UNIVERSITÄTSLEHRGANG

FÜR INFORMATIONSRECHT UND RECHTSINFORMATION

AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

eVoting

Juristische und technische Anforderungen an elektronische Partizipationsmöglichkeiten

MASTERTHESIS

zur Erlangung des akademischenGrades

Master of Advanced Studies (MAS)

für Informationsrecht und Rechtsinformation

Begutachter: Ao Univ. Prof. Dr. Gerhard Strejcek

Mag. Agnes Berlakovich

im September 2001

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	anderer Ansicht
aaO	Zum angegeben Ort
AB	Ausschussbericht
Abg.	Abgeordnete, -er
ABGB	Allgemeines Bürgerliches Gesetzbuch
Abs	Absatz
Anm	Anmerkung
Art	Artikel
Bd	Band, Bände
BG	Bundesgesetz
BGBl	Bundesgesetzblatt
BlgNR	Beilagen zu den Stenographischen Protokollen des Nationalrates (Nummer, Gesetzgebungsperiode, Seite)
BM	Bundesminister(ium)
BmBWK	Bundesministerium für Bildung, Wissenschaft und Kultur
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichtes (Band, Seite)
B- VG	Bundes- Verfassungsgesetz, BgBl 1930/1 idF BgBl I 1999/194
BVG	Bundesverfassungsgesetz
BWG	Bundeswahlgesetz vom 7. Mai 1956, dBGBl I, S. 383
BWO	Bundeswahlordnung vom 28. August 1985, dBGBl I, S. 1769
bzw	beziehungsweise

d	deutsche, -er, -es
dBGBl	(deutsches) Bundesgesetzblatt
ders	derselbe
e	electronic
E	Entscheidung
eAdministration	electronic Administration
eAssistance	electronic Assistance
eBusiness	electronic Business
eDemocracy	electronic Democracy
eGovernance	electronic Governance
eGovernment	electronic Government
eMail	electronic Mail
erg	ergänze
et al	at alii (und andere)
etc	etcetera
EU	Europäische Union
eVoting	electronic Voting
f	Und der (die) folgende
ff	Und die folgenden
FN	Fußnote(n)
GG	Grundgesetz über die Bunderepublik Deutschland vom 23. Mai 1949 (dBGBl I, S. 1)
GP	Gesetzgebungsperiode
Hrsg	Herausgeber
HSG	Hochschülerschaftsgesetz

html	hypertext transfer markup language
http	hypertext transfer protocol
HWO	Hochschülerschaftswahlordnung
i.A-	im Allgemeinen
ICANN	Internet Corporation for Assigned Names and Numbers
idF	in der Fassung
IT	Informationstechnologie
IVm	In Verbindung mit
iVoting	Internet- Voting
JBl	Juristische Blätter
JBöffR	Jahrbuch des öffentlichen Rechtes
JRP	Journal für Rechtspolitik
leg cit	legis citatae (der zitierten Vorschrift)
L-VG	Landes- Verfassungsgesetz
lit	litera
LT	Landtag
mE	meines Erachtens
MRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 1958 I 1998/30
NJW	Neue juristische Wochenzeitschrift
nöSTWO	niederösterreichische Wahlordnung für Statutarstädte, LGBl 0360-2
NR	Nationalrat
NRWO	Nationalratswahlordnung, BGBl 1992/471 idF BGBl I 1998/161
NZZ	Neue Zürcher Zeitung

ÖLP	Österreichisches Jahrbuch für Politik
ÖJZ	Österreichische Juristenzeitung
OS	operating system (Betriebssystem)
ÖH	Österreichische Hochschülerschaft
Präs	Präsident
PVG	Bundes- Personalvertretungsgesetz, BGBl 1967/133 idF BGBl I 1998/123
Rdnr	Randnummer
RL	Richtlinie
RV	Regierungsvorlage
Rz	Randziffer
SigG	Signaturgesetz
SigRL	Signaturrichtlinie
SigV	Signaturverordnung
sog	sogenannte, -r, -s
sten Prot d NR	Stenographische Protokolle des Nationalrats
StGB	Strafgesetzbuch, BGBl 1974/60 idF BGBl I 1998/153
StV	Staatsvertrag
StVW	Staatsvertrag von Wien, BGBl 1955/152
TCP/IP	Transfer Control Protocol/ Internet Protocol
URL	Uniform Resource Locator
VAbstG	Volksabstimmungsgesetz, BGBl 1973/79 (wv)idF BGBl 1993/339
VBefrG	Volksbefragungsgesetz, BGBl 1989/356 idF BGBl 1994/162
VBegG	Volksbegehrengesetz, BGBl 1973/344 (wv) idF BGBl I 1998/162

VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
vgl	vergleiche
VwGH	Verwaltungsgerichtshof
WEvG	Wählerevidenzgesetz, BGBl 1973/601 (wv) idF BGBl 1996/117
WRÄG	Wahlrechtsänderungsgesetz 1990, BGBl 1990/148
wv	wiederverlautbart
WWW	World Wide Web
Z	Ziffer
z	zu, -m, -r
zB	zum Beispiel
ZfV	Zeitschrift für Verwaltung
ZPMRK	Zusatzprotokoll zur MRK
ZRP	Zeitschrift für Rechtspolitik

Einleitung

Das Internet hat sich zu einem unverzichtbaren Bestandteil der privaten und auch geschäftlichen Kommunikation entwickelt. Die Frage, ob dieses Medium auch für demokratische Partizipation genutzt werden sollte, wird nicht erst seit dem Wahldilemma in den USA – und dies äußerst kontroversiell- diskutiert.

Die Befürworter sehen in der Nutzung neuer Medien, insbesondere des Internet, ein Mittel zur Wiederbelebung und Erneuerung von Demokratie, oder gehen sogar davon aus, dass die neuen Medien von der „Zuschauer- zur Beteiligungsdemokratie“ führen werden[1]. Die Gegner kritisieren den Einsatz dieser Medien als „Junk- Demokratie“[2] und unnötige Maßnahme. Kritiker halten den Bestrebungen auch entgegen, dass es sich lediglich um „hypes“ aus dem eElfenbeinturm handelt, vorangetrieben von Unternehmen, die daran verdienen können und genutzt von Politikerinnen und Politikern, die sich als Modernisierer empfehlen möchten.[3]

Die Diskurs von der politischen bzw. politikwissenschaftlichen Seite auf die juristische Ebene hebend, geht es primär um die Frage, ob durch den Einsatz Neuer Medien bei Wahlen die Einhaltung der verfassungsmäßig gebotenen Wahlgrundsätze gegeben ist.
Diese Frage stellt sich in Österreich vor allem bei Wahlen zu den allgemeinen Vertretungskörpern, wo Gesetzeslage und Rechtsprechung des VfGH eine eindeutige Linie vorgeben.[4]
Differenzierter ist, von der juristischen Seite betrachtet, die Frage bei anderen Wahlen, wie z.B. bei solchen zu Berufsvertretungen, wo der VfGH keine so strenge Einhaltung der Wahlgrundsätze fordert.
Diese Linie des VfGH bei den Wahlen zu Berufsvertretungen hat auch die Hoffnung des Gesetzgebers geweckt, dass die Regelungen des Hochschülerschaftsgesetzes

[1] Leggewie: Netizens oder: der gut informierte Bürger heute. Ein neuer Strukturwandel der Öffentlichkeit? Chancen demokratischer Beteiligung im Internet - anhand US-amerikanischer und kanadischer Erfahrungen, Bonn 1996,
[2] siehe: Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen in Multimedia & Recht, abrufbar unter http://www.i-vote.de/projekt/index.html, abgerufen am 30. 8. 2001
[3] Möller, „e-Politik“ - Was bringt das Netz der Demokratie?, http://orae.fes.de:8081/fes/docs/WEST_UND_SUEDEUROPA/E-POLITIK2%20MOELLER.HTM, abgerufen am 10. 8. 2001
[4] Siehe Kapitel 5

(HSG), die die erste gesetzlich vorgesehene Möglichkeit einer Online- Wahl in Österreich vorsehen der Prüfung des Höchstgerichtes standhalten.

Die Frage, die sich zusätzlich, oder besser gesagt vorrangig stellt, ist die, ob die technische Entwicklung schon so weit fortgeschritten ist, dass man Wahlen via Internet durchführen kann.
Durch den Einsatz von Kryptographie und digitalen Signaturen[5] können zwar die notwendigen Voraussetzungen der Vertraulichkeit, Integrität, Authentifikation und Verbindlichkeit und durch blinde Signaturen auch die Wahrung des Wahlgeheimnisses erreicht werden.

Ob aber das Internet als junges Medium so weit entwickelt und so sicher ist, dass es für demokratische Partizipation genutzt werden kann, ist jedoch einen andere Frage und wie die regelmäßigen Berichte über erfolgreiche Hackingversuche zeigen, wohl (noch?) zweifelhaft.

Die vorliegende Arbeit stellt einen Versuch dar, die (verfassungs-) rechtlichen und technischen Fragestellungen des Wählens über Internet aufzuzeigen und mögliche Strategien für Österreich darzustellen[6]. Aufgrund der Vergleichbarkeit der Rechtslage werden Anleihen insbesondere an der Diskussion in Deutschland und dem dort entwickelten Modell genommen.

[5] Siehe Kapitel 4.2

[6] Abgesehen von den oben genannten Bereichen Recht und Technik darf jedoch die sozio- kulturelle Komponente nicht vergessen werden. Die Nutzung des Internet hat längst noch nicht alle Bevölkerungsgruppen durchdrungen und das Vertrauen in die Sicherheit der Neuen Technologien ist auch bei jenen, die es regelmäßig nutzen, nicht besonders hoch. Dieser Problembereich wird jedoch nur erwähnt, da eine weitergehende Auseinandersetzung mit diesem Bereich den Rahmen dieser Arbeit sprengen würde.

Entwicklung

Während die Diskussionen zu diesem Thema in Österreich erst am Beginn stehen[7], gibt es in anderen Ländern, insbesondere in den USA, schon seit einigen Jahren Initiativen zur Entwicklung von Konzepten von elektronischer Demokratie und zur Realisierung von E-Voting- Projekten[8].

Die erste öffentliche Diskussion zum Thema der Durchführung von Wahlen über offene Netze ist die New Yorker »Crypto« Konferenz[9] von 1982, auf der u.a. David Chaum[10] erstmals sein Konzept der blinden Signaturen vorgestellt hat .

Da zu diesem Zeitpunkt die Verbreitung von Computernetzwerken sehr gering war blieben die Überlegungen praktisch folgenlos, bis zu Beginn der 90- er- Jahre, als der Internet- Boom einsetzte.

Fujioka, Okamoto und Oha entwickelten 1992, auf Grundlage der Konzepte von Chaum, ein erstes Protokoll für ein »practical secret voting scheme for large scale elections«[11]. In den folgenden Jahren hat es einige weitere Vorschläge gegeben, aber erste praktische Umsetzungen gab es erst Ende des vergangenen Jahrhunderts.

So hatten bei den Vorwahlen der demokratischen Partei in Arizona Wahlberechtigte die Möglichkeit, zwischen dem 7. und 10. März 2000 von einem beliebigen Rechner aus zu wählen. Am 11. März 2000, dem eigentlichen Wahltermin, standen in den 124 Wahlbüros des Bundesstaates neben den herkömmlichen Urnen auch Wahlrechner zur Verfügung.
Unter der Administration von Bill Clinton wurde auch eine Forschungsgruppe eingesetzt, die die Möglichkeiten und Risken des Internet- voting erkunden soll.[12]

---

[7] Siehe Interuniversitäres Institut für interdisziplinäre Forschung und Fortbildung (IFF), Abteilung Politische Bildung, http://polbil.uibk.ac.at/pat/iud/wos
[8] zB das Center for Democracy and Technology in Washington, Politik Digital und die Initiative D 21 in Deutschland, Initiative von Abgeordneten in Deutschland (www.eifonline.org/index.htm)
[9] siehe: David Chaum, Ronald L. Rivest, Alan T. Sherman (Eds.): Advances in Cryptology: Proceedings of CRYPTO '82. Plemum, New York, 1983 abrufbar unter: http://dblp.uni-trier.de/db/conf/crypto/
[10] siehe: http://www.chaum.com/
[11] in: Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology -- AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244-251, Gold Coast, Queensland, Australia, 13-16 December 1992. Springer-Verlag., <http://theory.lcs.mit.edu/~dmjones/hbp/auscrypt/auscrypt92.html>
[12] siehe: http://www.internetpolicy.org/>

Ehrgeizige Bestrebungen gibt es vor allem in Deutschland und der Schweiz.
Die vom deutschen Bundestag eingesetzte Forschungsgruppe Internetwahlen[13] hat sich als Ziel die Durchführung von Wahlen via Internet im Jahre 2010 als Alternative zu den herkömmlichen Wahlen gesetzt.
Bis zum Jahr 2006 sollen digitale und vernetzte Wahlurnen zum Einsatz kommen und bis 2010 könne man sich, so hat der deutsche Innenminister verkündet, eine Online-Bundestagswahl vom heimischen Computer aus vorstellen.[14]
Am 2. 2. 2000 fand im Rahmen dieses Projektes auch die erste über das Internet durchgeführten rechtsverbindliche Wahl statt. Und zwar bestand die Möglichkeit, das Studentenparlament an der Universität Osnabrück parallel zur Wahl in der Wahlzelle auch per Internet zu wählen[15]. Rund zehn Prozent der Wahlberechtigten haben diese Möglichkeit genutzt.
Am 12. Juli 2001 fand eine weitere (Test-)Wahl im Rahmen des Projektes Internetwahlen statt. In Esslingen am Neckar konnten die Jugendgemeinderäte neben der Präsenzwahl auch über das Internet gewählt werden[16].

In der Schweiz gibt es zwei Projekte des Bundesrates zusammen mit Kantonen und Gemeinden: „virtueller Amtsschalter“ oder „Guichet virtuel“ und eVoting. Insgesamt sieht der Bund gemäß NZZ für den Bereich eGovernment bis 2004 Aufwendungen von insgesamt Sfr. 52,7 Mio vor[17].

[13]< http://www.i-vote.de/projekt/index.html>Die Forschungsgruppe Internetwahlen ist eine interdisziplinäre Forschungseinrichtung an der UNiversität Osnabrück unter der Leitung von Prof. Otten. Sie besteht seit Oktober 1998 und wird aus Mitteln des Bundesministeriums für Wirtschaft und Technologie gefördert. Ihre Zielsetzung besteht in der Klärung der technischen, juristischen und politischen Voraussetzungen für die Durchführung von rechtskräftigen Wahlen im Internet sowie in der praktischen Umsetzung dieser Forschungsergebnisse in verschiedenen Projekten. Die Zielsetzung des Projektes *„Wahlen im Internet“* besteht in der Entwicklung eines anwendungsreifen Verfahrens zur Durchführung von Wahlen im Internet als Alternative zur herkömmlichen Brief- und Urnenwahl
[14] Seidler, Schilys Visionen: Deutschlands Weg zur Online- Wahl, in: Spiegel Online, 3. Mai 2001 <http://www.spiegel.de/politik/deutschland/0,1518,131673,00.htm>
[15] Kosten des Projektes in der Höhe von 1,3 Mio. D-Mark wurden vom Bundesministerium für Wirtschaft und privaten Sponsoren getragen
[16] Auswertungs- und Erfahrungsberichte zu diesen Wahlen sind unter <http://www.jgrwahl.esslingen.de/dokumentation.html>veröffentlicht (abgerufenam 31.8.2001)
[17] Erste Fanfarenstöße für den virtuellen Staat, E-Government verändert Verwaltung und Demokratiein in Neue Zürcher Zeitung (NZZ) vom 7. 9. 2000, abrufbar unter: <http://www.nzz.ch/sonderbeilagen/orbit00/orbit__fel.html> (abgerufen am 15. 7. 2001)

Im Oktober 2000 wurde die Wahl des Direktoriums der ICANN[18] anhand Internet durchgeführt. An der Wahl nahmen mehr als 76.000 registrierte User aus der ganzen Welt teil.

