1.2006 Schriftenreihe

Der Österreichische Städtebund informiert.

Internet, E-Government und Recht

Internet, E-Government und Recht

Schriftenreihe des Österreichischen Städtebundes
Internet, E-Government und Recht

Herausgeber:
Österreichischer Städtebund
1082 Wien, Rathaus
Telefon: 01/4000-89980
Telefax: 01/4000-7135
E-Mail: post@staedtebund.gv.at
Internet: http://www.staedtebund.gv.at
ISBN: 3-9502038-1-8

Schriftleitung:
Generalsekretär Dkfm. Dr. Erich Pramböck

Koordination:
Mag. Gabriela Forchtner, Österreichischer Städtebund
Mag (FH) Julia Reifensteiner, Public Management Consulting
Dr. Ronald Sallmann, Public Management Consulting

Autoren:
Prof. Dr. Dr. Walter Blocher
Dr. Wilfried Connert
Dr. Albrecht Haller
MR Dr. Waltraut Kotschy
Dr. Clemens Thiele
Erhard Vallant
Prof. Dr. Andreas Wiebe, LLM.

Im Sinne einer besseren Lesbarkeit werden Rechtstexte in der neuen deutschen Rechtschreibung abgedruckt.

Umschlaggestaltung und DTP-Produktion:
Karin Wieser, Grafic & Design
1120 Wien, Hufelandgasse 1/2/9
www.grafic.at

Druck:
Druckerei Uhl, Demczuk & Huber GmbH, 3002 Purkersdorf

Wien, April 2006

ISBN: 3-9502038-3-4

Vorwort

Es kann mit Fug und Recht behauptet werden, dass in den letzten 10 Jahren im Bereich der Informationstechnologie kein Stein auf dem anderen geblieben ist. Entwicklungen wie ein weltumspannendes Informations-, Kommunikations- und Transaktionsnetzwerk in Form des Internets oder eine „Informatisierung" der öffentlichen Verwaltung, wie dies bei E-Government geschieht, waren noch vor wenigen Jahren nicht absehbar. Dementsprechend groß war auch der Nachholbedarf der Legislative in diesem Bereich, da die bestehenden Rechtsnormen nicht auf derart vielfältige elektronische Interaktionsmöglichkeiten ausgelegt waren und damit erheblichen Interpretationsspielraum schafften. Dieser sorgte insbesondere bei der öffentlichen Verwaltung für einen hohen Grad an Rechtsunsicherheit, da deren hoheitliches Handeln ausschließlich auf der Grundlage von Gesetzen und Verordnungen erfolgt. Umfragen des Österreichischen Städtebundes aus den Jahren 2000 und 2003 bestätigten diese Problemlage.

Dem Bedarf nach klarer Regulierung Rechnung tragend wurden seitens des Gesetzgebers in den letzten Jahren massive Anstrengungen unternommen, die Bundesgesetzgebung in wesentlichen Fragen wie der elektronischen Identität, der Akzeptanz elektronischer Dokumente oder der elektronischen Zustellung zu novellieren. Für komplett neue Anforderungen wie beispielsweise zentrale Register wurden darüber hinaus auch neue Rechtsnormen entwickelt, die in einem eigenen E-Government-Gesetz gipfelten. Wie bei jeder sehr raschen Entwicklung wird auch hier die Zeit zeigen, inwieweit diese Anpassungen in der täglichen Verwaltungspraxis – aber auch der Judikatur – praktikabel sind.

Tatsache ist jedenfalls, dass neben den technischen Herausforderungen für modernisierungswillige Städte und Gemeinden mittlerweile auch beträchtliche Kenntnisse der aktuellen Rechtsmaterie im Umfeld von Internet und E-Government erforderlich sind. Eben dieser Bedarf war auch Anstoß für den Österreichischen Städtebund, im Spätherbst 2005 eine Fachtagung zum Themenkreis „Internet, E-Government und Recht" zu veranstalten.

Die vorliegende Publikation im Rahmen der Schriftenreihe des Österreichischen Städtebundes wurde von PuMa – Public Management Consulting bearbeitet und ist eine Sammlung inhaltlich erweiterter und vertiefter Beiträge der Fachtagung. Sie spannt einen breiten Bogen von rechtlichen Fallstricken, die bei kommunalen Internetauftritten zu beachten sind, über eine Darstellung der technisch wie rechtlich überaus komplexen österreichischen Lösung elektronischen Datenschutzes bis hin zu einer kritischen Reflexion der aktuellen E-Government-Entwicklung aus der Perspektive der kommunalen Praxis.

Mögen die einzelnen Beiträge inhaltlich auch einen breiten Bogen spannen, so zieht doch die Auseinandersetzung mit den jeweils wichtigsten Rechtsfragen in den unterschiedlichen Gebieten einen roten Faden durch die gesamte Publikation und jeder – mit Rechtsfragen im Umfeld der elektronischen Interaktion konfrontierte – Mitarbeiter wird in dem einen oder anderen Beitrag für seine Tätigkeit wichtige und interessante Hinweise finden. Der Österreichische Städtebund hofft, dass mit dem vorliegenden Band seiner Schriftenreihe ein weiterer wichtiger Baustein in der praxisnahen Rechtsinformation seiner Mitgliedsgemeinden gesetzt werden konnte.

Dkfm. Dr. Erich Pramböck
Generalsekretär

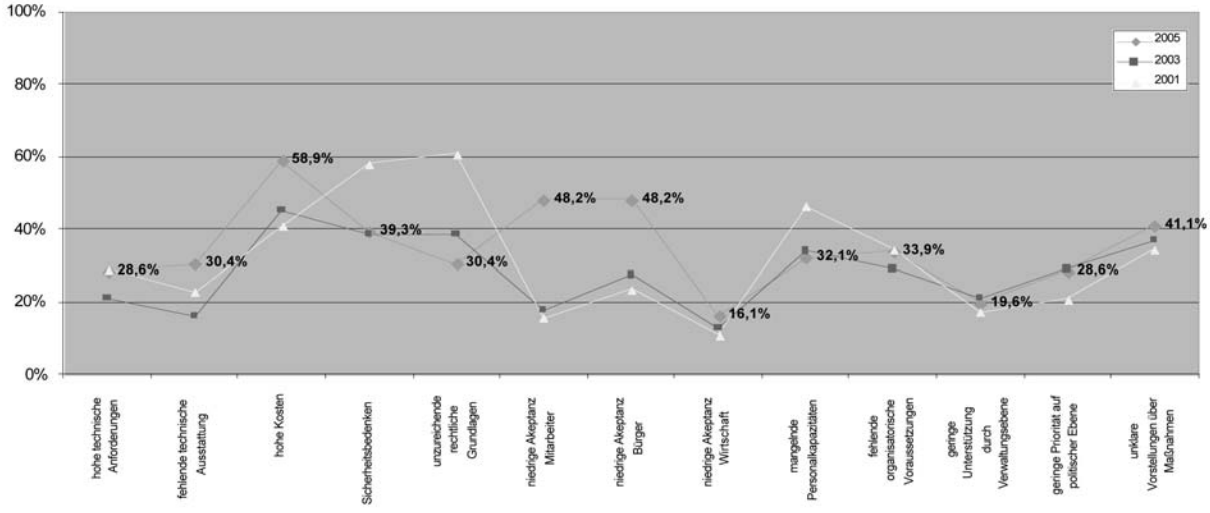
INHALTSVERZEICHNIS

EINLEITUNG & EXECUTIVE SUMMARY

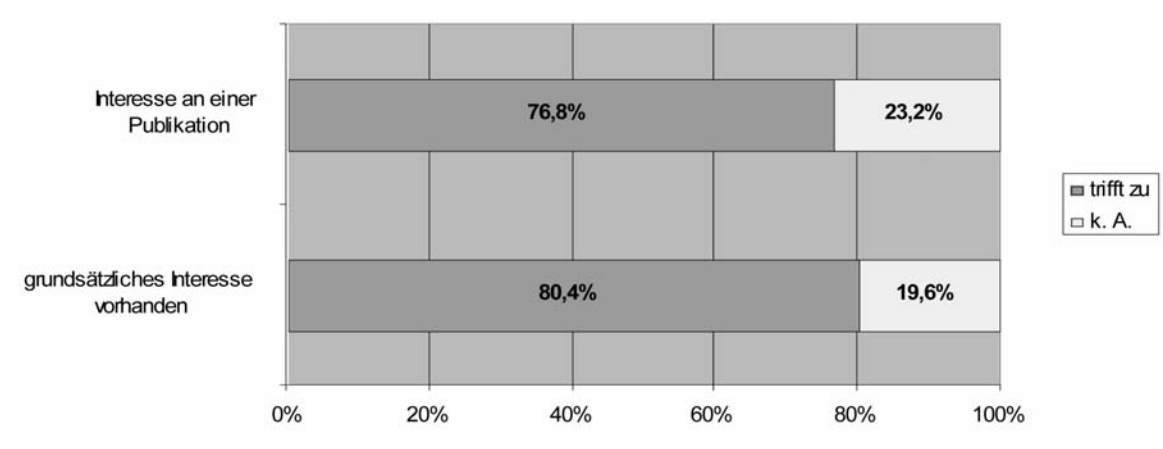
Am 25.10.2005 fand im Wiener Rathaus auf Einladung des Österreichischen Städtebundes im Rahmen dessen fachspezifischer Veranstaltungsreihe eine Fachtagung unter dem Titel „Internet, E-Government und Recht“ statt. In einem dichten Tagesprogramm wurde versucht, den Teilnehmern einen Überblick über aktuelle rechtliche Entwicklungen in den beiden eng verwandten Bereichen zu geben, wobei ein Halbtag E-Government gewidmet war und der zweite Halbtag hauptsächlich auf die Präsenz von Kommunen im Internet und damit verbundene (rechtliche) Problemstellungen fokussierte. Schließlich hat sich die Rechtsmaterie im Umfeld des IKT-Einsatzes in den letzten Jahren zu einem hochkomplexen und ziemlich umfangreichen Spezialgebiet entwickelt.

Dass aufgrund dieser Tatsache auch in den Städten und Gemeinden rechtliche Unsicherheiten bei der Nutzung von E-Government bzw. dem Internet bestehen, zeigt eine Umfrage, die von PuMa – Public Management Consulting im Auftrag des Österreichischen Städtebundes für den Städtetag durchgeführt worden war: Zwar waren nur 30 % der Befragten der Meinung, dass der rechtliche Rahmen für E-Government unzureichend sei und damit ein Problem darstelle (bei einer ähnlichen Befragung 2001 vertraten noch doppelt so viele diese Meinung), Fragen zum Informationsstand über aktuelle Gesetze bzw. Verordnungen aus dem Bereich E-Government kamen kaum auf Bekanntheitswerte über 35 %. Daraus erklärt sich auch der Bedarf an einschlägiger Information, da die Frage nach dem Interesse an einer Fachtagung von 80 % zustimmend beantwortet wurde und 77 % der Befragten auch eine einschlägige Publikation befürworteten.

Große und sehr große Probleme bei der Einführung von E-Government
(Zeitreihenvergleich 2001, 2003 und 2005)



Fachveranstaltung „Internet & Recht“



Der nunmehr vorliegende Band aus der Schriftenreihe des Österreichischen Städtebundes ist eine Sammlung von Beiträgen der Referenten eingangs genannter Fachtagung, in denen diese die Inhalte ihrer Vorträge eingehend ausführen und erläutern.

Der erste Teil der Fachtagung war den aktuellen rechtlichen Entwicklungen im Bereich E-Government gewidmet. Mit Dr. Connert vom Amt der Tiroler Landesregierung konnte ein Autor gewonnen werden, der dem „innersten Kreis“ der E-Government-Experten angehört und die seltene Eigenschaft eines Rechtsgelehrten mit exzellenten technischen Kenntnissen in sich vereint. Die Anforderung an seinen Beitrag war eine überblicksartige Darstellung der neuen gesetzlichen Regelungen vor allem im Bereich der „Kernfunktionen“ von E-Government wie Identifikation/Authentifizierung, der elektronischen Zustellung, dem Portalverbund sowie den zentralen Registern und Datensammlungen.

E-Government-Gesetz zur rechtlichen Absicherung der Gebietskörperschaften bei elektronischen Verfahren

E-Government steht im Gegensatz zu E-Business bzw. E-Commerce sehr stark unter dem Einfluss der wechselseitigen Bedingtheit von Technik und Recht. Auf der einen Seite schaffen technische Entwicklungen faktische Tatsachen, welche bei der rechtlichen Gestaltung berücksichtigt werden müssen. Hinzu kommt, dass der rechtliche Gestaltungsprozess häufig der technischen Entwicklung hinterherläuft, da in Gesetzen nicht von vornherein alle zukünftigen, technisch möglichen Optionen vorhergesehen und abgedeckt werden können. Auf der anderen Seite schaffen Gesetze wiederum die Rahmenbedingungen für einen rechtlich abgesicherten Einsatz neuer Technologien, was insbesondere für die öffentliche Verwaltung und deren staatliche Vollzugstätigkeit auf Grundlage des verfassungsrechtlichen Legalitätsgebots von Bedeutung ist.

In den letzten Jahren wurden auf Bundesebene bereits einige wichtige gesetzliche Anpassungen, zuletzt im Rahmen des Verwaltungsreformgesetzes 2001, vorgenommen. Es hat sich aber herausgestellt, dass für den Echtbetrieb mancher technischer Verfahren im E-Government-Bereich noch zusätzlicher gesetzlicher Regelungsbedarf besteht.

Mit dem „E-Government-Gesetz“ BGBl I Nr. 10/2004 (enthält das E-Government-Gesetz im engeren Sinne sowie Änderungen in AVG 1991, Zustellgesetz, Meldegesetz 1991, Vereinsgesetz 2002 und Gebührengesetz 1957) verfolgt der Gesetzgeber aus Gründen der Übersichtlichkeit einen ganzheitlichen Ansatz, indem alle zusätzlich notwendigen Regelungen in einem eigenen Gesetz zusammengefasst wurden, anstelle viele kurze Regelungen ins Verwaltungsrecht einzustreuen.

