US Administration drops Internet voting plans for presidential elections*. http://europa.eu.int/idabc/en/document/2126/348, Februar 2004. Letzter Zugriff: 04.02.2006.

[USA04b] *US e-voting controversy fuelled by problems experienced during Democratic primaries*. http://europa.eu.int/idabc/en/document/2232/348, März 2004. Letzter Zugriff: 04.02.2006.

[USA04c] *US elections 2004: e-voting passes major test with some glitches*. http://europa.eu.int/idabc/en/document/3448/348, November 2004. Letzter Zugriff: 04.02.2006.

[Was] *Was ist W.I.E.N.?* http://www.forschungsprojekt-wien.de/was_ist_wien.html. Letzter Zugriff: 09.02.2006.

[WD05] WEDDELING, SONJA und KLAUS DIEHL: *Schritt für Schritt in Richtung eVoting*. http://www.politik-digital.de/edemocracy/evoting/evoting051031.shtml, September 2005. Letzter Zugriff: 09.02.2006.

[Wei04] WEINER, ERIC: *The Bombay Ballot – What the U.S. can learn from India's electronic voting machines*. http://www.slate.com/id/2107388, Sptember 2004. Letzer Zugriff: 04.02.2006.

[Wil04] WILM, PETER: *Elektronische Wahlen - Eine Informationsbroschüre für den Wahlbürger*. http://www.elektronische-wahlen.de/staatlich/elektronische-wahlen.pdf, 2004. Letzter Zugriff: 09.02.2006.

6 Möglichkeiten der politischen Beteiligung im Internet

Möglichkeiten der politischen Beteiligung im Internet

Dirk Räder

3. Februar 2006

6.1 Einleitung

Diese Ausarbeitung entstand im Rahmen des Seminars „eDemokratie — Informatikanwendungen in der Politik“ an der Carl-von-Ossietzky Universität Oldenburg im Wintersemester 2005/2006 bei Ingo Ibelings. Sie untersucht verschiedene Möglichkeiten, wie sich der Bürger oder eine Gruppe von Bürgern im Internet politisch beteiligen können. Dazu werden zunächst einige der am meisten verwendeten Formen von Webanwendungen vorgestellt und ihr Aufbau bzw. ihre Funktionsweise erläutert. Bei der Vorstellung der Webanwendungen wird vorrangig auf Produkte aus dem Bereich der Open Source Software (OSS) eingegangen, da kommerzielle Produkte einfach wesentlich teurer im Einkauf und Betrieb sind. Anschließend werden die einzelnen Formen auf ihre Nutzbarkeit für die politische Beteiligung untersucht. Dabei werden insbesondere die folgenden Punkte betrachtet:

- Was kann gepostet werden (Text, Links zu anderen Seiten, Multimedia-Dateien)?

- Wer kann Texte veröffentlichen und ändern (jeder, alle registrierten Nutzer, nur einzelne Personen)?
- Kann der Autor eines Textes oder Abschnitts von Jedermann festgestellt werden?
- Lassen sich die Beiträge moderieren (können sie gesperrt / geändert / gelöscht werden)?
- Wie einfach ist die Benutzeroberfläche sowohl für Benutzer als auch für Moderatoren bzw. Administratoren?
- Gibt es die Möglichkeit, Benutzungsregeln bei Registrierung anerkennen zu lassen? Können diese Regeln selbst formuliert werden?

Auch rechtliche Aspekte, die für Betreiber solcher Webanwendungen relevant sind, werden kurz erläutert.

6.2 Webanwendungen

Zunächst wird nun eine Ausgangssituation geschaffen, auf der die weitere Betrachtung der einzelnen Webanwendungen aufbaut. Anschließend stellt dieses Kapitel drei der gängigsten Formen von Webanwendungen, die dem Informations- und Meinungsaustausch dienen, vor.

6.2.1 Ausgangssituation

Ein Bürger möchte sich politisch aktiv betätigen; diese Betätigung soll aber unabhängig von Parteien erfolgen. Gleichzeitig möchte er anderen Interessierten die Möglichkeit geben, sich ebenfalls zu betätigen. Dazu soll eine eigene Webanwendung bereit gestellt werden. Da der Bürger aber nur wenig Ahnung von Webservern und ihrem Betrieb hat, will er diese Aufgaben einem Dienstleister überlassen und lediglich ein fertiges Produkt einkaufen. In diesem Produkt soll dann die Webanwendung installiert werden. Auch möchte er für den Fall, dass

sich Leser über Beiträge von Nutzern beschweren (was auch Strafverfolgungen durch die Staatsanwaltschaft enthalten kann), alle Beiträge bzw. Änderungen von Beiträgen nachverfolgen und die Autoren der Beiträge benennen können. Des weiteren soll die Anwendung sämtlichen gesetzlichen Rahmenbedingungen wie beispielsweise Medien- und Teledienstestaatsvertrag genügen. Daraus ergeben sich einige Anforderungen an die Webanwendung, die im Folgenden zusammengefasst werden.

- Die Webanwendung muss sich mit den gängigen Angeboten von Webhostern betreiben lassen. Diese umfassen in der Regel Unterstützung für in PHP geschriebene Anwendungen, eine MySQL-Datenbank zur Datenspeicherung sowie eine Domain zur Erreichbarkeit.

- Die Webanwendung muss die Registrierung von Benutzern ermöglichen und gleichzeitig sicher stellen, dass nur registrierte Benutzer Beiträge veröffentlichen können. Bei der Registrierung sollten nach Möglichkeit Benutzungsregeln verbindlich anerkannt werden müssen.

- Es muss unter anderem ein Impressum auf der Webanwendung untergebracht werden, dass mindestens den Namen, die Anschrift, Telefon- und Faxnummer sowie Email-Adresse des Betreibers enthält.

- Das Impressum muss leicht erkennbar, unmittelbar erreichbar (max. 2 Klicks von jeder Stelle der Webanwendung aus laut OLG München, Urteil vom 11.09.2003, Az.: 29 U 2681/03) und ständig verfügbar sein.

Wünsche an die Funktionalitäten wurden schon auf der vorigen Seite formuliert. Nachdem nun die Situation und die Anforderungen an die Anwendung geklärt sind, werden nun die drei Formen Wiki, Blog und Forum kurz vorgestellt und anschließend in Bezug auf die Ausgangssituation und ihre bisherigen Anwendungen durch Parteien und öffentliche Stellen untersucht.

6.2.2 Wiki

„Ein Wiki, auch WikiWiki und WikiWeb genannt, ist eine im World Wide Web verfügbare Seitensammlung, die von den Benutzern nicht nur gelesen, sondern auch online geändert werden kann. [...] Der Name stammt von wikiwiki, dem hawaiianischen Wort für „schnell“.“ Zitat von `http://de.wikipedia.org/wiki/Wiki`, Stand: 29.01.2006

Das bekannteste Wiki, aus dem auch die hier angegebene Zitate stammen, ist Wikipedia. Es handelt sich dabei um eine Online-Enzyklopädie, deren Inhalte nicht von bezahlten Redakteuren bereitgestellt wird, sondern von jedem, der Informationen beitragen möchte. Die einzelnen Beiträge werden dabei einem durch die Tatsache, dass jeder Benutzer sie ändern kann, einem stetigen Lektorat unterzogen. Die von Wikipedia eingesetzte Webanwendung heißt Mediawiki und ist unter der GNU Public License (GPL) als Open Source Software veröffentlicht. Sie ist zu finden unter `http://www.mediawiki.org`. Da es sich bei dieser Anwendung nach Meinung des Autors um das technologisch ausgereifteste und durch die Massennutzung von Wikipedia am besten gewartete Wiki-System handelt, wird diese Ausarbeitung für den Bereich Wiki ausschließlich Mediawiki betrachten.

6.2.3 Blog

„Weblogs, auch Blogs genannt, sind Online-Journale, die sich durch häufige Aktualisierung und viele Verlinkungen auszeichnen. Die meisten Blogs setzen bei einem neuen Artikel einen oder mehrere zentrale Server davon in Kenntnis. Jedes Weblog ist ein für sich eigenes Journal.“ Zitat von `http://de.wikipedia.org/wiki/Blog`, Stand: 29.01.2006

Weblogs oder Blogs haben zunächst als im Internet veröffentlichte Tagebücher angefangen und sich bald zu einem Massenphänomen entwickelt. Große Internetfirmen wie Google bieten kostenlos Blogs unter griffigen Domains wie `http://www.blogger.com` an, so dass hier nicht zwingend eigene

Webanwendungen installiert werden müssen. Ein Beispiel für OSS-Blogs ist b2evolution (http://b2evolution.net). Es unterstützt mehrere Sprachen, mehrere Benutzer und je Benutzer mehrere Blogs. Eine Weiterentwicklung von Blogs sind die durch Apples iPod bekannt gewordenen Podcasts bzw. Video-Podcasts, die ebenfalls kurz vorgestellt werden.

6.2.4 Forum

„Ein Webforum ist ein Diskussionsforum auf einer Website. Es ist eine Alternative zu älteren Medien wie Usenet oder früher gebräuchlicher Bulletin Board Systems sowie Mailinglisten.
Üblicherweise besitzt ein Webforum ein bestimmtes Thema und ist in Unterforen bzw. Unterthemen unterteilt. Im Gegensatz zum Chat erfolgt die Kommunikation nicht in Echtzeit, sondern asynchron. Es können Diskussionsbeiträge (Postings) hinterlassen werden, welche die Interessierten lesen und beantworten können. Mehrere Beiträge zum selben Thema werden wie im Usenet zusammenfassend als Faden (Thread) oder Thema (Topic) bezeichnet. “ Zitat von http://de.wikipedia.org/wiki/Webforum, Stand: 29.01.2006

Foren sind eine Weiterentwicklung des Usenets und haben diese Art der Diskussion in das World Wide Web verlagert. Auch hier existieren Anbieter, die kostenlose Foren bereitstellen, beispielsweise http://www.forumromanum.de. Genauso bieten aber auch verschiedene Open Source Projekte Forum-Software an. Eines der bekanntesten Forensysteme ist hier phpBB (http://www.phpbb.com), welches durch viele Zusatzprogramme und Modifikationen nahezu allen Bedürfnissen angepasst werden kann.

