

Rechtsgrundlage zur elektronischen Wahl

Thomas Menzel

*Arbeitsgruppe Rechtsinformatik
Institut für Rechtsvergleichung, Universität Wien
A-1010 Wien, Schottenbastei 10-16
thomas.menzel@univie.ac.at*

Schlagnote: E-Voting, elektronische Wahl, Hochschülerschaftswahl, elektronische Signatur, e-Democracy, e-Government

Abstract: Mit der Novelle 2001 zum Hochschülerschaftsgesetz wurden in Österreich erstmals die rechtlichen Grundlagen für elektronische Wahlen zu einem gesetzlich eingesetzten, öffentlich-rechtlichen Vertretungskörper geschaffen. Im Beitrag sollen diese gesetzlichen Rahmenbedingungen vorgestellt und näher erläutert werden.¹

1. Entstehungsgeschichte

Von Seiten der Österreichischen Hochschülerschaft wurde im Begutachtungsverfahren zur HSG-Novelle 2001 der Wunsch vorgebracht, eine Möglichkeit für die Durchführung der Wahl auf elektronischem Weg zu schaffen, um wie bei anderen Vertretungskörpern Wahlen dezentral durchführen zu können. Dadurch soll der Zugang der Wahlberechtigten zur Stimmabgabe erleichtert werden. Dies soll einerseits dazu beitragen, die Wahlbeteiligung zu erhöhen, andererseits soll die demokratische Legitimation der gewählten Vertretung auf diese Weise gestärkt werden.

Insbesondere für die Durchführung der Wahlen an teilweise dislozierten Bildungseinrichtungen mit wenig Studierenden soll damit auch eine Erleichterung bei der Durchführung der Wahlen dadurch geschaffen werden, dass die Aufgaben der Wahlkommissionen mit weniger Aufwand wahrgenommen werden können.

¹ Da die Änderung im Rahmen eines durch Abgeordnete zum Nationalrat eingebrachten Abänderungsantrags erfolgte, sind die Erläuterungen zu diesen neuen Bestimmungen nur in den stenographischen Protokollen des Nationalrats (St Prot des NR, XXI. GP, 56. Sitzung, S 202-209 zu finden. Um diese auch einer breiteren Leserschaft zur Verfügung zu stellen, sollen in diesem Beitrag nach einer Beschreibung der neuen gesetzlichen Regelungen auch die erläuterten Bemerkungen, die der Autor als Textvorschlag für den Abänderungsantrag erstellt hat, vorgestellt werden.

2. Zentrale Rechtsgrundlage

Zentrale Rechtsgrundlage für e-Voting an den österreichischen Hochschulen ist hier die Neugestaltung des § 34 HSG², der in einer technologie-neutralen Formulierung die Grundlagen für eine Ausdehnung des Wahlsystems auch auf die elektronische Stimmabgabe ermöglicht. Dabei ist durch das eingesetzte Verfahren die Einhaltung folgender Grundsätze zu garantieren:

- Den Sicherheitsanforderungen sicherer elektronischer Signaturen gemäß dem Signaturgesetz und den Anforderungen des Datenschutzgesetzes 2000 muss entsprochen werden.
- Die Wahrung des Wahlgeheimnisses muss durch Methoden gewährleistet werden, die garantieren, dass die ausgefüllten Wahlformulare anonymisiert und nicht rückverfolgbar bei den Wahlkommissionen zur Auszählung gelangen.
- Die Verifikation der Identität des Stimmberechtigten ist durch die Wahlkommission vor Übermittlung des leeren Wahlformulars durchzuführen, damit die Stimmabgabe durch Nichtberechtigte und die Abgabe mehrerer Stimmen durch eine Person ausgeschlossen ist.
- Die Unverfälschtheit des ausgefüllten Wahlformulars ist durch den Einsatz sicherer elektronischer Signaturen garantiert.
- Die Geheimhaltung der Wahldaten während der Übertragung zur Wahlkommission wird durch Verschlüsselung dieser Daten erreicht.
- Eine grundsätzliche Anforderung an elektronische Wahlsysteme betrifft die Normierung, dass die Wahlkommission die Möglichkeit haben muß, alle ihr in diesem Gesetz übertragenen Aufgaben auch hinsichtlich der elektronischen Stimmabgabe durchführen zu können.
- Weiters ist durch das elektronische Wahlsystem gleicher Übereilungsschutz bei der Stimmabgabe und sind hinsichtlich der Funktionalität der Wahlkioske an den Universitäten die Anforderungen an den Sichtschutz zu gewährleisten.