Das E-Government Gesetz schafft vor allem in folgenden Bereichen den notwendigen rechtlichen Rahmen für einen abgesicherten Einsatz elektronischer Medien in der Verwaltungspraxis:

- Eindeutige elektronische Identifikation
- Elektronische Standarddokumente
- Datenschutz im E-Government
- Bürgerkarten und Verwaltungssignatur
- Portalverbundsysteme
- Verzeichnisse und Register
- Elektronische Zustellung
- E-Governance und Bürgerbeteiligung

Nachdem mit August 2005 die letzten notwendigen Durchführungsverordnungen zum E-Government-Gesetz in Kraft getreten sind und auch das Stammzahlen- und die Ergänzungsregister bereits 2006 zur Verfügung stehen sollen, ist im Zuge der Nutzung dieser Infrastruktur auch umfassende Kenntnis des rechtlichen Hintergrundes notwendig.

Bereichsabgrenzung aus datenschutzrechtlichen Gründen

Gerade der Bereich der Authentifizierung mittels Bürgerkarte, dem auch das Stammzahlen- und die bereits erwähnten Ergänzungsregister (ein Ergänzungsregister für natürliche Personen und eines für „sonstige Betroffene“) zuzuordnen sind, zählt zu den komplexesten und kompliziertesten E-Government-Themen. Fr. MR Dr. Kotschy, als Leiterin der Stammzahlenregisterbehörde die erste Adresse für diesen Fachbereich, erläutert in ihrem Beitrag sehr anschaulich die Funktionsweise und das Zusammenspiel von Stammzahlenregister, Ergänzungsregistern und der Bereichsabgrenzung.

Faktum ist, dass Städte und Gemeinden bei ihren Datenanwendungen, die mit personenbezogenen Daten von Bürgern operieren, zukünftig nicht um den Einsatz von bereichsspezifischen Personenkennzeichen umhinkommen werden. Damit soll im Zuge elektronischer Verfahren eine eindeutige Kennzeichnung von Bürgern nur innerhalb eines Verwaltungsbereichs möglich sein, um datenschutzrechtliche Nachteile für den Bürger auszuschließen.

Die bereichsspezifischen Personenkennzeichen werden aus der Stammzahl gebildet, welche wiederum eine Ableitung der ZMR-Zahl darstellt und auf der Bürgerkarte (bei deren Aktivierung) abgelegt wird. Bei der Meldung einer Datenanwendung beim Datenverarbeitungsregister (DVR) ist daher in Zukunft auch das bPK mitzumelden. Da eine flächendeckende Verbreitung der Bürgerkarte in absehbarer Zeit voraussichtlich nicht erreicht wird, besteht auch die Möglichkeit, die Datensätze einer Datenanwendung mit einer „Erstausstattung“ an bPKs versehen zu lassen.

Dieser Vorgang erfordert allerdings ein gesondertes Verfahren. Ein maßgebliches Kriterium für die erfolgreiche Ausstattung mit bPKs wird auch die Qualität der auszustattenden Daten sein.

Eine für Städte und Gemeinden interessante Neuerung stellt auch das „Ergänzungsregister für sonstige Betroffene“ dar, das u. a. auch Organen von Gebietskörperschaften die Möglichkeit bietet, eine elektronische Identität für die privatwirtschaftlichen Aufgaben zu erlangen.

Kritische Reflexion von E-Government aus der Perspektive einer Stadt

Gerade im Bereich der Authentifizierung kommt der hohe Komplexitätsgrad zum Vorschein, der entsteht, wenn versucht wird, die gesetzlichen Anforderungen bestmöglich abzubilden. Unter diesem Licht ist auch der Beitrag von OAR Vallant vom Magistrat Klagenfurt zu verstehen, der als Vertreter des Österreichischen Städtebundes Mitglied im Datenschutzrat ist. Sein Beitrag stellt eine kritische Reflexion des bereits erreichten E-Government-Entwicklungsstandes aus der Sicht der täglichen Verwaltungspraxis dar. Hier zeigt sich auch, dass offensichtlich eine Kluft zwischen technisch und rechtlich bereits Möglichem und der tatsächlichen Anwendung bzw. Anwendbarkeit in der Praxis besteht. Einerseits wird die mangelhafte Abstimmung zwischen den bereits vorhandenen Registern kritisiert, andererseits die unzureichende Nutzung derselben. So werden von Behörden offensichtlich nach wie vor häufig Meldebestätigungen von Bürgern als Nachweis verlangt, obwohl diese durch eine einfache ZMR-Abfrage behördenseitig festgestellt werden können.

Weitere kritische Punkte betreffen die bisher mangelhafte Auseinandersetzung mit bzw. elektronische Umsetzungsbereitschaft von Registern im Personenstands- und Staatsbürgerschaftsbereich sowie im Wahlwesen, wo besonders aufkommensstarke Verfahren angesiedelt sind. In einem abschließenden Resümee gab der Autor weiters Empfehlungen an die gesetzgebenden Gebietskörperschaften, bei welchen Aktivitäten aus seiner Sicht dringender Umsetzungs- oder Abstimmungsbedarf besteht.

Rechtliche Fallstricke beim Betrieb von Internetauftritten

Der zweite Teil der Veranstaltung fokussierte auf die Präsenz der Städte und Gemeinden im Internet. Da diese als Anbieter von Informationen und teilweise auch Dienstleistungen auftreten, sind einige rechtliche Grundlagen – z. B. im Bereich des Urheberrechts, des E-Commerce-Gesetzes oder des Medienrechts – zu beachten, die für die Gebietskörperschaften ebenso gelten wie für jedes andere Unternehmen im Internet. Darüber hinaus gibt es Rechtsbereiche, die insbesondere für Städte und Gemeinden von vorrangiger Bedeutung sind, wie beispielsweise das Namensrecht. Rechtsstreitigkeiten um Internetdomänen beschäftigen mittlerweile seit einem Jahrzehnt die Gerichte, sodass hier bereits höchstgerichtliche Entscheidungen vorliegen.

Schutz von Domänennamen vor unrechtmäßiger Aneignung bzw. Nutzung

Dr. Clemens Thiele, Experte für Rechtsfragen rund um Internetdomänen, erläutert in seinem Beitrag die rechtlichen Rahmenbedingungen eines „virtuellen Ortsschutzes“ anhand von Fallbeispielen aus aktueller Praxis. Grundsätzlich ist unbestritten, dass Städte und Gemeinden an der aus ihrer Bezeichnung

und der Landeskennung (.at) gebildeten Internetadresse namensrechtliche Unterlassungs- und Beseitigungsansprüche geltend machen können. Der Erfolg hängt jedoch in hohem Maß von weiteren Faktoren ab, insbesondere der inhaltlichen Gestaltung der unter einem strittigen Domänennamen geführten Website oder einer nachweisbaren „Behinderungsabsicht" durch die Reservierung eines Domänennamens.

Auch beim Betrieb einer gemeindeeigenen Internetsite sind einige rechtliche Rahmenbedingungen zu beachten. Zwar richten sich beispielsweise die Bestimmungen des E-Commerce-Gesetzes nicht primär an öffentlich-rechtliche Körperschaften, jedoch ist zu bedenken, dass Städte und Gemeinden auch im Rahmen der Privatwirtschaftsverwaltung tätig und somit im Internet präsent sind. Diese rechtlichen Aspekte kommunaler Internetauftritte wurden von Prof. Dr. Wiebe näher erläutert. So sind von den Kommunen unter bestimmten Umständen ebenso die Informationspflichten nach dem E-Commerce-Gesetz einzuhalten. Auch das Mediengesetz sieht Informationspflichten vor. Bei der Haftung von Inhalten kommunaler Websites ist das anwendbare Recht wiederum abhängig davon, ob es sich um hoheitliches Handeln (Amtshaftungsgesetz – AHG) oder Aktivitäten im Rahmen der Privatwirtschaftsverwaltung (Zivilrecht) handelt. Darüber hinaus haben öffentliche Rechtsträger gegenüber privaten Webseitenbetreibern zusätzliche, besondere Obliegenheiten zu erfüllen, wie beispielsweise die Einhaltung von Grundrechten (Diskriminierungsverbot).

Rechtslage beim Einsatz von E-Mails, insbesondere Massenmails (SPAM)

Auf einen speziellen Internetdienst, nämlich den Einsatz von E-Mail durch die öffentliche Verwaltung, geht Prof. Dr. Dr. Blocher in seinem Beitrag näher ein. Das Thema E-Mail ist aus rechtlicher Sicht vor allem vor dem Hintergrund der ausufernden Zunahme unerwünschter Werbemails und SPAM-Mails interessant. Zwar gibt es eine rechtliche Handhabe gegen SPAM, diese greift jedoch kurz, da die Herkunft solcher E-Mails oftmals nicht klar nachvollziehbar ist oder seinen Ursprung in einem exotischen Land nimmt. Aber auch als Absender von Massenmails sind einige Grundregeln zu beachten. Diese finden sich vor allem im E-Commerce-Gesetz und im Telekommunikationsgesetz. So gibt es beispielsweise die Regelung, dass E-Mails und SMS, welche die Verbrauchersphäre eines Empfängers betreffen, ohne dessen vorherige Einwilligung unzulässig sind, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt oder sich an mehr als 50 Empfänger richtet.

Urheberrecht ist häufiger Streitgegenstand bei Internetseiten

Auf die inhaltliche Gestaltung kommunaler Websites kommt schließlich Dr. Haller zu sprechen. Auch in diesem Bereich gibt es einige rechtliche Fallstricke, die es zu beachten gilt. Gerade im Bereich der künstlerischen (grafischen) Gestaltung (z. B. Logos) kommt es immer wieder zu Unklarheiten und gerichtlichen Auseinandersetzungen. Das Urheberrecht sieht hier klare Regelungen vor in Bezug auf den Urheberrechtsschutz, die Inhaberschaft und Schutzinhalte. In diesem Zusammenhang geht Dr. Haller in seinem Beitrag auf die vielfältigen Schutzrechte ein, die in Zusammenhang mit geistig-schöpferischen Werken – wozu auch Internetauftritte zählen – entstehen. Die Bandbreite reicht hier von unmittelbarem Werksschutz beispielsweise auf Fotos, Grafiken oder das spezifische Layout einer Website bis hin zu verwandten Schutzrechten oder

Leistungsschutzrechten, die in Zusammenhang mit der Publikation urheberrechtlich geschützter Werke entstehen.

Die Betrachtung umfasst auch Bereiche, mit denen im ersten Moment vielleicht gar keine Urheberrechte in Verbindung gebracht werden, wie Bilder von Webcams, Fotos von Mitarbeitern oder sogar Linksammlungen. Um nicht nachträglich in urheberrechtliche Streitigkeiten mit daraus resultierenden unerwarteten Kosten verwickelt zu werden, zahlt es sich daher immer aus, vor Vergabe eines Auftrages im Bereich der Internetgestaltung auch die urheberrechtlichen Rahmenbedingungen zu regeln. Auch die Varianten von Lizenzverträgen werden in dem Beitrag kurz dargestellt.

Die Fachtagung zum Thema „Internet, E-Government und Recht“ zeigte sehr deutlich, dass noch lange nicht alle rechtlichen Fragen, aber auch Hürden in Zusammenhang mit einer Nutzung moderner Informations- und Kommunikationstechnologien durch die öffentliche Hand geklärt respektive den Betroffenen vollinhaltlich bekannt sind. Daraus resultieren auch das hohe Interesse an der Thematik und der Bedarf an detaillierter Information. Schließlich legitimiert sich die Tätigkeit öffentlich-rechtlicher Körperschaften auf der Grundlage von Gesetzen, woraus sich auch die Verpflichtung zu einer besonderen Vorbildwirkung ergibt.

Kapitel 1

RECHTSRAHMEN FÜR E-GOVERNMENT UND ZENTRALE REGISTER

Dr. Wilfried Connert

1.1 ABSTRACT

Das E-Government-Gesetz, das im Jahre 2004 in Kraft trat, stellt den zentralen rechtlichen Rahmen für die elektronische Kommunikation und Transaktion von und mit Behörden dar. Während in diesem Gesetz nur die wesentlichen Rahmenbedingungen geschaffen wurden, gehen begleitende Verordnungen wesentlich detaillierter auf die Umsetzung ein. Inhaltlich regelt das E-Government-Gesetz bisher aufgrund nicht gegebener technischer Möglichkeiten auch nicht eindeutig rechtlich geklärte Situationen und schafft damit wesentlich mehr Rechtssicherheit für die öffentliche Hand. Auf der anderen Seite erfordern komplexe technische Strukturen auch komplexe rechtliche Regelwerke. Großes Augenmerk wurde vor allem dem Datenschutz geschenkt, um Missbrauch durch Verknüpfung elektronisch gespeicherter Daten von vornherein zu verhindern.

Die Regelungen des E-Government-Gesetzes betreffen unmittelbar alle Ebenen der Verwaltung, also Bund, Länder und Gemeinden gleichermaßen, wenn diese Aktivitäten im Bereich des E-Government setzen. In manchen Teilbereichen geht das Gesetz auch über das hinlängliche Verständnis von E-Government hinaus und nimmt damit direkten Einfluss auf die laufende Verwaltungstätigkeit – auch von Städten und Gemeinden. So wird beispielsweise unverfälscht eingescannten Dokumenten der Status eines Originals eingeräumt, was den Einsatz von Dokumentenmanagement- und ELAK-Systemen absichert (§ 13 AVG). In diesem Zusammenhang steht auch die nunmehrige Notwendigkeit, interne Erledigungen - wenn sie elektronisch erfolgten –auch elektronisch zu signieren.

Einen Schwerpunkt des E-Government-Gesetzes bildet generell das Thema der „elektronischen Identität", wobei für die Städte und Gemeinden zwar keine aktive Umsetzungsverpflichtung erwächst, jedoch die Annahme elektronisch signierter Dokumente grundsätzlich möglich sein muss. Für eine Übergangsphase bis Ende 2007 sieht das E-Government-Gesetz unter der Bezeichnung „Verwaltungssignatur" weiters eine elektronische Signatur mit niedrigeren Sicherheitsanforderungen vor.
Allerdings kann eine Behörde selbst einschränken, unter welchen Bedingungen (z. B. Größenbeschränkung für Anhänge) sie auf elektronischem Wege Anbringen entgegennimmt.