In den folgenden Kapiteln werden nun die einzelnen Webanwendungen auf ihre Nutzbarkeit für politische Betätigung hin untersucht.

6.3 Wiki

Für die weitere Untersuchung wird sowohl für das Wiki als auch für die beiden anderen Anwendungen Blog und Forum von einer Neuinstallation der genannten Programmen mit den jeweiligen Standardeinstellungen ausgegangen.

Technische und rechtliche Anforderungen

- Mediawiki erfordert ein beliebiges Betriebssystem (Linux wird empfohlen), einen beliebigen Webserver (Apache2 wird empfohlen) mit PHP-Unterstützung, PHP ab Version 4.3 und MySQL ab Version 3.23. Damit kann es auf nahezu jedem Hosting-Angebot, dass dynamische Webseiten via PHP und MySQL unterstützt, installiert werden. Zur einfachen Installation wird ein Installationsprogramm mitgeliefert.
- Mediawiki unterstützt nur automatische Anmeldungen. Allerdings kann das Recht, neue Benutzer anzulegen, auf die Administratoren beschränkt werden. Es kann ebenso eingestellt werden, dass nur registrierte Benutzer Beiträge verfassen oder ändern können. Nutzungsbedingungen müssen nicht explizit anerkannt werden.
- Das Impressum kann als normaler Beitrag eingestellt werden, der gegen Veränderungen geschützt wird. Über eine Fusszeile, die automatisch unter jeder Seite eingefügt wird, kann das Impressum mittels eines Klicks erreicht werden.

Mediawiki erfüllt also diese Anforderungen und kann von der technischen Seite her bedenkenlos eingesetzt werden.

Betrachtung der vorhandenen Funktionen

In den Standardeinstellungen können zunächst nur Texte mit den durch das Sys-

tem angebotenen Formatierungen verfasst werden; jeder, auch nicht registrierte Gäste, können dabei beliebige Artikel verfassen und ändern. Ein Hochladen von Bildern, Audio- oder Videodateien ist zunächst nicht erlaubt.

Um die notwendigen Änderungen der Konfigurationsdatei in Erfahrung zu bringen, muss die englischsprachige Dokumentation von Mediawiki durchgesehen werden. Diese ist in Form einer Frage-Antwort-Sammlung verfasst, so dass schnell die passenden Einstellungen gefunden sind und vorgenommen werden können. Nachdem die Konfiguration passend geändert wurde, können nun nur noch registrierte Benutzer Beiträge verfassen und ändern. Allerdings ist die Registrierung noch immer jedermann zugänglich. Hier lässt sich nur eine Beschränkung der Art einbauen, dass lediglich Administratoren neue Benutzer registrieren dürfen. Dies führt je nach Popularität des Wikis schnell zu einem erheblichen Zeitaufwand.

Änderungen an den einzelnen Artikeln können jederzeit über den Link „Versionen“ eingesehen werden. Somit kann jeder Nutzer genau sehen, wer wann was im Artikel geändert hat. Außerdem können (registrierte) Nutzer auch alte Versionen wieder als Aktuell markieren, was zur Behebung von Vandalismus (siehe unter Nachteile) sehr hilfreich ist.

Die Oberfläche des Wikis ist recht übersichtlich gehalten und ermöglicht eine intuitive Bedienung. Sie ist allerdings noch nicht vollständig übersetzt, es wird noch an den Übersetzungen gearbeitet. Die Gestaltung der Oberfläche kann über ein Vorlagensystem nahezu beliebig an die Wünsche und eine etwaige Corporate Identity angepasst werden. Weniger angenehm weil gewöhnungsbedürftig ist die Syntax für Formatierungen und Verlinkung der Beiträge. Hier sollten vom Betreiber entsprechende Hilfeseiten und Anleitungen bereit gestellt werden, oder zumindest auf die Anleitungen von `http://de.wikipedia.org` verwiesen werden.

Nachteile und Risiken

Ein großes Risiko von Wikis sind Vandalen, die Artikel mutwillig verunstalten, verfälschen und/oder vollständig leeren. Sie haben allerdings nur kurzzeitig Erfolg, da jederzeit alte Versionen eines Artikels wiederhergestellt werden können. Problematischer sind dagegen gerade für den Einsatz im politischen Bereich die oft weit auseinander gehenden Meinungen der Nutzer. Sie können dazu führen, dass einzelne Artikel immer wieder hin- und her geschrieben werden. Darunter leidet die Verfügbarkeit und Geschwindigkeit des ganzen Wikis, während keine produktiven Ergebnisse erreicht werden. Auch können durch die Möglichkeit, quasi-anonym zu veröffentlichen, leicht Streitigkeiten entstehen, die im Interesse einer produktiven Beteiligung eigentlich vermieden werden sollten.

Einsatz im politischen Bereich

Vermutlich aufgrund der genannten Nachteile sind im politischen Bereich keine Installationen von Mediawiki oder anderen Wiki-Systemen bekannt. Eine gute Einsatzmöglichkeit würde sich bei der in einer anderen Arbeit dieses Seminars vorgestellten VVVD bieten: Hier könnte eine Wiki genutzt werden, um die recherchierten Informationen redaktionell aufbereitet und Partei-Usern zur Verfügung zu stellen.

6.4 Blogs

Die weitere Ausarbeitung beschäftigt sich primär mit dem Blog-System b2evolution, berücksichtigt aber auch das Angebot `http://www.blogger.com` von Google.

Technische und rechtliche Anforderungen

- b2evolution ist wie Mediawiki auch vollständig in PHP geschrieben und kommt daher mit einem beliebigen Betriebssystem und Webserver zurecht. Als Datenbank wird MySQL voraus gesetzt, was aber bei Hosting-Angeboten Standard ist. Somit lässt sich b2evolution auf nahezu allen gängigen Hosting-Angeboten für dynamische Webseiten installieren.

- b2evolution unterstützt die Registrierung von Benutzern und kann über unterschiedlichen Stufen von Berechtigungen ermitteln, was die einzelnen Benutzer tun dürfen. Generell darf jeder jedes Blog einsehen, es besteht aber die Möglichkeit, Beiträge auszublenden.

- Es ist leider von b2evolution nicht vorgesehen, ein Impressum des Seitenbetreibers bzw. des jeweiligen Blogbetreibers einzubinden. Allerdings können in das Linkblog Einträge eingestellt werden, die auf jeder Seite angezeigt werden. Hier könnte also das Impressum untergebracht oder zumindest verlinkt werden.

- blogger.com ist bereits eine fertig installierte Webanwendung, hier müssen keine Installationen vorgenommen werden.

- Bei blogger.com wird eine Benutzerregistrierung angeboten. Jeder Benutzer kann dabei mehrere Blogs verwalten. Jedes Blog darf dabei von jedem, egal ob registriert oder nicht, eingesehen werden.

- Auch blogger.com bietet keine eigene Möglichkeit, ein Impressum zu veröffentlichen. Viele der Beispiel-Oberflächen enthalten bereits eine Linkliste, so dass hier ein Link auf das Impressum erzeugt werden kann. Dieser Link erfüllt auch die Anforderungen des OLG München.

Damit können auch b2evolution und blogger.com zur politischen Betätigung eingesetzt werden.

Betrachtung der vorhandenen Funktionen – b2evolution

b2evolution ermöglicht den angemeldeten Nutzern, Beiträge in ihren jeweiligen Blogs zu veröffentlichen. Dabei kann für jeden Beitrag festgelegt werden, ob er für alle sichtbar ist, nur für Benutzer, die als Mitglied dieses Blogs geführt werden oder nur für den Autor (als eine Art persönliche Notiz). Weiter lässt sich für jeden Beitrag einstellen, ob er von Anderen kommentiert werden darf. Diese Kommentare können auch zu Diskussionen über das durch den Blog-Beitrag angesprochene Thema führen. Zu jedem Beitrag lassen sich dabei auch Datei bzw. Bilder hochladen, die direkt im Beitrag verlinkt werden. Es sind also zunächst keine Änderungen an den Konfigurationsdateien selbst notwendig; alle Änderungen, die man als Betreiber eventuell vornehmen möchte, können bequem über die Weboberfläche durchgeführt werden. Die Registrierung von neuen Nutzern kann dabei freigegeben werden, in den Grundeinstellungen müssen aber die Administratoren jeden Benutzer von Hand anlegen.

Jeder Beitrag und jeder Kommentar, der in b2evolution veröffentlicht wird, wird mit Namen und Zeitstempel angezeigt. Somit kann jeder Leser verfolgen, wer wann welchen Beitrag veröffentlicht hat.

b2evolution verwendet für seine Oberfläche zwei Ebenen: zum einen die Anzeigeebene, auf der die einzelnen Beiträge mit all ihren Kommentaren angezeigt werden und zum anderen die Administrationsebene, auf der sämtliche Einstellungen vorgenommen und neue Beiträge verfasst werden. Beide sind übersichtlich strukturiert und ermöglichen eine intuitive Bedienung, die keiner großen Anleitung bedarf. Dennoch sind viele der Optionen mit kurzen Erläuterungen versehen und es existiert eine umfassende Onlinedokumentation, die alle Einstellungen gut verständlich erklärt. Das Aussehen der Anzeigeebene kann über so genannte Skins verändert werden; diese können die Nutzer auch selber verfassen und vom Administrator installieren lassen.