Inzwischen hat sich ein Wettbewerb zwischen einzelnen Staaten, insbesondere zwischen Deutschland und den USA, zur Entwicklung eines tauglichen Wahlsystems entwickelt.
So plädiert Jörg Tauss, Mitglied des deutschen Bundestages, dafür, die Entwicklung der Technik nicht den Amerikanern zu überlassen, die mittlerweile auch Wahl-Soft- und Hardware entwickeln. „So hätten die Anstrengungen für sichere Online-Wahlen auch einen segensreichen Effekt für Deutschlands angeschlagenen Ruf als High-Tech-Schmiede und den hiesigen E-commerce." [19]

[18] ICANN (=Internet Corporation for Assigned Names and Numbers), <http://www.icann.org/>
[19] <http://www.elektronische-demokratie.de/> (abgerufen am 5.8.2001)

1. Einordnung

1.1 Definition

Das *Internet Policy Institute*[20] in den USA unterscheidet zwischen Poll site voting, Kiosk voting und Remote Internet voting als Kategorien des elektronsichen Wählens.

Bei **Poll site voting**[21] erfolgt die Wahl (persönlich) elektronisch in der Wahlzelle. Das Wählerverzeichnis ist „zentral" erfasst, der Wähler kann in jeder beliebigen Wahlzelle seine Stimme geben; das Ausstellen von Wahlkarten würde somit entfallen. Dieses System stellt trotz Einsatzes von neuen Technologien noch immer eine Wahl unter der Kontrolle der Wahlkommission dar. Die Identifikation und Authentifikation der Wähler findet noch immer durch die Mitglieder der Wahlkommission statt.

Technisch gesehen sind hier die Sicherheitsrisken minimal, da die einzelnen „Wahlcomputer" via Intranet[22] mit dem Zentralrechner der Wahlbehörde verbunden sind.

Kiosk voting bedeutet, dass die Wahlmaschinen nicht mehr in Wahllokalen stehen, sondern an allgemeinen Plätzen wie Einkaufszentren, Schulen oder Bibliotheken.

Die Wahlgeräte stehen unter der Kontrolle der Wahlkommission und die technische Ausgestaltung des IT- Systems die Einhaltung von Sicherheits- und Datenschutzsstandards ermöglichen.

Bei **Remote Internet Voting** ist die Abgabe der Stimme von jedem Rechner, der Internetzugang hat, möglich. Da keine Kontrolle über die „Wahlmaschinen" vor Ort möglich ist, ist eine zentrale Steuerung von Sicherheitsrisken nur schwer möglich.

[20] Internet Policy Institute, Report of the National Workshop on Internet Voting: Issues and Research Agenda, März 2001
[21] Internet Policy Institute, Report of the National Workshop on Internet Voting, S. 1

Für die vorliegenden Arbeit wurde folgende Unterscheidung vorgenommen[23]:

eVoting ist als Überbegriff für alle Wahlverfahren anzusehen, bei dem Registrierung der Wähler, Abgabe der Stimme oder Auswertung der abgegebenen Stimmen mittels elektronischer Unterstützung durchgeführt wird.[24]

Online- Voting: darunter ist ein System zu verstehen, bei dem die Abgabe und die Auszählung der Stimmen elektronisch erfolgt.[25]

Internet- Voting (iVoting): die Stimmabgabe findet mittels eines Computers über Internet, also über ein offenes Netzwerk statt.

1.2 eVoting[26] als Teil des eGovernment[27]

Unter eGovernment wird eine neue Phase des Einsatzes von Informations- und Kommunikationstechnologien im Bereich Regierung und öffentliche Verwaltung verstanden.

1.2.1 Elemente des eGovernment

Es ist zwischen der inneren und der externen Perspektive des E- Government zu unterscheiden. [28]

---

[22] Intranet ist in der Regel eine privates Netzwerk eines Unternehmens. In den meisten Fällen existiert eine Verbindung zum Internet über eine Gateway. Verwendet werden Internet- Standards. Zweck ist üblicherweise, die unternehmensinterne Informationsstruktur zu verbessern.
[23] Wobei der Schwerpunkt der Arbeit im Bereich des iVoting liegt
[24] vgl. Menzel, Evoting an österreichischen Hochschulen, in Schweighofer, Menzel, Kreuzbauer (Hg.) Auf dem Weg zur ePerson , Schriftenreihe Rechtsinformatik Bd. 3, S.283
[25] Menzel, Evoting an österreichischen Hochschulen, S. 283
[26] aA: Kubicek/Wind differenzieren zwischen E-Business, E- Government und E- Democracy und sehen E-Voting als Element von E- Democracy: siehe: Wie modernisiere ich Wahlen? Der lange Weg vom Pilotprojekt zum Online- Voting bei einer Bundestagswahl, siehe in: <http://polbil.uibk.ac.at/pat/iud/wos/0003.htm>
[27] Informationen zu eGovernment in Österreich sind unter <http://www.bmols.gv.at/frameitkoo.html>abrufbar.
[28]Aichholzer, Schmutzer, E- Government, Elektronische Informationsdienste auf Bundesebene in Österreich, Endbericht, Studie im Auftrag des Bundeskanzleramtes , Juli 1999, Wien, Institut für Technikfolgen-Abschätzung der österreichischen Akademie der Wissenschaften

Die interne Perspektive umfasst Datenbanken, Workflow- Systeme etc. und dient dem Ziel der Verbesserung des Informationsmanagements und verwaltungsinterner Prozessabläufe.
Als Ziel dieser Systeme ist die Veränderung organisatorischer Beziehungen sowohl auf horizontaler Ebene (zwischen Dienststellen, Abteilungen, Ministerien etc.) als auch auf vertikaler Ebene (zwischen Einrichtungen der Bundes- Landes- und Kommunalverwaltung) anzusehen.

Die externe Einsatz von IT umfasst die elektronische Bereitstellung von Informationen und Dienstleistungen sowie Kommunikationsmöglichkeiten wobei das Hauptaugenmerk auf der Verbesserung der Beziehung zwischen Staat und Bürgern liegt.

Bestimmte Anwendungen des eGovernment werden oft auch als Teilbereich des eCommerce[29] verstanden. Für die Unterscheidung ist auf diejenige zwischen Hoheits- und Privatwirtschaftsverwaltung zu verweisen[30].
Für die Zuordnung eines bestimmten Aktes als eGovernment oder als eCommerce ist auch hier die Form des staatlichen Handelns entscheidend[31].

Ziele der externen Perspektive sind zumeist ein verbesserter Zugang zu Information, erhöhte Transparenz der Öffentlichen Verwaltung, Vereinfachung der Behördenkontakte und der Verwaltungsverfahren, Unterstützung der demokratischen Rechte und der politischen Partizipation, sowie Kosteneinsparungen.

Der Einsatz von IT an der Schnittstelle zwischen öffentlicher Verwaltung und Bürgern bzw. Unternehmen ist in die Informationsinfrastruktur heutiger Gesellschaften eingebunden, welche aus drei – aufeinander aufbauenden Ebenen besteht:

---

[29] Aichholzer, Schmutzer nennen hier v.A. Anwendungen in Zusammenhang mit Amtwegen

[30] *„Von **Hoheitsverwaltung** spricht man, wenn der Staat in der Verwaltung als Träger der ihm eigentümlichen „Gewalt", also mit „Imperium", auftritt.*
*In der **Privatwirtschaftsverwaltung** dagegen tritt der Staat nicht als Träger seiner hoheitlichen Befugnisse auf, sondern bedient sich für sein Handeln der Rechtsformen zur Verfügung stehen. Dabei handelt es sich einerseits um Rechtsgeschäfte des Zivilrechts, insbesondere um das Instrument des Vertrages, andererseits aber auch um Akte auf dem Gebiet des öffentlichen Rechts (insbesondere des Verwaltungsrechts), die auch von von den Rechtsunterworfenen gesetzt werden können.*" (Antoniolli-Koja, Allgemeines Verwaltungsrecht, 3, 1997, 23)

- **Telekommunikationsnetzwerk** (Übergangskanäle, Endgeräte),

- **Elektronische Dienste** (Internet, Pay- TV, value-added services, etc.,)

- **Anwendungen** (Tele- Lernen, Tele- Administration, Informationsangebote in verschiedenen Bereichen etc.

Auf der Ebene der **elektronischen Dienste** unterscheiden *Aichholzer* und *Schmutzer* drei Typen (Information, Kommunikation, Transaktion), welche jeweils in drei verschiedenen **Anwendungsbereiche**n (Alltag, Behördenkontakte, politische Partizipation) zum Einsatz kommen.

Information ist der Abruf von verschiedenen aufbereiteten Daten (z. B. Dokumente Datenbanken).
Die Informationen werden von dem Benutzer individuell ausgewählt. Eingaben dienen nur dazu, Inhalte auszuwählen. Beispiel sind die elektronischen Informationsdienste des Parlaments[32].

Kommunikation ist der Austausch von Nachrichten zwischen einzelnen Personen oder in Gruppen mit einem gemeinsamen Interesse[33].

Transaktion ist die Auslösung von Prozessen der Güterbewegung oder der Erbringung von Dienstleistungen[34].

Unter der Perspektive **verschiedener Interaktionsmuster** kann folgende Unterscheidung elektronischer Dienste getroffen werden:

One-to-one: direkte Kommunikation zwischen Bürgern und Beamten oder Politikern (zunehmend).

[32] <http://www.parlinkom.gv.at>
[33] z.B. E-mail, Diskussionsforen
[34] z.B. elektronische Formulare

One-to-many: eine Verwaltungseinrichtung oder ein Politiker macht eine Aussendung an mehrere Bürger (eher sehr selten).

Many-to-one: einzelne Bürger greifen auf Informationsangebote von Einrichtungen des politischen Systems zu (häufig) oder einzelne Bürger übermitteln Daten an Einrichtungen des politischen Systems, z.B. Behördenformulare oder Stimmabgabe (noch selten).

Many-to-many: einzelne Bürger und möglicherweise auch Politiker kommunizieren auf einer Diskussionsplattform (zunehmend).

Auf der **Anwendungsebene** unterscheiden *Aichholzer* und *Schmutzer* bei den elektronischen Diensten im Bereich Regierung und Verwaltung folgende drei Bereiche:

Alltag: elektronische Unterstützung der alltäglichen Lebensgestaltung

Behördenkontakte: elektronische Unterstützung der Abwicklung von Verwaltungsangelegenheiten

Politische Partizipation: elektronische Unterstützung politischer Prozesse der Meinungsbildung und Entscheidungsfindung

Tabelle 1: Anwendungsbereiche und Typen von elektronischen Diensten im eGovernment[35]

	Informations-dienste	**Kommunikations-dienste**	**Transaktions-dienste**
Alltag	Informationen zur Lebensgestaltung (Arbeit, Wohnen, Bildung, Gesundheit, Freizeit, etc.)	- Diskussionsforen zu Alltagsfragen - Job- oder Wohnungsbörse	z.B. Kartenreservierung/-bestellung, Kursanmeldung
Behördenkontakte	- Behördenwegweiser - Öffentliche Register - Ausschreibungen	E-Mail Kommunikation mit Beamten	Einreichung von Anträgen oder Formularen
Politische Partizipation	- Gesetze, Parlamentstexte, Konsultationsdokumente - Hintergrund-informationen bei Entscheidungsprozessen	- Diskussionsforen zu politischen Themen - E-Mail kommunikation mit Politikern - Workspace bei Planungs- und Entscheidungsprozessen	- Abstimmungen oder Wahlen - Umfragen - Petitionen

1.3 conclusio

eVoting ist ein Teilbereich einer Gesamtentwicklung, die unter den Oberbegriff eGovernment subsumiert werden kann[36].

[35] Aichholzer/Schmutzer, eGovernment, S. 15

[36] Aus der Sicht der Wähler betrachtet, kann eVoting aber auch als Teil von eDemocracy gesehen werden.

2. Technik: Grundlagen des Internet

2.1 Intranet und Internet

Um einen Überblick für mögliche Problembereiche, die die Durchführung von Wahlen über das Internet mit sich bringen kann, ist vorerst ein Überblick über die Funktionsweise des Internet und seiner Dienste notwendig.

Als Internet wird die Menge aller Rechner (= hosts) bezeichnet, die über geeignete Verbindungseinrichtungen unter Nutzung des TCP/IP- Protokolls[37] miteinander kommunizieren.
Es stellt ein offenes Netzwerk bzw. eigentlich einen Zusammenschluss mehrerer Netzwerke dar, die eine einheitliche Struktur bilden. Aus dieser Vielzahl von Netzen entsteht aus Sicht des Anwenders ein homogenes und transparentes Gebilde, dessen heterogener Charakter den Benutzern verborgen bleibt. Den Netzen und Rechnern sind Namen gemäß dem Domain Name System (DNS) zugeordnet.

Um den Datenaustausch aller mit dem Internet verbundenen Rechner zu ermöglichen, wurde das TCP/IP[38]- Protokoll entwickelt. Diese beiden Protokolle beschreiben auf mehrere Ebenen verteilt[39] eine Reihe von Diensten und ermöglichen eine Reihe von Anwendungen, wie WWW und eMail[40].

Während das Internet eine völlig uneingeschränkte Kommunikation erlaubt, ist das Intranet ein vom öffentlichen Bereich durch Firewalls abgeschirmtes System.

---

[37] Im Allgemeinen werden unter einem Protokoll Regeln verstanden, die über den Ablauf und die Form von Interaktionen bestimmen. Um ein beliebiges Protokoll durchzuführen, werden mindestens zwei Beteiligte benötigt (Personen, Personengruppe, Computer bzw. deren Benutzer). Außerdem muss zwischen den Beteiligten ein Kommunikationskanal offen sein, über den Informationen ausgetauscht werden (Stimme, Datenverbindung,...)

[38] TCP/IP: Transfer control protocol/Internet protocol

[39] TCP/IP- Modell besteht aus vier Schichten; das ISO/OSI- Modell unterscheidet sieben verschiedene Schichten. Näheres dazu zB unter <http://atpforest.tuwien.ac.at/opt/kde/share/doc/HTML/en/knetdump/index-4.html> (abgerufen am 30.8.2001)

[40] Andere Anwendungen: news, File Transfer (ftp), Remote- Login (telnet), Synchrone Kommunikation (Chatting, ICQ, Shared Wokspace, Netmeeting), Edutainment (Education and Entertainment), Interactive Video.

2.1.1World Wide Web- WWW

Das WWW ist ein mulimediales hypertextbasierendes[41] Informationssystem im Internet.

2.1.1.1 Technische Grundlagen des WWW[42]

2.1.1.1.1 TCP/IP- Transmission Control Protocol/ Internet- Protocol

Mit TCP/IP wird eine ganze Protokollfamilie bezeichnet, die den Datenaustausch in heterogenen Netzwerken ermöglicht.
Das Transmission Control Protocol (TCP), teilt die Daten auf und setzt sie wieder zusammen, IP ist für die Zustellung der Pakete von Sender an Empfänger verantwortlich. TCP/IP ist der Internet- Standard, mit Hilfe dessen die Daten paketweise versendet werden.

2.1.1.1.2 HTTP- Hypertext Transfer Protocol

ist die Grundlage des Datentransfers im World Wide Web.
HTTP dient der Kommunikation zwischen Web- Server und Web- Client[43] und ist die Grundlage des World Wide Web auf Anwendungsebene. HTTP ist im Prinzip ein einfaches Protokoll: der Server wartet auf Anfrage des Clients, z.B. des Web-Browsers[44], nach Dokumenten, die via URL[45] adressiert ist. Ist das Dokument an der betreffenden Adresse vorhanden, wird es vom Server geliefert.

2.1.2 eMail

[41] „Das Prinzip des Hypertext (...): Innerhalb eines Textes (oder allgemeiner: eines Dokuments) bestehen Verweise auf einen anderen oder mehrere andere Texte, die Links. (...) In einem Multimedia- Dokument fungieren auch Bilder als Links. (...) Die so erzeugte Vernetzung schafft eine globale Informationsstruktur, in der theoretisch jedes Dokument mit jedem via Hyperlink verbunden werden kann.“ (Jünger/Oswald/Richter, WWW-Technik und Webdesign, S. 9)
[42] Jünger/Oswald/Richter, WWW-Technik und Webdesign, S. 22
[43] siehe Tabelle Seite 20
[44] Browser ist ein Anwenderprogramm (client), das (hauptsächlich) HTML- definierte Seiten von einem Server mittels einem speziellen Protokoll (http) anfordert und beim user anzeigt
[45] URL= Uniform Resource Locator, wird im Netz verwendet, um Informationen vollständig zu bezeichnen.