Die Einhaltung dieser im Gesetz grundsätzlich normierten Anforderungen ist durch eine in der Hochschülerschaftswahlordnung³ nähere Determination des elektronischen Wahlsystems zu erreichen. Die konkrete

² BGBl I 22/1999 idF BGBl I 18/2001.

³ Gegenwärtig ist die Anpassung der Hochschülerschaftswahlordnung (BGBl II Nr 122/2001) noch nicht erfolgt. Vor Erlass der an ein elektronisches Wahlsystem angepassten Verordnung ist der Datenschutzrat anzuhören.

Sicherheitsüberprüfung der eingesetzten technischen Komponenten muss von einer Bestätigungsstelle gemäß § 19 Signaturgesetz bestätigt werden.

Flankiert werden diese Ziele noch durch Regelungen über die elektronische Verlautbarung der Wahlvorschläge, technische Beratung der Wahlkommission durch eine Bestätigungsstelle und Möglichkeiten zum Abbruch der Wahl bei Beeinträchtigung der eingesetzten technischen Komponenten.

3. Wegfall der Unmittelbarkeit

Gemäß der Judikatur des Verfassungsgerichtshofes⁴ werden bei Wahlen zu Berufsvertretungen nicht die gleichen strengen Anforderungen an das persönliche und geheime Wahlrecht wie bei Wahlen zu allgemeinen Vertretungskörpern (Nationalrat, Landtag, etc.) gestellt. Dies ermöglicht die Einführung der Briefwahl oder eben auch der elektronischen Stimmabgabe. Die Briefwahl wurde in einigen Wahlordnungen schon berücksichtigt.

§ 46 Abs 2 Arbeiterkammer-Wahlordnung⁵ ordnet beispielsweise an, dass die oder der Wahlberechtigte den Stimmzettel unbeobachtet und unbeeinflusst auszufüllen hat, so bei Briefwahl nicht in der Wahlzelle geschieht. Diese Verpflichtung des Wählers gilt auch für die elektronische Wahl und ist durch das von ihm gesetzte Verhalten sicherzustellen. Die Stimmabgabe an Wahlterminals stellt dies genauso sicher wie die Stimmabgabe mittels Briefwahl.

Ebenso sieht § 22 der Bundes-Personalvertretungs-Wahlordnung⁶ für Wahlen dieser Personalvertreter die Möglichkeit der Briefwahl vor.

Im eingeschränkten Anwendungsbereich der Stimmabgabe im Ausland durchbricht auch § 60 NRW das Unmittelbarkeitsgebot, indem er unter gewissen Auflagen die Briefwahl zulässt.

4. Technologieneutralität

In § 34 HSG wurde – der Konzeption des Signaturgesetzes und der Signaturverordnung folgend - keine genaue Determinierung der einzusetzenden technischen Komponenten aufgenommen. Da sich diese rasch ändern können, soll die genaue Determination in der Wahlordnung erfolgen,

⁴ Erkenntnis vom 29. Februar 1996, W I-2/95.

⁵ BGBl II 340/1998.

⁶ BGBl 215/1967 idF BGBl II 294/1999.

die leichter an Weiterentwicklungen der Technik anpassbar ist. Die Verordnungsmächtigung zur eingesetzten Technik, die beim System anzuwenden ist, stellt eine Anpassung der Sicherheitsaspekte an den sich rasch ändernden Stand der Technik sicher. Die zukünftige Verwendung neuer, sicherheitstechnisch durchaus sinnvoller Komponenten würde zwangsläufig zu Gesetzeswidrigkeit führen. Zur Sicherung des Qualitätsstandards wurden allgemeine Bedingungen festgelegt, die jedenfalls von den eingesetzten technischen Komponenten zu erfüllen sind. Damit ist gewährleistet, dass alle Funktionen, die Datenschutz und grundlegende Prinzipien an eine Wahl stellen, auch durch das eingesetzte System gewährleistet sein müssen.