Betrachtung der vorhandenen Funktionen – blogger.com

Wie auch b2evolution erlaubt blogger.com jedem Benutzer, mehrere Blogs zu führen. Für die einzelnen Beiträge können dabei leider nicht so umfangreiche Einstellungen vorgenommen werden (nur Kommentare zulassen oder nicht). Auch hier können die Kommentare zur Diskussion über das im Beitrag angerissene Thema genutzt werden. Auch hier werden die Beiträge namentlich gekennzeichnet, jedoch werden die wenigsten Profile von ihren Benutzern auch mit Namen gefüllt. So ist eine Identifikation von Kommentatoren nur schwer möglich. Das Hochladen von Bildern ist ebenfalls möglich und wird, da es sich bei blogger.com um eine Google-Produkt handelt, auch in andere Google-Anwendungen wie Picasa integriert. Für die Benutzer ist diese Art der Integration durchaus angenehm, jedoch ist nicht ersichtlich, ob die Daten- und vor allem Passwortübertragung verschlüsselt erfolgt oder nicht. Denn im Gegensatz zu den gängigen Hosting-Angeboten ist es bei blogger.com möglich, die gesamte Datenübertragung verschlüsselt abzuwickeln, was ein nicht zu verachtender positiver Aspekt ist. Das Erscheinungsbild der einzelnen Blogs kann ganz nach Wünschen des Nutzers ausfallen; er kann eines der vorgefertigten Beispiele nehmen oder sich ein eigenes Design entwickeln.

Nachteile und Risiken

Für eine Webanwendung, die nach dem Wunsch des Betreibers Interaktion zwischen verschiedenen Nutzern ermöglichen soll, sind Blogs nur sehr eingeschränkt geeignet. Sie sind darauf ausgelegt, dass ein (oder wenige) Autoren ihre Eindrücke, Meinungen, Ideen, Konzepte und Bewertungen zu verschiedensten Themen vielen Lesern mitteilen. Den Lesern wird dann die Möglichkeit zum Feedback gegeben, was aber für eine interaktive Diskussion zwischen gleichberechtigten Nutzern nicht als ausreichend angesehen wird. Risiken wie Vandalismus oder Missbrauch lassen sich für Blogs nahezu vollständig aus-

schalten, da der Betreiber festlegen kann, wer Beiträge veröffentlichen darf und wann Kommentare von Lesern der Allgemeinheit zugänglich gemacht werden.

Einsatzgebiete

Durch den im vorigen Abschnitt erläuterten Kommunikationsweg, auch „One-to-many-Kommunikation“ genannt, eignen sich Blogs, um mit relativ einfachen Mitteln eine Vielzahl von Menschen zu erreichen. Dabei können die unterschiedlichsten Inhalte vermittelt werden. Sei es ein Tagebuch, das keine Tabuthemen kennt, Einschätzungen zu tagesaktuellen Themen, Entwicklungsberichte oder Selbstdarstellungen.

Einsatz im politischen Bereich

Dies machen sich einige der großen Parteien und viele ihrer Spitzenpolitiker zu Nutze, indem sie eigene Blogs veröffentlichen. So finden sich Blogs der FDP unter `http://blog.fdp.de`, die der Grünen unter `http://blog.gruene.de` und die der SPD unter `http://www.roteblogs.de`. Damit können sich die einzelnen Politiker direkt an die Bevölkerung wenden, ohne große Umwege über Pressemitteilungen und Medien gehen zu müssen. Neben den rein textbasierten Blogs gibt es auch verschiedene Weiterentwicklungen. So kann inzwischen jede dem Autor bekannte Blogsoftware auch Bilder oder andere Mediendateien in die Beiträge integrieren und auf dem Server abspeichern.

Multimediale Blogs

Weitaus interessanter sind die so genannten Podcasts. Hierbei handelt es sich um Audio- oder Videodateien, die mit Hilfe von Apple iTunes veröffentlicht

werden. Diese Dateien können sowohl am PC als auch auf iPods abgespielt werden und stehen nach erfolgreichem Download auch unterwegs zur Verfügung. Noch einen Schritt weiter geht die Webseite `http://www.phonecaster.de`; hier können die einzelnen Beiträge via Telefon oder Voice over IP (VoIP, Internettelefonie) aufgesprochen und abgehört werden. Sie stehen so weltweit an jedem Telefon zur Verfügung. Durch die aufkommende Telefonie-Pauschalgebühren oder „Flatrates“ werden auch Phonecasts eine rasche Verbreitung finden.

6.5 Forum

Im Rahmen dieser Ausarbeitung wird die ausgereifte und als stabil sowie ausreichend performant einzustufende Software phpBB untersucht. Sie findet unter anderem Einsatz bei `http://forums.gentoo.org`, einem Forum mit über drei Millionen Beiträgen sowie über 100.000 registrierten Benutzern.

Technische und rechtliche Anforderungen

- phpBB ist, wie der Name suggeriert, in PHP geschrieben und kommt mit unterschiedlichen Datenbanken zurecht, darunter MySQL, PostgreSQL und Microsoft SQL-Server. Damit kann auch PHP auf den gängigen Hosting-Angeboten für dynamische Webseiten eingesetzt werden.
- Es verfügt über ein umfassendes und einfach zu konfigurierendes Berechtigungssystem, so dass hier für jedes einzelne Unterforum explizit Lese-, Schreib- und Moderationsrechte vergeben werden können.
- Ein Impressum kann über verschiedene Navigationsleisten (abhängig vom verwendeten Darstellungsstil) verlinkt werden.
- Es kann vorgegeben werden, dass nur registrierte Benutzer Beiträge verfassen dürfen. Im Verlauf der Registrierung können auch Regeln bekannt gegeben werden, die anerkannt werden müssen – oder die Registrierung wird abgebrochen.

Es spricht also von technischer und rechtlicher Seite nichts gegen den Einsatz von phpBB auf Webseiten zur politischen Beteiligung.

Betrachtung der vorhandenen Funktionen

Innerhalb von phpBB selber können Textbeiträge gepostet werden, die mittels eigener Markierungen um Links zu anderen Webseiten, Grafiken sowie Audio- und Videodateien erweitert werden können. Des weiteren können auch Dateien an die einzelnen Postings angehängt werden (vgl. Email-Anhang). Die Freigaben, wer welche Foren sieht und in welchen er/sie Beiträge veröffentlichen kann, lassen sich durch das feingranulare Rechtesystem sehr präzise steuern, so dass hier keine allgemeine Aussage getroffen werden kann.

Zu jedem Beitrag werden neben dem Autor auch seine IP-Adresse sowie ein Zeitstempel gespeichert, so dass bei Streitfällen eine Identifikation sogar bei Beiträgen von nicht-registrierten Nutzern möglich ist. Zusätzlich wird bei jedem Beitrag angezeigt, von welchem Teilnehmer er verfasst wurde.

Je nach den Berechtigungen, die den einzelnen Benutzern gegeben wurden, können diese auch Beiträge oder ganze Diskussionen löschen, verschieben oder schließen, so dass ein weiteres Antworten nicht mehr möglich ist. Des weiteren können einzelne Foren so eingestellt werden, dass neue Beiträge erst nach einer Freigabe durch Moderatoren für alle Nutzer sichtbar werden.

Die Benutzeroberfläche ist auf eine intuitive Bedienung ausgelegt und ermöglicht auch Neulingen einen raschen und erfolgreichen Einstieg in Foren-Aktivitäten. Sie kann wie auch schon bei Wikis und Blogs beschrieben über Skins nahezu beliebig angepasst werden. Des weiteren können über eine Vielzahl von Modifikationen und Erweiterungen noch weitere Funktionen ergänzt oder bestehende verbessert werden.

Es werden auch kostenlose Foren angeboten; diese werden aber meist durch Werbung finanziert. Diese Werbeeinblendungen werden in der Regel nicht thematisch passend ausgewählt; auch können sie direkt in die Darstellung einge-

blendet werden, was den Lesefluss unheimlich stört und den Leser so aus dem Kontext reißt. Von solchen Foren wird daher generell abgeraten; hier ist es besser, wenige Euro pro Monat in ein entsprechendes Hosting-Angebot zu investieren.

Nachteile und Risiken

Ein Nachteil von populären Foren ist ganz klar der administrative Aufwand: Die Moderatoren müssen regelmäßig die Beiträge überprüfen, ob sie den Forenregeln, den guten Sitten – und im politischen Bereich auch der politischen Korrektheit – genügen. Gegebenenfalls müssen sie gegen Verstöße vorgehen und Beiträge löschen oder Benutzer des Forums verweisen. Des weiteren können sich, wie auch schon bei Wikis, Vandalen registrieren und das Forum durch unsinnige Beiträge oder Massenveröffentlichungen verschandeln. Auch kann ein Forum zur Verbreitung von rechtsradikaler und anderer Propaganda missbraucht werden. Gerade dieses Risiko lässt sich aber durch aufmerksame Moderatoren und Nutzer relativ gering halten.

Einsatzgebiete

Foren sind, wie auch das UseNet, aus dem sie sich entwickelt haben, zur Interaktion zwischen den einzelnen Nutzern gedacht. Sie leben von Diskussionen, Meinungs- und Erfahrungsaustauch und Informationsweitergabe zwischen den Benutzern. Sie eignen sich für politische Beteiligung also vor allem zum (moderierten?) Diskurs über aktuelle Themen sowie zur Veröffentlichung von Nachrichten. Dabei sollten allerdings mehrere Moderatoren gemeinsam ein Auge auf die politische Korrektheit der Beiträge haben und hier rechtzeitig einschreiten, wenn illegale Äußerungen jedweder Art entdeckt bzw. durch andere Nutzer gemeldet werden.

Des weiteren können Teile des Forums über das Rechtesystem so eingestellt werden, dass sie die Funktionen von Blogs vollständig übernehmen — es müs-

sen also nicht zwingend zwei Webanwendungen genutzt werden, wenn Forum und Blog durch den selben Bürger betrieben werden sollen.

Einsatz im politischen Bereich

Diskussionsforen werden vom Bundestag sowie den Parteien CDU/CSU und FDP angeboten. Des weiteren gibt es unter `http://www.politikforum.de` ein von der Berliner Firma polidia GmbH betriebenes überparteiliches und unabhängiges Forum. Es hat aktuell (30.01.2006) über 16.000 registrierte Benutzer und wird durch polidia auch redaktionell betreut mit Nachrichten und Meldungen aus aller Welt aktuell gehalten. Ein anderes Forum (`http://www.politik-forum.de`) musste nach über sieben Jahren Dauerbetrieb seine Tore schließen, da es immer wieder zu Missbrauch kam. Durch dieses Beispiel wird eindeutig gezeigt, dass gerade politisch motivierte Foren einer aktiven Betreuung und Moderation bedürfen.