Der elektronische Briefverkehr wird im Internet über das Simple Mail Transfer Protocol (SMTP) abgewickelt.[46] SMTP ist jedoch schon ein recht altes Protokoll, das den modernen, multimedialen Anforderungen des Internets nicht mehr ganz gerecht wird. Daher werden zum inhaltlichen Gestalten von Nachrichten weitere Standards und Protokolle benutzt: MIME[47] ist eine multimediale Erweiterung zu SMTP und HTML[48] ist die Seitenbeschreibungssprache, die auch zum Gestalten von EMail-NAchrichten eingesetzt werden kann.
POP[49] und IMAP[50] erlauben den Empfängern das Verwalten ihrer Mailbox und das Lesen erhaltener Nachrichten.

2.1.3 Server- Client- Prinzip[51]

Anwendungen des Internet funktionieren nach dem Client-Server- Prinzip.
Ein Client (Kunde, Auftragnehmer) ist eine Komponente, die von einem Server eine bestimmte Dienstleistung anfordert (request) und auf eine Antwort wartet.
Ein Server (Diensteerbringer) ist eine Komponente, die Aufträge von Clients entgegennimmt, diese Aufträge beantwortet und eine Antwort (response) an den Client zurücksendet.

Die Initiative für die Kommunikation geht immer vom Client aus (Siehe Tabelle 1 auf der folgenden Seite).

[46] Raepple, Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2. Auflage, Heidelberg, 2001
[47] Multipurpose Internet Mail Extension- Standard
[48] Hypertext Markup Language
[49] Post Office Protocol
[50] Internet Message Access Protocol
[51] Schneider, Werner: Taschenbuch der Informatik, Fachbuchverlag Leipzig, 3. Auflage, S. 530

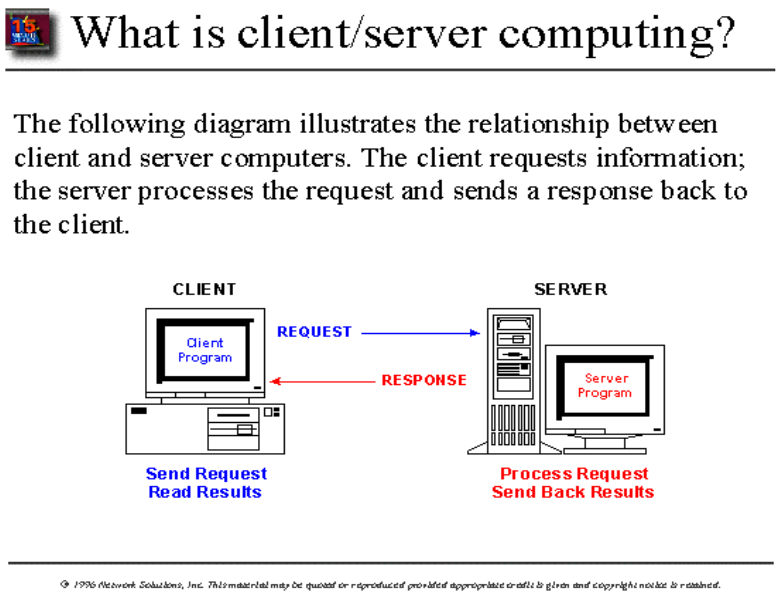

Tabelle 1: Funktionsweise des Client- Server- Prinzips[52]

2.2 Conclusio

Das Internet ist ein noch sehr junges Medium und in welche Richtung es sich entwickeln wird, ist noch völlig unklar.

Als offenes Netzwerk ist das Internet bzw. die darin verbundenen Netze und Rechner jedenfalls (Sicherheits-)Risken ausgesetzt, mit denen sich Kapitel 3 auseinandersetzt.

Vorweg: die Sicherheitsprobleme sind bei einem nach außen abgeschirmten Intranet nicht in der Form gegeben. Diesen Aspekt könnte man zB für die Implementierung eines zentralen Online- Wählerverzeichnisse nutzen.

[52] http://www.tuwien.ac.at/demel/lv97/15min/cliensrv/sld006.htm (abgerufen am 19.8.2001)

3. Technik: Internet und Sicherheit[53]

3.1 Sicherheit von IT- Systemen

Die inzwischen schon fast täglichen Berichte über Einbrüche in sicher geltende Computersysteme und die Schädigungen von Systemen durch Viren und Würmer zeigen die bestehenden Schwächen von Netzwerken auf.

Der Aufbau von Sicherheitsstrukturen muss ein unverzichtbarer Bestandteil von IT-Systemen sein.

Von Maßnahmen zur Sicherheit von IT- Systemen ist insbesondere die Wichtigkeit solcher zum Schutz der Integrität und Verfügbarkeit von Daten und Programmen, sowie der Vertraulichkeit von Daten hervorzuheben.

Zwecks Einordnung von Risken wird zwischen unbeabsichtigten Fehlern und Ereignissen[54] und beabsichtigten Angriffen[55] unterschieden. Wobei bei den beabsichtigten Angriffen noch die Differenzierung der Risken in solche von außen[56] und von innen[57] zu treffen ist.

3.2 Security und Safety

Im Englischen werden die Begriffe „Security“ für Schutz von beabsichtigten und „Safety“ für jenen vor unbeabsichtigten Ereignissen verwendet.

Der Bereich Datenschutz befasst sich insbesondere mit Security vom IT-Systemen.

---

[53] Federrath, Hannes/ Pfitzmann, Andreas: Datenschutz und Datensicherheit, in Schneider, Werner, Taschenbuch der Informatik, Leipzig 2000: S. 587 ff.
[54] z.B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler
[55] z.B. z.B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware
[56] z.B. Hacker
[57] z.B. Insider, z.B. Administratoren, Programmierer)

Schutzziele sind die Vertraulichkeit (Anonymität, Unbeobachtbarkeit, Unverkettbarkeit, Pseudonymität, Abhörsicherheit, Sicherheit gegen unbefugten Gerätezugriff), die Integrität (Zurechenbarkeit, Übertragungsintensität, Abrechnungssicherheit) und die Verfügbarkeit (Ermöglichen von Kommunikation) von Daten .

Eine der Möglichkeiten, um potentielle Risken auszuschließen bzw. zu minimieren ist die **Zugangskontrolle**[58].
Die in IT Systemen derzeit noch am häufigsten vorkommende Form der Identifizierung ist das Passwort.

3.3 Gefahrenquellen in/für IT- Systeme(n)[59]

Hier sind vorerst Computerviren[60] und Trojanische Pferde[61] zu nennen.

Viren und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle oben genannten Schutzziele, also auch die Vertraulichkeit von Daten. Im schlimmsten Fall können Viren und Trojanische Pferde ihre Schadenfunktion modifizieren und sogar sich selbst zerstören, nachdem sie ihre „Aufgabe“ erfüllt haben, um die Spuren zu vernichten.

In Betriebssystemen[62] können Fehler auftreten, die unautorisierten Zugang für Hacker durch Ausnützen von Sicherheitslöchern zulassen. Je nach Betriebssystem gibt es unterschiedliche Methoden, diese zu manipulieren: Trojanische Pferde[63],

---

[58] Unter Zugangskontrolle (admission control) versteht man, dass ein IT- System die Identitäten seiner Kommunikationspartner erfragt, prüft und nur mit berechtigten Partnern weiter kommuniziert. zB.: Handgeometrie, Fingerabdruck, Aussehen, Eigenhändige Unterschrift, Retina- Muster, Stimme, Tipp-Charakteristik (Tastenschlag), Papierdokument, Metallschlüssel, Magnetstreifenkarte, Chipkarte, Taschenrechner, Passwort, Antworten auf Fragen.

[59] Die Darstellung der Gefahrenquellen erfolgt nicht abschließend, sondern es sind nur die (...) Gefahrenquellen angeführt. Weiterführende Literatur: Raepple, Sicherheitskonzepte für das Internet, Heidelberg 2001, 61 ff

[60] Ein Computervirus ist ein ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine so genannte Schadenfunktion ausführt.

[61] Ein Trojanisches Pferd ist ein Computerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadenfunktion ausführt[61].“

[62] Ein Betriebssystem (operating system) stellt das Bindeglied zwischen der Hardware eines Computers einerseits und dem Anwender bzw. seinen Programmen andererseits dar, Es umfasst

Würmer oder Wurmsegmente[64], Viren[65], Logische Bomben[66], Trap doors[67].

In Netzen gibt es Formen der Tarnung (z.B. spoofing), bei der ein Rechner vorspiegelt, ein anderer zu sein[68]. In vielen Betriebssystemen gibt es den Begriff des „trusted host". Vereinfacht gesagt sind dies Rechner, denen gegenüber der eigene Rechner „offen" ist. Tarnt sich ein fremder Rechner als vertrauenswürdiger Host, wird das Eindringen erleichtert."[69]

Datenpakete können auf ihrem Weg im Internet grundsätzlich abgehört oder verändert, unverschlüsselte Passwörter ausgelesen werden. Abhilfe schafft hier der Einsatz von krypographischen Verfahren.[70]

Ein Beispiel für die Störung einer Wahl über das Web waren die Kommunalwahlen im März 2001 in Hessen, wo mit Müh und Not ein Hackerangriff - es wurden bis zu 5000 Zugriffe gleichzeitig mit großen Informationsmengen gestartet- abgewehrt werden konnte. Daneben kam es aufgrund fehlerhafter Computerkennungen zu fehlerhaften Kreiswahlergebnissen[71].

3.4 Sonstiges: Cookies

Programme, die zusammen mit den Eigenschaften des Computers „die Grundlage der möglichen Betriebsarten dieses Systems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen.

[63] Trojanische Pferde sind Programme, die einerseits die gewünschte bzw. offizielle Funktion ausführen, aber gleichzeitig vom Manipulateur beabsichtigte Nebenwirkungen ausführen.

[64] Würmer oder Wurmsegmente sind Programme, die sich selbständig über ein Netz verbreiten und auf anderen Rechnern verbreiten können. Spezialisten des Computersicherheitsunternehmens Silicon Defense <http://www.silicondefense.com/> halten es für möglich, dass mit Wurm- Attacken das gesamte Internet innerhalb von 30 Sekunden lahmgelegt wird.

[65] Viren sind Programme, die sich in andere Programme hineinkopieren (reproduzieren) und zeit- oder ereignisgesteuert Schäden hervorrufen.

[66] Logischen Bomben sind zusätzliche Programmfunktionen, die vom Programmierer eingebaut werden. Sie treten erst nach einer gewissen Dauer bzw. bei einem bestimmten Ereignis zu Tage

[67] Trap doors sind Programmfunktionen, die einen nicht autorisierten Zugang zum System ermöglichen

[68] z.B. spoofing

[69] Plate, Jürgen/ Henning, Peter A.in: "Internet und Intranet" in „Taschenbuch der Informatik", S 710 f

[70] Siehe Kapitel 4

[71] Erstmals Hacker-Störaktionen bei einer Wahl in Deutschland, in Spiegel Online vom 19. März 2001 http://www.spiegel.de/netzwelt/politik/0,1518,123392,00.html, abgerufen am 8.8.2001

Ein Cookie ist eine kleine Textdatei, die der Browser auf Anweisung eines WWW-Servers auf die Festplatte des Benutzers speichert. Später kann derselbe Server die Datei, deren Inhalt und Lebensdauer er bestimmen kann, wieder auslesen. Allerdings kommt es vor, dass ein Cookie- Server Kooperationen mit mehreren Websites vereinbart. Implementiert dann auf jeder Seite der Gemeinschaft eine Funktion, die ein Cookie auf die Festplatte des Benutzers schreibt, welche eindeutige Nutzerinformationen speichert und auch die besuchte Seite notiert. Da der Server die Seitenbesuche der gesamten Seitengemeinschaft genau nachvollziehen kann, ist es auch möglich, das genaue Benutzerverhalten des Nutzers nachzuvollziehen.[72]

In Zusammenhang mit Wahlen ist die Wichtigkeit eines speziellen „Wahlbrowsers“ mit eingeschränkten Funktionen zu betonen[73].

3.5 Maßnahmen zur Risikominimierung

Eine Erhöhung der Rechnersicherheit kann erreicht werden, indem man Server unter Verschluss hält, um so einen Zugriff auf diese zu verhindern. Öffentliche Datenbereichen sollten immer von sonstigen Bereichen abgeschottet werden; der Schutz von Netzwerken durch „Firewalls“ [74] sollte die Regel darstellen.

Speziell bei sensiblen Systemen, bei denen Datenschutz eine große Rolle spielt, ist es besonders wichtig, Sicherheitsmaßnahmen für die Anwenderseite mitzuplanen. Hier ist auf die Struktur von i-vote zu verweisen, wo ein redundanter Sicherheitsaufbau vorliegt und ein eigener Browser sowie ein eigenes Betriebssystem entwickelt worden sind[75].

Die Schlussfolgerungen aus dem Status Quo der Technik sind jedoch unterschiedlich. Während die Forschungsgruppe Internetwahlen in Deutschland fest davon überzeugt ist, im Jahre 2010 die ersten Bundestagswahlen via Internet

[72] Jünger/Oswald/Richter: WWW-Technik und Web- Design, S 43
[73] Siehe Kapitel 7
[74] Eine Firewall kanalisiert die Kommunikation, indem alle Daten von und nach außen über dieses System laufen.
[75] Siehe Kapitel 7

durchführen zu können, kommt das Internet Policy Institute zu dem Schluss, dass noch zu viele Frage um Sicherheit und Zuverlässigkeit der Technik offen sind, und daher Wahlen über Internet in den nächsten Jahren nicht zugelassen werden sollten[76].

3.6 Conclusio

Wahlen über das Internet sind technischen Risken ausgesetzt. Dies sollte jedoch nicht dazu führen, dass man sich des Themas nicht annimmt. Vielmehr könnte die Forcierung von derartigen Projekten zu einer Erhöhung der Netzsicherheit führen.

Auf der anderen Seite ist das Bewusstsein der Internetnutzer für mögliche und notwendige Sicherheitsmaßnahmen auf Anwenderseite zu schärfen. Der einzelne Nutzer sollte sich dessen bewusst werden, dass er selber auch einiges zur Datensicherheit beitragen kann.

[76] Internet Policy Institute, Report in the National Workshop on Internet Voting, Washington 2001, S. 2

4. Vertraulichkeit, Integrität, Authentifikation, Verbindlichkeit

Neben Lösungen für die Speicherung und Auszählung der Stimmen[77] hat ein Wahlsystem folgende widersprüchliche Anforderungen zu erfüllen: der Wähler muss als solcher eindeutig identifiziert werden können, und andererseits darf die erfolgte Identifikation nicht dazu führen, dass die Wahlentscheidung für einen Dritten sichtbar bzw. zurückverfolgbar wird.

Zusammengefasst geht es um die Lösung folgender Aspekte: der Unsicherheit, ob der, mit dem ich kommuniziere wirklich derjenige ist, der er vorgibt zu sein bzw. auf der anderen Seite, ob die Informationen, die ich über das Netz schicke auch wirklich nur von demjenigen lesbar sind, für den sie gedacht sind; sowie ob die Informationen, die gesendet werden, nicht verfälscht bzw. geändert werden. Bei Wahlen darf kein Rückschluss auf das Wahlverhalten möglich sein.

4.1 Vertraulichkeit: Kryptographie

Der Einsatz von Kryptographie bietet die Möglichkeit, oben genannte Risiken zu minimieren bzw. auszuschalten.

4.1.1. Was ist Kryptographie[78]?

Das Wort Kryptographie leitet sich aus den griechischen Wörtern "krypto" (ich verberge) und "graphe" (das Schriftstück) ab. Kryptographie ist die Wissenschaft, die sich mit der Absicherung von Nachrichten beschäftigt.