Für den Fall, dass Erledigungen die öffentliche Verwaltung elektronisch verlassen, sieht das E-Government-Gesetz das Anbringen einer Amtssignatur vor und auch die elektronische Zustellung – bisher zwar grundsätzlich möglich, aber mit einigen rechtlichen Unsicherheiten verbunden – wurde neu geregelt. Auch diese Regelungen kommen jedoch nur bei elektronischer Datenübermittlung zum Tragen. Weitreichendere Konsequenzen – insbesondere auch für Städte und Gemeinden - ergeben sich aus der datenschutzrechtlich begründeten und mittels Verordnung vorgeschriebenen Segmentierung der öffentlichen Verwaltung in „Verwaltungsbereiche", über die personenbezogene Daten nicht einfach im Klartext – d. h. unverschlüsselt – weitergegeben werden dürfen. In Klärung befindet sich noch, inwieweit diese Regelung auch bei verwaltungsinternen Datenanwendungen (z. B. Dokumentenmanagement-Systeme oder ELAK) mit teilweise zentralem Datenstock zur Anwendung gelangt.

Einen weiteren Schwerpunkt des E-Government, der alle Gebietskörperschaften betrifft, stellt die Schaffung zentraler Register für die am häufigsten benötigten Datenbestände dar. Es sind dies das Zentrale Melderegister (Meldedaten), das Gebäude- und Wohnungsregister (geocodierte Bebauungsdaten von Liegenschaften), das Adressregister (Adressdaten) sowie weitere Hilfsregister, die im Umfeld der eindeutigen Identitätsfeststellung von Personen benötigt werden (Stammzahlenregister, Ergänzungsregister). Entscheidet sich eine Stadt oder Gemeinde also dazu, E-Government-Dienstleistungen für ihre Verwaltungskunden anzubieten, so kommt eine Reihe von Verordnungen zu im E-Government-Gesetz ausgeführten Regelungen zum Tragen.

1.2 EINLEITUNG

Mit August 2005 sind die letzten notwendigen Durchführungsverordnungen zum E-Government-Gesetz in Kraft getreten. Auch die Umsetzung der notwendigen Infrastruktur ist weiter fortgeschritten. Der aktuelle Stand und ein Überblick über die zentralen Register sollen daher dargestellt werden.

Mit dem „E-Government-Gesetz" BGBl I Nr. 10/2004 (enthält das E-Government-Gesetz im engeren Sinne sowie Änderungen in AVG 1991, Zustellgesetz, Meldegesetz 1991, Vereinsgesetz 2002 und Gebührengesetz 1957) wurde für die E-Government-Kernfunktionen eine sichere rechtliche Basis geschaffen. Auch wenn zum Zeitpunkt des Inkrafttretens am 1.3.2004 die technischen und organisatorischen Konzepte weitgehend fertig waren, dauerte es doch noch, bis mit 1.8.2005 die letzte Durchführungsverordnung vorlag und seit Mitte November 2005 das Stammzahlen- und die Ergänzungsregister zur Verfügung stehen.

Der erste Teil dieser Darstellung stellt Kernfunktionen und den Stand der rechtlichen Regelung dar. Der zweite Teil geht auf zentrale Register und Datensammlungen ein. Es folgt ein Ausblick, was da noch zu tun ist/wäre.

1.3 KERNFUNKTIONEN FÜR E-GOVERNMENT

1.3.1 Signaturen

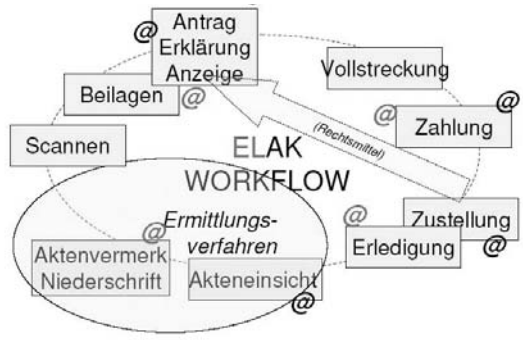
Zertifizierungsdiensteanbieter, das sind dem Signaturgesetz (SigG) entsprechende private Unternehmen, überlassen einem Signator Signaturerstellungsdaten (geheimer Schlüssel) und Signaturprüfdaten (öffentlicher Schlüssel) und bestätigen mit einem Zertifikat die Zuordnung der Signaturprüfdaten zum Signator. Signaturen im Sinne des Signaturgesetzes (SigG) können daher immer nur einer bestimmten natürlichen Person zugeordnet werden. Die Gültigkeit des Zertifikates erlischt durch Zeitablauf (da die technische Entwicklung nicht auf Dauer abgesehen werden kann) sowie durch Widerruf durch den Signator (was dieser jederzeit tun kann, aber tun muss, wenn er den Verdacht hat, dass die Signaturerstellungsdaten in fremde Hände geraten sein könnten).

Eine gültige elektronische Signatur auf einem elektronischen Dokument stellt sicher, dass das Dokument vom Inhaber des Zertifikates mit seinem geheimen Schlüssel signiert worden ist und unverändert ist. Der Empfänger kann dies prüfen, indem er einerseits den Signiervorgang mit dem zugehörigen bekannten öffentlichen Schlüssel des Signators durchführt – und zum gleichen Ergebnis kommt – und andererseits die Gültigkeit des Zertifikates beim Zertifizierungsdiensteanbieter in einem öffentlich zugänglichen Verzeichnis abfragt.
Für die sogenannte „sichere Signatur" werden erhöhte Anforderungen an die Identifikation des Signators (Ausweisleistung und persönliche Anwesenheit beim erstmaligen Zugang), die Verwahrung der Signaturerstellungsdaten (derzeit nur auf einer Chipkarte mit eigenem Prozessor zulässig) und die Infrastruktur beim Zertifizierungsdiensteanbieter gestellt. Ab 2005 ausgestellte Bankomatkarten sind bereits dafür vorgesehen.

Der Rechtsrahmen durch die EU-Signatur-Richtlinie (Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen; Amtsblatt Nr. L 013 vom 19.1.2000, S. 0012-0020) und das Signaturgesetz (SigG) in der Fassung BGBl I Nr. idF BGBl I Nr. 32/2001, stellen sicher, dass Signaturen auch im EU-Raum Gültigkeit haben.

Nach § 1 SigG gilt dies auch für den elektronischen Verkehr mit den Behörden und Gerichten. §§ 3 und 4 regeln die Rechtswirkungen elektronisch signierter Dokumente.

Verwaltungsverfahren



1.3.2 Identifikation, Authentifizierung, Vollmacht

Ein Signaturzertifikat stellt zwar die Zuordnung einer Signatur zu einer bestimmten Person sicher, führt jedoch noch nicht zu einer eindeutigen Identifikation der Person: es enthält nur den Namen, nicht jedoch weitere Angaben zur Person; eine Person kann mehrere Signaturen und damit Zertifikate haben; Zertifikate sind nur zeitlich begrenzt gültig.

Für Personen mit Wohnsitz in Österreich wird daher durch eine Ableitung aus der ZMR-Zahl im Zentralen Melderegister eine eindeutige Stammzahl gebildet. Für Personen ohne Wohnsitz in Österreich gibt es die Möglichkeit der Eintragung in ein Ergänzungsregister. Die Stammzahlenregisterbehörde bildet einen Personenbindungsdatensatz mit der Stammzahl, Name, Geburtsdatum und dem öffentlichen Schlüssel der Person (Signator).

Mit der Prüfung der elektronischen Signatur auf einem Antrag kann über den Personenbindungsdatensatz neben der Authentizität (Dokument stammt vom Signator und ist unverändert) auch die Identität des Signators sichergestellt werden.

Aus der Stammzahl darf für die Verwendung in den Anwendungen der Verwaltung je Verfahrensbereich ein bereichsspezifisches Personenkennzeichen abgeleitet werden (bPK), für die Verwendung in der Wirtschaft ein wirtschaftsbereichsspezifisches Personenkennzeichen (wbPK).

Für juristische Personen bilden die Firmenbuchnummer, die ZVR-Zahl aus dem Zentralen Vereinsregister oder die Ordnungsnummer aus dem neu geschaffenen Ergänzungsregister die jeweiligen Stammzahlen. Diese können unverändert in den Anwendungen gespeichert werden.

Da aber nur natürliche Personen Eingaben signieren können, bedarf es elektronischer Vollmachten zur Abbildung der Vertretungsbefugnisse für juristische Personen.

Dazu kommt noch die Vertretung von natürlichen Personen mit entsprechender elektronischer Vollmacht.

Dieser ganze Komplex wird unter dem Begriff „Konzept Bürgerkarte“ geführt.
Rechtsgrundlagen:
§§ 1-13 E-Government-Gesetz (E-GovG) BGBl I Nr. 10/2004
E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV) BGBl II Nr. 289/2004 (schafft 36 Bereiche)
Stammzahlenregisterverordnung (StZRegV) BGBl II Nr. 57/2005
Ergänzungsregisterverordnung (ERegV) BGBl II Nr. 241/2005

1.3.3 Verwaltungssignatur

Es wird noch einige Zeit dauern, bis Wirtschaft und Bevölkerung über viele sichere elektronische Signaturen verfügen werden. Daher wurde für den Zugang zur Verwaltung neben der sicheren Signatur eine einfachere Variante der Signatur zugelassen, die aber trotzdem ausreichende Sicherheit bietet (= Verwaltungssignatur). Bereits verfügbare Beispiele sind die „Handy-Signatur“ und die auf der E-Card der Sozialversicherung mögliche Signatur.

Rechtsgrundlage:
Verordnung des Bundeskanzlers, mit der die sicherheitstechnischen und organisationsrelevanten Voraussetzungen für Verwaltungssignaturen geregelt werden (VerwSigVO) BGBl II Nr. 159/2004.

1.3.4 Anbringen, Scannen von Dokumenten

Nach § 13 Abs. 1 AVG hat die Behörde die Adressen sowie die allenfalls bestehenden besonderen technischen Voraussetzungen, unter welchen Anbringen rechtswirksam eingebracht werden können, durch Anschlag an der Amtstafel und im Internet kundzumachen. Damit können zulässig E-Mail-Adressen, Datenformate, aber auch Beschränkungen der Dateigröße (z. B. 10 MB) verbindlich festgelegt werden. Da von der Erfüllung dieser Voraussetzungen abhängt, ob ein

Anbringen gültig und damit auch fristgerecht eingebracht worden ist, müssen diese Festlegungen durch Verordnung erfolgen.

§ 13 Abs. 1 AVG legt auch fest: „Als Kopie gilt jede inhaltlich unverfälschte Wiedergabe des Originals." Damit ist das Scannen von Papierdokumenten für den elektronischen Akt abgesichert.

Rechtsgrundlage:
§ 13 AVG idF BGBl I Nr. 10/2004

1.3.5 Erledigungen, Amtssignatur

§ 18 AVG sieht für interne Erledigungen – das gilt auch für Aktenvermerke und Niederschriften – die eigenhändige Unterschrift oder die Fertigung mit elektronischer Signatur vor. Mitteilungen an Beteiligte über den Inhalt interner Erledigungen (externe Erledigungen) sind entweder eigenhändig (auch mit elektronischer Signatur) zu unterfertigen, von der Kanzlei zu beglaubigen oder mit der Amtssignatur zu versehen.

Damit soll analog zur Authentifizierung bei dem Anbringen für den Empfänger einer elektronischen Erledigung sichergestellt werden, dass er prüfen kann, ob die Erledigung von den angegebenen Behörden stammt und unverfälscht ist.

Die Amtssignatur besteht aus einer Bildmarke, Angaben aus dem Zertifikat und dem Signaturwert. Da die Amtssignatur eine Signatur nach dem Signaturgesetz ist, kann sie nur einer bestimmten natürlichen Person zugeordnet werden, die im Zertifikat aufscheint. Sie kann aber auf einem Server installiert und von Programmen genutzt werden.

Hier ist noch viel Umsetzungsarbeit zu leisten.

Rechtsgrundlagen:
§ 18 AVG idF BGBl I Nr. 10/2004
§ 19 E-GovG

1.3.6 Zustellung

Die elektronische Zustellung wurde im Zustellgesetz gänzlich neu geregelt:

- Wer elektronische Zustellung will, registriert sich bei einem zugelassenen Zustelldienst.
- Die Behörde, die elektronisch zustellen kann und will, kann über einen zentralen Verzeichnisdienst den Zustelldienst der Partei finden und die Erledigung an diesen zur Bereitstellung senden.
- Der Zustelldienst fordert zweimal elektronisch und einmal schriftlich zur Abholung auf.
- Durch den Zugriff über die Bürgerkarte ist die Identifikation sichergestellt und kann ein Nachweis über die erfolgte Zustellung geführt werden.

Für die technische Umsetzung stehen Programmmodule zur Verfügung (MOA ZS). Das BKA betreibt für eine Übergangszeit bereits einen Zustelldienst unter www.zustellung.gv.at.

Rechtsgrundlagen:
Zustellgesetz (ZustG) idF BGBl I Nr. 10/2004
Zustellformularverordnung idF BGBl II Nr. 235/2005: legt das Formular für die postalische Verständigung fest
Zustelldiensteverordnung (ZustDV) BGBl II Nr. 233/2005, in Kraft seit 28.7.2005: regelt die Voraussetzungen zur Anerkennung als Zustelldienst

1.3.7 Aktenvorlage

Wenn Akten voll elektronisch geführt werden, stellt der elektronische Akt das Original dar. Es kann und soll daher auch nur der elektronische Akt an eine Oberbehörde vorgelegt werden. Dazu sollen Standardformate verwendet werden, damit die Oberbehörde in den Akt Einsicht nehmen kann.

Rechtsgrundlage:
§ 21 E-GovG

1.3.8 Gebührenbefreiung

Eingaben und Beilagen, die mit der Bürgerkarte gefertigt sind, sind von Gebühren befreit, um einen Anreiz für den Einsatz der Bürgerkarte zu schaffen. Damit sind schon bei einer Eingabe im Jahr die laufenden Kosten für die Bürgerkarte gedeckt.

Rechtsgrundlage:
Gebührengesetz 1957 idF BGBl Nr. 10/2004.