Nachdem nun die gängigsten Webanwendungen kurz vorgestellt und für den Einsatz im politischen Umfeld untersucht wurden, wird im nächsten Kapitel ein Fazit gezogen und eine Handlungsempfehlung für den in der Ausgangssituation vorgestellten Wunsch gegeben.

6.6 Fazit

Ein Wiki sollte nur eingesetzt werden, wenn die Rechte zur Veröffentlichung und vor allem Veränderung von Beiträgen stark eingeschränkt werden können – ansonsten ist die Gefahr von Vandalismus und Missbrauch zu hoch. Es lässt sich allerdings durchaus als zusätzliche Informationsquelle und eine Art Lexikon, in dem wichtige oder interessante Beiträge aus der eigentlichen Webanwendung gesammelt werden, einsetzen.

Blogs stellen eine One-to-many-Kommunikation mit einem Rückkanal dar. Sie eignen sich vornehmlich, um anderen Bürgern die eigene Meinung oder Betrachtungen zu aktuellen Geschehnissen zugänglich zu machen. Somit sind sie durch die eingeschränkte Interaktionsmöglichkeiten der Nutzer untereinander nicht als eigene Webanwendung geeignet. Es wird vielmehr empfohlen, bei Interesse an einem Blog eines der kostenlosen Angebote zu nutzen.

Ein Forum bietet gute Interaktionsmöglichkeiten zur politischen Diskussion, die durchaus lebhaft werden können. Um diese Lebhaftigkeit nicht in Streitereien Beleidigungen ausarten zu lassen, müssen sinnvolle und nachvollziehbare Regeln vereinbart werden. Es ist wichtig, dass Moderatoren das Forum regelmäßig, am besten täglich, sichten und auf Einhaltung der Regel achten sowie Verstöße gegen sie löschen und entsprechend Benutzer verwarnen oder gar aus dem Forum entfernen. Des weiteren ist eine redaktionelle Betreuung zu empfehlen, die das Forum mit aktuellen Meldungen aus der Politik versorgt. Dadurch sollen die Nutzer auf dem neuesten Stand gehalten werden und gleichzeitig Grundlagen für weitere Diskussionen geliefert werden. Je nach Popularität des Forums kann dabei durchaus ausreichend Arbeitsaufwand für eine Vollzeitstelle anfallen, so dass weitere Moderatoren aus den Reihen der Nutzer gewonnen werden sollten.

Falls eine solche Webanwendung durch Werbung finanziert werden soll, wird empfohlen diese Werbung von außerhalb des politischen Bereichs zu beziehen. Ansonsten kann sehr schnell bei Werbung für nur eine Partei der Verdacht der Parteilichkeit des Forums aufkommen, was ja gerade dem in der Ausgangssituation geschilderten Wunsch widerspricht.

Im Falle des Missbrauchs als Propagandamaschine sollten die entsprechenden Beiträge nicht einfach so gelöscht werden sondern in der Öffentlichkeit unzugängliche Bereiche verschoben und die Staatsanwaltschaft informiert werden. Über die Protokolldaten des Forums kann der Verfasser dieser Beiträge zügig ermittelt und belangt werden. Auf dieses Vorgehen sollte auch in den Forenregeln hingewiesen werden.

Die Empfehlung zum Betrieb einer interaktiven und politischen Webanwendung lautet also, ein Forum wie phpBB zu benutzen und diesem eine gute redaktionelle Betreuung zukommen zu lassen.

7 Datenschutz und Anonymität bei politischen eProzessen

Datenschutz und Anonymität bei politischen eProzessen

Wolfgang Deeken

3. Februar 2006

Datenschutz ist ein Grundrecht in Deutschland und es wird durch den Umgang mit personenbezogenen Daten immer häufiger das Recht auf diese informelle Selbstbestimmung beeinträchtigt. Dies wird auch bei politischen eProzessen deutlich, die im Behördenverkehr im Moment zunehmend angeboten werden. Dazu gehören neben ersten Projekten für Online-Wahlen auch signierte Anwendungen für Bürger, die diese von zu Hause statt auf dem Amt ausführen können oder aber auch die elektronische Vorsteuererklärung, die zur Nutzung sogar vorgeschrieben ist.

Das von Staat und Wirtschaft 2003 in Leben gerufene „Bündnis für elektronische Signaturen“ versucht, vorhandene Karteninfrastrukturen mit ausgereiften Anwendungen für Behörden zu verbinden und den Bürgern so durch einheitliche Sicherheitsvorgaben und durch fortgeschrittene und qualifizierte elektronische Signaturen ein umfassendes Anwendungsgebiet an Behördendiensten anbieten zu können.

Elektronische Wahlen wurden in Deutschland bisher nur im Rahmen von Projekten wie dem Projekt „W.I.E.N. - Wählen in elektronischen Netzwerken“ als Folgeprojekt des vom Bundesministerium für Wirtschaft und Arbeit geförder-

ten Projekts „Wählen via Internet (i-vote)“ durchgeführt. Dabei wurden z. B. bei der T-Systems CSM erfolgreich Betriebswahlen durchgeführt, die durch ein eigenes Wahlsystem auf beliebigen Arbeitsplätzen so abgesichert wurden, dass die erforderlichen Datenschutz- und Sicherheitsaspekte erfolgreich in das Wahlsystem integriert wurden und das Projekt zu einem positiven Gesamtergebnis gekommen ist.

Ein weiteres positives Beispiel ist der Behördenverkehr in Bremen, der seit 1999 durch das Projekt media@komm begleitet wurde und aus dessen Rahmen sich die E-Government-Software Governikus entwickelt hat. Diese dient als E-Government-Sicherheits-Middleware für sicheres und rechtsverbindliches E-Government und bündelt alle für solche Online-Transaktionen erforderlichen Funktionalitäten wie Ver- und Entschlüsseln, Erstellung und Prüfung von Signaturen, Ver- und Entpacken von Daten, Benachrichtigungen und sogar den Anstoß für Zahlvorgänge. Damit ist aus einem Projekt des BMWA eine Software entstanden, die datenschutz- und sicherheitstechnischen Ansprüchen genügt und für die weitere Verbreitung bei Behörden geeignet und getestet ist.

Die elektronische Steuererklärung (Elster) dagegen ist ein Negativbeispiel für Datensicherheit, da bei der seit dem 01.01.2005 vorgeschrieben elektronischen Umsatzsteuervorerklärung keine technischen Maßnahmen zur Authentifizierung der Antragsteller vorgesehen waren. Erst durch die Inbetriebnahme eines behördlichen ElsterPortals am 04.01.2006 wurden die Mängel beseitigt und Möglichkeiten zur Authentifizierung der Nutzer bereit gestellt.

Allgemein gibt es in der deutschen Politik leider viele Fälle, wo der Datenschutz aufgrund von „Terrorabwehr und Verbrechensbekämpfung“ auf der Strecke bleibt und der Weg zum gläsernen Menschen immer weiter geht. Aktuell sind dies z. B. die am 14.12.2005 vom Europäischen Parlament beschlossene Vorratsdatenspeicherung von Verbindungsdaten in der Telekommunikation, die nun in den Mitgliedsstaaten umgesetzt werden soll und zumindest den elektronischen Bürger gläsern macht. Auch das Mautsystem in Deutschland soll auf einmal, obwohl ausdrücklich für den Zweck der Mauterhebung bestimmt, für die Fahndung nach Flüchtigen eingesetzt werden. Viele Bürger unterstützen diese Entwicklung leider aufgrund fehlenden Datenschutzbewusstseins, den

meisten wird jedoch noch gar nicht klar sein, was der Staat in Zukunft mit diesen Daten vorhat und wie er sie nutzt. Diese Entwicklung muss kritischer beobachtet und hinterfragt werden, sonst müssen wir auf unsere Grundrechte wohl bald ganz verzichten.

7.1 Einleitung

Beim Umgang mit Behörden und durch die Nutzung des Internet allgemein kommt immer häufiger der Wunsch auf, Behördengänge online abwickeln zu können. Diese politischen eProzesse sind gedacht zur Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen Institutionen der Exekutive (Behörden), sowie zwischen diesen Institutionen und Bürgern (G2C), Unternehmen (G2B) und weiteren staatlichen Institutionen (G2G) durch den Einsatz von Informations- und Kommunikationstechnologien.

Das Ziel sind schnellere und unkompliziertere Dienstleistungen für den Bürger und Kostenersparnis beim Staat, der dabei von einer Vaterrolle in eine dienstleistungsorientierte Partnerrolle gewandelt werden soll.

In diesem zunehmenden Maß an Behördenverkehr über öffentliche Netze sind Datenschutz und Anonymität äußerst wichtig, deswegen wird in dieser Ausarbeitung dargestellt, wie bei verschiedenen politischen eProzessen der Datenschutz bzw. die Anonymität berücksichtigt werden und was in diesem Sinne für zukünftige Entwicklungen geplant ist.

Außerdem wird noch einmal auf aktuelle Datenschutzdiskussionen eingegangen, die Projekte des Staates betreffen. Abschließend gibt es dann noch ein kurzes Fazit.

7.2 Datenschutz

Datenschutz bezeichnete ursprünglich den Schutz personenbezogener Daten vor Missbrauch. Der Begriff wurde gleichgesetzt mit Schutz der Daten. Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Der Datenschutz versucht also, den so genannten gläsernen Menschen verhindern.

Auf Bundesebene regelt das Bundesdatenschutzgesetz (BDSG) den Datenschutz für die Bundesbehörden und den privaten Bereich (d. h. für alle Wirtschaftsunternehmen). Daneben regeln die Landesdatenschutzgesetze der Bundesländer den Datenschutz in Landes- und Kommunalbehörden.