Als Kryptoanalyse wird die Kunst bezeichnet, chiffrierte Nachrichten aufzubrechen, also deren geheime Inhalte lesbar zu machen. Zusammenfassend wird jener Zweig der Mathematik, der Kryptographie und Kryptoanalyse umfasst, als Kryptologie bezeichnet. Nicht abgesicherte Daten werden als Klartext, abgesicherte Daten als Chiffretext bezeichnet. Der Vorgang, Klartext in Chiffretext umzuwandeln, wird als

[77] Siehe Kapitel 7

Chiffrierung (auch Verschlüsselung) bezeichnet. Der umgekehrte Vorgang, die Umwandlung von Chiffretext in Klartext, wird als Dechiffrierung (Entschlüsselung) bezeichnet.
Bereits im klassischen Altertum sind Nachrichten chiffriert worden, um sie vor fremden Augen zu schützen. Julius Caesar vertauschte beispielsweise nach einer einfachen Regel die einzelnen Buchstaben des lateinischen Alphabets, so dass der Text für einen Uneingeweihten wie ein unsinniger Buchstabensalat aussah. Caesar hat Verschlüsselung dermaßen oft angewendet, dass Valerius Probus ein eigenes Buch über Caesars Verschlüsselungsmethoden schrieb. In Caesars „Gallische Kriege“ ist auch erste Einsatz von Kryptographie für militärische Zwecke dokumentiert.[79]

An moderne Kryptographie werden im wesentlichen vier Anforderungen gestellt[80]: Vertraulichkeit, Intergrität, Authentifikation und Verbindlichkeit.

- **Vertraulichkeit**: der Inhalt eines Dokumentes soll nur von dazu befugten Personen gelesen werden können

- **Integrität**: der Inhalt eines Dokumentes soll nicht unbemerkt verändert werden können

- **Authentifikation**: der Urheber eines Dokuments soll feststellbar sein; kein anderer soll sich als Urheber ausgeben können

- **Verbindlichkeit**: Der Urheber eines Dokumentes soll seine Urheberschaft nicht abstreiten können.

Ein weiteres Ziel kann in manchen Situationen **Anonymität** sein. Damit ist nicht nur die Vertraulichkeit des Nachrichteninhaltes, sondern sogar des Kommunikationsvorganges als solchem gemeint.

---

[78] Singh, The Code Book, The Secret History of Codes and Code- Breaking, London 1999,
[79] Singh, The Code Book, S. 10
[80] http://www.wolfgang-kopp.de/krypto.html

4.1.2.Grundbegriffe: Algorithmen und Schlüssel[81]

Um Kryptographie tatsächlich anwenden zu können, müssen sich Sender und Empfänger auf ein bestimmtes Verfahren einigen, das sie verwenden möchten: den Algorithmus.
Dem Verfahren wird ein variabler Parameter hinzugefügt, der sogenannte Schlüssel. Auch auf diesen müssen sich die Beteiligten einigen, er bleibt jedoch ihr Geheimnis.

Die Gesamtheit eines Algorithmus und aller zu ihm kompatiblen Schlüssel, Klartexte und Chiffretexte nennt man ein Kryptosystem.[82]

Die anhand der Kryptographie erstellten Systeme zur Verschlüsselung von Nachrichten werden eingeteilt in symmetrische und asymmetrische Verfahren.

4.1.3. Symmetrisches Verfahren

Sender und Empfänger einigen sich auf einen Schlüssel, der zum ver- und entschlüsseln verwendet wird. Der Schlüssel ist eine Zahl, wobei bei den meisten symmetrischen Verfahren der zu verschlüsselnde Text in Blöcke zerlegt wird und jeder dieser Blöcke mit dem Schlüssel verschlüsselt wird. Der große Vorteil von symmetrischer Kryptographie ist die Schnelligkeit.
Das Problem bei diesem System ist die sichere Übertragbarkeit des Schlüssels. Bevor man bei dieser Methode verschlüsselt miteinander kommunizieren kann, ist ein Austausch des Schlüssels notwendig. So beschäftigten in den 70-er Jahren große Gesellschaften, insbesondere Banken „dispatch- rider“, deren Aufgabe es war, die Schlüssel in einem verschlossenen Koffer den Kunden auf der ganzen Welt zu überbringen: die Kosten dieser Übertragungsmethode stiegen jedoch mit der Zeit in das Unermessliche und so wurden die damaligen mathematischen und technischen Errungenschaften der 70- er- Jahre begrüßt.[83] Durch die Anwendung modularer arithmetischer Einwegfunktionen[84] gelang es, eine Methode zu finden, die

[81] http://www.wolfgang-kopp.de/krypto.html
[82] http://www.wolfgang-kopp.de/krypto.html
[83] Singh, Code Book, S. 251
[84] Modulare arithmetische Einwegfunktionen sind leicht zu erstellen, aber sie sind nicht reversibel (z.B. das Mischen von blauer und gelber Farbe, das Aufschlagen eines Eis)

ermöglichte, dass die an der Kommunikation beteiligten sich über einen Schlüssel einigten, ohne sich treffen zu müssen.
Die Notwendigkeit eines sicheren Kanals bleibt jedoch ein Manko symmetrischer Kryptographie.[85]

4.1.4.Asymmetrisches Verfahren (public- key kryptography)

Mit der Entwicklung des asymmetrischen Schlüssels durch Wissenschaftler des MIT[86] Ende der 70-er- Jahre wurde der Grundstein für sichere verschlüsselte Kommunikation auch in elektronischer Form gelegt. Das bekannteste Verfahren ist das RSA.[87]
Jeder Beteiligte verfügt über zwei zusammengehörige Schlüssel: einen öffentlichen Schlüssel (public key), zum Verschlüsseln verwendet wird und einen privater Schlüssel (private key) zum Entschlüsseln.
Der öffentliche Schlüssel wird öffentlich zugänglich gemacht (z. B. durch Hinterlegung in einer frei einsehbaren Datenbank): mit diesem kann dann die Nachricht an den „Besitzer“ des jeweiligen öffentlichen Schlüssels verschlüsselt werden. Diese Nachricht kann dann mit dem privaten Schlüssel, - der nur für den user, dem er zugeordnet ist, zugänglich ist- entschlüsselt werden.

4.1.5. Hybride Verfahren

Bei hybriden Verfahren[88] werden symmetrische und asymmetrische Verfahren kombiniert, um die Nachteile der beiden Systeme –ein asymmetrischer Schlüssel ist „groß“ und braucht viel Kapazität, bei einem symmetrischer Schlüssel besteht die Notwendigkeit des sicheren Schlüsselaustausches- auszuschließen.

[85] http://www.wolfgang-kopp.de/krypto.html
[86] Massachusetts Institute of Technology
[87] benannt nach den Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman
[88] zB PGP (Pretty Good Privacy), das von Phil Zimmerman entwickelte Verfahren,

4.2. Integrität, Authentifikation und Verbindlichkeiten: digitale Signatur

Die oben dargestellten Kryptosystheme dienen dem Ziel der Vertraulichkeit und werden als Konzelationssysteme bezeichnet. Um die Ziele Integrität, Authentikation und Verbindlichkeit zu erreichen, ist der Einsatz von Authentifikationssystemen, und zwar von digitalen Signaturen notwendig.[89]

4.2.1 Exkurs: Signaturrichtlinie und Signaturgesetz

Am 19. 1. 2000 ist die europäische Richtlinie über gemeinschaftliche Signaturen in Kraft getreten[90]. Sie zielt darauf ab, Hindernisse für den Binnenmarkt zu beseitigen. Die rechtliche Anerkennung elektronischer Signaturen auf Gemeinschaftsebene sowie der freie Verkehr von Diensten und Produkten in Zusammenhang mit elektronischen Signaturen sollen durch die RL gewährleistet werden.

Schwerpunkt der RL sind Regelungen zum Marktzugang für Zertifizierungs-dienstenabieter und zur rechtlichen Anerkennung elektronischer Signaturen. Darüber hinaus werden Haftungsregelungen und Regelungen zur rechtlichen Anerkennung von Zertifikaten aus Drittstaaten getroffen.
Damit diese gegenüber Privaten wirksam werden kann, hatte bis zum 19. 7. 2001 durch die Mitgliedsstaaten eine Umsetzung in nationales Recht zu erfolgen.

Sogenannte fortschrittliche Signaturen, die auf einem qualifizierten Zertifikat beruhen und unter Verwendung einer sicheren Signaturerstellungseinheit erstellt werden, sind von den Mitgliedsstaaten in ihren Rechtswirkungen grundsätzlich den eigenhändigen Unterschriften gleichzustellen[91]. Eine „fortgeschrittene elektronische Signatur“ muss dem Signator ausschließlich zugeordnet sein, die Verwendung muss der alleinigen Kontrolle des Signators unterstehen und sie muss die Authenzität (Echtheit) und

[89] Authentifikationssysteme sind ebenfalls kryptographische Systeme.
[90] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. Nr. L 13 vom 19.1.2000
[91] Art 5 Abs 1 SigRL

Integrität (Unverfälschtheit) der Nachricht gewährleisten[92]. Qualifizierte Zertifikate müssen den in Anhang I zur Richtlinie dargestellten Mindestinhalt aufweisen. Zudem können qualifizierte Zitate nur von solchen Zertifizierungsstellen ausgestellt werden, die bestimmten Mindestanforderungen entsprechen. Diese Mindestanforderungen sind in Anhang II der Richtlinie dargestellt.

Das Signaturgesetz wurde am 14. 7. 1999 vom Nationalrat einstimmig beschlossen und ist mit 1. 1. 2000 in Kraft getreten[93]. Österreich war damit der erste Mitgliedstaat, der die SignaturRL umgesetzt hat[94].
Die rechtliche Definition einer sicheren elektronischen Signatur findet sich in § 2 Z 3 SigG[95]. Signaturgesetz und Signaturverordnung stellen an eine sichere elektronische Signatur zahlreiche technische Anforderungen. Um eine sichere elektronische Signatur zu erzeugen, benötigt der Signator nicht nur ein qualifiziertes Zertifikat, sondern auch eine sichere Signaturerstellungseinheit, wie eine Chipkarte mit der entsprechenden Signatursoftware. überprüfen

4.2.2 Beschreibung und Funktionsweise elektronischer Signaturen[96]

Zur Erstellung einer digitalen Signatur auf einem elektronischen Dokument kommt das Public- Key- Verfahren in entgegengesetzter Richtung zum Einsatz. Die Verschlüsselung erfolgt mit dem privaten, die Entschlüsselung mit dem öffentlichen Schlüssel. Da das Verschlüsseln einer ganzen Nachricht aufgrund der Komplexität asymmetrischer Verfahren oft zu lange dauern würde, wird das zur Signatur vorgesehene Dokument durch eine Einwegfunktion auf wenige Byte verdichtet (=Hashfunktion). Der Hash wird anschließend mit dem privaten Signaturschlüssel

[92] Art 2 Zi 2 SigRL
[93] BGBl Nr. I 1999/190
[94] Durch einige Änderungen, die mit 30. Dezember 2000 in Kraft getreten sind, wurde das SigG an die SigRL angepasst. Die Novelle sieht unter anderem vor, dass ein qualifiziertes Zertfifkat iSd § 5 nicht mehr mit einer „sicheren elektronischen Signatur“ gem. § 2 Z 3 versehen sein muss, sondern nur noch die Anforderungen des § 2 Z 3 lit a bis d erfüllen muss, dh das Erfordernis der Verwendung bestimmter Komponenten und Verfahren entfällt.
[95] Die sichere elektronische Signatur entspricht im Prinzip der fortgeschrittenen elektronischen Signatur des Art 2 Z 2 SigRL, die jedoch zusätzlich auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen des SigG und der Verordnungen auf Grundlage des SigG entspricht.
[96] vgl. Brenn, Signaturgesetz, Wien, 1999, 36 ff, Forgo, Was sind und wozu dienen digitale Signaturen in ecolex 1999, 235, Schönberger/Pilz/Reiser/Schmölzer, Sicher & echt: Der Entwurf eines Signaturgesetzes in MR 1998, 107

des Absenders chiffriert. Zur Überprüfung der digitalen Unterschrift liegen dem Empfänger die Nachricht sowie die angehängte Signatur vor. Um die Identität des Unterschreibenden und die Integrität des Dokumentes zu kontrollieren, berechnet der Empfänger wiederholt den Hash- Wert der Nachricht nach der gleichen Funktionsvorschrift wie der Absender und dekodiert mit dem öffentlichen Schlüssel des Unterzeichners die digitale Signatur. Beide auf diese Weise erhaltenen Dokumente werden verglichen. Stimmen diese nicht überein, ist die Unterschrift als ungültig zu betrachten. Stimmen beide Werte überein, können folgende Annahmen getroffen werden:
Das Dokument wurde auf dem Weg vom Sender zum Empfänger nicht verändert.
Die Signatur ist eindeutig an das übertragene elektronische Dokument gebunden.[97]

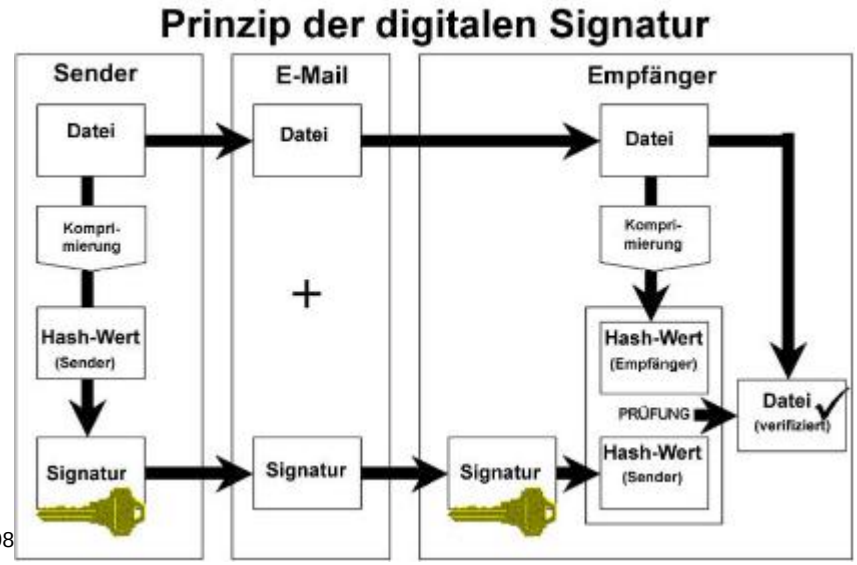

Tabelle [98]

4.2.3. Public Key Infrastructure

Um die Schlüsseldaten jedoch eindeutig einer Person zuordnen zu können, benötigt man elektronische Schlüsselzertifikate. Die Zertifizierung eines öffentlichen Schlüssels beglaubigt die Identität seines Besitzers. Diese erfolgt durch sogenannte „ „Trust- Center“ oder Zertifizierungsdienste.[99]

[97] Raepple, Sicherheitskonzepte für das Internet, S 147 f
[98] <http://private.addcom.de/k/kaktus2000/sign_wie.html>
[99] Zertifizierungsdiensteerbringer benötigen für die Aufnahme ihrer Tätigkeit kein Genehmigung. Sie müssen sich vor Beginn ihrer Tätigkeit bei der für die Überwachung zuständigen Behörde anmelden.

Diese verstehen sich als Sicherheitsinstanz für alle Nutzer im Netz und übernehmen Zertifizierungsaufgaben in Form von Ausstellen, Bereitstellen, Aktualisieren und Sperren der elektronischen Ausweise (Zertifikate). Sie überprüfen, ob ein zur Beglaubigung eingereichter öffentlicher Schlüssel und eine Person mit eindeutigem Namen wirklich zusammengehören. Ist dies der Fall, erzeugt der Zertfizierungsdiensteanbieter ein elektronisches Schlüsselzertfikat. Dieses beinhaltet den Namen seines Besitzers und der ausgebenden Zertfizierungsstelle sowie deren digitale Signatur, die für die verlässliche Zuordnung zwischen dem öffentlichen Schlüssel und seinem Besitzer bürgt.

Das Verlangen auf Ausstellung eines Zertifikats kann aber gem. § 8 Abs 2 SigG auch bei einer Registrierungsstelle eingebracht werden, die für den Zertifizierungs-diensteanbieter tätig ist.

Die sicherste Realisierung von digitale Signaturen stellen jene in Form von Chipkarten (SmartCards) dar.

Nach heutigem Stand der Technik sind nur digitale Signaturen auf Basis der Chipkartentechnologie in der Lage, die Sicherheitsanforderungen der Signaturrichtlinie zu erfüllen. Derzeit kommen daher nur solche Signaturen als sichere elektronische Signaturen im Sinne des Signaturgesetzes in Betracht.[100]

In Österreich gibt es zum gegenwärtigen Stand noch keinen Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt. Die Voraussetzungen für die Zuteilung sicherer elektronischer Signaturen ist also in Österreich noch nicht gegeben.
Es würde im Moment nur die Möglichkeit bestehen, ausländische Unternehmen, wie etwa VeriSign[101] mit Sitz in Amerika und T-TeleSec[102] mit Sitz in Deutschland, in Anspruch zu nehmen.