5. Prüfung nach dem Stand der Technik

Um ein hohes Sicherheitsniveau zu erreichen, sind die eingesetzten Komponenten auf ihre Qualitätsaspekte hinsichtlich des Einsatzes vertrauenswürdiger Sicherheitstechnologie zu überprüfen. Bestätigungsstellen führen diese Aufgabe im Rahmen des Signaturgesetzes bereits durch. Ihr Know How bezüglich der Evaluation von IT-Sicherheitstechnik, technische Hilfestellung im Bereich der IT-Sicherheit für öffentliche Einrichtungen und internationale Forschungstätigkeit in diesem Bereich gewährleisten auch die Qualität der von ihr als geeignet anerkannten Komponenten. Besonders schützenswert sind die bei der Wahlkommission eingesetzten Systeme, da hier alle Wahldaten zusammenlaufen, und die unmittelbar zum Wahlvorgang benötigten Komponenten am Rechner des Wählers (Wahlsoftware, Komponenten zur Verifikation der Identität zum Einsatz der sicheren elektronischen Signaturen, Bürgerkarte, elektronischer Studierendenausweis). Alle diese Komponenten müssen daher auf offengelegten Standards beruhen, die von einer Bestätigungsstelle überprüft werden können. Nicht so hohe Anforderungen müssen an die restlichen Komponenten der privaten PCs des Wählers gestellt werden. So ist es unverhältnismäßig, zum Beispiel für die einmalige Stimmabgabe alle zwei Jahre ein besonderes, eigens zertifiziertes Betriebssystem am Gerät des Wählers vorzuschreiben. Hier reicht die Sicherheit, die auch für den Einsatz des elektronischen Studierendenausweises und der Bürgerkarte vom Heim-PC vorgesehen ist.

6. Verweis auf Signaturgesetz

§ 18 Abs 2 Signaturgesetz definiert für die sichere elektronische Signatur, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorganges dargestellt werden müssen. Sollte bei der Stimmabgabe ein System eingesetzt werden, welches das ausgefüllte Stimmformular zuerst verschlüsselt und danach den Signaturvorgang auslöst, ist eine sinnvolle Darstellung der Wahldaten unmittelbar vor dem Signieren nicht möglich, da nur mehr die nicht sinnvoll lesbaren verschlüsselten Daten dargestellt würden. Deswegen werden nur die gleichen Sicherheitserfordernisse und nicht die gleichen Anforderungen wie bei sicheren elektronischen Signaturen normiert. Abgesehen von dieser nötigen Ausnahme sollen alle Anforderungen an sichere elektronische Signaturen, die der Wahrung der Verifikation der Identität und der Authentizität dienen, erfüllt werden.

Insbesondere dient der Einsatz sicherer elektronischer Signaturen der Verwirklichung des Grundsatzes des persönlichen Wahlrechts. § 2 Z 2 Signaturgesetz definiert sichere elektronische Signaturen als ausschließlich dem Signator zugeordnet. Sie ermöglichen die Identifizierung des Signators und werden mit Mitteln erstellt, die der Signator unter seiner alleinigen Kontrolle halten kann. Diese Sicherstellung der Verifikation der Identität des Wählers durch den Einsatz sicherer elektronischer Signaturen bei der Abgabe des Wahlformulars in Verbindung mit der in Abs 5 Z 6 normierten Verpflichtung der oder des Wahlberechtigten zur persönlichen Stimmabgabe gewährleistet die Erfüllung des Grundprinzips der persönlichen Wahl in gleicher Weise wie bei der Briefwahl.

7. Verweis auf das Datenschutzgesetz 2000

Die Gewährleistung des hinreichenden Schutzes der Wahl- und Wählerdaten ist unmittelbar mit der Sicherheit der Datenspeicherung im eingesetzten System verbunden, da jede Sicherheitslücke nicht nur zu Manipulation der Daten, sondern auch zu deren Auslesen benutzt werden kann. Um dies zu vermeiden, sind nicht nur die Sicherheitsanforderungen des Signaturgesetzes einzuhalten, sondern auch die im DSG 2000 normierten Anforderungen an die Datensicherheit zu berücksichtigen.

8. Trennung von Identifikation und Anonymität

Neben den im allgemeinen Teil der Erläuterungen festgelegten Ausführungen zur Einhaltung der Wahlgrundsätze bei der elektronischen Wahl erfordert die Sensibilität der Verarbeitung dieser Daten die eigenen Bestimmungen des § 34 Abs 4 bis 7 HSG, um ein hohes Maß an Sicherheit gesetzlich zu gewährleisten.