Neben den allgemeinen Datenschutzgesetzen gibt es eine Vielzahl bereichsspezifischer Datenschutzregelungen. Diese gehen den Regelungen des allgemeinen Datenschutzrechts vor.

Die öffentlichen Stellen des Bundes sowie die Unternehmen, die geschäftsmäßig Telekommunikations- oder Postdienstleistungen erbringen, unterliegen der Aufsicht durch den Bundesbeauftragten für den Datenschutz. Die Landesbehörden werden durch die Landesdatenschutzbeauftragten kontrolliert. Die privaten Unternehmen (bis auf Telekommunikation und Post) unterliegen der Aufsicht der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die beim Landesdatenschutzbeauftragten oder bei den Landesbehörden (z. B. Innenministerium) angesiedelt sind.

Neben dem Datenschutz hat die Datensicherheit das Ziel, Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen. Dabei unterscheidet man in der Regel die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit. Anforderungen zur Datensicherheit von personenbezoge-

nen Daten ergeben sich aus dem gesetzlichen Datenschutz. Datensicherheit umfasst aber auch andere Daten, z. B. Vertragsdaten, Bilanzdaten oder Forschungsergebnisse.

Datensicherheit ist eine Voraussetzung von Datenschutz. Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, dass vertrauliche bzw. personenbezogene Daten nicht in die Hände von Unbefugten gelangen. Hierbei spricht man in der Regel von technischen und organisatorischen Maßnahmen zum Datenschutz, welche speziell beim Design verschiedener Anwendungen äußerst wichtig sind. Häufig befindet sich eine Beschreibung der Datensicherheit in einem Datenschutzkonzept oder Sicherheitskonzept.

Weitere Maßnahmen zur Datensicherheit umfassen unter anderem die physische bzw. räumliche Sicherung von Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen der Datensicherung und die Verschlüsselung. Wichtige Voraussetzung ist die Sicherheit der verarbeitenden Systeme. Ein effektives Sicherheitskonzept berücksichtigt jedoch neben technischen Maßnahmen auch organisatorische und personelle Maßnahmen, wie z. B. das Schaffen geeigneter Organisations- und Managementstrukturen oder die Schulung und Sensibilisierung von Personen.

7.3 Anonymität

Anonymität beschreibt Handlungen, bei denen die Identität des Handelnden nicht preiszugeben wird. Das ist z. B. wichtig bei Online-Wahlen, wo die Wahl der Teilnehmer geheim bleiben muss. In dem Fall muss der Wähler allerdings zusätzlich identifiziert werden, um eine Mehrfachwahl zu vermeiden.

Anonymität ist vor allem häufig zu finden in Online- und Forensystemen oder bei Umfragen, sofern diese anonym erfolgen. Einige Vor- und Nachteile von Anonymität werden im Folgenden aufgelistet:

Vorteile:

- Meinungsfreiheit in hohem Grade
- Meinung kann offen geäußert werden

Nachteile:

- Extreme Ansichten werden dargelegt
- Meinungen Anderer könnten abfällig behandelt werden

7.4 Fallbeispiele

7.4.1 Signaturbündnis

Staat und Wirtschaft haben am 3. April 2003 in Berlin das „Bündnis für elektronische Signaturen“ gegründet, mit dem sie auf Initiative der Bundesregierung die elektronische Signatur in Deutschland gemeinsam fördern wollen. Die Vision des Bündnisses ist es, dass Bürger mit

- jeder beliebigen Chipkarte
- jedem Kartenleser
- eine Vielzahl - idealerweise alle -
- der verfügbaren Applikationen aus
- eCommerce und E-Government

nutzen können.

Um diese Vision Realität werden zu lassen, setzt das Bündnis auf Netzwerkeffekte durch die Einbindung von:

- Vorhandenen Karteninfrastrukturen
- Ausgereiften eCommerce-/ eBusiness-Applikationen

- BundOnline 2005 - Anwendungen

Die Bündnispartner einigten sich in einer gemeinsamen Erklärung insbesondere über technische Standards für die eingesetzten Anwendungen und Produkte, den Einsatz multifunktionaler Chipkarten, einheitliche Sicherheitsvorgaben und vor allem über die Verwendung fortgeschrittener und qualifizierter elektronischer Signaturen. In einem Zeitraum bis Ende 2005 wollen alle Bündnispartner ihre Konvergenzziele erreicht haben und somit den Nutzen des Bündnisses für alle Beteiligten ausschöpfen. Das Bündnis soll weiterhin helfen, Partner zu finden, um gemeinsam leichter die nötigen Anfangsinvestitionen zu tragen und von Beginn an einen großen Nutzerkreis und attraktive Angebote bieten zu können.

Das Signaturgesetz oder anders: „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ hat in diesem Zusammenhang den Zweck, Rahmenbedingungen für elektronische Signaturen zu schaffen. Ziel ist es, erhöhte Rechtssicherheit für den Internet basierten Geschäftsverkehr und daher natürlich auch für politische eProzesse zu schaffen. Das Signaturgesetz reguliert hierfür den Markt der Anbieter von Zertifizierungsdienstleistungen, der Zertifizierungsdiensteanbieter. Dies jedoch nur insofern, als diese sogenannte qualifizierte Zertifikate ausstellen.

Das Signaturgesetz bestimmt die Anforderungen an diese Zertifikate und an ihre Aussteller. Die Zertifikate müssen einen bestimmten Mindestinhalt haben. Die Anbieter müssen die Aufnahme ihres Geschäftsbetriebs bei der Bundesnetzagentur anzeigen und ein den Vorgaben des Gesetzes und der zugehörigen Signaturverordnung entsprechendes Sicherheitskonzept vorlegen. Ausgestellte Zertifikate müssen in ein jederzeit abrufbares Verzeichnis eingestellt und auf Verlangen des Inhabers unverzüglich gesperrt werden. Für Fehler besteht eine Verschuldenshaftung mit Beweislastumkehr.

Diese Vorschriften bahnen den Weg für eine sichere Nutzung von qualifizierten Signaturen und ermöglichen ein umfassendes Anwendungsgebiet bei richtiger Umsetzung. Das Problem, das weiterhin besteht, ist, dass Behörden ohne eine entsprechende Verbreitung der Signaturen wenig Sinn darin sehen werden, passende Applikationen anzubieten. Andererseits werden Anwender ohne ein grö-

ßeres Anwendungsgebiet die Mühen scheuen, sich eine Signatur zu besorgen (Henne-Ei-Problematik). Dennoch bieten immer mehr Kommunen ihre Dienste elektronisch an und durch die Projekte vom Bund wird ein großer Schritt in die richtige Richtung getan, so dass das Signaturbündnis dafür sorgen sollte, in naher Zukunft viele Dienste mit qualifizierten Signaturen nutzen zu können.

7.4.2 Elektronische Wahlen

Elektronische Wahlen sind ein breites Anwendungsgebiet der politischen eProzesse. Dabei kann es sich gleichermaßen um eine Bundestagswahl als auch um Wahlen in großen Firmen handeln, mit der Ausnahme, dass elektronische Wahlen in großen Firmen schon erfolgreich durchgeführt wurden. Die Stimmabgabe erfolgt bei elektronischen Wahlen nicht mit Stimmzettel und Urne, sondern über ein elektronisches Medium, wie zum Beispiel das Internet. Die Herausforderungen dabei sind die Anonymität bei gleichzeitiger Nachvollziehbarkeit und Unverfälschbarkeit der Wahl.

Zwei Formen der elektronischen Abstimmung können unterschieden werden:

- elektronische Abstimmung mit zertifizierter Hard- und Software in offiziellen Abstimmungslokalen („Geschlossene“ oder „Ende-zu-Ende-Systeme“);
- elektronische Abstimmung von jedem Eingabegerät (z. B. private PC's, Handies) mit nicht zertifizierter Software („Offene Systeme“).

Je nach Verwendungszweck des Wahl-Systems ist die Sicherheit bei der korrekten Ergebnisermittlung, sowie der Einhaltung der Wahlgeheimnisses unterschiedlich kritisch zu sehen. Gegebenenfalls sind die folgenden Aspekte zu berücksichtigen:

- Das eingesetzte Protokoll sollte die Anonymität des Wählers sicherstellen. Der Wähler soll seine Wahl später nicht nachweisen können (Quittungsfreiheit). Dritte sollen nicht in der Lage sein können, das Wahlge-

heimnis zu brechen. Die Wahlbehörden und die Administratoren etwaiger zentraler Wahlserver sollen nicht in der Lage sein, das Wahlgeheimnis brechen zu können.

- Das eingesetzte Protokoll sollte die Korrektheit des Ergebnisses sicherstellen. Weder Wähler, Dritte, noch die Administratoren etwaiger zentraler Wahlserver sollen in der Lage sein, die Ermittlung des korrekten Wahlergebnisses verhindern zu können.

- Das eingesetzte Protokoll sollte eine universelle Verifizierbarkeit des Ergebnisses zulassen, damit gewährleistet ist, dass jeder Wähler Vertrauen in das Ergebnis gewinnen kann.

- Ein schwierig zu kontrollierendes Sicherheitsproblem bei Internetwahlen ist die Sicherheit der Client-Rechner. Es muss sichergestellt werden, dass der PC oder das Eingabegerät des Wählers tatsächlich den Stimmzettel so ausgefüllt abgibt wie der Wähler ihn ausgefüllt hat und angezeigt bekommt. Ansonsten könnten die PCs der Wähler massenhaft automatisiert angegriffen werden und somit das Wahlergebnis beliebig verfälscht werden, ohne dass dazu eine Sicherheitslücke in der Wahlsoftware oder in der Systemsoftware der zentralen Wahlserver vorhanden sein muss. Dies kann z. B. durch den Einsatz von Chipkarten erreicht werden, jedoch nur, falls sichergestellt wird, dass die Leser ausschließlich Kartenlesegeräte verwenden, die über eine eigene Tastatur und über ein eigenes Display verfügen und die Verschlüsselung des Stimmzettels auf der Chipkarte vorgenommen wird. Eine andere Möglichkeit stellt die Installation der Wahlclientsoftware auf einer selbstbootenden CD dar, falls es gelingt, diese CD mit sämtlichen von den Wählern eingesetzten Hardwarekonfigurationen lauffähig zu bekommen.