1.3.9 Übergangsbestimmungen

Verwaltungssignatur: nur bis Ende 2007

Fertigung im ELAK ohne elektronische Signatur (z. B. über Anmeldung mit Benutzerberechtigung): nur bis Ende 2007

Elektronische Ausfertigungen ohne Unterschrift, Beglaubigung oder Amtssignatur (= bisherige Rechtslage): nur bis Ende 2007

Weiterführung bisher zulässiger behördlicher Zustelldienste: nur bis Ende 2007

Gebührenbefreiung: nur bis Ende 2006

1.3.10 Portalverbund

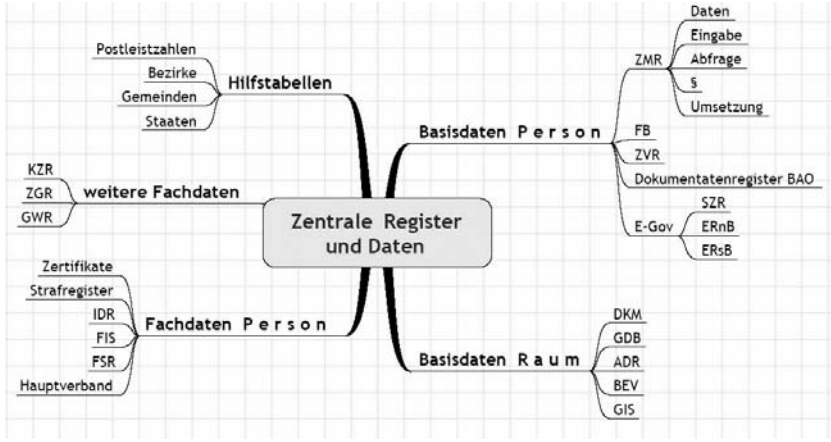
Der Portalverbund ermöglicht den Zugang zu allen auf diesem Wege bereitgestellten Anwendungen über dezentrale Stammportale, wo die Berechtigungen eingetragen werden.

Der Portalverbund besteht aus technischen, organisatorischen und rechtlichen Festlegungen (siehe http://reference.e-government.gv.at).

Basis ist die Portalverund-Vereinbarung, der die Portalbetreiber und Anwendungsverantwortlichen beitreten. Dazu kommt die Verpflichtungserklärung der einzelnen zugriffsberechtigten Stellen.

Aktueller Stand der Portale und Anwendungen unter http://www.cio.gv.at/it-infrastructure/portal/pv-beitritt-kundmachung.pdf sowie unter http://reference.e-government.gv.at.

1.4 ZENTRALE REGISTER UND DATEN



Jeweils dargestellt werden:

- Daten
- Erfassung/Eingabe der Daten
- Möglichkeiten der Abfrage und Kosten
- Rechtsgrundlagen
- Status der Umsetzung

Da unter den Kommunen auch die Städte mit eigenem Statut sind, die auch als Bezirksverwaltungsbehörden tätig sind und zunehmend Aufgaben von den Bundespolizeidirektionen übertragen erhalten, wird auch ein Augenmerk auf diesen Bereich gelegt.

1.4.1 Basisdaten zur Person

1.4.1.1 Zentrales Melderegister (ZMR)

Daten	Vorname, Familienname, Geburtsdatum, Geschlecht, Staatsbürgerschaft; Wohnsitz(e), ZMR-Zahl Weiters können Standarddokumente zu Personenstand und Staatsbürgerschaft eingetragen werden.
Eingabe	Meldebehörden, Anmeldung durch Personenstandsbehörden bei der Geburt, Eingabe der Staatsbürgerschaft durch die Evidenzstellen, Änderung von Name und Geschlecht durch Personenstandsbehörden
Abfrage	Meldebehörden Abfrageberechtigte Stellen (Behörden und Notare als Gerichtskommissäre, Sozialversicherungsträger) gem. § 16a Abs. 4 MeldeG, andere Körperschaften öffentlichen Rechts und Private gem. § 16a Abs. 5 MeldeG, Einzelpersonen über das Internet unter https://meldung.cio.gv.at/egovMB/ außer für Meldebehörden gebührenpflichtig, für die Länder Pauschalierung nach § 15 Abs. 5 MeldeV bis Ende 2006.
§	Meldegesetz 1991 (MeldeG) idF BGBl I Nr. 10/2004; Meldegesetz-Durchführungsverordnung (MeldeV) idF BGBl Nr. 274/2004 § 17 E-GovG BGBl. I Nr. 10/2004
Umsetzung	realisiert mit der Anwendung ZMR II des Bundesministeriums für Inneres; in Betrieb; Nach dem Aufbau aus den einzelnen Melderegistern der Gemeinden parallel mit der Volkszählung 2001 ist die Verbesserung der Datenqualität mittlerweile vor allem durch den Abgleich mit den Daten des Hauptverbandes weit fortgeschritten.

1.4.1.2 Firmenbuch

Im Firmenbuch werden eingetragen:
OHG, KG, OEG, AG, GesmbH
Vollkaufleute
Genossenschaften, Versicherungsvereine, Sparkassen
Privatstiftungen, Europäische Interessenvereinigungen und Gesellschaften

Daten	Bezeichnung, Rechtsform, Sitz, Anschrift, Organe und Vertretungsbefugnis elektronische Urkundensammlung im Aufbau auch Berechtigungen aus dem zentralen Gewerberegister (ZGR)
Eingabe	Handelsgerichte, Zugriff auf ZGR
Abfrage	ist öffentliches Buch Einsicht bei den Handelsgerichten und bei Notaren im Internet über Abgabestellen Gebühren laut Verordnung Körperschaften öffentlichen Rechts laut Verordnung über die Bundesrechenzentrum GmbH; gegen Gebühr je Transaktion
§	Firmenbuchgesetz (FBG) Firmenbuchdatenbankverordnung idF BGBl II Nr. 395/2004
Umsetzung	in Anwendung mit Web-Oberfläche; Verfügbarkeit im Portalverbund wünschenswert; bei den natürlichen Personen als Organwalter sollten die bPKs erfasst werden, damit die Vertretungsbefugnis über elektronische Vollmachten abgebildet werden kann

1.4.1.3 Zentrales Vereinsregister (ZVR)

Daten	Bezeichnung, Sitz, Datum des Entstehens, Satzung, Beendigung; ZVR-Nr.; Organe (Identifikation, bPK, Funktion)
Eingabe	Vereinsbehörden (Bezirksverwaltungsbehörden) im Wege über die örtlichen Vereinsregister
Abfrage	Vereinsbehörden, andere Behörden, Körperschaften öffentlichen Rechts jedermann (kostenlos; über Name oder ZVR-Zahl = öffentliches Buch)
§	Vereinsgesetz 2002 (VerG) idF BGBl I Nr. 10/2004, Vereinsgesetz- Durchführungsverordnung (VerGV) BGBl II Nr. 60/2005
Umsetzung	In Anwendung seit Jänner 2006.

1.4.1.4 Dokumentationsregister nach § 115 BAO

Daten	Art der selbständigen Erwerbstätigkeit und Berufsberechtigung
Eingabe	Finanzverwaltung
Abfrage	Auftraggeber des öffentlichen Bereichs auf Ersuchen des Betroffenen, oder Betroffene selbst (erhalten Auszug)
§	§ 16 E-GovG BGBl I Nr. 10/2004
Umsetzung	noch offen

1.4.1.5 Register zur Identifikation für E-Government

Stammzahlenregister (SZR)

Daten	Identifikation und Stammzahl durch Ableitung aus ZMR (nur temporär), Vollmachten
Eingabe	Ableitung aus ZMR, Vollmachten über Antrag der Beteiligten
Abfrage	Auftraggeber des öffentlichen Bereichs, Auftraggeber des privaten Bereichs, Parteienvertreter, Registrierungsstellen über Antrag des Betroffenen www.stammzahlenregister.gv.at
§	E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV) BGBl II Nr. 289/2004 (schafft 36 Bereiche) Stammzahlenregisterverordnung (StZRegV) BGBl II Nr. 57/2005
Umsetzung	Stammzahl in Betrieb, Vollmachten noch offen

Ergänzungsregister natürliche Personen (ERnP)

Daten	wie ZMR, aber ohne Wohnsitz, Ordnungsnummer
Eingabe	Registrierungsstelle über Antrag des Betroffenen, Auftraggeber des öffentlichen Bereichs
Abfrage	Auftraggeber des öffentlichen Bereichs, Auftraggeber des privaten Bereiches Parteienvertreter, Registrierungsstellen über Antrag des Betroffenen
§	E-Government-Bereichsabgrenzungsverordnung E-Gov-BerAbgrV

	BGBl II Nr. 289/2004 (schafft 36 Bereiche) Ergänzungsregisterverordnung (ERegV) BGBl II Nr. 241/2005
Umsetzung	in Betrieb seit 15.11.2005

Ergänzungsregister sonstige Betroffene (ERsB)
Für juristische Personen, die weder im Firmenbuch noch im ZMR eingetragen sind.

Daten	Bezeichnung, Sitz, Anschrift, Rechtsform, vertretungsbefugte Organwalter, Ordnungsnummer
Eingabe	Stammzahlenregisterbehörde, über Einbringungsstellen (Rechtsanwälte, Notare, Wirtschaftstreuhänder), durch Gesetz oder VO eingerichtete Institutionen auch für ihrer Aufsicht unterstehende Einrichtungen
Abfrage	öffentliches Register, jedermann unter www.ersb.gv.at (vorgesehen)
§	Ergänzungsregisterverordnung (ERegV) BGBl II Nr. 241/2005
Umsetzung	in Betrieb

1.4.2 Basisdaten zum Raum

1.4.2.1 Digitale Katastermappe (DKM)
Die DKM ist der technische Teil der Grundstücksdatenbank.

Daten	Festpunktnetz, technische Daten zu den Grundstücken (Nummer, Eckpunkte, Fläche, Änderungen)
Eingabe	Bundesamt für Eich- und Vermessungswesen
Abfrage	ist öffentliches Buch, Online-Zugriff und Abgabe auf Datenträger gebührenpflichtig
§	Vermessungsgesetz (VermG) Grundstücksdatenbankverordnung (GDBV) idF BGBl II Nr. 48/2002 Tarife des BEV siehe www.bev.gv.at
Umsetzung	in Anwendung

1.4.2.2 Grundstücksdatenbank (GDB)

Die Grundstücksdatenbank enthält die rechtlichen

Daten	Einlagezahlen mit Parzellen, Rechten (A-Blatt), Eigentumsverhältnissen (B-Blatt), Lasten (C-Blatt) elektronische Urkundensammlung im Aufbau
Eingabe	Grundbuchsführer bei den Bezirksgerichten
Abfrage	ist öffentliches Buch, Einsicht bei Gericht sowie Online-Zugriff über Abfragestellen gegen Gebühr, Online-Zugriff über die Bundesrechenzentrum GmbH mit Gebühr EUR 1,09 je Transaktion
§	Grundbuchsumstellungsgesetz Grundstücksdatenbankverordnung (GDBV) idF BGBl II Nr. 48/2002
Umsetzung	in Anwendung mit Web-Oberfläche, Verfügbarkeit im Portalverbund wünschenswert, bei den Berechtigten sollten die bPKs erfasst werden, damit die aktuelle Anschrift über das ZMR festgestellt werden kann und eine sichere Zustellung in Verwaltungsverfahren (sicher aber auch für die Justiz) möglich wird

1.4.2.3 Adressregister (ADR)

Daten	Adressen zu Grundstücken, Adressen zu Gebäuden
Eingabe	Gemeinden
Abfrage	Gemeinden (kostenlos), Einzelabfragen über Internet kostenlos Andere Online-Zugriffe oder Abgabe von Datenbeständen kostenpflichtig laut Verordnung; Pauschalierung für die Länder
§	§ 47 Vermessungsgesetz idF BGBl I Nr. 9/2004, Adressregisterverordnung (AdrRegV) StF: BGBl II Nr. 218/2005
Umsetzung	Eingabe zusammen mit Gebäude- und Wohnungsregister noch immer im Aufbau

1.4.2.4 Weitere Daten des BEV

Weiters vertreibt das BEV gegen Entgelt (siehe auf www.bev.gv.at auch Abgabebedingungen und Preise)

- Grundkarten im Maßstab 1 : 50.000 und 1 : 200.000
- Luftbilder
- Orthofotos
- Digitales Geländemodell

1.4.2.5 geoland.at

Unter www.geoland.at stellen die Bundesländer Geodaten grenzübergreifend ins Netz und informieren auch, welche Daten jeweils bei ihnen bezogen werden können.

Hinweisen möchte ich in diesem Zusammenhang auf die bisher leider erfolglosen Verhandlungen zwischen Bund und Ländern zu einer gemeinsamen Geodatenpolitik sowie auf die Arbeiten des EU-Vorschlags für eine RL zur Schaffung einer Raumdateninfrastruktur in der Gemeinschaft, KOM 2004/0175 (Inspire), wonach Geo-Basis-Daten kostenlos zur Verfügung gestellt werden müssten.

1.4.3 Fachdaten zur Person

1.4.3.1 Zertifizierungsdienste

Daten	Person, Signaturprüfdaten (öffentlicher Schlüssel), Dauer der Gültigkeit, Widerruf, weitere Vermerke
Eingabe	Zertifizierungsdiensteanbieter
Abfrage	jedermann über Internet
§	Signaturgesetz
Umsetzung	vom jeweiligen Zertifizierungsdiensteanbieter

1.4.3.2 Strafregister

Daten	Person (sichere Identifikation), gerichtliche Strafen
Eingabe	Justiz
Abfrage	Sicherheitsbehörden, andere Behörden, die die Zuverlässigkeit beurteilen müssen
§	Strafregistergesetz, Sicherheitspolizeigesetz (SPG)
Umsetzung	im Programmpaket EKIS realisiert, in Anwendungen mit Weboberfläche im Portalverbund verfügbar (Sicherheitsklasse 3!)

1.4.3.3 Identitätsdokumenteregister (IDR)

Daten	Person (sichere Identifikation), ausgestellter Reisepass Eintragungen im Reisepass, Passverbot, ausgestellter Personalausweis
Eingabe	Bezirksverwaltungsbehörden
Abfrage	Bezirksverwaltungsbehörden, Exekutive
§	Passgesetz 1992
Umsetzung	realisiert, Produktion beim BMI ermöglicht Abgehen von der Zuständigkeit der Wohnsitzbehörden

1.4.3.4 Fremdeninformationssystem (FIS)

Derzeit sind mehrere Teilanwendungen für die Fremdenpolizei- und Sicherheitsbehörden beim BMI in Betrieb, die aber in einer neuen Anwendung zusammengefasst werden sollen.