Die Behörde untersucht, ob der Diensteanbieter die gesetzlichen Regelungen zu Ausstellung von Zertifikaten erfüllt. Ist dies der Fall erlässt, die Behörde einen positiven Bescheid. Der Bescheid kann jedoch von der Behörde widerrufen werden, wenn diese feststellt, dass der Dienstanbieter nicht mehr die gesetzlichen Anforderungen erfüllt (§ 6 SigG).

[100] Brenn, Signaturgesetz, 37
[101] Siehe dazu die Website von VeriSign unter http://www.verisign.com [abgerufen am 25.08.2001].

4.3 Lösung von Widersprüchen: Blinde Signaturen [103]

Digitale Signaturen gewährleisten Sicherheit über die Authenzität und Identität des Versenders einer Nachricht, was zum Zeitpunkt der Registrierung eines Wählers eine absolute Notwendigkeit darstellt. Zum Zeitpunkt der Auszählung der Wählerstimme darf der Rückschluss auf den Wählenden jedoch keinesfalls gegeben sein.

Um die notwendige Anonymisierung des Stimme des Abstimmenden realisieren zu können, ist der Einsatz von **blinde**n **Signaturen** notwendig.

Eine Erweiterung der digitalen Signaturen im Hinblick auf Anonymitätsaspekte stellen die **blinden Signaturen** dar, die 1982 von David Chaum[104] erfunden wurden.

Man unterscheidet drei Typen von blinden Unterschriften:

- Die **verdeckte Unterschrift**: Durch die zum Zeitpunkt der Unterschrift hinzugefügten Signaturparameter kann der Unterzeichner ein Dokument ohne Vorlage der Unterschrift später wiedererkennen und sogar dem Besitzer zuordnen.
- Die **schwach blinde Unterschrift**: Der Unterzeichner kann ein Dokument wiedererkennen und es dem Besitzer zuordnen, aber nur dann, wenn er auch gleichzeitig seine Unterschrift darunter sieht.
- Die **stark blinde Unterschrift**: Auch wenn der Unterzeichner ein Dokument inklusive seiner Unterschrift sieht, kann er es dem Besitzer nicht zuordnen.

Wenn man von blinden Unterschriften spricht, so meint man i.A. stark blinde Unterschriften.

4.3.1 Funktionsweise blinder Signaturen

---

[102] Siehe dazu die Website des Telekom Trust Center T-TeleSec unter http://www.telesec.de [abgerufen am 25.08.2001].
[103] http://www.chaum.com/; http://cip.uni-trier.de/licht/seminar/sigcash2.htm, abgerufen am 20.7. 2001
[104]< http://www.chaum.com/;>

- Die Unterschrift: Ein Dokument wird von jemandem ohne Kenntnis des Inhalts unterschrieben, d.h. nicht der Inhalt, sondern die Tatsache der Vorlage durch eine bestimmte Person zu einem bestimmten Zeitpunkt wird bestätigt.

- Der Prüfungsvorgang: Nach Vorlage des Dokuments und der Unterschrift kann überprüft werden, ob die Unterschrift zum Dokument gehört und ob sie rechtmäßig erlangt wurde.

- Die Anonymität: Der Unterschriftsvorgang kann nicht rekonstruiert werden, d.h. es kann zwar noch entschieden werden, ob eine Unterschrift gültig ist oder nicht, jedoch können Aktionen nicht mehr mit Personen verknüpft werden. Dies bedeutet auch, daß keine sogenannten "Dossier Creations" stattfinden können, was die Vorstufe zum "gläsernen" Bürger darstellte.

Allgemein ermöglichen blinde Signaturen **Rechtssicherheit trotz Anonymität**.[105]

4.4 Conclusio

Die Verwendung digitaler Signaturen und der Aufbau von Public Key Infrastrukturen sind Grundvoraussetzungen für eVoting. Zum gegenwärtigen Zeitpunkt bereiten diese jedoch noch erhebliche technische und organisatorische Probleme[106].

---

105 Anwendungen für Blinde Signaturen
- Electronic Money (rechtskräftig, aber anonym)
- Beglaubigte Pseudonyme, z.B. Krankenkassenabrechnung:
  Bei Ausgabe der Versichertenkarten unterschreibt die Krankenkasse Pseudonyme für alle Versicherten blind. Damit ist sichergestellt, daß die Kasse keine personenbezogenen Krankheitsgeschichten sammeln kann, aber dennoch in der Lage ist, Statistiken über Krankheitsbilder anzufertigen und vor allem festzustellen, ob eine Behandlung bei einem "ihrer" Versicherten stattfand und zu Recht in Rechnung gestellt wurde.
- Anonyme Berechtigungsausweise, d.h. die Berechtigung für etwas kann ohne die Preisgabe der Identität nachgewiesen werden
- Geheime, von Dritten blind beglaubigte Verträge (z.B. Testamentsbeglaubigungen durch einen Notar)
- Elektronische Wahlen (unter Wahrung des Wahlgeheimnisses)

[106] So sind bei den Wahlen zum Studierendenparlament an der Universität Osnabrück folgende Probleme aufgetreten: Kartenlesegeräte waren nicht ausreichend vorhanden, eine Reihe von Kompatibilitätsproblemen wurde nicht bedacht, viele PIN- Codes und Signatur- Smartcards wurden nicht rechtzeitig verschickt (Stomper, Hürdenlauf zum Online- Urnengang, in Homepages 1/2001, 11)

5. Verfassungsrecht und demokratische Rechte

5.1 Repräsentative Demokratie: verfassungsrechtliche Grundlagen des Wahlrechts[107]

Wahlen sind das entscheidende Element der repräsentativen Demokratie[108], das Wahlrecht das wichtigste politische Grundrecht[109], das die österreichische Rechtsordnung vorsieht.
Regelungen finden sich neben Art 1 B-VG[110], der programmatischen Einleitungsbestimmung der Bundesverfassung, in folgenden in Verfassungsrang stehenden Bestimmungen:

5.1.1 Artikel 23a Bundes- Verfassungsgesetz

„Die von der Republik Österreich zu entsendenden Abgeordneten zum Europäischen Parlament werden auf Grund des gleichen, unmittelbaren, geheimen und persönlichen Wahlrechtes der Männer und Frauen, die vor dem 1. Jänner des Jahres der Wahl das 18. Lebensjahr vollendet haben und am Stichtag der Wahl entweder die österreichische Staatsbürgerschaft besitzen und nicht nach Maßgabe des Rechts der Europäischen Union vom Wahlrecht ausgeschlossen sind oder die Staatsangehörigkeit eines anderen Mitgliedstaates der Europäischen Union besitzen und nach Maßgabe des Rechts der Europäischen Union wahlberechtigt sind, nach den Grundsätzen der Verhältniswahl gewählt."

5.1.2 Artikel 26 Bundes- Verfassungsgesetz

„Der Nationalrat wird vom Bundesvolk auf Grund des gleichen, unmittelbaren, geheimen und persönlichen Wahlrechtes der Männer und Frauen, die vor dem 1. Jänner des Jahres der Wahl das 18. Lebensjahr vollendet haben, nach den Grundsätzen der Verhältniswahl gewählt."

---

[107] Dujmovits, Auslandsösterreicherwahlrecht und Briefwahl, Wien, 2000, 19
[108] Dujmovits, Auslandsösterreicherwahlrecht und Briefwahl, Wien, 2000, 19
[109] Nowak, Das Wahl- und Stimmrecht als Grundrecht in Österreich, EuGRZ 1983, 89 (92); Nowak/Strejcek, Das Wahl- und Stimmrecht, in: Machacek/Pahr/Stadler (Hrsg), Grund- und Menschenrechte in Österreich, Band III (1997), 1 (42)
[110] „Österreich ist eine demokratische Republik. Ihr Recht geht vom Volk aus."

5.1.3 Artikel 60 Bundes- Verfassungsgesetz

„Der Bundespräsident wird vom Bundesvolk auf Grund des gleichen, unmittelbaren, geheimen und persönlichen Wahlrechtes gewählt; (...). Stimmberechtigt ist jeder zum Nationalrat Wahlberechtigte."

5.1.4 Artikel 95 Bundes- Verfassungsgesetz

„Die Gesetzgebung der Länder wird von den Landtagen ausgeübt. Deren Mitglieder werden auf Grund des gleichen, unmittelbaren, geheimen und persönlichen Verhältniswahlrechtes aller nach den Landtagswahlordnungen wahlberechtigten männlichen und weiblichen Landesbürger gewählt."

5.1.5 Artikel 117 Bundes- Verfassungsgesetz

„Die Wahlen in den Gemeinderat finden auf Grund des gleichen, unmittelbaren, geheimen und persönlichen Verhältniswahlrechts aller Staatsbürger statt, die in der Gemeinde den Hauptwohnsitz haben."

5.1.6 Artikel 8 des Staatsvertrages von Wien[111]

„Österreich wird eine demokratische, auf geheime Wahlen gegründete Regierung haben und verbürgt allen Staatsbürgern ein freies, gleiches und allgemeines Wahlrecht sowie das Recht, ohne Unterschied von Rasse, Geschlecht, Sprache, Religion oder politische Meinung zu einem öffentlichen Amte gewählt zu werden."

5.1.7 Artikel 66 Absatz 1 des Staatsvertrages von St. Germain-en Laye[112]

„Alle österreichischen Staatsangehörigen ohne Unterschied der Rasse, der Sprache oder Religion sind vor dem Gesetze gleich und genießen dieselben bürgerlichen und politischen Rechte."

[111] Staatsvertrag von Wien betreffend die Wiederherstellung eines unabhängigen und demokratischen Österreich, BGBl 1955/152

5.1.8 Artikel 3 des 1. Zusatzprotokolles zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten[113]

„Die Hohen vertragsschließenden Teile verpflichten sich, in angemessenen Zeitabständen freie und geheime Wahlen unter Bedingungen abzuhalten, die die freie Äußerung der Meinung des Volkes bei der Wahl der gesetzgebenden Organe gewährleisten."

5.2 Direkte Demokratie

Die österreichische Verfassung sieht folgende direktemokratische Partizipations-möglichkeiten vor.

5.2.1 Volksbegehren

Gemäß Art 41 Abs. 2 B- VG ist jeder von 100.000 Stimmberechtigten oder von je einem Sechstel der Stimmberechtigten dreier Länder gestellte Antrag (Volksbegehren) von der Hauptwahlbehörde dem NR zur geschäftsordnungsmäßigen Behandlung vorzulegen. Das Volksbegehren kann in Form eines Gesetzesentwurfes gestellt werden.

Ein Konkretisierung erfolgt durch das VBegG 1973, das als Ausführungsgesetz das Verfahren von Volksbegehren regelt.

Dieses Verfahren besteht aus drei Abschnitten: dem Einleitungsverfahren (die Einleitung ist beim BMI zu beantragen), dem Eintragungsverfahren und dem Ermittlungsverfahren.

Stimmberechtigt sind alle Staatsbürger, die am Stichtag das Wahlrecht zum Nationalrat haben und in einer Gemeinde des Bundesgebietes den Haupwohnsitz haben. Ausgeübt wird das Stimmrecht durch Eintragung in die Eintragungsliste.

---

[112] Staatsvertrag von St.-Germain-en-Laye vom 10. September 1919, StGBl 1920/303. Abschnitt V des III. Teiles, darunter auch Art 66 steht gemäß Art 149 Abs. 1 B-VG in Verfassungsrang.

[113] Zusatzprotokoll zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 1958/210, in Verfassungsrang durch Art II Z 7 BVB BGBl 1964/59

5.2.3 Volksbefragung

Gemäß Art 49 b B- VG ist diese auf Beschluss des Nationalrates. Gegenstand der Volksbefragung muss eine Angelegenheit von grundsätzlichlicher und gesamtösterreichischer Bedeutung sein, zu deren Regelung die Zuständigkeit des der Bundesgesetzgebers gegeben ist. Einer Volksbefragung ist eine Frage zugrunde zu legen, die mit „ja“ oder „nein“ zu beantworten ist.

5.2.4 Volksabstimmung

Gemäß Art 43 B- VG ist ein Gesetzesbeschluss des NR -nach Beendigung des Verfahrens gem. Art 42 B- VG, jedoch vor deiner Beurkundung durch den Bpräs- wenn der Nationalrat dies beschließt oder wenn es die Mehrheit der Mitglieder des Nationalrates durch einen schriftlichen Antrag an den Präsidenten des Nationalrates verlangt, einer Volksabstimmung zu unterziehen. Die Volksabstimmung ist sodann vom Bundespräsidenten auf Vorschlag und unter Gegenzeichnung der Bundesregierung anzuordnen (Art 46 Abs. 3, Art 67 Abs. 1 und 2 B-VG; § 1 VabstG). Stimmberechtigt sind die zum Nationalrat aktiv wahlberechtigten (Art 46 Abs. 2 B-VG; § 5 VabstG). Das Verfahren für die Volksabstimmung ist gesetzlich zu regeln; dies geschah durch das Volksabstimmungsgesetz (VabstG).

6 Briefwahl und Verfassungsrecht[114]

6.1 Juristische Einordnung des Wahlmails

Eine Wahl über Internet erfolgt, technisch gesehen, mittels eMail. Dieses stellt, wenn es verschlüsselt versendet wird, einen Brief dar.[115] iVoting ist in der verfassungsrechtlichen und –politischen Diskussion als Briefwahl zu betrachten [116].
Eine Briefwahl wird „regelmäßig als Form der Wahlrechtsausübung beschrieben, deren Spezifikum die Abwesenheit des Wählers vom Wahllokal ist[117]."

6.1 Grundsatz: persönliche Stimmabgabe am Ort des Hauptwohnsitzes[118]

Der Wahlberechtigte[119] hat die Wahl persönlich in der Wahlzelle vorzunehmen (60, 70, 74 Abs 3 und 74 NRWO). Dadurch soll eine Absicherung des geheimen Wahlgrundsatzes erfolgen.[120]
Ort der Ausübung des Wahlrechts ist grundsätzlich der Ort, in dessen Wählerverzeichnis[121] der Wahlberechtigte eingetragen ist.[122]

---

[114] Da das Thema Wahlen via Internet in der österreichischen Literatur bisher nicht berücksichtigt worden ist, wird in diesem Bereich auf die Diskussion in Deutschland, zurückgegriffen. Siehe insbes.
[115] Wagner, Unbefugter Zugriff auf e-mail, ecolex 2000, 273
[116] Aber: es kommt in der Wertung noch eine andere Wertung hinzu: Bits sind Bits. Zusätzlich sind somit bei etwaigen Regelungen auch die einschlägigen Bestimmungen in anderen Materien (TKG, SPG) zu beachten, denn ob eine eMail ein Wahlmail ist oder nicht, ist, ohne dass man den Inhalt betrachtet, nicht sichtbar.
[117] Pesendorfer, Briefwahl und Verfassungsrecht, Der Staatsbürger 1978, 73 (73)
[118] „Der Hauptwohnsitz einer Person ist dort begründet, wo sie sich in der erweislichen oder aus den Umständen hervorgehenden Absicht niedergelassen hat, hier den Mittelpunkt ihrer Lebensbeziehungen zu schaffen; trifft diese sachliche Voraussetzung bei einer Gesamtbetrachtung der beruflichen, wirtschaftlichen und gesellschaftlichen Lebensbeziehungen einer Person auf mehrere Wohnsitze zu, so hat sie jenen als Hauptwohnsitz zu bezeichnen, zudem sie das überwiegende Naheverhältnis hat." (Art 6 Abs 3 B- VG, eingefügt durch Bundesverfassungsgesetz BGBl 504/1994).
[119] Wahlausschließungsgründe sind gem. § 22 NRWO die rechtskräftige Verurteilung wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer mehr als einjährigen Freiheitsstrafe.
[120] Walter/Mayer, Grundriss des österreichischen Verfassungsrechts, 9, RZ 309
[121] gem. § 24 NRWO ist der Wahlberechtigte grundsätzlich in das Wählerverzeichnis des Ortes einzutragen, wo er seinen Hauptwohnsitz hat. Für im Ausland lebende Wahlberechtigte bestimmt sich der Ort ihrer Eintragung in das Wählerverzeichnis nach den Angaben in der Wählerevidenz; s. FN 113
[122] § 37 Abs 1 NRWO

6.1.1 Ausnahme: Wahlkartenwahl im Inland

Hält sich der Wähler am Wahltag voraussichtlich nicht am Ort der Eintragung in das Wählerverzeichnis aufhält, hat er Anspruch auf Ausstellung einer Wahlkarte[123]. Die Wahlkarte ist als verschließbarer Umschlag herzustellen[124]. Ein amtlicher Stimmzettel und ein verschließbaren Kuvert sind in den Briefumschlag zu legen und dem Wahlberechtigten auszufolgen. Dieser hat den Briefumschlag bis zur Stimmabgabe sorgfältig zu verwahren[125].
Der Wahlleiter der Wahlbehörde, vor der der Wähler dann die Stimmabgabe vornimmt, hat den Briefumschlag zu öffnen und dem Wahlkartenwähler den inliegenden amtlichen Stimmzettel und das beiliegende Wahlkuvert auszuhändigen[126].
Der Wahlberechtigte nimmt dann die Wahlhandlung persönlich in der Wahlzelle vor.