Die Bestimmungen dienen der erforderlichen gesetzlichen Determinierung der Verordnungsmächtigung des § 48 HSG. 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 werden die Grundsätze der Wahlen auch für die elektronische Durchführung explizit normiert. Besonders die heikle Situation, dass einerseits zur Vermeidung von Wahlbetrug die Identität des Wahlberechtigten im Rahmen der Ausgabe des Stimmzettels verifiziert werden muss, andererseits zur Wahrung des Wahlgeheimnisses keinerlei Rückschluss von den abgegebenen Wahldaten auf die Person des Wählers möglich sein darf, ist gesetzlich angeordnet. Zur Realisierung ist zum Beispiel in der zu erlassenden Verordnung die strikte Trennung der Wahldaten - also des anonym abgegebenen elektronischen Wahlformulars - und der Wählerinnen- und Wählerdaten - jene Daten, die bei der Ausgabe des Wahlformulars zur Verifikation der Identität dienen - auf unterschiedlichen Speichermedien, die Verschlüsselung des Wahlformulars, das Konzept der blinden elektronischen Signatur oder des Mixings anzuordnen. Weiters muss ausgeschlossen werden, dass während der Wahl andere Zugriffe, wie zum Beispiel das Setzen von Cookies, auf den Rechner, der zur Abgabe der Stimme benutzt wird, Rückschlüsse auf das Wahlverhalten ermöglichen. Die strikte Löschung aller personenbezogenen Daten nach Einlangen des Wahlformulars beim Rechner der Wahlkommission und die ausschließliche Speicherung der Wahldaten ist durch Verordnung sicherzustellen. Ein Mischvorgang nach Abschluss der Wahl vor dem Auswerten der Wählerdaten ist ebenfalls zu gewährleisten.

9. Schutz des Wahlgeheimnisses

Dies ist die wohl die zentralste und zugleich von technischer Seite auch komplexeste Anforderung an ein elektronisches Wahlsystem, da analog zu konventionellen Wahlsystemen einerseits eine Verifikation der Identität des Wählers bei der Übermittlung des leeren Wahlformulars er-

folgen muss, um die Wahlberechtigung zu überprüfen und die doppelte Abgabe von Stimmen durch eine Person auszuschließen, andererseits die abgegebenen Stimmen völlig anonymisiert in die Urne gelangen müssen. Eine Beschreibung eines geeigneten technischen Systems würde den Umfang dieses Beitrags sprengen. In dieser Abhandlung sollen auch nur die rechtlichen Rahmenbedingungen für eVoting behandelt werden, sie baut bezüglich der technischen Grundlagen auf einem Artikel des Autors, der im vorjährigen Tagungsband⁷ erschienen ist. Derzeit wird an der Wirtschaftsuniversität Wien gerade an der Entwicklung eines geeigneten Systems gearbeitet, das von *Prosser* ausführlich im nächsten Beitrag in diesem Band besprochen wird.

10. Schutz vor Übereilung

Durch die Notwendigkeit des Betretens der Wahlzelle, bevor der Wahlzettel bei konventioneller Wahl erst ausgefüllt werden kann, ist ein hoher Schutz vor Übereilung gegeben. Der Gefahr einer unüberlegten Stimmabgabe mittels schnellem Mausklick ist durch geeignete Programmgestaltung und Benutzerführung bei der elektronischen Stimmabgabe zu begegnen. So muss der Wähler vor Abgabe der Stimme explizit auf die Teilnahme an der Wahl durch Ausfüllen des Wahlformulars aufmerksam gemacht werden. Sie oder er hat diese Meldung des Programms zu bestätigen, bevor sie oder er zum Wahlformular gelangt. Die Bildoberfläche, die sich dem Wahlberechtigten im Rahmen der Stimmabgabe präsentiert, muss der zentralen Bedeutung der demokratischen Stimmabgabe gerecht werden.

11. Verlautbarung der Wahlvorschläge

Die elektronische Wahl soll auch nicht am Studienort anwesenden Studierenden die Wahl ermöglichen. Dies erstreckt sich nicht nur auf die Möglichkeit zur Teilnahme, auch die Information über die Wahlvorschläge müssen als Grundlage zur Willensbildung bei der Wahl den Studierenden zur Kenntnis gebracht werden. Um auch nicht anwesende Studierende zu erreichen, wird das gleiche Medium zum Transport dieser Information benutzt, das auch für die Übertragung der Wahldaten verwendet wird. Damit ist gewährleistet, dass jede Teilnehmerin oder jeder Teilnehmer an

⁷ Auf dem Weg zur ePerson – Aktuelle Fragestellungen der Rechtsinformatik 2001, 281.

der elektronischen Wahl auch Einsicht in die Wahlvorschläge nehmen kann. Die Einschränkung der Authentizität wurde analog zur bestehenden Regelung über die Authentizität des im Internet bereitgestellten Inhalts des Bundesgesetzblattes gemäß § 7 Abs 2 BGBIG übernommen, da die Server, auf denen diese Wahlvorschläge publiziert werden, nicht zwingend den Sicherheitsanforderungen der bei der Wahlkommission eingesetzten technischen Komponenten gemäß § 34 Abs 6 HSG entsprechen müssen. Weil die Richtigkeit der im Internet zur Verfügung gestellten Information bei Zweifel durch die abfragenden Studierenden auch auf anderem Wege (Nachfrage mittels Brief, Telefon, e-mail, Fax) festgestellt werden kann, ist die Einschränkung der Authentizität nur auf die konventionelle öffentliche Bekanntmachung gerechtfertigt.