1.4.3.5 Führerscheinzentralregister (FSR)

Daten	Person (Identifikation, Anschrift), erteilte Lenkerberechtigungen, Auflagen Entzug der Lenkerberechtigung, Strafen laut Vormerksystem
Eingabe	Bezirksverwaltungsbehörden über die örtlichen Führerscheinregister
Abfrage	Bezirksverwaltungsbehörden, Exekutive
§	Führerscheingesetz (FSG), Führerscheingesetz-Durchführungsverordnung (FSG-DV)
Umsetzung	in Betrieb, wesentliche Änderungen durch Novelle: Antrag kann über Fahrschulen eingebracht werden

1.4.3.6 Hauptverband

Daten	Person, Versicherungsträger, Arbeitgeber
Eingabe	Versicherungsträger
Abfrage	berechtigte Verwaltungsbehörden
§	Berechtigung ist für die einzelne Vollzugsmaterie nachzuweisen
Umsetzung	noch in Anwendung, Einbindung in den Portalverbund 2006

1.4.4 Weitere Fachdaten

1.4.4.1 Kraftfahrzeugzentralregister (KZR)

Daten	Fahrzeughalter (Identifikation, Anschrift) Fahrzeug (Kennzeichen, Zulassung, technische Daten)
Eingabe	aus den örtlichen Registern der Bezirksverwaltungsbehörden und Versicherungen als Zulassungsstellen in der Gemeinschaftsanwendung beim Versicherungsverband
Abfrage	Zulassungsstellen, Exekutive, weitere Behörden, Privatpersonen bei berechtigtem Interesse über die Bezirksverwaltungsbehörden
§	Kraftfahrzeuggesetz (KFG 1967), Kraftfahrzeugdurchführungsverordnung (KDV 1967)
Umsetzung	realisiert in Verbindung mit dem Gemeinschaftsprojekt BMI, Ländern, Versicherungsverband, noch nicht im Portalverbund

1.4.4.2 Zentrales Gewerberegister (ZGR)

Daten	Gewerbeinhaber (Unternehmer/Unternehmen), Gewerbeberechtigungen, gewerberechtliche Geschäftsführer, Betriebsstätten verbunden mit Firmenbuch und Register der Versicherungsvermittler
Eingabe	Gewerbebehörden
Abfrage	jedermann, über Gewerbebehörden kostenlos, im Internet über Abgabestellen (www.bmwa.gv.at/BMWA/Themen/Unternehmen/Gewerbe/Gewerbeordnung/8_gewerberegister.htm), 1,07 je Abfrage, Gewerbebehörden kostenlos über BRZ GmbH, auch über Firmenbuch als Zusatzinformation

§	§§ 365 ff Gewerbeordnung 1994
Umsetzung	3270 Anwendungen, noch nicht im Portalverbund

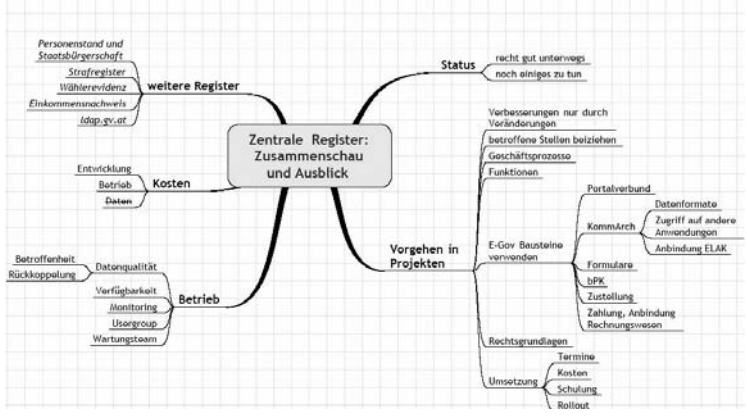
1.4.4.3 Gebäude- und Wohnungsregister (GWR)

Daten	statistische Daten zu Gebäuden, statistische Daten zu Wohnungen
Eingabe	durch Gemeinden als Baubehörden
Abfrage	über Statistik Austria, soll zukünftige periodische Zählungen ersetzen
§	Gebäude- und Wohnungsregistergesetz (GWR-Gesetz) BGBl I Nr. 9/2004
Umsetzung	in Betrieb, Dateneingabe gemeinsam mit Adressregister Problem der Identifikation der Einheiten, da nach den Bauordnungen eine verbindliche Kennung für Wohnungen nicht vorgesehen ist

1.4.4.4 Hilfstabellen

Tabellenbestände, die von vielen Stellen benötigt, aber letztlich von einer zuständigen Stelle gewartet werden, z. B. Staaten und Staatsbürgerschaften, sollen über www.help.gv.at zur Verfügung als Bestand oder Link zur Verfügung gestellt werden

1.5 ZUSAMMENSCHAU UND AUSBLICK



Nach diesem raschen Überblick erscheint ja alles optimal. Ganz so ist es in der Praxis nicht. Der Weg war oft steinig. Doch wenn wir Steine aus dem Weg räumen, können wir ihn auch einmal damit pflastern.

1.5.1 Vorgehen in Projekten: Organisation und Technik

Wenn E-Government Verbesserungen bringen soll, muss es auch zu Veränderungen innerhalb der Verwaltung kommen. Veränderungen nicht nur bei den technischen Hilfsmitteln, sondern in den Arbeitsabläufen bis hin zur Arbeitsverteilung. Dies trifft die Menschen in den Organisationen der Verwaltung und die Organisationen selbst.

Neben dem Fokus auf zentrale Register und wie diese zu ihren Daten kommen, müssen auch die Abläufe in den Organisationen unterstützt werden, wo die Daten entstehen. Dazu gehört auch die Ein- und Anbindung an die lokale EDV-Umgebung - und das eventuell bei 120 Bezirkshauptmannschaften und 2.358 Kommunen.

Zum EDV-Projekt kommt als Herausforderung noch ein Organisationsentwicklungsprojekt hinzu.

Bewährt haben sich hier
- saubere Analysen
- Abstimmung auf breiter Ebene
- Einsatz der E-Government-Bausteine (Portalverbund, Schnittstellen zu Anwendungen und Registern, Formulare, bPK, Zustellung, Zahlungsverkehr)
- Klärung der Finanzierung
- Schaffung der rechtlichen Voraussetzung

1.5.2 Betrieb

Zentrale Register und Anwendungen können großen Nutzen stiften. Sie erzeugen aber auch Abhängigkeiten. Mehr Komponenten und Vernetzung machen die Systeme komplexer.

Die dezentralen Organisationen müssen aber darauf bauen können, dass die Anwendungen verfügbar sind. Vor ihnen stehen die Antragsteller im Bürgerbüro oder in der Gemeindekanzlei und haben kein Verständnis, warum gerade heute nichts weitergeht.

Dasselbe gilt auch für die Komponenten, die von Wirtschaft und Bevölkerung eingesetzt werden sollen. Sie müssen einfach zu installieren und zu bedienen sein und sollen sich nicht laufend ändern.

Als Lösungsansätze möchte ich nur skizzieren
- ausreichend Zeit für Test und Implementierung
- Anleitung und Hilfen für die Betreiber und Anwender
- klare Schnittstellen als Ansatz für Monitoring
- offene Information der Anwender-Usergroup
- Wartungsteam für Abstimmung und Beauftragung von Änderungen und Erweiterungen
- Prozess zur Erreichung und Sicherung der Datenqualität

Österreich ist nicht so groß, dass das nicht noch besser gelingen könnte.

1.5.3 Kosten

Die Kostenfrage ist noch immer ungelöst. Häufig wird die Einhebung von Abfragegebühren durch Gesetz und Verordnung festgelegt. Den bedauernswerten Anwendungsbetreiber bedrängt der Finanzminister von beiden Seiten: kein Geld für die Anwendung, aber möglichst viele Einnahmen erzielen. Dabei wird nicht differenziert, was eigentlich abgegolten wird, die Entwicklungskosten der Anwendung, die Betriebskosten oder der Vertrieb von Daten, die vielleicht sogar von den abfragenden Stellen eingemeldet worden sind.

Damit E-Government nicht am gegenseitigen Rechnung stellen, Budgetieren und Rechnungen prüfen scheitert, brauchen wir größere Lösungsansätze. Wenn vielleicht auch die Summen, um die es geht, nicht so riesig sind, sollten sich doch die Partner am Finanzausgleich einmal damit beschäftigen. Bisher ist das leider noch nicht gelungen.

1.5.4 Weitere Register

Die angeführten Register sind nicht das Ende des Weges. Schon sind weitere Wünsche recht konkret:

1.5.4.1 Personenstand und Staatsbürgerschaft

Das Anführen von Standarddokumenten im ZMR war nur ein Anfang, der sich aus den dort gespeicherten Daten wie Geburtsdatum, Personenstand und Staatsbürgerschaft ergab. Am Ende muss ein zentrales Personenstands- und Staatsbürgerschafts-Register stehen, das direkt von den zuständigen Behörden geführt wird.

1.5.4.2 Strafregister

Sicherheitsbehörden können heute bereits auf das Strafregister online zugreifen. Auch ein Strafregisterauszug kann online beantragt werden, dieser dauert allerdings noch ein paar Tage, da nicht alle alten Daten online zur Verfügung stehen. Anderen bleibt nur der Gang zum Gemeindeamt, die den Antrag aufnimmt. Bis zur Antwort dauert es dann 2 Wochen. Die Gemeinden können nunmehr nach § 5 Abs. 3 E-GovG auch Online-Anträge für den Betroffenen einbringen, eine andere Lösung wäre es, die Gemeinden direkt zu Abfrage und Ausgabe der Bescheinigungen zu ermächtigen. Das bedarf einer Novelle des Strafregistergesetzes.

1.5.4.3 Wählerevidenz

Von da ist es zu einer neuen Wählerevidenz nur ein kleiner Schritt: aktuelle Personendaten, Wohnsitz in Österreich etc.

1.5.4.4 Einkommensnachweis

Für zahllose Verfahren, vor allem bei Förderungen, werden Einkommensnachweise verlangt. Diese sollten über Ermächtigung des Betroffenen auch online über entsprechende Schnittstellen von der Finanzverwaltung beschafft werden können. Eine mustergültige Lösung ist dabei mit den Studienbeihilfen bereits realisiert.

1.5.4.5 ldap.gv.at

Basisdaten über Behörden werden auf verschiedenen Ebenen benötigt:

- im Portalverbund (Kennung der Organisation, Zertifikate)
- bei der Anforderung eines bPK oder Fremd-bPK
- für eine Kooperation der Bürgerportale
- als behördeninternes Verzeichnis und Telefonbuch

Über die technischen Strukturen herrscht schon weitgehend Einigkeit. Der organisatorische Überbau muss noch fertig gestellt werden.

Abschließend noch ein paar Feststellungen und Ziele für die nächsten 2 Jahre:

- Die technisch-organisatorischen Konzepte für E-Government in Österreich sind gut, universell anwendbar und stehen allen offen. Sie sind rechtlich abgesichert. Dabei kommen uns unsere (geringe) Größe und unsere Kooperationskultur zu Gute.
- Jetzt müssen wir sie aber auch in konkreten Anwendungen umsetzen. Wir müssen vom Labor in die raue Wirklichkeit bei 2.358 Gemeinden, bei Bürgerinnen und Bürgern, kleinen Betrieben sowie in unseren eigenen Dienststellen.
- Vernetzung und der E-Government-Baukasten erlauben uns neue Formen der Abläufe; zentrale Daten sind möglich und notwendig – unabhängig davon, ob diese auch lokal zur Verfügung stehen sollen.
- Erfolgreiche Projekte, die auch schlummernde Verbesserungspotentiale heben sollen, brauchen ihre Zeit und können nicht in 4 Wochen während einer verkürzten Gesetzes-Begutachtungsfrist aus dem Boden gestampft werden.

Uns bleibt also weiterhin viel zu tun.

E-Government ist nicht Selbstzweck, sondern Mittel zum Zweck und steht jetzt in unserer Werkzeugkiste zur permanenten Verbesserung der Verwaltung – nach außen, intern und zwischen den Verwaltungsstellen – bereit.

Kapitel 2

AKTUELLES AUS DER STAMMZAHLEN-REGISTERBEHÖRDE – WAS KANN DIE STAMMZAHLEN-REGISTERBEHÖRDE BEREITS ANBIETEN?

MR Dr. Waltraut Kotschy

2.1 ABSTRACT

Integraler Bestandteil des E-Government-Konzepts ist die eindeutige elektronische Identifikation von Personen. Damit verbunden ergibt sich jedoch auch die Notwendigkeit datenschutzrechtlicher Vorkehrungen, um eine Verknüpfbarkeit solcherart eindeutig identifizierter, personenbezogener Daten zu verhindern. Hauptbestandteil dieser Vorkehrungen ist das so genannte „bereichsspezifische Personenkennzeichen" (bPK), ein Code, der sich aus einer verwaltungsbereichsabhängigen Ableitung aus der Stammzahl einer natürlichen Person ergibt. Um ein bPK zu erhalten, bedarf es daher zweierlei Dinge, einerseits einer Stammzahl, die jeder Eigentümer einer Bürgerkarte auf dieser gespeichert hat, andererseits einer Verwaltungsbereichskennzahl, mit der diese Stammzahl verschlüsselt wird. Das Ergebnis ist ein personen- und verwaltungsbereichsbezogener Code, der sich nicht zurückführen lässt und auch keine Verknüpfungen über definierte Verwaltungsbereichsgrenzen erlaubt.