- Solange nicht ein universell verifizierbares Wahlprotokoll eingesetzt wird, ist sicherzustellen, dass die verwendete Systemsoftware (Betriebssystem, Compiler, etc.) der zentralen Wahlserver keine Sicherheitslücken aufweist, sowie die Wahlsoftware im Allgemeinen, wie auch das verwendete Protokoll im Speziellen keine Sicherheitslücken aufweist. Dies kann eine außerordentlich schwierige Aufgabe sein.

- Bei besonders kritischen Wahlen (wie z. B. Bundestagswahlen) ist zudem sicherzustellen, dass die Wähler tatsächlich Vertrauen in die ergriffenen Sicherheitsmaßnahmen haben, sollen diese das Ergebnis auch tatsächlich akzeptieren. Auch dies kann angesichts der technischen Komplexität eine enorm schwierige Aufgabe sein.

Diese Aspekte umzusetzen versucht das Wahlsystem „i-vote“ des Projekts „W.I.E.N.“. Das Projekt „W.I.E.N. - Wählen in elektronischen Netzwerken“ als Folgeprojekt des auch vom Bundesministerium für Wirtschaft und Arbeit (BMWA) geförderten Projekts „Wählen via Internet“ („i-vote“) dient der Entwicklung und Erprobung unterschiedlicher Typen von Elektronischen Wahlen in überschaubaren Bereichen im nicht-parlamentarischen Raum, wie z. B. Betriebsrats-, Personalrats-, Aktionärs- oder auch Sozialwahlen. Dabei stehen neben der Anpassung der Technik die organisatorische Gestaltung, rechtliche Fragen und die Akzeptanz bei den Wählenden im Mittelpunkt. Ziel ist es, erprobte Wahlverfahren bereitzustellen, die ein sicheres und einfaches Wählen über offene Kommunikationsnetzwerke, vernetzte Wahllokale und mobile Endgeräte ermöglichen.

Bisher kamen rechtsgültige Internet-Wahlverfahren unter Einbindung elektronischer Signaturen nur bei Wahlen mit einer kleineren Wählerschaft zum Einsatz. Erfahrungen mit Online-Wahlen aus vernetzten Wahllokalen mit Tausenden von Wählerinnen und Wählern für ein Großunternehmen, eine gesamte Region oder ein Land, liegen derzeit nicht vor. Die Schwerpunkte des Projekts liegen im Aufzeigen von sicheren, generischen Wahlsystemen unter Vernetzung von Wahllokalen und in der Erprobung elektronischer Signaturen unter Berücksichtigung mobiler Strukturen.

7.4.3 Behördenverkehr Bremen

Bremen ist eine der drei bundesdeutschen Städte, die den Zuschlag zum Modellversuch des durch das Bundeswirtschaftsministerium für Wirtschaft und Arbeit geförderten Projektes media@komm erhalten haben (neben Esslingen

und Nürnberg). Untersucht und prototypisch erprobt wurde in diesen parallelen Versuchen die Einführung von Chipkarten in verschiedenen Bereichen von Behörden und kommunalen Strukturen.

Studien haben ergeben, dass Menschen das Internet vor allem für Behördenkontakte nutzen wollen. Formularserver und Online-Formulare ersparen jedoch nur wenige Behördengänge, da weiterhin persönliche Unterschriften nötig sind. Die rechtliche Voraussetzung für digitale Signaturen als Unterschriftersatz wurde 1998 geschaffen. Durchgeführt wurde das Bremer Projekt durch eine eigens gegründete Gesellschaft, an der neben Sparkasse und lokalem ÖPNV auch zwei Softwarehäuser beteiligt waren. Zentraler Gedanke war, dass für den Erfolg des Projekts gleichzeitig benötigt werden:

1. eine Plattform zur Steuerung und Abwicklung der Verfahren,
2. attraktive Anwendungen und
3. technische Zugangsmedien für die Bürger.

Ein Anwendungsszenario war z. B. das Ummelden nach einem Umzug. Mit der Chipkarte würde sich ein Bürger am eigenen Rechner oder an einem öffentlichen Terminal bei einer zentralen Verwaltungsstelle (Bürgerbüro, Ortsamt) identifizieren und die Aktionen/Formulare auswählen, die er ausführen will (sich anmelden, Auto, Hund, Strom, Rundfunkgebühren etc.). Ein Teil der Daten kann automatisch von einem Formular ins andere übertragen werden, Folgeaktionen können angestoßen werden. Indem Anwendungsbündel geschaffen werden, ist statt mehreren Behördengängen keiner oder maximal einer notwendig. Hauptanwender der Karte sind jedoch professionelle Mittler, für die ebenfalls Anwendungsbündel geschaffen werden, z. B. Rechtsanwälte, Notare und Steuerberater sowie Architekturbüros, die z. B. Bauanträge stellen etc.

Die Chipkarte verwendet asymmetrische Verschlüsselungsverfahren mit öffentlichen und privaten Schlüsseln zum Verschlüsseln, Entschlüsseln und Signieren. Registrierungsstellen vergeben Schlüssel an die Bürger und Trust-Center der Telekom verwalten die Schlüssel, um z. B. Signaturen überprüfen zu können. Der Bürger verschlüsselt im Verkehr mit Behörden jedes Formular mit

dem öffentlichen Schlüssel der entsprechenden Behörde. Dies trenne die Daten voneinander und erfülle das Zweckbindungsgebot des Datenschutzes.

Das Projekt wurde in drei Phasen unterteilt. Von 1999 bis 2002 wurde eine eigene Signaturkarte in der Kommunikation zwischen Steuerberatern und Finanzamt sowie Rechtsanwälten und Gerichten erprobt. Da die Sparkasse Bremen seit 2000 sowieso Geldkarten eingeführt hat, konnte diese ohne allzuviele Zusatzkosten um Signatur und Zusatzapplikationen erweitert werden. Seit 2002 wird die ec-Karte mit der Geldkarte integriert. Media@komm nutzt also die vorhandenen Ressourcen der Sparkasse mit. Ein vorteilhafter Seiteneffekt ist, dass man damit an das bestehende Vertrauen der Bankkunden in die Bank und ihre vorhandenen Gewohnheiten anknüpfen könne. Viele Verwaltungsvorgänge verlangen zudem das Bezahlen einer Gebühr. Die Integration vermeidet das Herumhantieren mit mehreren Karten während eines Vorgangs und appelliert so an die Bequemlichkeit der Bürger.

Da nicht alle Bürger die notwendigen technischen Fähigkeiten für den elektronischen Behördenverkehr erlernen werden, sei mit einer Quote von vorerst 20% bei der Anwendung durch Bürger zu rechnen. In den USA läge die Sättigungsgrenze bei 40%. Die Chipkarte solle den gewohnten Umgang mit Behörden nicht ersetzen, sondern erweitern. Dies ergebe sich von selber, da viele Formulare so kompliziert seien, dass sie ohnehin nicht ohne Hilfe ausfüllbar seien. Daher solle es so etwas wie „betreute Nutzerplätze“ in Ortsämtern und Bürgerämtern geben, sowie Call-Center. Chancen und Risiken von Chipkarten sind eine nicht entscheidbare Frage, es käme auf die Funktionen und die innere Organisation der Verwaltungsvorgänge an. Da es keine Partizipation per se gebe (ohne konkreten Grund), sei daran gedacht, Beteiligungsverfahren dort zu integrieren, wo es sich sozusagen ergibt.

Der Vertreter des Landesbeauftragten für den Datenschutz, Uwe Schläger, lobte in einem Statement bei einer Podiumsdiskussion das Projekt für die Einbindung der Datenschützer, die von Anfang an die Soll-Konzepte prüfen. Da das Projekt bundesweite Bedeutung habe - eines der drei Pilotprojekte soll bundesweit erweitert werden - gäbe es die Möglichkeit, stellvertretend Sicherheitsmechanismen durchzudiskutieren. Das Bremer Projekt könne zudem beweisen,

dass die qualifizierte deutsche Signatur nach deutschem Signaturgesetz durchführbar und wirtschaftlich machbar sei, was von der EU bezweifelt wurde (das europäische Signaturgesetz stellt schwächere Auflagen als das deutsche). Die Datenschutzprobleme deuteten sich jedoch an unerwarteten Stellen an, oft im Detail. Beispielsweise sei die Plattform ursprünglich gedacht worden als reine Weiterleitungsstelle, so als ob man einen Brief in einen verschlossenen Umschlag stecke. Probleme ergeben sich aber, wenn Bürger auch nachts Formulare ausfüllen, die Behörde aber nicht rund um die Uhr besetzt ist. In vielen Anwendungen sind nämlich Plausibilitätskontrollen notwendig, beispielsweise ob eine Adresse tatsächlich existiert. Daher muss ein Teil der Daten auf der Plattform gespiegelt werden, was komplizierte technische Lösungen erfordert, um den Datenschutz zu gewährleisten. Zudem müssten etliche Gesetze geändert werden, um die Verfahren zu vereinfachen oder die elektronische Signatur als Ersatz für das persönliche Erscheinen zu erlauben.

Eine wichtige Frage war, ob es überhaupt möglich sei, eine zentrale Anlaufstelle für alle Behördenkontakte anzubieten. Zum einen könne der dortige Berater nicht alle möglichen Formulare so gut kennen wie spezialisierte Beamte. Zum anderen sei dies ein datenschutzrechtliches Problem. Das Bürgerbüro stößt auf datenschutzrechtliche Grenzen, wenn derselbe Beamte alle Lebenslagen betreuen soll. Dies sei ein weiterer Grund, die Anwendungen in einigermaßen unkritische Pakete zu bündeln, obwohl es gelegentlich Gründe gibt, z. B. bei einer Ummeldung nicht sofort allen Behörden die gleiche Information zu geben. Es bestehe die Gefahr, durch workflow-artige Abläufe einen impliziten Zwang zu schaffen. Außerdem trat die Frage auf, wie groß die Gefahr einer Zusammenlegung von Karten sei. Es sei schon auffällig, dass nach dem Zurückstellen der AsylCard-Pläne durch die Bundesregierung nun in Bayern geplant wird, ausgerechnet in Nürnberg - einer der media@komm-Städte - eine AsylCard zu testen.