6.1.2 Ausnahme: Wahlkartenwahl im Ausland

Art 26 Abs 6 vorletzter Satz B-VG sieht eine Ausnahmeregelung für die Stimmabgabe im Ausland bei Wahlen zum Nationalrat, bei der Wahl zum Bundespräsidenten sowie bei Volksabstimmungen vor: diese müssen nicht vor einer Wahlbehörde erfolgen.

Diese Regelung der Stimmabgabe im Ausland wurde vom Gesetzgeberv beschlossen, nachdem der VfGH mit dem sogenannten „Auslandsösterreichererkenntnis“ § 2 Wählerevidenzgesetz 1973 BGBl 601 (WEvG) wegen Verfassungswidrigkeit aufgehoben hatte[127]. Die aufgehobene Bestimmung hatte als Voraussetzung für die Aufnahme in die Wählerevidenz den ordentlichen Wohnsitz in einer österreichischen Gemeinde vorgesehen.

[123] § 38 Abs 1 NRWO; Die Ausstellung der Wahlkarte ist gem. § 39 Abs 1NRWO bei der Gemeinde, von der der Wahlberechtigte in das Wählerverzeichnis eingetragen wurde, beginnend mit dem Tag der Wahlausschreibung bis spätestens am dritten Tag vor dem Wahltag mündlich oder schriftlich zu beantragen. Im Ausland kann die Ausstellung der Wahlkarte auch im Weg einer österreichischen Vertretungsbehörde beantragt werden.
[124] § 39 Abs 2 NRWO
[125] § 39 Abs 3 NRWO
[126] § 68 NRWO
[127] VfSlg 12.023/1989

Aus Art 26 1 B- VG könne jedoch, so der VfGH, keine Beschränkung des Wahlrechtes zum Nationalrat auf Staatsbürger mit österreichischen Wohnsitz abgeleitet werden.
In Folge dieses Erkenntnisses wurde dann dem § 2 WEvG ein Abs. 5 eingefügt: „Wahl- und Stimmberechtigte, die ihren ordentlichen Wohnsitz in das Ausland verlegen und diesen Umstand der Gemeinde, in der sie ihren ordentlichen Wohnsitz aufgeben, schriftlich anzeigen, sind für die Dauer ihres Auslandsaufenthaltes, längstens jedoch über einen Zeitraum von 10 Jahren, in der Wählerevidenz zu führen(...)."

Die Stimmabgabe im Ausland ist folgendermaßen geregelt: der Wahlkartenwähler hat die Wahlkarte samt dem darin enthaltenen ungeöffneten Wahlkuvert der zuständigen Wahlbehörde zu übermitteln. Um bei der Ermittlung des Wahlergebnisses berücksichtigt zu werden, muss das Wahlkuvert spätestens am achten Tag nach dem Wahltag, 12 Uhr, bei der zuständigen Landeswahlbehörde einlangen[128].
Um rechtsgültig wählen zu können, bedarf der Wahlberechtigte jedoch auf der Wahlkarte der Bestätigung von Seiten der österreichischen Vertretungsbehörde[129], eines Notars oder einer ähnlichen Einrichtung[130], des Einheitskommandanten[131] oder von zwei Zeugen mit österreichischer Staatsbürgerschaft[132]. Bestätigt werden muss die Identität des Wählers, der Ort und der Zeitpunkt, in welchem der Wähler „das Wahlkuvert verschlossen in die Wahlkarte zurückgelegt hat".

Die Regelung des § 60 NRWO ist in der Lehre umstritten. Kritisiert wird, dass nicht der Verfassungsgesetzgeber deutlich und selbst eine Abwägung zu Gunsten des allgemeinen Wahlrechts vorgenommen hat, sondern der einfache Gesetzgeber mit den Regelungen des § 60 NRWO allen, auch den am Wahltag im Ausland befindlichen Wahlberechtigten die Stimmabgabe ermöglicht, ohne dass

[128] § 60 Abs 6 NRWO
[129] § 60 Abs. 2 NRWO
[130] § 60 Abs. 2 NRWO
[131] § 60 Abs 3 NRWO
[132] § 60 Abs 4 NRWO

entsprechende Vorkehrungen für die Sicherung der freien Willensentscheidung sowie der persönlichen und geheimen Stimmabgabe getroffen werden[133].

Insbesondere die Möglichkeit der Wahl vor zwei Zeugen -die häufig im Familienkreis, wo Beeinflussungen nicht gänzlich ausgeschlossen werden können, vor sich geht und nur eine geringe Gewährleistung für die Einhaltung des geheimen und persönlichen Wahlrechts beinhaltet- sei nicht mit dem persönlichen und geheimen Wahlprinzip in Einklang zu bringen [134] und sei daher verfassungsrechtlich bedenklich.

Die Regelung der Stimmabgabe im Ausland kann auch, so Strejcek, als Briefwahl qualifiziert werden[135]. In diesem Fall ist ein Widerspruch zur Rechtsprechung des VfGH zu Briefwahlen gegeben.

6.1.3 VfGH: Briefwahl verfassungswidrig

Der VfGH hat in seiner Entscheidung vom 16. 3. 1985, G 18/85[136] , dem sogenannten „Briefwahlerkenntnis“, die Briefwahl als verfassungswidrig erklärt und die nö Wahlordnung für Statutarstädte[137], aufgehoben. Diese hatte die Möglichkeit der Abgabe der Wählerstimme in der Form vorgesehen, dass ein Wähler, der die Verwendung der ihm zugekommenen Wahlkarte mit Wahlbrief auszuüben beabsichtige, den Stimmzettel in seinem privaten Bereich selbst (persönlich) auszufüllen und in eine Wahlkuvert zu legen habe. Das Gesetz schrieb vor, dass diese dem Wähler obliegende Ausfüllung des Stimmzettels „unbeobachtet“ geschehen müsse. Den Wähler hätte die Verpflichtung getroffen, eine auf der Wahlkarte vorgedruckte Erklärung, der Stimmzettel sei von ihm persönlich unbeobachtet ausgefüllt worden, zu unterfertigen.[138] Die Wahlkarte und das Wahlkuvert mit Stimmzettel hätten dann in einem mit einer Siegelmarke zu

[133] Strejcek, Zur Neuregelung der Stimmabgabe im Ausland durch die Nationalrats- Wahlordnung 1992, ZfV 1993, 431 (436 ff)
[134] Strejcek, Zur Neuregelung der Stimmabgabe im Ausland durch die Nationalrats- Wahlordnung 1992 436 ff; Schick, Probleme der Wahlrechtsreform 1992, ÖJZ 1994, 289 (294f),
[135] Strejcek, Zur Neuregelung der Stimmabgabe im Ausland durch die Nationalrats- Wahlordnung 1992 436 ff; Schick, Probleme der Wahlrechtsreform 1992, ÖJZ 1994, 289 (294f)
[136] VfSlg 10.462
[137] LGBl 0360-2
[138] Vgl: Rechtslage in Deutschland

verschließenden amtlichen Wahlbriefumschlag durch die Post den Wahlbehörden zugesendet werden sollen. Die nöLReg begündete die Regelungen damit, dass diese dem allgemeinen Wahlrecht dienen würden.

Der VfGH begründete die Aufhebung der Bestimmungen damit, dass die angefochtene Regelung zum einen dem Grundsatz der „geheimen“ Wahl widerspreche, zum anderen das Prinzip der „persönlichen“ Wahl verletze und legte im Leitsatz folgendes fest:

Das Recht auf geheime Wahl verpflichte den Staat, so der VfGH, zur Zurverfügungstellung aller notwendigen Einrichtungen, um die korrekte Abhaltung geheimer Wahlen zu gewährleisten und zu sichern. Das im B-VG für Wahlen zu allgemeinen Vertretungskörpern expressis verbis verankerte Persönlichkeitsprinzip würde die Schaffung von Wahlordnungen, die zwingend sicherstellen , dass alle zu zählenden Stimmen wirklich von jenen Personen stammen, die sie abgeben, gebieten. Aus dem Persönlichkeitsprinzip schloss der VfGH, dass die physische Präsenz des Wählers, sei es im Stimmlokal, sei es vor einer sog. „fliegenden“ oder sonstigen Wahlkommission oder einem die Aufgaben einer solchen Kommission adäquat besorgenden Staatsorgan, notwendige Voraussetzung für die Teilnahme an der Wahl sei.

Auffällig ist der Widerspruch zwischen den Regelungen des § 60 NRWO, die -gestützt auf die Erzeugungsregel des Art 26 Abs 6 vorletzter Satz- vorsehen, dass die Stimmabgabe „nicht vor einer Wahlbehörde“ erfolgen muss und dem „Verbot“ der Briefwahl durch das Briefwahlerkenntnis. Eine Stimmabgabe, die nicht vor einer Wahlbehörde erfolgt, und keine Briefwahl darstellt, ist nur schwer bis gar nicht denkbar.

6.3 Conclusio

Die Zulässigkeit einer Briefwahl kann nur durch einen Beschluss des Verfassungsgesetzgebers erreicht werden. Die Entscheidung, ob eine derartige Methode der Wahlausübung zulässig ist oder nicht, ob also dem allgemeinen Wahlrecht auf der einen Seite oder dem geheimen und persönlichen Wahlrecht auf

der anderen Seite der Vorzug zu geben ist- fällt also in den rechtspolitischen Handlungsspielraum des Verfassungsgesetzgebers.
Wobei dieser die technische Komponente und deren Sicherheit in der Bewertung mit zu berücksichtigen hat.

7. iVoting und Wahlrechtsgrundsätze

Die nachfolgende Darstellung der (österreichischen) Wahlgrundsätze beinhaltet eine Beurteilung der Verfassungsmäßigkeit von Wahlen mittels Internet, wobei auf die vom BVerfG zur Briefwahl und den von der deutschen Literatur[139] zum Wählen über Internet angestellten Überlegungen zurückgegriffen wird.

Beurteilt wird die Zulässigkeit der Internet- Wahlen als Alternative zur Präsenzwahl. Voraussetzung für die Möglichkeit des Stimmabgabe über Internet ist das Vorliegen eines Verhinderungsgrundes am Wahltag.

Exkurs: Rechtslage in Deutschland[140]

Durch eine Novellierung des Wahlgesetzes wurde im Jahre 1956 die Möglichkeit der Ausübung des Wahlrechtes mittels Briefwahl eingeführt. Eine wesentliche Bedingung für die Briefwahl ist nach geltender Rechtslage das Vorliegen von Verhinderungsgründen am Wahltag. Abwesenheit, Krankheit etc. berechtigen zur Stimmabgabe in Form einer Briefwahl. Während diese Regelung in der Lehre umstritten ist[141], sieht der BVerfG sie als verfassungskonform und als nicht den gleichen und persönlichen Wahlgrundsätzen widersprechend .

---

[139] Siehe insbes. Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen in Multimedia & Recht, abrufbar unter http://www.i-vote.de/projekt/index.html

[l] Briefwahl in anderen Staaten: in Frankreich, Niederlanden und Belgien, Spanien, Italien und in gibt es keine Fernwahl. Franzosen und Niederländer ersetzen die Briefwahl durch ein ganz anderes System der Stimmabgabe, wenn Wähler am Wahltag verhindert sind: Sie haben das Prinzip der Wahlvollmacht im Wahlrecht verankert. Griechen wie Belgier praktizieren Wahlpflicht und verlangen von ihren Wählern, dass sie sich ohne Ausnahme ins Wahllokal begeben, um die Stimme abzugeben. Griechen wiederum müssen in die Wahllokale ihrer Geburtgemeinde, können also nicht dort wählen wo sie gerade wohnen. Wer nicht wählt, wird mit Bußgeld belegt. Nur wer gesundheitlich verhindert ist, kann mit ärztlichem Attest der Wahl fernbleiben. Berufliche Hinderungsgründe kann es in Griechenland nicht geben, da während der Wahl alle Betriebe schließen und die Nation in heftige Reisetätigkeit verfällt, die zudem vom Staat finanziert werden muß. Analysten schätzen, dass jede Wahl in Griechenland 1 - 2% des BSP kostet.

[141] Während ein Teil der Lehre sie als verfassungskonform und nicht gegen die Grundsätze der freien und geheimen Wahl verstoßend beurteilt (vgl. Schreiber 1997, BVerfGE Bd. 21 und Bd. 59, zur Problematik des Ansteigens der Briefwähler vgl. vor allem BverfGE Bd. 59), kritisiert ein anderer Teil sie als bedenklich.

Als Ausnahmeregelung konzipiert, wird die Möglichkeit der Briefwahl inzwischen von einem großen Anteil der Wahlberechtigten genutzt.[142]

7.2 Allgemeines Wahlrecht

7.2.1 Grundsatz

Dieser Grundsatz ist zwar nicht ausdrücklich genannt, ist aber aus Art 26 Abs. B- VG abzuleiten[143] und bedeutet, dass allen Staatsbürgern, die das Wahlalter erreicht haben, das Recht zusteht, zu wählen und gewählt zu werden. Das allgemeine Wahlrecht ist eine Ausgestaltung des Gleichheitssatzes im Wahlrecht. Verwirklicht ist es durch die grundsätzliche Zuerkennung des Wahlrechts an alle Staatsbürger ab einem bestimmten Alter. [144]

7.2.2 iVoting

Da dem Bürger durch eine Wahl über Internet eine zusätzliche Möglichkeit zur Wahlteilnahme eingeräumt wird, entspricht dies dem Grundsatz der Allgemeinheit. Der BverfG hat in seinem Erkenntnis zur Briefwahl festgestellt, dass der mit der Briefwahl verbundene staatliche Schutz- und Kontrollverlust nicht grundsätzlich zu beanstanden sei, da Wahrung von Wahlgeheimnis und Wahlfreiheit dem einzelnen Bürger anvertraut würden.

Die Möglichkeit der Internet-Wahl sollte jedoch, so wird in der Diskussion in Deutschland betont[145], wie schon bei der Briefwahl, von der vorherigen Glaubhaftmachung eines Verhinderungsgrundes abhängig. Die Wahl via Internet sollte nicht die Regel darstellen, sondern nur für diejenigen Wähler möglich sein, die am Wahltag an der Teilnahme an der Wahl verhindert sind.

---

[142] Bei den Bundestagswahlen 1994 hatten 6,4 Millionen oder 13,4 Prozent der Wähler ihre Stimme per Briefwahl abgegeben, bei ihrer Einführung im Jahr 1957 waren es nur 4,9 Prozent (FAZ vom 16.09.98: 1); In Verbindung mit der Höhe der Wahlbeteiligung zeigen diese Zahlen - wenn man vom Rückgang der Wahlbeteiligung bei den Bundestagswahlen 1990 und 1994 zunächst einmal absieht, für die sich auch andere Gründe anführen ließen -, daß das geltende Wahlrecht „in der Form der Kombination Urnen-/Wahlgeräte-/Briefwahl die Teilnahme an der politischen Willensbildung des Volkes durch Wahlen in bester Weise ermöglicht“ (Schreiber 1997: 480).