Aus dieser Technik heraus ergeben sich somit einige Anforderungen:

- *Das Tätigkeitsfeld der öffentlichen Verwaltung muss in Verwaltungsbereiche unterteilt werden, deren Kennziffern die Grundlage für eine Ableitung der bPK bilden. Diese Unterteilung betrifft selbstverständlich alle Gebietskörperschaften und damit auch Städte und Gemeinden. Je spezifischer der Aufgabenbereich einer Behörde, desto unkomplizierter ist der Einsatz von bPKs, da nur einer oder wenige Verwaltungsbereiche zum Tragen kommen. Je differenzierter der Aufgabenbereich und je kleiner der Verwaltungsapparat – wie dies in Städten und insbesondere Gemeinden der Fall ist –, desto aufwändiger wird es, bPKs in elektronischen Verfahren einzusetzen; hinzu kommt, dass gerade im kommunalen Bereich viele Verfahren bereichsübergreifend laufen oder im Sinne der Verwaltungsmodernisierung und des Kundenservice (Verfahrensvereinfachung und -verkürzung) miteinander verknüpft wurden, wie dies beispielsweise im Anlagenrecht der Fall ist (Verknüpfung Gewerbeverfahren und Bauverfahren).*

- *Eine Stammzahl wäre eigentlich nur für in Österreich gemeldete Personen (also solche, die im Zentralen Melderegister erfasst sind) vorhanden. Da elektronische Verfahren aber einen wesentlich weiteren Adressatenkreis ansprechen, war es notwendig, auch Vorkehrungen für diese zu treffen: Natürliche Personen, die nicht im ZMR gespeichert sind, können sich im „Ergänzungsregister für natürliche Personen" registrieren lassen und erhalten damit eine Stammzahl. Für im Firmenbuch registrierte Unternehmen ist die Firmenbuchnummer gleichzeitig auch Stammzahl, Gleiches gilt für Vereine mit dem Vereinsregister. Allen übrigen Organisationen, die nicht von einem dieser Register erfasst werden, steht es frei, sich im „Ergänzungsregister für sonstige Betroffene" zu registrieren.*

- *Die Ableitung der bereichsspezifischen Personenkennzeichen kann im Idealfall mittels der auf der Bürgerkarte gespeicherten Stammzahl im Zuge eines elektronischen Verfahrens erfolgen. Da die flächendeckende Verbreitung der Bürgerkarte jedoch noch längere Zeit in Anspruch nehmen wird, ist auch die Möglichkeit vorgesehen, Datenanwendungen direkt durch die Stammzahlenregisterbehörde – also ohne Einsatz einer Bürgerkarte – mit bPKs ausstatten zu lassen.*

Verantwortlich für den Datenschutz in Österreich ist die Datenschutzkommission, in deren Kompetenzbereich fällt auch die Tätigkeit als Stammzahlenregisterbehörde. Eine Erstausstattung von Datenanwendungen mit bPKs erfolgt in zwei Schritten, zuerst ist eine Registrierung beim Datenverarbeitungsregister erforderlich, erst dann kann ein Antrag auf bPK-Erstausstattung bei der Stammzahlenregisterbehörde gestellt werden.

2.2 GRUNDLEGENDE VORBEMERKUNGEN ZUM EINSATZ VON BEREICHSSPEZIFISCHEN PERSONENKENNZEICHEN

Das österreichische E-Government-Konzept verpflichtet die Auftraggeber des öffentlichen Bereichs, nur **bereichsspezifische Personenkennzeichen (bPKs)** in ihren Datenanwendungen einzusetzen: Damit wird die in vielen Teilen der öffentlichen Verwaltung notwendige eindeutige Kennzeichnung von Bürgern ermöglicht, ohne gleichzeitig die datenschutzrechtlichen Nachteile von einheitlichen Personenkennzeichen in Kauf nehmen zu müssen.

Voraussetzung für die Bildung von bereichsspezifischen Personenkennzeichen ist das Vorhandensein einer **Stammzahl.** Diese wird für natürliche Personen, soweit sie in Österreich gemeldet sind, durch Verschlüsselung der ZMR-Zahl gebildet, bei sonstigen natürlichen Personen durch Verschlüsselung der Eintragungszahl im Ergänzungsregister. Der dafür verwendete geheime Schlüssel wird von der **Datenschutzkommission** in ihrer Zuständigkeit als **Stammzahlenregisterbehörde** verwaltet.

Da die Stammzahl nur auf der Bürgerkarte eines Bürgers gespeichert werden darf und dadurch in seinem Herrschaftsbereich verbleibt, darf die Verwaltung in ihren Datenanwendungen zur eindeutigen Identifikation der Bürger keine Stammzahlen verwenden, sondern nur „unterschiedliche" kryptographische Ableitungen aus der Stammzahl, die sogenannten „bereichsspezifischen Personenkennzeichen": Jeder Bürger hat zwar nur eine (quasi-geheime) Stammzahl, aber mehrere unterschiedliche bereichsspezifische Personenkennzeichen, mit welchen er in den behördlichen Datenbanken der unterschiedlichen staatlichen Bereiche gespeichert ist. Die bereichsspezifischen Personenkennzeichen werden aus der Stammzahl durch so genannte **„Einweg**ableitungen" gebildet, d. h. dass man von einem bekannten bereichsspezifischen Personenkennzeichen nicht auf die (quasi-geheime) Stammzahl zurückrechnen kann. Für nicht-natürliche Personen, das sind

zum Beispiel Firmen, Vereine, Organe von Körperschaften öffentlichen Rechts (z. B. Gemeinden, Städte) etc., wird die zu ihrer eindeutigen Identifikation im E-Government notwendige Stammzahl nicht durch ein besonderes kryptographisches Verfahren gebildet und geschützt, da hier kein sinnvolles Interesse an der Geheimhaltung dieser „Identitätsnummer" besteht: Laut Handelsgesetzbuch etwa müssen Firmen ihre Firmenbuchnummer in allen ihren Korrespondenzen öffentlich führen; dasselbe gilt für Vereine und ihre Vereinsregisternummer nach dem Vereinsgesetz. Vor diesem Hintergrund schien es nicht geboten, den elektronischen Identifikator für nichtnatürliche Personen in gleicher Weise zu schützen wie den der natürlichen Personen. Für alle Identitäten, die im Firmenbuch eingetragen sind, wird daher die Firmenbuchnummer als Stammzahl verwendet; Vereine haben als Stammzahl ihre Nummer im Zentralen Vereinsregister. Nichtnatürliche Personen, die weder im Firmenbuch noch im Vereinsregister einzutragen sind, können durch Eintragung in das Ergänzungsregister (siehe Kapitel 2.4) eine eindeutige Identifikationsnummer erhalten, die als Stammzahl verwendet werden kann.

Für nicht-natürliche Personen werden auch keine bereichsspezifischen Personenkennzeichen eigens gebildet - sie scheinen vielmehr in den Datenanwendungen der Verwaltung mit ihrer Stammzahl (= Firmenbuchnummer oder Vereinsregisternummer oder Ergänzungsregisternummer) auf.

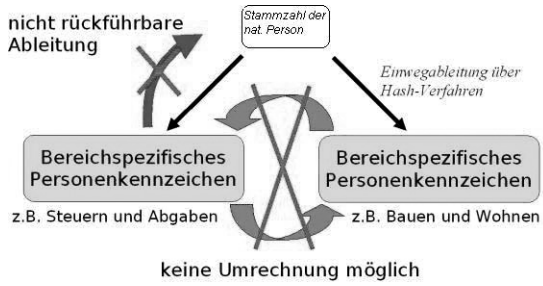
Das bereichsspezifische Personenkennzeichen (bPK) dient zur eindeutigen Identifikation eines Bürgers in einer Datenanwendung einer Behörde. Das bPK ist daher – vergleichbar etwa einem zusätzlichen eindeutigen Namen - ein automationsunterstützt verarbeitetes Datum im Sinne des Datenschutzgesetzes 2000. Deshalb muss es auch in der Meldung der Datenanwendung beim Datenverarbeitungsregister aufscheinen, damit es verwendet werden darf. Handelt es sich um eine Standardanwendung, ist die Frage der Zulässigkeit der Verwendung von bPKs bereits durch die Standard- und Musterverordnung abgeklärt.

Die Bildung eines bPKs erfolgt, wie bereits erwähnt, durch Anwendung eines kryptographischen Verfahrens, und zwar eines Hash-Verfahrens auf die Stammzahl des Bürgers zusammen mit der genormten Bezeichnung jenes Bereichs, dem die Datenanwendung, für die das bPK errechnet werden soll, zugeordnet ist:

[Stammzahl + Bereichsbezeichnung] Hash = bPK

Der Bereich, dem eine Datenanwendung zuzurechnen ist, und seine „genormte" Bezeichnung ergeben sich aus der E-Government-Bereichsabgrenzungsverordnung, BGBl. II Nr. 289/2004, sowie aus den anlässlich der Registrierung der Datenanwendung im Datenverarbeitungsregister getroffenen Festlegungen.

Einwegableitung



Anstoß zur Bildung eines bPK

Der Anstoß zur Bildung eines bPK eines Bürgers für eine bestimmte Datenanwendung kann nun in zweifacher Art geschehen:

Einmal dadurch, dass sich der Bürger elektronisch mit Hilfe seiner Bürgerkarte an die Behörde wendet; bei der Kommunikation mit einer bürgerkartenfähigen Datenanwendung wird das bPK automatisch gebildet und der Datenanwendung zur Verfügung gestellt.

Da die flächendeckende Verwendung der Bürgerkarte jedoch noch lange nicht erreicht sein wird und ein wichtiges Interesse an einer qualitätvollen eindeutigen Identifikation der Bürger in der Verwaltung schon derzeit vielfach besteht, bietet das E-GovG auch die Möglichkeit, die Datensätze einer Datenanwendung auf Antrag einer Behörde mit bPKs ausstatten zu lassen, und zwar durch entsprechendes Herantreten an die Stammzahlenregisterbehörde.

Im Folgenden sollen die Verfahren zur Erlangung von bPKs, so wie sie derzeit von der Stammzahlenregisterbehörde angeboten werden, dargestellt werden.

2.3 DIE ERRECHNUNG VON BPKS DURCH DIE STAMMZAHLENREGISTERBEHÖRDE OHNE EINSATZ DER BÜRGERKARTE DES BETROFFENEN BÜRGERS

Bei jedem Neuzugang von Datensätzen in einer Datenanwendung mit personenbezogenen Daten stellt sich das Problem der eindeutigen Identifizierung des Betroffenen, wenn dieser keine Bürgerkarte verwendet hat. Das österreichische E-Government-Konzept stellt den Behörden hiefür eine Online-Abfrage an das Stammzahlenregister zur Verfügung, durch die das bPK zur Identifizierung – bei Vorliegen gewisser Voraussetzungen – errechnet werden kann.

Bei der Umstellung der Verwaltung auf E-Government-Applikationen wäre allerdings die bPK-Errechnung im Wege von Einzelabfragen an das Stammzahlenregister ein äußerst mühsamer Prozess, weshalb für die Erstausstattung einer Datenanwendung mit bereichsspezifischen Personenkennzeichen ein eigenes Verfahren (§ 10 Abs. 2 E-GovG) entwickelt wurde, das von der Stammzahlenregisterbehörde nunmehr bereits als Service angeboten wird. Sein Ablauf soll in der Folge näher beschrieben werden.

2.3.1 Die Erstausstattung einer gesamten Datenanwendung mit bPKs

Wenn eine gesamte Datenanwendung mit bPKs ausgestattet werden soll, besteht[1] die Möglichkeit, bei der Stammzahlenregisterbehörde eine Erstausstattung mit bPKs zu beantragen.

2.3.1.1 Die Registrierung im DVR als Antragsvoraussetzung

Damit einem Antrag auf Erstausstattung entsprochen werden kann, muss zuerst die Datenanwendung, die mit bPKs ausgestattet werden soll, beim Datenverarbeitungsregister registriert sein, und zwar mit der Datenart „bPK". Vor jedem Antrag sollte daher geprüft werden, ob diese Voraussetzung von der für die Datenverarbeitung verantwortlichen Stelle durch entsprechende Meldung an das DVR tatsächlich bereits geschaffen wurde.

Wenn eine Standardverarbeitung durchgeführt wird, ist bereits durch die Standard- und Musterverordnung geregelt, inwieweit ein bPK verarbeitet werden darf. In allen anderen Fällen muss der Auftraggeber der Datenanwendung unter Zugrundelegung der Bereichsabgrenzungsverordnung[2] seine Datenanwendung einem der dort festgelegten Bereiche zuordnen und in die Registrierung der Datenart „bPK für diesen Bereich" in seiner Datenanwendung beim Datenverarbeitungsregister (DVR) beantragen.[3] Sobald im DVR diese Registrierung vorgenommen wurde, kann der Antrag auf bPK-Erstausstattung bei der Stammzahlenregisterbehörde gestellt werden.

2.3.1.2 Der Antrag auf Erst-Ausstattung

Zur Antragstellung stellt die Stammzahlenregisterbehörde auf www.stammzahlenregister.gv.at ein Formular zur Verfügung, in dem folgende Angaben gemacht werden müssen:

- Name (sonstige Bezeichnung) und Anschrift des Auftraggebers
- Name, Telefonnummer und E-Mail-Adresse des Sachbearbeiters beim Auftraggeber
- Das Verwaltungskennzeichen des Auftraggebers[4]
- Die DVR-Nummer des Auftraggebers
- Die laufende Nummer und Bezeichnung der registrierten Daten- oder Musteranwendung – beides ist im öffentlichen DVR-Register jederzeit einsehbar, bzw. dem Registerauszug aus dem DVR zu entnehmen
- Alternativ dazu ist, wenn es sich bei der Datenanwendung um eine Standardanwendung handelt, diese entsprechend dem in der Standard- und Musterverordnung enthaltenen Code zu bezeichnen (z. B. „SA024")
- Die Anzahl der mit bPKs auszustattenden Datensätze (in Größenordnungen: z. B. 1.000 oder 10.000 oder 100.000 etc.)

---

1 Gem. § 17 der Stammzahlenregisterverordnung

2 Siehe dazu die E-Government-Bereichsabgrenzungsverordnung BGBl II, 2004, 289. Verordnung vom 15. 07.2004

3 http://www.dsk.gv.at/formd.htm

4 Das Verwaltungskennzeichen ist ein eindeutiges Kennzeichen für Organisationseinheiten der öffentlichen Verwaltung. Es setzt sich zusammen aus Ebene (z. B. Bund, Gemeinde, Land), Bereich (z. B. FA, GA, 5BA) und einem Schlüssel (Zahl). Siehe dazu: http://reference.e-government.gv.at/uploads/media/vkz-1-1-0-2003-0515_02.pdf

Die Stammzahlenregisterbehörde prüft den Antrag und leitet ihn, wenn alle Voraussetzungen vorliegen, zur Ausführung an das BMI/ZMR weiter. Die Art der Übergabe der Daten ist vom Auftraggeber mit dem BMI zu vereinbaren.

Für das Gelingen der eindeutigen Identifikation der Betroffenen aufgrund der dem BMI/ZMR zur Verfügung gestellten Identitätsdaten ist die Qualität dieser Daten entscheidend.

2.3.1.3 Datenqualität

Als Ergebnis des Vergleichs- und Errechnungsvorgangs sind neben den Antragsdaten bPKs nur für jene Personen rückzumitteln, die aufgrund der übermittelten Daten einem Eintrag im ZMR oder im Ergänzungsregister eindeutig zugeordnet werden konnten (§ 15 Abs. 3 der Stammzahlenregisterverordnung).