In Frage gestellt wurde auch das Argument, die Chipkarte solle bequem für die Bürger sein. Viele Behördenvorgänge werden vom Einzelnen nur sehr selten benötigt. Dann aber steht dieser jedesmal neu vor dem Problem, mit der Technik und mit dem Formular klarzukommen, sich durch Fehlermeldungen hindurchzukämpfen und auszuprobieren. Wenn von den Projektverantwortlichen ausgesagt werde, diese neue Technik solle die alte nur ergänzen, nicht ersetzen,

stellen sich zwei Fragen: Wer bezahlt das Ganze? Und: Wer verdient daran? Der Haupteffekt tritt bei den Mittlern auf, die häufig die gleichen Vorgänge durchführen. Es profitieren vor allem neue Servicebereiche. Beispielsweise hätten sich einige Speditionen selber bei den Projektträgern gemeldet.

Von untersuchten 100 Behördengängen (die selber bereits nur ein Bruchteil der existierenden sind) sind nur 20 sinnvoll elektronisierbar. Der Rest ist laut der Untersuchung zu widerspenstig. Hier stellt sich die Frage, ob dies den Aufwand rechtfertigt. Zumindest der normale Bürger profitiert demnach kaum, wohl aber die professionellen Mittler und Serviceanbieter. Doch auch wenn 20 Verfahren sehr wenig erscheinen, lässt sich daraus noch nichts über die endgültig sich ergebende Durchdringung der Verwaltung durch elektronische Behördenkontakte aussagen.

Im Rahmen des Projektes media@komm hat die Firma bremen online services GmbH und Co. KG (bos) die E-Government-Sicherheits-Middleware Governikus für sicheres und rechtverbindliches E-Government entwickelt. Auf Grundlage der Förderbedingungen hat sich der Bund ein unentgeltliches, nicht ausschließliches und übertragbares Nutzungsrecht an Governikus in der zum Ende des media@komm- Projekts vorliegenden Version (Governikus 1.1) einräumen lassen. Dieses Nutzungsrecht hat der Bund Ende 2003 auf die Länder übertragen und diese zugleich ermächtigt, das Nutzungsrecht auf ihre Kommunen (Gemeinden und Gemeindeverbände) zu übertragen.

Zwischenzeitlich liegt Governikus in der Version 2.2 vor. Zur Nutzung von Governikus 2.x sind all die Stellen berechtigt, die dem Projekt Pflege Governikus beigetreten sind bzw. die auf Grund einer gesonderten Vereinbarung zur Nutzung berechtigt sind.

Governikus bündelt alle für sichere und rechtsverbindliche Online-Transaktionen erforderlichen Funktionalitäten: Governikus ver- und entschlüsselt Nachrichten, erstellt und prüft Signaturen, ver- und entpackt Daten, erstellt Zeitstempel, benachrichtigt über erfolgreichen Versand und Zustellung und stößt sogar Zahlverfahren an. Eingehende Daten können direkt an ein Fachverfahren übergeben und dort ohne Medienbruch weiter verarbeitet werden.

Damit ist aus dem Projekt media@komm in Bremen ein System entstanden, dass datenschutzrechtlichen Aspekten genügt von von weiteren Behörden eingesetzt werden könnte. Wie dies umgesetzt wird, muss die Zukunft zeigen.

7.4.4 Elektronische Steuererklärung (Elster)

Unternehmen, die seit Anfang 2005 pflichtgemäß ihre Steuerdaten per Internet ans Finanzamt übermitteln, müssen einkalkulieren, dass böswillige Geschäftspartner falsche Daten in ihrem Namen einreichen könnten. Während gedruckte Steuerformulare klar machen, dass man beim Ausfüllen die Richtigkeit der gegebenen Auskünfte per Unterschrift zu bestätigen hat, liegt der Fall bei der elektronischen Umsatzsteuer-Voranmeldung anders.

Bevor ein Betrieb vorschriftsgemäß am Elster-Verfahren für Umsatzsteuer- und Lohnsteuer-Voranmeldungen teilnehmen darf, muss er die Richtigkeit seiner Angaben mittels einmaliger schriftlicher Teilnahmeerklärung zusichern. Danach erfolgen die Anmeldungen zwar verschlüsselt (durch 3DES und RSA) und auch die Integrität wird durch einen Hash-Code sicher gestellt, aber ohne Authentifizierung gegenüber dem Finanzamt. So kann jeder einem Unternehmen einen Streich spielen, indem er irgendwelche Zahlen unter Angabe von dessen Steuernummer beim Finanzamt einreicht. Gegen dieses Risiko wendet sich nun der Bund der Steuerzahler in Schulterschluss mit dem Bundesbeauftragten für den Datenschutz. Sollten es die Finanzbehörden „nicht schaffen, ein einwandfreies Verfahren zu gewährleisten, muss die Software so lange abgeschaltet werden“ äußerte dessen Sprecherin gegenüber der Presse.

Unberechtigte Abbuchungen kann der Steuerzahler zwar durch einfache Erklärung korrigieren lassen, aber selbst wenn das in allen Fällen auf Anhieb funktionieren sollte, bleibt den Firmen ein beträchtlicher Mehraufwand für die ständige Nachprüfung der verwendeten Angaben in Steuerbescheiden.

Seit dem 04.01.2006 gibt es ein behördliches Elster-Webportal, das authentisierte Steuerdaten von registrierten Absendern entgegennimmt. Die Authen-

tifizierung eines registrierten Benutzers gegenüber dem Portal basiert auf einer Public-Key-Infrastruktur und einem persönlichen Zertifikat. Diese Daten können entweder in einem verschüsselten Software-Zertifikat auf Diskette/Festplatte oder auf einem USB-Device (genannt Elster-Stick) mit integriertem Kartenleser und Chip gespeichert werden. Vorhandene Signaturkarten bestimmter Hersteller/Trustcenter können ebenfalls weiter genutzt werden, darunter Datev-Cards.

Man sieht, Funktionalität wird leider oft der Datensicherheit bzw. dem Datenschutz vorgezogen. In diesem Fall ist es jedoch auch positiv zu sehen, dass inzwischen (über ein Jahr nach gesetzlicher Verpflichtung zur Nutzung!) Möglichkeiten zur Absicherung der eProzesse gegeben sind.

7.5 Politik und Datenschutz

Die Politik entscheidet fast täglich über Vorgänge oder Neuerungen, die den Bürger zum Schutz der Allgemeinheit überwachen. Dass der Datenschutz dabei ziemlich auf der Strecke bleibt, wird durch Terrorabwehr und erhöhte Sicherheit gerechtfertigt. In diesem Zusammenhang kommt allerdings auch immer wieder der Hinweis auf den „gläsernen Menschen“, der durch einen überwachenden Staat immer mehr durchleuchtet wird. Die Verwender dieses Begriffes verweisen auf die zunehmende Überwachung der Menschen, neue technische Überwachungsmethoden sowie das steigende Interesse des Staates an Informationen über seine Bürger. Sie befürchten einen vollständigen Verlust der Privatsphäre und eine daraus resultierende Anpassung der Menschen an das vom Staat als normgerecht vorgegebene Verhalten.

Dafür gibt es einige aktuelle Beispiele, angefangen mit der Vorratsspeicherung von Verbindungsdaten in der Telekommunikation. Bereits Anfang 2004 nahm die EU einen Anlauf, um die Speicherung der Verbindungsdaten aller Arten von Telekommunikation und deren Weitergabe an die staatlichen Behörden gesetzlich zu regeln. Bei den Überwachungsplänen in Brüssel, die vom EU-Rat und der EU-Kommission mit Nachdruck vorangetrieben wurden, geht es prinzipiell

um die Speicherung der Verbindungs- und Standortdaten, die bei der Abwicklung von Diensten wie Telefonieren, SMS, E-Mailen, Surfen oder Filesharing anfallen. Mit Hilfe der Datenberge sollen Profile vom Kommunikationsverhalten und von den Bewegungen Verdächtiger erstellt werden.

Die Kommission etwa erhoffte sich durch die Vorratsdatenspeicherung bessere Möglichkeiten zur Prävention, Aufklärung und Verfolgung schwerer Straftaten, vor allem im Bereich Terrorismus und organisierter Kriminalität. Ein Harmonisierungsbedarf innerhalb der EU sei gegeben, da einzelne Mitgliedsstaaten nationale Maßnahmen zur Vorratsdatenspeicherung verabschiedet hätten oder dies planen würden.

Die Auseinandersetzung in den einzelnen Mitgliedsländern, auf EU-Ebene zwischen Rat, Kommission und Parlament sowie zwischen EU-Behörden und den jeweiligen Ratspräsidentschaften zog sich über Jahre hin. Aber auch wenn auf EU-Ebene ein endgültiger Beschluss gefasst ist, bleibt noch ein gewisser Spielraum, wie die EU-Mitgliedsstaaten die Richtlinie in nationales Recht umsetzen. So sind am 14.12.2005 Speicherfristen von sechs bis 24 Monaten beschlossen worden, wobei die nationalen Gesetze ihre Fristen selbst definieren können.

Ein Rechtsinformatiker der Uni Köln fürchtet nach dem Beschluss, dass die Sicherheitsbehörden mit dem Durchwinken ihrer alten Träume zur Vorratsdatenspeicherung Blut geleckt haben und weitere drastische Kontrollmöglichkeiten einfordern. Als erstes sei mit der Einführung einer Pflicht für Betreiber von Internet-Cafes zu rechnen, immer den Personalausweis der Kunden zu verlangen und eine Kopie davon aufzubewahren. Zudem würden sie wohl angehalten, ihren vollständigen Traffic vorzuhalten.