[143] Mayer, Heinz: Kommentar zum B-VG, Zi I.1. S. 162

[144] Walter/Mayer, Grundriss des österreichischen Bundesverfassungsrechts, 9, RZ 306

[145] Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen

Solange nicht alle Wählerverzeichnisse vernetzt sind, sollte ein vorheriger Antrag verfahrenstechnisch erforderlich bleiben, denn sonst würde ein entsprechender Hinweis im Wählerverzeichnis vor Ort fehlen und Doppelwahl wäre möglich: Internet-Wahl und traditionelle Stimmabgabe in die Wahlurne im Wahllokal[146].

Die technische Ausstattung (Chipkarte, Lesegerät, eventuell auch Broswer, Betriebssystem) verursacht Kosten. Hier stellt sich die Frage, wen die Kostentragungspflicht für die technische Ausstattung trifft. Sollte der Wähler die Kosten für die Ausstattung selber tragen müssen und würden diese Kosten zu einem Abschreckeffekt führen, könnte dies eine Verletzung des allgemeinen Wahlrechts bedeuten.

Die Möglichkeit von Internetwahlen würde das Prinzip des allgemeinen Wahlrechtes stärken, solange die dem Wähler entstehenden Kosten keinen Abschreckeffekt mit sich bringen.

7.3 Gleiches Wahlrecht

7. 3.1 Grundsatz

Diesem Grundsatz wird entsprochen, wenn alle Wähler mit der Stimme, die sie abgeben, den gleichen Einfluss auf das Wahlresultat haben (gleicher Erfolgswert), sodass das potentielle Gewicht jeder Stimme dasselbe ist.[147] Es darf also niemand eine doppelte Stimmabgabe vornehmen.[148]

[146] Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen

[147] (einschränkend Koja, ÖVA 1963, 159; VfSlg 1381, 3653, 6207; gleicher Zählwert); Einschränkungen des gleichen Erfolgswertes der abgegebenen Stimmen ergeben sich z.B. aus der im Art. 26 B- VG vorgeschriebenen Verteilung der Mandatszahl nach der Bürgerzahl (nicht nach der Zahl der Wahlberechtigten) und durch die Einteilung des Bundesgebietes in Wahlkreise, da schon zufolge der Unmöglichkeit einer vollkommen exakten Verteilung der (endlichen) Zahl der Mandate auf die Wahlkreise die Stimme in jedem Wahlkreis ein anderes Gewicht hat.

[148] Walter/Mayer, Grundriss, 9, RZ 307

7.3.2 iVoting

Dies bedeutet bei einer Wahl über Internet, dass der einzelne Wähler sich identifizieren muss, bevor er seine Stimme abgeben kann, um zu verhindern, dass ein Dritter statt seiner wählt oder dass seine Stimmen während der Übertragung geändert wird. Technisch kann dies durch den Einsatz digitaler Signaturen gelöst werden.[149] Der Wähler würde sein Wahl- Mail bzw. deren Hashwert mit seinem eigenen privaten Schlüssel verschlüsseln, die Entschlüsselung dieser Wahl- Mail zur Wahlauswertung erfolgt mit dem öffentlichen Schlüssel des Wählers.[150]
Technisch setzt das aber voraus, dass der Wähler über einen entsprechend zertifizierten Schlüssel und die dem Signaturgesetz entsprechende Hardware-Ausstattung (Lesegerät etc.) verfügt.

Die zweite Komponente dieses Wahlgrundsatzes bedeutet, dass allen Wahlvorschlägen gleiche Chancen eingeräumt werden müssen. Daher sind im Internet an den virtuellen Stimmzettel und die Bildschirmmaske dieselben Anforderungen zu stellen wie an den gedruckten Stimmzettel. Den Wahlvorschlägen muss jeweils derselbe Raum eingeräumt werden. Im Rahmen der Einheitlichkeit der Wahl darf es zu keinen Abweichungen zwischen dem gedruckten Wahlzettel des Wahlkreises und seinem elektronischen Pendant kommen. Auch muss sicher gestellt werden, dass die Entscheidung des Wählers bei einer Wahl mittels Verbindung im Internet unverfälscht die zentrale Auswertung erreicht. Nur so kann eine ordnungsgemäße Wahl durchgeführt werden. Wird das technisch nicht garantiert, ist eine Internet-Wahl unzulässig.

7.4 Unmittelbares Wahlrecht

7.4.1 Grundsatz

Die Wahlberechtigten müssen (damit der Wählerwiller verlässlich zum Ausdruck kommt) die Personen, die sie in den jeweiligen Vertretungskörper entsenden wollen,

[149] Siehe Kapitel 4.2
[150] Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen

selbst bezeichnen, ein Wahlmännersystem ist durch diesen Grundsatz ausgeschlossen.

7.4.2 iVoting

Dies ist keine Frage, die eine Briefwahl oder eine Wahl über Internet berührt, sondern eine Frage des Wahlverfahrens.

7.5 Freies Wahlrecht

7.5.1 Grundsatz

Damit sind der Grundsatz der „Freiheit der politischen Willensbildung und Betätigung“ und das Postulat der „Reinheit der Wahlen“[151], in deren Ergebnis der wahre Wille der Wählerschaft zum Ausdruck kommen soll[152], ausgesprochen. Die Wahlwerbung soll nicht sinnwidrig beschränkt[153] und der Wähler in der Freiheit seiner Wahl nicht in rechtlicher oder faktsicher Weise beeinträchtigt werden. Der Sicherung dieser Freiheit dienen die Strafbestimmungen der §§ 261 bis 268 StGB.[154]

7.5.2 iVoting

Werbeeinblendungen auf dem Bildschirm würden diesen Grundsatz verletzen.
Dem vom BVerfG bei der Briefwahl große Bedeutung zugemessenen Versicherung an Eides statt, dass der Wähler den Stimmzettel persönlich und unbeeinflusst ausgefüllt hat, könne, so betonen Befürworter einer Internet- Wahl in Deutschland, bei der Internet- Wahl durch die persönliche Signatur entsprochen werden.
Die Möglichkeit zur bewusst ungültigen Stimmabgabe müsste auch bei der Wahl via Internet gegeben sein.

[151] VfSlg 2936
[152] VfSlg 2037
[153] vgl. VfSlg 3000, 4527, 7821
[154] Walter/Mayer, Grundriss 9, RZ 311

7.6 Geheimes Wahlrecht

7.6.1 Grundsatz

Dieser Grundsatz verlangt, dass die Abgabe der Stimme stets in einer für die Wahlbehörde[155] und die Öffentlichkeit nicht erkennbaren Weg zu geschehen hat.

.

Im oben zitierten „Briefwahlerkenntnis“ vertritt der VfGH auch die Auffassung, dass der Verfassungsgrundsatz „den Staat zu positiven Leistungen (...) verpflichtet“; es seien alle erforderlichen Einrichtungen (Wahlzellen) zur Verfügung zu stellen. Die NRWO sichert diese Rechtsmeinung des VfGH durch das Vorschreiben der Abgabe der Stimme in einer Wahlzelle und der Abgabe der Stimmzettels in undurchsichtigen Kuverts.

7.6.2 iVoting

Die Situation in Deutschland zeigt jedoch, dass bei vergleichbarer Rechtslage[156] auch eine im Vergleich in Österreich andere Interpretation des geheimen Wahlrechtes in Zusammenhang mit einer Briefwahl möglich ist und somit auch in weiterer Folge bei einer Internet- Wahl denkbar wäre.
Nach der Rechtsprechung des BVerfG kommt dem Wahlberechtigten selbst die Verantwortung für die Einhaltung des Wahlgeheimnisses zu.

Zum Schutz der Beförderung von Briefen besteht der strafrechtliche Schutz des Briefgeheimnisses[157] gemäß § 118 StGB[158] . Diese Regelungen des StGB sind

[155] zB VfSlg 10.908, 11.738
[156] vgl. Art 38 I GG
[157] Verfassungsrechtlicher Schutz des Briefgeheimnisses in Art. 10 StGG, RGBl. Nr. 142/1867, Art. 10 MRK, BGBl. Nr. 210/1958.
[158] § 118. (1) Wer einen nicht zu seiner Kenntnisnahme bestimmten verschlossenen Brief oder ein anderes solches Schriftstück öffnet, ist mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (2) Ebenso ist zu bestrafen, wer, um sich oder einem anderen Unbefugten Kenntnis vom Inhalt eines nicht zu seiner Kenntnisnahme bestimmten Schriftstücks zu verschaffen, 1. ein verschlossenes Behältnis, in dem sich ein solches Schriftstück befindet, öffnet oder 2. ein technisches Mittel anwendet, um seinen Zweck ohne Öffnen des Verschlusses des Schriftstücks oder des Behältnisses (Z. 1) zu erreichen. (3) Ebenso ist zu bestrafen, wer einen Brief oder ein anderes Schriftstück (Abs. 1) vor Kenntnisnahme durch den Empfänger unterschlägt oder sonst unterdrückt. (4) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen. Wird die Tat jedoch von einem Beamten in Ausübung seines Amtes oder unter Ausnützung der ihm durch seine Amtstätigkeit

analog auch auf elektronische Post und somit auch auf ein Wahlmail anwendbar. Voraussetzung ist jedoch, dass diese verschlüsselt ist, da nur eine verschlüsselte eMail als verschlossener Brief gesehen werden kann.
Zur Einhaltung des geheimen Wahlgrundsatzes ist weiters erforderlich, dass kein Rückschluss auf das Wahlverhalten des einzelnen Wählers möglich ist.
Die Verwendung von kryptographischen Methoden trägt zur Einhaltung dieses Grundsatzes bei Wahlen über Internet bei.

Eine Einflussnahme, insbesondere in bestehenden Anhängigkeitsverhältnissen, wird wohl ausser bei der Wahl in der Wahlzelle nie ausgeschlossen werden können.

„Wie bei der Briefwahl kann jedoch weder die Freiheit vom Einfluss Dritter bei der Stimmabgabe noch die Geheimhaltung (der Blick über die Schulter auf den Bildschirm bei der Stimmabgabe) staatlich gewährleistet werden. Diese Defizite sprechen dafür, auch in Zukunft am Vorliegen bestimmter Verhinderungsgründe für die Distanzwahl außerhalb des Wahllokals festzuhalten.“[159]

7.7 Persönliches Wahlrecht

7.7.1 Grundsatz

Die Abstimmung hat, um die Verfälschung des Wählerwillens hintanzuhalten, durch persönliche Stimmabgabe des Wahlberechtigte selbst zu geschehen; die Wahl durch Stellvertreter ist ausgeschlossen sind. [160] Der VfGH und Teile der Lehre sehen durch diesen Wahlgrundsatz die Briefwahl ausgeschlossen.

In der österreichischen Lehre werden unterschiedliche Akzentuierungen des persönlichen Wahlrechtes vertreten. Dass die Wahl durch Stellvertreter

---

gebotenen Gelegenheit begangen, so hat der öffentliche Ankläger den Täter mit Ermächtigung des Verletzten zu verfolgen.
[159] Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen in Multimedia & Recht, abrufbar unter <http://www.i-vote.de/projekt/index.html>
[160] Walter/Mayer, Grundriss 9, RZ 309

ausgeschlossen ist, ist unbestritten[161]. Nach einer weitergehenden Meinung verbiete das Prinzip der persönlichen Wahlrechts nicht nur die Wahl durch Stellvertreter, sondern wird eine zweite unverzichtbare Wesenskomponente dieses Prinzips in der persönlichen Anwesenheit des Wahlwilligen im Stimmlokal erblickt.

Der Grundsatz des persönlichen Wahlrechts erstreckt sich aber nach auch auf andere Wahlentscheidungen, wie z. B. das Unterschreiben eines Wahlvorschlages[162] oder die Zustimmung zur Aufnahme in einen Wahlvorschlag[163].

7.7.2 iVoting

Durch den Einsatz digitaler Signaturen könne, so wird in der Diskussion in Deutschland betont, diesem Grundsatz entsprochen werden.

7.8 Verhältniswahlrecht

Verhältniswahlrecht besteht- im Gegensatz zum einfacheren (übersichtlicheren) Mehrheitswahlrecht und im Gegensatz zum Minderheitswahlrecht darin, dass alle politischen Kräfte von zahlenmäßig erheblicher Bedeutung eine Vertretung im Parlament nach Maßgabe ihrer Stärke gesichert haben.

7. 10 Conclusio

Bei der Vereinbarkeit zwischen Verfassungsrecht und iVoting ist auf die Feststellungen zu der Thematik Briefwahl und Verfassungsrecht[164] zu verweisen, da es auf eine Abwägung zwischen dem allgemeinen Wahlrecht auf der einen Seite und dem geheimen und persönlichen Wahlrecht auf der anderen Seite hinausläuft.

---

[161] Adamovich, Grundriß des österr. Staatsrechts, 1927, 134; Frisch, Lehrbuch des österr. Verfassungsrechts, 1932, 76, Adamovich/ Spanner, Handbuch des österreichischen Verfassungsrechts, 5. Auflage, 1957, 166

[162] VfSlg 5166

[163] VfSlg 2037

[164] Siehe Kapitel 5

Zusätzlich ist jedoch in die verfassungsrechtliche Beurteilung die technische (Sicherheits-) Komponente mit ein zu beziehen.
Aufgrund der großen Bedeutung des Wahlrechts als wichtigstes politisches Grundrecht sollte nicht leichtfertig damit umgegangen werden.
Andererseits sollte man den Bereich eVoting von öffentlicher Seite keinesfalls weiterhin links liegen lassen und eine Forschungsgruppe nach dem Vorbildern in Deutschland bzw. der Schweiz andenken, die auch mit der Koordination bzw, Durchführung von Testwahlen betraut werden sollte.
Die Österreichische Hochschülerschaft, bzw. vorerst einzelne überschaubare Einheiten dieser würden sich aufgrund der geltenden Rechtslage für eine Testwahl anbieten.

Exkurs: Hochschülerschaftsgesetz (HSG) - Novelle 2001

Mit einer Novelle des Hochschülerschaftsgesetzes 1973[165], die mit 1. 2. 2001 in Kraft getreten ist, wurde die Möglichkeit der Durchführung der ÖH- Wahlen mittels elektronischer Datenübertragung geschaffen[166].

Die Entscheidung, ob ein elektronisches Verfahren zum Einsatz kommt, obliegt gem. § 48 HSG der bzw. dem für Wissenschaft zuständigen Bundesminister in Verordnungsform[167].

Geplant sind zwei Stufen der elektronischen Wahl: vorerst soll in speziell geschaffenen Wahlterminals in den universitären Räumlichkeiten die Möglichkeit der elektronischen Stimmabgabe gegeben sein. Im Endausbau soll Studierenden der österreichischen Universitäten, die zum Zeitpunkt der Wahl im Ausland studieren, die Möglichkeit der elektronischen Stimmabgabe ermöglicht werden.

[165] BGBl 18/2001
[166] Gemäß der Judikatur des Verfassungsgerichtshofes (vgl. zB. Erkenntnis vom 29. Februar 1996, W I-2/95) werden bei Wahlen zu Berufsvertretungen nicht die gleichen strengen Anforderungen an das persönliche und geheime Wahlrecht, wie bei Wahlen zu allgemeinen Vertretungskörpern gestellt
[167] Wobei in § 34 relativ genaue Vorgaben für ein einzusetzendes Wahlverfahren vorsieht.

Im Falle der Durchführung der Wahlen auf elektronischem Wege sieht § 34 Abs. 4 HSG sieht vor, dass das zum Einsatz kommende System den Sicherheitsanforderungen sicherer elektronischer Signaturen gemäß dem Signaturgesetz entsprechen muss und unter Berücksichtigung der Anforderungen des Datenschutzgesetzes 2000 an die Datensicherheit so ausgestaltet sein muss, dass die Einhaltung der Grundlagen des § 34 Abs 1 HSG [168] gewährleistet ist.

Der Konzeption des Signaturgesetzes und der Signaturverordnung folgend wurde im HSG keine genaue Determinierung der einzusetzenden technischen Komponenten aufgenommen worden ist. Um eine flexible Anpassung an technische Entwicklungen zu ermöglichen, soll die genaue Determinierung in der Wahlordnung erfolgen.