Ein bPK kann nur dann generiert werden, wenn die übermittelten Daten einen eindeutigen Treffer ergeben. Es müssen zumindest Familienname, Vorname und Geburtsdatum korrekt übermittelt werden. *Besonders bei häufig vorkommenden Namen werden diese 3 Attribute aber nicht ausreichen, sodass aufgrund von Mehrfachtreffern kein bPK ermittelt werden kann.*

2.3.1.4 Ergänzungsregister

Personen, die im ZMR nicht gefunden werden, können im Ergänzungsregister für natürliche Personen eingetragen werden. Die dort bei der Eintragung vergebene Ordnungszahl wird in der Folge als Stammzahl verwendet.

Der Abschluss der Entwicklungsarbeiten an diesem Teil des Ergänzungsregisters steht unmittelbar bevor, sodass davon ausgegangen werden kann, dass dieser Dienst von der Stammzahlenregisterbehörde Ende dieses Jahres angeboten werden kann.

2.3.2 Die Bildung von bPKs im Wege von Einzelabfragen an das Stammzahlenregister

Die Einzelabfrage wird meist erst in zweiter Stufe eingesetzt werden, d. h. nachdem zuerst die Gesamtausstattung einer Datenanwendung mit bPKs vorgenommen wurde und sich in der Folge Neuzugänge ereignen, die nicht mit einer Bürgerkarte an die Behörde herangetragen wurden. Die Einzelabfragen des Stammzahlenregisters zur bPK-Errechnung erfolgen im Online-Dialog, wobei sehr kurze Antwortzeiten angestrebt werden.

2.3.2.1 Registrierung

Auch diese Vorgangsweise setzt voraus, dass die Datenanwendung, für die bPKs errechnet werden sollen, in entsprechender Weise im DVR registriert ist. Dies muss jedoch nicht in jedem Einzelfall nachgewiesen werden, sondern wird vollautomatisch geprüft: Die betroffene Datenanwendung ist durch eine eindeutige Zahl im DVR gekennzeichnet, die auch in der Errechnungsabfrage für Zwecke des Abgleichs anzugeben ist.

2.3.2.2 Zugang zur Einzelabfrage

Es ist vorgesehen, dass der Zugang zur StZReg-Abfrage über den Portalverbund genommen wird: Das Stammzahlenregister ist eine Applikation im Portalverbund. Ein Abfragender muss

daher die im Portalverbund vorgesehenen Berechtigungen besitzen und in der erforderlichen technischen Umgebung[5] arbeiten, um seinen Request abschicken zu können und die Antwort zu erhalten.

Die Zugangsberechtigungen werden vom jeweils befugten Portaladministrator (Leituser) vergeben.

Die Eingliederung der bPK-Abfrage in den Arbeitsprozess erfolgt in derselben Weise wie bei anderen Anwendungen im Portalverbund.

Das Transportprotokoll ist ein durch TLS (Transport Layer Security)[6] mit verpflichtendem Client-Zertifikat gesichertes http (HyperText Transmission Protocol), und der Austausch der Nachrichten erfolgt nach dem Standard SOAP (Simple Object Access Protocol) 1.1.[7] Durch den Einsatz dieser standardisierten Datenaustauschprotokolle wird eine größtmögliche Freiheit bei der Entwicklung und Gestaltung der darauf beruhenden Anwendungen sichergestellt.

2.3.2.3 Datenqualität

Weiters ist eine möglichst gut geprüfte und bereinigte Führung der Stammdaten der betroffenen Bürger (Datenqualität) notwendig, um im StZReg erfolgreich die Berechnung eines bPK abfragen zu können. Im Folgenden sei an einigen Beispielen[8] gezeigt, wodurch erfolglose Anfragen verursacht sein können:

ZMR-Eintrag	Ihre Suche	Ergebnis
Vorname = Gabriela	Gabriele Gaby	kein Treffer kein Treffer
Vorname = Karl Heinz	Karl-Heinz Karl Heinz	kein Treffer wird gefunden – Karl Heinz kein Treffer (es muss der erste Vorname sein)
Marie-Luise	Marie Luise Marie	wird gefunden – Marie-Luise kein Treffer
Familienname = Müller-Meier	Müller Müller Meier Meier-Müller	kein Treffer kein Treffer kein Treffer
Bečak	Becak	wird gefunden – Bečak

[5] Siehe dazu die technischen Spezifikationen des BM.I. auf der Webseite: https://portal.bmi.gv.at/ref/szr
[6] http://www.ietf.org/html.charters/tls-charter.html
[7] http://www.w3.org/TR/soap/
[8] www.jusline.at

2.3.3 Die Basisfunktionen des Stammzahlenregisters für Einzelabfragen[9]

- **GetBPK:** Mit dieser Funktion können bPKs abgefragt bzw. ermittelt werden, wenn die Identifikationsdaten bekannt sind. Die Stammzahlenregisterbehörde liefert somit das bereichsspezifische Personenkennzeichen (bPK) für die in der Anfrage eindeutig identifizierte natürliche Person und den entsprechend angegebenen Bereich. Bei dieser Funktion hängt das Ergebnis wesentlich von der Qualität der verfügbaren Personendaten ab.

- **TransformBPK** „transformiert" bPKs, das heißt ein bPK aus dem eigenen Bereich wird in ein bPK eines anderen Bereiches umgerechnet und dem Anfragenden – mit dem Schlüssel des Adressaten verschlüsselt[10] – zur Verfügung gestellt.

- **ValidateIdentityLink** kann eine Personenbindung gegen das Basisregister vergleichen.[11] Geprüft werden dabei die Gültigkeit der elektronischen Signatur der Personenbindung sowie die Zugehörigkeit der Stammzahl zu der in der Personenbindung bezeichneten natürlichen Person. Als zusätzliche Dienstleistung kann mit dieser Anfrage auch ein bPK für einen anzugebenden Zielbereich („Fremd-bPK") aus der Stammzahl der Personenbindung abgeleitet werden.

Diese Einzelabfragen stehen den im Portalverbund zur Abfrage des Stammzahlenregisters befugten Organwalter im Online-Zugriff zur Verfügung. Jede Abfrage wird zur allfälligen Kontrolle missbräuchlicher Verwendung protokolliert.

2.3.4 Errechnung von FremdbPKs auf Vorrat

Für diesen Vorgang – der jeweils mit größerem Rechenaufwand verbunden ist, da er grundsätzlich alle Datensätze einer Datenanwendung betrifft – ist ebenso wie für die Erstausstattung von Datenanwendungen mit bPKs jeweils eine eigene Vereinbarung mit der Stammzahlenregisterbehörde erforderlich.

Wenn regelmäßig, insbesondere aufgrund gesetzlicher Anordnung, personenbezogene Daten aus einer Datenanwendung an Datenwendungen eines anderen Bereichs übermittelt werden müssen, dürfen die beim Übermittlungsempfänger verwendeten bPKs in verschlüsselter Form beim Übermittelnden auf Vorrat gespeichert und im Anlassfall mit übermittelt werden, um fehlerhafte Zuordnungen beim Übermittlungsvorgang zu vermeiden (§ 17 der Stammzahlenregisterverordnung).

[9] https://portal.bmi.gv.at/ref/szr/specszr.pdf
[10] Dadurch kann nur der Empfänger „sein bPK" entschlüsseln und in seiner Datenanwendung verwenden.
[11] Eine Personenbindung ist ungültig, wenn eine Person gestorben ist oder die Signatur nicht validiert werden kann.

Zu diesem Zweck müssen über ein auf www.stammzahlenregister.gv.at zur Verfügung gestelltes Formular folgende Angaben gemacht werden:

- Für welchen Bereich FremdbPKs beantragt wird
- Für welche Behörde diese FremdbPK beantragt wird
- Der öffentliche Verschlüsselungsschlüssel der Behörde, der die Daten übermittelt werden sollen. Der öffentliche Schlüssel dieser Behörde ist vom Antragsteller im Antrag an die Stammzahlenregisterbehörde anzugeben. Dies ist erforderlich, solange es noch keinen zentralen Verzeichnisdienst gibt, bei dem die Zertifikate (Schlüssel) der Behörden hinterlegt werden müssen.
- Die Rechtsgrundlage der beabsichtigten Datenübermittlung: Dies dient der Kontrolle der Einhaltung der Zuständigkeiten der involvierten Behörden.

2.4 DAS ERGÄNZUNGSREGISTER FÜR SONSTIGE BETROFFENE

Als weiteres wichtiges Service neben der bPK-Berechnung und -Umrechnung bietet die Stammzahlenregisterbehörde den Organen von Gebietskörperschaften die Möglichkeit an, eine elektronische Identität für den Privatwirtschaftsverkehr zu erlangen durch Eintragung in das „Ergänzungsregister für sonstige Betroffene (ERsB)“. In diesem Register können auch die Vertretungsbefugnisse eingetragen und damit elektronisch nachgewiesen werden – das Register ist öffentlich über das Internet einsehbar.

Das Ergänzungsregister für sonstige Betroffene wurde eingerichtet, um jenen Entitäten, die weder im ZMR noch im Firmenbuch noch im Vereinsregister eingetragen werden können, die elektronische Kommunikation im E-Government zu ermöglichen, indem eine Stammzahl für sie generiert wird. Dies gibt auch öffentlichen Stellen, die im Rahmen der Privatwirtschaft agieren wollen, die Möglichkeit, eine elektronische Identität zu erlangen.

Das Ergänzungsregister für sonstige Betroffene ist im Wege des Portalverbunds für Eintragungen erreichbar bzw. über die Webseite www.ersb.gv.at öffentlich einsehbar.

Institutionen, die unmittelbar durch Gesetz oder Verordnung eingerichtet sind, können für sich und für ihre Teilorganisationen bzw. für die ihrer gesetzlichen Aufsicht unterliegenden Organisationen einen Antrag auf Eintragung in das ERsB direkt an die Stammzahlenregisterbehörde stellen.[12] Die Vorgangsweise ist auf der Webseite der Stammzahlenregisterbehörde näher erläutert.

[12] Siehe dazu § 10 Abs. 1 der Ergänzungsregisterverordnung

Kapitel 3

E-GOVERNMENT IN DER PRAXIS DER GEMEINDE-VERWALTUNG

Erhard Vallant

3.1 ABSTRACT

„Anspruch und Wirklichkeit“ titelt das erste Kapitel des nachfolgenden Beitrages. E-Government wird gerne als Instrument, ja sogar als Motor der Verwaltungsmodernisierung bezeichnet. Tatsächlich konnten in den letzten Jahren viele Probleme und Hürden in Zusammenhang mit einer elektronischen Verfahrensabwicklung beseitigt werden. E-Government war auch unbestritten ein Antrieb zu verwaltungsübergreifender Kooperation und hat Reformmaßnahmen in anderen Bereichen begünstigt oder sogar initiiert.

Dennoch darf nicht übersehen werden, dass E-Government in nur wenigen Jahren tief in bestehende Verwaltungsstrukturen eingreift, die in Jahrhunderten gewachsen sind – und damit auch in die Arbeitswelt tausender öffentlich Bediensteter. Daher wird es einerseits notwendig sein, den unmittelbar betroffenen Mitarbeitern und auch den Anwendern den Nutzen von E-Government zu vermitteln, andererseits aber auch jenen Bereichen der Verwaltung besonderes Augenmerk zu widmen, wo durch gezielte Technikunterstützung massive Effizienzsteigerungen bzw. Ressourceneinsparungen möglich sind.

Verfahren wie „Hundeanmeldung“ oder „Heurigenanmeldung“ im Sinne von E-Government elektronisch abzubilden, mag zwar im Sinne eines Pilotversuchs sinnvoll sein, das eigentliche Innovations- und Einsparungspotential liegt aber in anderen, wesentlich transaktionsintensiveren und vor allem verwaltungsübergreifenden Verfahren. So gibt es beispielsweise zwischen Personenstandsbehörden ein umfassendes Mitteilungswesen und das Personenstandwesen insgesamt zeichnet sich durch extrem hohe Datenkonsistenz und hohe Fallzahlen aus. Allerdings beschränkt sich der datenmäßige Wirkungskreis – bis auf seit kurzem vornehmbare, punktuelle Anmerkungen im ZMR (Standarddokumentenregister) – auf den örtlichen Bereich.

Ein weiterer Bereich, in dem noch Nachholbedarf in Bezug auf E-Government besteht, ist das Wahlwesen. Die Bandbreite reicht hier von einer Umstellung auf elektronische Stimmabgabe bis hin zur Durchführung von Wahlen in Form von E-Voting. Innovations- und Einsparungspotential wäre aufgrund des hohen Volumens an Anwendungsfällen jedenfalls vorhanden.

Weitere Reformvorschläge in Bezug auf bestehende E-Government-Applikationen betreffen Verbesserungen bei bestehenden Registern sowie eine verbesserte Abstimmung zwischen den Registern. So könnte in vielen Bereichen durch einfache ZMR-Abfrage auf das Beibringen einer Meldebestätigung verzichtet werden. Änderungen bei Adressbeständen wie beispielsweise der Wohnadresse sollten sich automatisch auch auf andere Register wie z. B. das KFZ-Register oder das Waffenscheinregister übertragen.

Auf der anderen Seite sollte auch bei E-Government das Subsidiaritätsprinzip stärker als bisher forciert werden gemäß dem Grundsatz, dass „Daten dort zu verarbeiten sind, wo sie entstehen“. Hier besteht im Bereich der Datenübermittlung für die Wählerevidenz noch massiver Nachholbedarf und auch die Aktivitäten rund um die Abkopplung der bisher lokal verfügbaren Meldedaten im Rahmen eines „webbasierten lokalen Meldewesens“ sind vor

dem Hintergrund der daraus resultierenden Folgen für andere lokale Kompetenzbereiche wie Statistik oder Stadtplanung zu überdenken.

Ein weiteres lokales Register, das von den Städten und Gemeinden (bzw. Staatsbürgerschaftsverbänden) geführt wird, ist die Staatsbürgerschaftsevidenz, der in Form eines zentralen Registers ebenfalls erhebliches Reformpotential innewohnen würde.
Natürlich bedarf es zwischen den bestehenden (und allfälligen noch neu hinzukommenden) Registern eines qualifizierten Abgleichs. Dass dieser nicht unproblematisch ist, hat bereits die Synchronisation von ZMR, Gebäude- und Wohnungsregister sowie Adressregister gezeigt. Für die vorgesehene Registerzählung wird daher noch einiges an Abstimmungsarbeit zu leisten sein.