Anonymizern könnte ebenso ein Bann drohen. Ferner werde die schon abgeschlossen geglaubte Kryptodebatte neu aufgemacht, da die Fahnder wieder eine Hintertür für den Zugang zum Klartext verlangen würden. Letztlich werden sich die Sicherheitsdienste gar dafür stark machen, mithilfe von Keyloggern und Trojanern sämtliche Tastatureingaben der PC-Nutzer mitschneiden zu dürfen. Nach den Einknicken des Parlaments bei der Telekommunikationsüberwachung

halten es Forscher für möglich, dass derlei Wünsche „schon nächste Woche auf die Agenda kommen könnten“.

Ein weiteres aktuelles Beispiel für Datenschutzprobleme in der Politik ist das Anfang 2005 eingeführte LKW-Mautsystem in Deutschland, das möglicherweise in naher Zukunft zur Fahndung von Fahrzeugen eingesetzt werden soll. Ins derzeit gültige Mautgesetz sind bei der Einführung zwar explizit „Sicherungen zur Zweckbindung der Daten“ eingebaut worden, die die polizeiliche Nutzung der Mautdaten ausdrücklich untersagen. Zu befürchten ist jedoch, dass die nun beabsichtigte Durchbrechung der Zweckbindung erst der Beginn ihrer völligen Auflösung sein wird. Dazu der stellvertretende Landesbeauftragte für den Datenschutz in Schleswig-Holstein, Dr. Johann Bizer: „Heute sollen die Mautdaten nur zur Bekämpfung des Terrorismus sowie der Organisierten Kriminalität verwendet werden, morgen werden sie dann wohl auch zur Verfolgung von Fällen einer ’mittleren Kriminalität’ verwendet. Und warum nicht auch zur Verhinderung von ’Sozialmissbrauch’, ’Schwarzarbeit’ oder zur Verfolgung von Unterhaltspflichtigen sowie - natürlich nur aus Sicherheitsgründen - auch zur Verkehrslenkung bei Großveranstaltungen?“. Wären Pläne zur Nutzung der Daten als Fahndungsdaten beim Beschluss des Mautsystems bekannt gewesen oder wäre die Zweckbindung der Daten nicht sichergestellt worden, hätte man das System wohl gar nicht erst verabschiedet.

Man könnte diese aktuelle Liste wohl endlos weiterführen z. B. mit der geplanten elektronischen Gesundsheitskarte oder dem neuen ePass, der seit dem 01. November 2005 trotz erheblicher Zweifel an der Zuverlässigkeit der vorgesehenen Technik ausgegeben wird. Das von der Verfassung garantierte Recht der Menschen auf informationelle Selbstbestimmung wird so immer mehr in Frage gestellt. Problematisch daran ist, dass viele Bürger diese Entwicklung unterstützen, weil sie wenig Datenschutzbewusstsein haben und Daten freiwillig weitergeben. So geht der Staat unter der Maßgabe der Straftatenbekämpfung zunehmend dazu über, von der Gefahrenabwehr zur Gefahrenvorsorge überzugehen und dem „gläsernen Menschen“ ständig einen Schritt näher zu kommen.

7.6 Fazit

Politische eProzesse finden in Deutschland zunehmend Verbreitung, doch muss dabei sichergestellt werden, dass die genutzten Daten ausschließlich der Zweckbindung dienen und deren Sicherheit gewahrt bleibt. Bei eProzessen ist Datenschutz leider oft noch zweitrangig und die Funktionalität steht im Vordergrund, es gibt allerdings schon einige vielversprechende Projekte, die von Anfang an auf datenschutzrechtliche Aspekte aufgebaut wurden und gute Chancen haben, sich weiter zu etablieren.

Die Politik schafft in aktuellen Debatten im Auftrag der Terrorbekämpfung einen Weg zum „gläsernen Menschen“, dieser Aspekt sollte von den Bürgern verstärkt wahr genommen und hinterfragt werden, bevor das Recht auf informelle Selbstbestimmung, dass im Grundgesetz verankert ist, völlig vom Staat ausgehebelt wurde.

Literaturverzeichnis

[Biz] BIZER, JOHANN: *DUD: eGovernment - Chance für den Datenschutz*. http://www.datenschutzzentrum.de/e-government/dud-200507.htm.

[Buna] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Bundesamt für Sicherheit in der Informationstechnik - Elektronische Signatur*. http://www.bsi.bund.de/esig/index.htm.

[Bunb] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Bündnis für elektronische Signaturen*. http://www.signaturbuendnis.de.

[Heia] HEISE: *Heise News: Mautdaten sind Fahndungsdaten*. http://www.heise.de/newsticker/meldung/68904.

[Heib] HEISE: *Heise News: Sicherheitsprobleme bei elektronischer Steuererklärung Elster*. http://www.heise.de/security/news/meldung/54408.

[Heic] HEISE: *Vorratsspeicherung von Verbindungsdaten in der Telekommunikation*. http://www.heise.de/ct/aktuell/meldung/66857.

[Hor] HORNECKER, EVA: *Behördenverkehr in Bremen ab jetzt mit Chipkarte - Bericht über eine Podiumsdiskussion*. http://fiff.informatik.uni-bremen.de/archiv/fiffhbaktion14a.html.

[LDA] LDA: *Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen*.

http://www.lda.brandenburg.de/sixcms/detail.php?id=87111\&template=allgemein_lda.

[Mar] MARTIN SCHALLBRUCH: *Das Signaturbündnis - Ende der Signaturdiskussion*. http://www.politik-digital.de/egovernment/esignatur/sig1.shtml.

[o.Va] O.V.: *eGovernment: Bremen Online Services*. http://www.bos-bremen.de.

[o.Vb] O.V.: *ELSTER Homepage*. https://www.elster.de/.

[o.Vc] O.V.: *ELSTEROnline Portal*. https://www.elster.de/eportal/.

[o.Vd] O.V.: *Sicherheitsleitfaden für Anwender von ELSTER*. https://www.elster.de/pro_sicher.php.

[Rum] RUMMEL AG: *Aktuelles: Achtung, ELSTER!* http://www.rummel-ag.de/winmacs/elster.htm.

[UKK] ULLMANN, MARKUS, FRANK KOOB und HARALD KELTER: *DuD: Lösungsansätze für die Realisierung von Online-Wahlen*. http://mitglied.lycos.de/mac_o_mania/extdoc/OnlinewahlenDUD.pdf.

[W.I] W.I.E.N.: *Forschungsprojekt W.I.E.N. - Wählen in elektronischen Netzwerken*. http://www.forschungsprojekt-wien.de.

[Wil] WILM, PETER: *Elektronische Wahlen - Eine Informationsbroschüre für den Wahlbürger*. http://www.elektronische-wahlen.de/staatlich/elektronische-wahlen.pdf.

Autoren

Edzard Weber
Ansätze für eine elektronische und selbstorganisierende Gesetzesfolgenabschätzung
weber@ePartizipation.de

Katja Neumann, Katja Witt
Balanced E-Government - Bürgernähe vs. Verwaltungsmodernisierung
Katja.Neumann@Informatik.Uni-Oldenburg.de
Katja.Witt@Informatik.Uni-Oldenburg.de

Winfried Klinker
Die Bürgerrechte im Internet - Bedrohungen und Schutzmöglichkeiten
Winfried.Klinker@informatik.uni-oldenburg.de

Anke Lederer, Hauke Tschirner
Elektronische Demokratische Parteien - am Beispiel der VVVD
Anke.Lederer@Informatik.Uni-Oldenburg.de
Hauke.Tschirner@Informatik.Uni-Oldenburg.de

Sönke Brummerloh, Mareike Wagner
Elektronische Wahlen im internationalen Vergleich
Soenke.Brummerloh@Informatik.Uni-Oldenburg.de
Mareike.Wagner@Informatik.Uni-Oldenburg.de

Dirk Räder
Möglichkeiten der politischen Beteiligung im Internet
Dirk.Raeder@mail.Uni-Oldenburg.de

Wolfgang Deeken
Datenschutz und Anonymität bei politischen eProzessen
Wolfgang.Deeken@fortytwo.Uni-Oldenburg.de

Zusammenfassung

Der vorliegende Seminarband entstand im Rahmen des Seminars „eDemokratie - Informatikanwendungen in der Politik“ im Wintersemester 2005/2006 an der Carl von Ossietzky Universität Oldenburg. Schwerpunkt der Lehrveranstaltung war eine inhaltliche Auseinandersetzung mit den Themengebieten *Elektronische Gesetzesfolgenabschätzung, Balanced E-Government, Bürgerrechte im Internet, Elektronische Demokratische Parteien, Elektronische Wahlen, Politische Beteiligung im Internet, Datenschutz und Anonymität*.

Es stand hierbei insbesondere die technische Realisierbarkeit internetbasierter Informatikanwendungen in einzelnen Politikfeldern im Vordergrund, wobei auch untersucht werden sollte, inwieweit die an politischen Prozessen beteiligten Akteure einen Zugang zu den unterschiedlichen Systemen erhalten können und welche Sicherheitsaspekte zu berücksichtigen sind. Die hier zusammengeführten Einzelbeiträge geben einen interessanten Einblick in die Thematik und sollen unter der URL `http://www.informatik-politik.de` zu weiteren Diskussionen anregen. Ich lade Sie daher herzlich ein, mein Vorhaben mit einem aktiven Beitrag (Vortragsfolien, Referat, URL, ...) zu unterstützen.

Abstract

These proceedings originate from the seminar: „eDemocracy - Applications of Computer Science in Politics“ which took place during winter semester 2005/2006 at the Carl-von-Ossietzky University of Oldenburg. Focus of the seminar were discussions on topics like *Balanced E-Government, Citizen Rights in the World Wide Web, Political Participation on the Internet* and others.

The chosen articles are meant to provide an insight into the topic and can be used as a starting point to discuss the adressed issues on `http://www.informatik-politik.de` as well. You are cordially invited to support my project with an active contribution (article, presentation foils, paper, URL etc.).