12. Abbruch bei Attacken gegen das System

Auf Grund von Angriffen (zum Beispiel: Denial of Service Attacks gegen die Server zur elektronischen Wahl) auf das elektronische Wahlsystem am Tag der Wahl selbst kann der Fall eintreten, dass die im vorhinein geprüfte Sicherheit erst unmittelbar am Wahltag beeinträchtigt wird. § 39 Abs 7 HSG berücksichtigt dieses Szenario und erlaubt dem Vorsitzenden der Wahlkommission (als Einzelperson und somit ohne Beschluss der Wahlkommission) kurzfristig auf den Eintritt so einer Situation zu reagieren. Die Beiziehung der Bestätigungsstelle gestattet die genaue Feststellung des eingetretenen Schadensmaßes und liefert die notwendige technische Expertise für die Entscheidung des weiteren Vorgehens nach einem Abbruch der Wahl oder einem temporären Anhalten des Systems. Beziehen sich Einsprüche gegen die Wahl auf Unregelmäßigkeiten der eingesetzten technischen Komponenten, soll sichergestellt werden, dass bei der Beurteilung der Einsprüche auch die erforderliche technische Expertise berücksichtigt wird.

13. Checks and Balances

Wie schon in § 34 HSG ausgeführt, erfordert die Möglichkeit des Einsatzes von technischen Komponenten nach dem letzten Stand der Technik eine gesetzliche technologieneutrale Regelung. Das konkret eingesetzte Verfahren wird im Rahmen der gesetzlichen Vorgaben durch Verordnung festgelegt. Zur Sicherung der Einhaltung aller Vorschriften des Datenschutzes ist die Anhörung des Datenschutzrates angeordnet. Zur Gewähr-

leistung der IT-Sicherheit kann zusätzlich auch eine Bestätigungsstelle gemäß § 19 Signaturgesetz konsultiert werden.

Weiters wird sichergestellt, dass die Teilnahme an der elektronischen Wahl den Studierenden freigestellt bleibt und bei jeder Wahl auch die Möglichkeit zur konventionellen Stimmabgabe besteht. Damit ist gewährleistet, dass es jedem Wahlberechtigten freisteht, ob er der im Rahmen der elektronischen Wahl notwendigen Verarbeitung ihre oder seine Daten durch die Teilnahme zustimmt oder die Stimme auf konventionellem Weg abgibt.

Literatur

- Brenn, C.*, Signaturgesetz (Kommentar), Manz, Wien, 1999.
- DuschaneK.A./Rosenmayr-KlemenZ, C.*, Datenschutzgesetz 2000 (Kommentar), Wirtschaftskammer Österreich, Wien, 2000.
- Filzmaier, P.* (Hg), Internet und Demokratie – The State of Online Politics, Studienverlag, Innsbruck, 2001.
- Menzel, T.*, E-Voting an österreichischen Hochschulen, in: *Schweighofer/Menzel/Kreuzbauer* (Hg), Auf dem Weg zur ePerson – Aktuelle Fragestellungen der Rechtsinformatik 2001, Verlag Österreich, Wien, 2001, S 281-292.
- Menzel, T.*, Rechtsrahmen des E-Government. In: Juristische Ausbildung und Praxis (JAP), Heft 4, Manz, Wien, 2001/2002, S 251.
- Posch, R./Karlinger, G./Konrad, D./Leiningen, A./Menzel, T.*, Weißbuch Bürgerkarte Stand 15. Mai 2002, verfügbar unter: <http://www.buergerkarte.at/weissbuch/20020515/WeissbuchBuergerkarte.20020515.pdf>.
- Rossnagel, A./Wedde, P./Hammer, V./Pordesch, U.*, Digitalisierung der Grundrechte, Westdeutscher Verlag, 1990.
- Schefbeck, G.*, Elektronische Demokratie, in: *Schweighofer/Menzel* (Hg), E-Commerce und E-Government – Aktuelle Fragestellungen der Rechtsinformatik, Verlag Österreich, Wien, 2000, S 89.
- Schreiner, H.*, Wahlen per Mausklick – Rechtliche Überlegungen zum I-Voting, in: *Schweighofer/Menzel/Kreuzbauer* (Hg), Auf dem Weg zur ePerson – Aktuelle Fragestellungen der Rechtsinformatik 2001, Verlag Österreich, Wien, 2001, S 259.