[168] § 34 Abs 1 sieht vor, sind ÖH- Wahlen auf Grund des „allgemeinen, gleichen und geheimen Verhältniswahlrechts gesondert für jedes dieser Organe durchzuführen. Das Wahlrecht ist persönlich auszuüben“

8.Informelle Gewaltenteilung: Juristische Anforderungen an ein Wahlsystem

8.1 System der „informellen Gewaltenteilung“[169]

Neben der richtigen Auszählung der Stimmen hat eine elektronisches Wahlsystem die Identifizierung des Wahlberechtigten vorzunehmen. Gleichzeitig muss dieses System die Rückverfolgung der Wählentscheidung unmöglich machen, also das Wahlgeheimnis wahren. Hinzu kommt noch der größtmögliche Schutz vor Cyberterrorismus.

Von der Forschungsgruppe Internetwahlen an der Universität Osnabrück wurde das System der Informellen Gewaltenteilung entwickelt, das einer näheren Betrachtung[170] lohnt.

Bei diesem System kommen drei verschiedene Instanzen, die jedoch logisch und physisch strikt voneinander getrennt sind, zum Einsatz:

- Zertifikatoren digitaler Signatur,
- Validatoren der Wahlaufsicht und
- Psephoren (öffentliche Urnen).

Um einen manipulativen Eingriff in das Wahlgeheimnis und das Wahlergebnis auszuschließen, verfügen diese drei Einheiten über keine gegenseitigen Zugriffsmöglichkeiten.

8.1.1 Zertifikatoren

Die Aufgabe dieser Einheit besteht in der Feststellung der Identität der wahlwilligen Person. Dies erfolgt durch die Überprüfung der digitalen Signatur.

[169] http://www.i-vote.at,
[170] Dies auch aufgrund der Tatsache, weil in der Ausarbeitung der HSG- Novelle am Modell von i-vote „Anleihe“ genommen worden ist.

Ein Wähler benötigt, um sein Wahlrecht über Internet ausüben zu können, eine digitale Signatur. Es gibt hier zwei Möglichkeiten: entweder der Wahlberechtigte erhält ein eigenes Zertifikat (mit Signatur) für die Wahl oder es wird auf bestehende Zertfizierungs- und Registierungsdienste zurückgegriffen.[171] Die Anforderungen an einen Zertifikator ergeben sich insbesondere aus dem Signaturgesetz.
Für Österreich ist hier auf das Projekt Bürgerkarte.at[172] zu verweisen, dessen Ziel eine universelle Karte für eGovernment- Dienste, insbesondere als Sozialversicherungskarte, darstellt.
Auch an einigen Universitäten gibt es Bestrebungen, Studierendenausweise in Chipkartenform, die auch eine Signaturfunktion haben, einzuführen.

8.1.2 Validatoren

Die Überprüfung der Wahlberechtigung erfolgt durch Abgleich mit dem elektrischen Wählerverzeichnis auf dem Server des Wahlvorstandes, dem Validator.

Alle Wahlvoten werden signiert und mit einem 1024- Bit- Schlüssel verschlüsselt. Über das Netz soll nur versendet werden, was nicht verschlüsselt werden muss. Zum Psephor gelangen nur die Sendungen mit den Voten, alle Hinweise auf die Wählerperson sowie zur IP werden eliminiert. Die Verschlüsselung der Voten erfolgt, um Manipulation und vorzeitige Auswertung im Urnenserver zu verhindern. Die Kommunikation mit dem Validator, die zur Überprüfung der Wahlberechtigung Angaben zur Identifizierung enthalten muss, erfolgt mit blinder Signatur.

Nach Feststellung von Identität, Wahlberechtigung und Wahlstatus wird der Zugang zur Wahl freigegeben und dem Wähler den Stimmzettel in Form einer Website aus. Das System sollte Fehler des Wählenden erkennen und erst wenn dieses der Bestätigungsknopf drückt, sollte der Stimmzettel in die Urne geschickt werden. Ungültiges Wählen muss möglich sein. Der Stimmzettel wird, bevor er verschickt wird, verschlüsselt. Der solcherart verschlüsselte Stimmzettel wird zum Wahlausschuss/Wahlkommission geschickt, von dessen Server mit dem Schlüssel der Wahlkommission blind signiert und zurückgesendet.

[171] vgl. auch Menzel, E-Voting an österreichischen Hochschulen, 287

8.1.3 Psephor

Das Votum gelangt völlig anonym zum Urnenserver.
Im Psephor werden die Stimmen „geschüttelt“, damit die ´Stimmen nicht in der Reihenfolge des Einlangens aufgezeichnet werden, sondern zufällig.

Sobald die Stimme beim Psephor eingeht, wird sich auf gewählt gesetzt. Sollte aus irgendeinem Grund die Kommunikation vorher abbrechen, kann der Wählende neu aufsetzen. Sollte die Verbindung komplett abbrechen, muss der Wähler noch die Möglichkeit haben, die Stimme in der Wahlzelle abgeben zu können.

Nach Ende der Wahl sendet der Psephor die Urne verschlüsselt an die jeweilige Wahlkommission, die Auszählung erfolgt automatisch. Jeder Wähler hat auch noch die Möglichkeit, mit einer Kontrollnummer die Auszählung seines Votums zu kontrollieren.

8.1.4 Sonstige Anforderungen

Zur Minimierung von Sicherheitsrisken werden bei i-Vote zusätzlich folgende Maßnahmen getroffen.

8.1.4.1 Redundanter[173] Sicherheitsaufbau

Damit eventuelle Denial of Service Attacken[174] nicht erfolgreich sein können, sollten die elektronisch geführten Stimmlokale so ausgerüstet sind, dass die Wahlgeräte selbst bei Totalausfall des Internets die Rolle der Rückhaltsysteme übernehmen und das sichere Wählen auch offline garantieren können.

---

[172] Siehe http://www.buergerkarte.at
[173] Redundanz im Bereich der Datenhaltung wird auch als Datenspiegelung bezeichnet. Dabei werden mehrere Festplatten zu einem Laufwerk verknüpft. Für den Rechner erscheint das gesamte Subsystem wie eine einzige Platte. Da die Daten aber intern redundant gehalten werden, entsteht bei Ausfall eines Systems kein Datenverlust, und der Betrieb kann störungsfrei fortgesetzt werden. (Raepple, Sicherheitskonzepte für das Internet, 2, 274)
[174] Denial of service Attacken sind Attacken, die sich gegen die Verfügbarkeit eines Systems und seine Anwendungen richten . (Raepple, Sicherheitskonzepte für das Internet, 2, 274)

Sollte ein Psephor ausfallen oder manipuliert werden, würde in diesem Fall nur die Wahl im Bereich des manipulierten Psephors nachgeholt werden müssen.

8.1.4.2 Betriebssystem, Browser

Die Forschungssgruppe Internetwahlen hat eine eigenes Betriebssystem und einen eigenen Wahlbrowser entwickelt.
Das Betriebssystem hat das nur vier Funktionen: Wahlbrowser starten, mit dem Internet verbinden, Modems, ISDN- Karten oder ADSL- Schnittstellen treiben/schließen und digitale Signatur lesen.
Der Browser hat zwei Funktionen: die Verbindung mit dem Wahlserver herstellen und wieder zu beenden.

8.2 Conclusio

Das Wahlsystem i-vote[175] wirkt zwar auf den ersten Blick sehr kompliziert, aber vom Aufbau scheint es grundsätzlich geeignet, um es zumindest für Testwahlen heranzuziehen.

[175] Siehe auch Wahlsimulator auf der Website des Projektes http://www.i-vote.de/projekt/index.html

9. Mögliche Strategien/ Zusammenfassung

- Die Einführung von eVoting bei Wahlen zu allgemeinen Vertretungskörpern kann nur in Form einer Änderung der Bundesverfassung erfolgen.

- iVoting soll keinen Ersatz der Wahl in der Wahlzelle darstellen, sondern nur eine Ausnahme, die als Voraussetzung die Glaubhaftmachung eines Verhinderungsgrundes bedarf.

- Bei der Beurteilung der Frage der Zulässigkeit von iVoting hat der Verfassungesgesetzgeber eine Abwägung zwischen dem geheimen und dem persönlichen Wahlgrundsatz auf der einen Seite und dem allgemeinen Wahlgrundsatz auf der anderen Seite zu treffen. Die (sicherheits-) Technische Komponente hat aber ebenfalls in der Beurteilung Berücksichtigung zu finden.

- Die Zulassungsvoraussetzungen für etwaige einzusetzende Wahlsysteme und – geräte bedürfen einer positivrechtlichen Verankerung. Unabhängig von der durch die Weiterentwicklung der Technik notwendigen Flexibilität der Regelung sind die grundsätzlichen Mindestanforderungen an ein elektronisches Wahlsystem gesetzlich zu regeln. In dieser Bestimmung sind die Grundsätze der Wahlen auch für die elektronische Durchführung explizit zu normieren.

- Die Verwendung digitaler Signaturen und der Aufbau von „Public Key Infrastructure“ sind beides Grundvoraussetzungen für eVoting. Zum gegenwärtigen Zeitpunkt bereiten diese jedoch noch erhebliche technische und organisatorische Probleme.

- Wahlen über Internet stellen jedoch im Moment noch ein zu großes Risiko für das Wahlverfahren dar und sollten bei Wahlen zu allgemeinen Vertretungskörpern nicht zum Einsatz kommen, bis nicht Fortschritte in substantiellen technischen und sozialwissenschaftlichen Themen erreicht sind.

- Technische Sicherheitsprobleme, die derzeit (noch?) bestehen, sollten nicht dazu führen, dass man sich dem Diskussionsprozess im Bereich der elektronische Wahlen verschließt. Eine Forcierung des Themas kann generell zu einer Erhöhung der Netzsicherheit führen.

- Die Einsetzung einer interdisziplinären Forschungsgruppe unter Einbeziehung von Wissenschaftlern und Mitgliedern von Wahlbehörden wäre ein ratsamer Ansatzpunkt für die Forcierung des Themas in Österreich. Diese Arbeitsgruppe sollte mit konkreten Aufgaben betraut und ihr sollten konkrete Ziele gesetzt werden.

- Die sozio- kulturellen (die Zugangsmöglichkeiten unterschiedlicher Bevölkerungs- und damit Wählergruppen zum Internet)[176] und die inhaltlich-motivationalen Komponenten (die Bereitschaft der Bürger, Gebrauch von den neuen Möglichkeiten der Stimmabgabe zu machen) des elektronischen Wählens dürfen neben technischen und juristischen Fragestellungen nicht vernachlässigt werden dürfen.

- Der Kostenfaktor muss von Anfang an mitbedacht werden und als einer der Entscheidungsgründe mitbedacht werden. Die Kosten, die der Wahlberechtigte zu tragen hat (Chipkarte, Lesegerät), dürfen auf keinen Fall einen abschreckenden Effekt haben.

- Ein Stufenplan, der auch Testwahlen berücksichtigt, sollte ausgearbeitet werden:
- Für eine Testwahl bieten sich vorerst kleine Einheiten innerhalb der österreichischen Hochschülerschaft an.
- In einer weiteren Phase könnte die Einführung eines zentralen Online-Wählerverzeichnisses angedacht werden. Diese würde die Wahlkartenwahl (im Inland) ersetzen.
- Der Einsatz von neuen Technologien bei direktdemokratischen politischen Rechten könnte eine weitere Maßnahme darstellen.

Literaturverzeichnis

Aichholzer, Schmutzer, E- Government, Elektronische Informationsdienste auf Bundesebene in Österreich, Endbericht, Studie im Auftrag des Bundeskanzleramtes , Juli 1999, Wien, Institut für Technikfolgen-Abschätzung der österreichischen Akademie der Wissenschaften

Adamovich, Grundriß des österreichisches Staatsrechts, 1927,

Adamovich, Funk: Österreichisches Verfassungsrech t3 (1997)

Brenn, Signaturgesetz, Wien, 1999

Chaum, Security without Identification- Card Computers to make Big Brother obsolete, Extendes and reversed version: Informatik- Spektrum, vol.10, 262-277 1987;

Chaum,Rivest, Sherman (Hrsg): Advances in Cryptology: Proceedings of CRYPTO '82. Plemum, New York, 1983 abrufbar unter: http://dblp.uni-trier.de/db/conf/crypto/

Dujmovits, Auslandsösterreicherwahlrecht und Briefwahl, Wien, 2000

Federrath, Pfitzmann, Datenschutz und Datensicherheit, in: Schneider, Werner, Taschenbuch der Informatik, Leipzig 2000: S. 587 ff

Fischer, Die Reform der Nationalratswahlordnung, 1992, ÖJP `92 (1993), 341 (335 f),

Forgo, Was sind und wozu dienen digitale Signaturen in ecolex 1999, 235,

Forschungsgruppe Internetwahlen http://www.i-vote.de/projekt/index.html>

Fujioka, Okamoto, Ohta, A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, Advances in Cryptology -- AUSCRYPT '92*,* volume 718 *of* Lecture Notes in Computer Science*,* pages 244-251, Gold Coast, Queensland, Australia, 13-16 December 1992. Springer-Verlag., <http://theory.lcs.mit.edu/~dmjones/hbp/auscrypt/auscrypt92.html>

Gisler, Spahnli, eGovernment- Eine Standortbestimmung, 2, Bern, 2001

Holzinger, in Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht (1999), Rz 39 zu Art 26 B-VG

Internet Policy Institute, Report in the National Workshop on Internet Voting, Washington 2001

Interuniversitäres Institut für interdisziplinäre Forschung und Fortbildung (IFF),_Abteilung Politische Bildung, http://polbil.uibk.ac.at/pat/iud/wos

Kubicek, Wind, Wie modernisiere ich Wahlen? Der lange Weg vom Pilotprojekt zum Online- Voting bei einer Bundestagswahl, siehe in: <http://polbil.uibk.ac.at/pat/iud/wos/0003.htm>

Leggewie, Netizens oder: der gut informierte Bürger heute. Ein neuer Strukturwandel der Öffentlichkeit? Chancen demokratischer Beteiligung im Internet - anhand US-amerikanischer und kanadischer Erfahrungen, Bonn 1996

Menzel, Evoting an österreichischen Hochschulen, in Schweighofer, Menzel, Kreuzbauer (Hg.) Auf dem Weg zur ePerson , Schriftenreihe Rechtsinformatik Bd. 3, S.283

Merkl, Zbl 1921, 603 ff.

Möller, „e-Politik“ - Was bringt das Netz der Demokratie?, http://orae.fes.de:8081/fes/docs/WEST_UND_SUEDEUROPA/E-POLITIK2%20MOELLER.HTM,

Neisser/Handstanger/Schick, Bundeswahlrecht, 2, (1994)

Nowak, Politische Grundrechte (1988), 331 f 356 f.

Nowak/Strejcek, Das Wahl- und Stimmrecht, in Machacek/Pahr/Stadler (Hrsg), Grund- und Menschenrechte in Österreich, Band III (1997), 1 (21)

Plate, Henning, "Internet und Intranet" in „Taschenbuch der Informatik", S 710 f

Posch, Bürgerkarte- elektronischer Ausweis im Netz, http://www.buergerkarte.at/Buergerkarte

Raepple, Sicherheitskonzepte für das Internet, 2, Heidelberg, 2001

Rüß, Wahlen im Internet: Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen in Multimedia & Recht, abrufbar unter http://www.i-vote.de/projekt/index.html

Schäffer, Die Briefwahl (1979)

Schäffer, Verfassungsinterpretation in Österreich (1971)

Schönberger/Pilz/Reiser/Schmölzer, Sicher & echt: Der Entwurf eines Signaturgesetzes in MR 1998, 107

Schweighofer, Menzel (Hg), E- Commerce und E- Government- Aktuelle Fragestellungen des Rechtsinformatik, Schriftenreihe Rechtsinformatik, Band 1, Wien, 2000

Seidler, „Schilys Visionen: Deutschlands Weg zur Online- Wahl", in: Spiegel Online, 3. Mai 2001 <http://www.spiegel.de/politik/deutschland/0,1518,131673,00.htm>

Singh, The Code Book, The Secret History of Codes and Code- Breaking, London 1999

*Strejcek***,** Zur Neuregelung der Stimmabgabe im Ausland durch die Nationalrats- Wahlordnung 1992, ZfV 1993, 431

Stomper, „Hürdenlauf zum Online- Urnengang", in Homepages 1/2001, 11

Wagner, Unbefugter Zugriff auf e-mail, ecolex 2000, 273