Trotz positiver Einstellung zu E-Government stellt der Beitrag unmissverständlich fest, dass noch zahlreiche offene Fragen zu klären sind und zeigt wesentliche Bereiche und Maßnahmen auf, die bisher trotz vorhandenem Reform- und Einsparungspotential zu stark vernachlässigt wurden.

3.2 ANSPRUCH UND WIRKLICHKEIT

Die E-Government-Offensive des Bundes hat in Kooperation mit Ländern, Städten und Gemeinden viele Projekte erfolgreich abgeschlossen. Neben der verstärkten Pflege der Registerkultur lag der Schwerpunkt der Aktivitäten vor allem in der Realisierung der Rahmenbedingungen für den elektronischen Transaktionsdienst. Auch der elektronische Zugang zu Verwaltungsinformationen und zu den öffentlichen Dienstleistungen für Bürger und Wirtschaft wurde auf allen Verwaltungsebenen vorangetrieben. Die Städte und Gemeinden haben weitgehend ihre internen Verwaltungsabläufe optimiert und automatisiert und vor allem die größeren Städte haben eigene E-Government-Anwendungen erfolgreich umgesetzt.

Man muss sich jedoch die Frage stellen, ob dadurch schon jenes Ausmaß an Informatisierung unseres Verwaltungsvollzuges und unserer Verwaltungsprozesse erreicht wurde, das der großen Masse der Menschen das Leben mit der als lästig empfundenen Bürokratie tatsächlich erleichtert, ob es weiters in den Städten und Gemeinden in den ressourcenintensiven Verwaltungsbereichen, wo wir im Auftrag des Bundes tätig sind, zumindest Ansätze von Kosteneinsparungen und Spuren von flächendeckenden elektronischen Services gibt.

Die jüngste Umfrage von Dr. Ronald Sallmann (Public Management Consulting) unter 56 Mitgliedsgemeinden des Städtebundes hat, kurz gefasst, u. a. festgestellt: „Sehr hohe Erwartungen werden der Wirtschaft und den Bürgern zugeordnet, bei hohen Kosten für die Verwaltung bei im Moment niedriger Akzeptanz bei Bürgern und Mitarbeitern“. Diese Rahmenbedingungen müssen uns nachdenklich stimmen.

Endziel jeder E-Government-Strategie muss wohl sein, dass ganz am Ende als Ergebnis dieser Informatisierung der Verwaltung eine möglichst große Zahl selbst handelnder Bürger sich auf elektronischem Weg die notwendigen Infos selbst holt und elektronische Transaktionen völlig

selbständig durchführt. Jeder vom Bürger ausgelöste Geschäftsprozess soll durch Technikunterstützung sowohl hinsichtlich des Zuganges, aber auch des Ablaufes effizient und ressourcensparend vor sich gehen.

Auf den Bürger bezogen, sind solche allgemeinen informationstechnischen Infrastrukturen derzeit – vor allem verwaltungsübergreifend – nur in Ansätzen vorhanden. Dies soll im Folgenden an einem Verwaltungsbereich (Meldeamt, Wahlamt, Standesamt, Passamt, Staatsbürgerschaftsstelle, Fundamt) veranschaulicht werden, in dem es um die Verarbeitung personenbezogener Daten im engeren Sinne geht.

Dies deshalb, weil in diesem Verwaltungsbereich fast 45 % aller Kundenkontakte einer Stadtverwaltung registriert werden können. Es ist außerordentlich lobenswert, sich darüber den Kopf zu zerbrechen, wie man Gewerbeanmeldungen, Baustellenmanagement, Grundstücksverkehr, Heurigenanmeldung etc. E-Government-fähig machen kann. Das ist zweifellos wirtschaftsfreundlich und nützt dem Wirtschaftsstandort Österreich. Aber das sind nicht die großen kostenintensiven Aufgaben einer Kommunalverwaltung. Hinzu kommt, dass man den Menschen nicht erklären kann, warum in Bereichen mit den weitaus häufigsten Kundenkontakten elementare informationstechnische Infrastrukturen fehlen.

Um jedes verengte Verständnis von E-Government hintanzuhalten, sollte vom Standpunkt einer Kommunalverwaltung folgende elektronische Infrastruktur für ein erfolgreiches E-Government vorhanden sein.

1. Die Bereitstellung leicht auffindbarer und verständlicher Informationen (Homepage)
2. Die elektronische Abwicklung von Verfahren (Transaktionsdienste, standardisierte E-Formulare)
3. Die Automatisierung (Optimierung) von internen Verwaltungsabläufen
4. Die elektronische Datenhaltung im Hintergrund (Register, Informationsverbund)
5. Die verpflichtende Nutzung vorhandener elektronischer Infrastrukturen
6. Einfache und komfortable Bedienung der Applikationen mit entsprechender Ausstattung von Schnittstellen zu anderen Registern (Usability)

Vor allem bei den Punkten 5 und 6 ist darauf zu achten, dass die gemeinsame Nutzung von Daten den Datenschutzgrundsätzen entspricht.

3.3 DAS STANDESAMT – EINE BEHÖRDE ALS VERVIELFÄLTIGUNGSMASCHINE

Im Bereich des Personenstandswesens hat die österreichische Registerkultur wohl den größten Nachholbedarf. Zwar haben die Städte und Gemeinden (Standesamtsverbände) seit Jahrzehnten anwender- und bürgerfreundliche Standesamts-Programme in Verwendung, jedoch eingeschränkt auf ihren jeweils örtlichen Bereich und mit unterschiedlichem Nacherfassungsgrad.

Es ist evident, dass eine korrekte und präzise geführte Personenstandsverwaltung für jede Gesellschaft von existenzieller Bedeutung ist. Die Vollziehung des Personenstandsrechtes durch

die Städte und Gemeinden hat in Österreich traditionell erstklassige Qualität. Zwar unauffällig im Hintergrund tätig, sind die Standesämter umso effizientere Servicestellen für den Bürger.

Allerdings funktionieren sie nach wie vor wie riesige Kopiermaschinen. Da gibt es die Mitteilungspflichten innerhalb der Personenstandsbehörden und zusätzlich an jene, so gegen die 20 Behörden und Institutionen, denen Personenstandsfälle laufend zu übermitteln sind. Das entspricht ca. 750.000 Poststücken, die Jahr für Jahr kreuz und quer in Österreich unterwegs sind.

Überdies normiert die Personenstandsdatenverordnung die Mitteilungspflicht aller Personenstandsfälle an die Gebietskrankenkasse (seit 1.9.2004 ausgesetzt, da EDV-Applikation noch nicht realisiert). Neu ist, dass ab 1.1.2006 alle Eheschließungen unter Beteiligung eines Drittstaatlers der Fremdenpolizeibehörde mitzuteilen sind.

Die Personenstandsregister sollten eigentlich die Basisregister für alle weiteren personenbezogenen Verwaltungsregister sein, insbesondere was die richtige Schreibweise der Namen der Menschen betrifft. Der österreichische Staat hat sich aber nie ernsthaft darum gekümmert, dass sich der personenstandsrechtliche Standard in der Namensführung auch verbindlich durch alle weiteren staatlichen Register zu ziehen hat. So weisen mehr als ein Drittel der Reisedokumente eine falsche oder unvollständige Namensführung auf; sogar so manche Bürgerkarte ist schon mit diesem Makel behaftet.

Beim ZMR hat sich dies erstmals als gravierender Mangel herausgestellt, weil durch unterschiedliche Namensführung die Personensuche beträchtlich erschwert wird. Vor allem bei der Vorbereitung der Registerzählung wird man feststellen, dass die unterschiedliche Namensführung einer Person in verschiedenen Registern erheblichen zusätzlichen Arbeitsaufwand bedeuten wird. Hauptbetroffen vom IT-Defizit des Bundes im Personenstandswesen sind naturgemäß die Städte mit Krankenanstalten. Unter der Last der Bürokratie denken diese daher laufend darüber nach, wie man in diesem Bereich Verwaltungsabläufe weiter optimieren könnte. Die Vernetzung mit den Krankenanstalten für die elektronische Übermittlung der Geburten und Sterbefälle ist hiebei ein wichtiges Thema.

Abhilfe wird nur ein vom Bund betriebener Informationsverbund in Form eines zentralen Personenstandsregisters schaffen. Kürzlich wurde in Slowenien und in der Schweiz ein zentrales Personenstandsregister eingeführt. In Österreich drängt die Zeit, weil naturgemäß solche Register erst nach vielen Jahren für den Bürger ihre volle Wirksamkeit entfalten.

3.4 E-GOVERNMENT UND WAHLEN – AUFHOLBEDARF IN ÖSTERREICH

Ein in jeder Hinsicht unbeackertes Feld in Bezug auf E-Government ist in Österreich die Abwicklung von Bundes-, Landes- und Gemeindewahlen inklusive aller Formen der direkten Demokratie wie Volksbegehren, Volksentscheide etc.

Einige Städte haben schon vor Jahren ihre Abstimmungsverzeichnisse für Volksbegehren von Papier auf elektronische Datenträger umgestellt und die elektronische Beantragung von Wahlkarten

ist zur Selbstverständlichkeit geworden. Allerdings geschieht dieses ohne formellen Identitätsnachweis. Da die elektronische Identität ohne digitale Signatur leicht fälschbar ist, ist hier die Möglichkeit eines Missbrauchs immer gegeben. Jetzt allerdings diesen Wahlkartenantrag bürgerkartenpflichtig zu machen, würde wahrscheinlich einen mittleren Aufstand unter den Wahlberechtigten verursachen.

Es liegt in der Natur der Sache, dass die mit der Abwicklung von Wahlen notwendige Präzision ein hohes Maß an kostenintensiver Bürokratie verursacht. Die Kernfrage lautet daher: Wie bekommt man den Geschäftsprozess „Abwicklung von Wahlen" technologisch so in den Griff, dass einerseits die Verwaltung Personalressourcen und damit Kosten spart und gleichzeitig Endergebnisse rasch verfügbar sind. Andererseits sollte die unbürokratische Teilnahme an der Wahl allen Alters- und sozialen Bevölkerungsschichten ohne Einschränkung möglich sein und die verfassungsrechtlichen Prinzipien in jeder Hinsicht gewahrt bleiben. Diesbezügliche Überlegungen werden weltweit angestellt und auch in vielen Ländern konkrete E-Government-Projekte umgesetzt. In Österreich besteht hier vor allem im Bereich der Gesetzgebung beträchtlicher Aufholbedarf.

3.4.1 E-Voting

Die Stimmabgabe erfolgt beim E-Voting über das Internet und nicht im Wahllokal. Diese Form der elektronischen Wahl wurde bisher vor allem bei der Wahl von Studentenparlamenten und Belegschaftsvertretungen erfolgreich umgesetzt. In Österreich hat Prof. Dr. Alexander Prosser mit der ersten Online-Wahl an der WU Pionierarbeit geleistet. Bei Wahlen in die allgemeinen Vertretungskörper wurde E-Voting auch im Ausland kaum noch praktiziert.

E-Voting wirft ähnliche Probleme auf wie die Briefwahl. Es wird bezweifelt, ob diese Form der Stimmabgabe mit den Grundprinzipien des freien, geheimen und persönlichen Wahlrechtes in Einklang zu bringen ist. Tatsächlich haben Untersuchungen, vor allem in der Schweiz, gezeigt, dass fast 50 % der Wahlberechtigten bezüglich E-Voting Sicherheitsbedenken haben. Und dies, obwohl von Experten glaubhaft versichert wird, dass es nicht möglich sei, Einzelstimmen zu hacken oder zurückzuverfolgen. Aufgrund der hohen Sicherheitsvorbehalte in der Bevölkerung wird aber die Stimmabgabe via Internet dennoch zumindest mittelfristig bei Bundes-, Landes- bzw. Gemeindewahlen in Österreich ausscheiden.

Anders bei Auslandsösterreichern: Durch die in diesem Bereich de facto praktizierte Briefwahl werden heute schon die Grundprinzipien „geheim und persönlich" faktisch durchbrochen. Darüber hinaus ist die Abwicklung des Auslandsösterreicher-Wahlrechtes sehr kostenintensiv. Es erscheint daher nur sinnvoll, E-Voting bei Auslandsösterreichern zuzulassen.

Ein klassischer Anwendungsfall für E-Government ist das Volksbegehren sowie die diversen Unterstützungserklärungen. Die Möglichkeit der Abgabe der Unterschrift über das Internet mittels digitaler Signatur wäre nicht nur eine beträchtliche Erleichterung, sondern auch ein wichtiger Beitrag zur Verbesserung der politischen Partizipation.

3.4.2 Elektronische Wahlgeräte

Elektronische Wahlgeräte ersetzen im Wahllokal den Stimmzettel. Weltweit in Verwendung, gibt es darüber in Österreich nicht einmal den Ansatz einer Diskussion. In Deutschland haben bei der letzten Bundestagswahl schon fast 5 % der Wahlberechtigten in 65 Städten papierlos gewählt. Die rechtlichen Rahmenbedingungen hiefür wurden in der BRD bereits im Jahre 1999 geschaffen. Die Akzeptanz bei den Wahlberechtigten kann aufgrund der bisherigen Erfahrungen als „sehr gut" eingestuft werden. Die Vorteile liegen insbesondere in den Kosteneinsparungen durch weniger Wahlpersonal, schnelleres Wahlergebnis und weniger Wahlsprengel. Die unbewusste Abgabe ungültiger Stimmen ist nicht mehr möglich und Zweifelsfragen über die Gültigkeit oder Ungültigkeit von Stimmen gibt es nicht mehr.

3.4.3 Elektronische Wahlkarte

Ein immer höherer Anteil von Wählern benötigt Wahlkarten. Anforderung und Zustellung von Wahlkarten sind seit Jahrzehnten eine umständliche Prozedur. Wer am Donnerstag vor der Wahl – durchaus in der gesetzlichen Frist – eine Wahlkarte anfordert, den bestraft beim Zustellvorgang nicht selten die Post. So mancher musste seine Ambitionen, an einer Wahl teilzunehmen, begraben, weil die Zustellung im letzten Augenblick nicht mehr zustande kam. Die Zustellung der Wahlkarte auf elektronischem Weg würde dieses Problem entschärfen. Unter Beiziehung des ZMR, in dem man als Wahlkartenwähler registriert ist, könnte man dann die Stimme in einem von der Gemeinde vorher festgelegten Wahllokal abgeben.

3.4.4 Rechtliche Adaptierung der Wahlgesetze vordringlich

In Anbetracht dessen, dass vor allem die großen Städte nicht einmal die Hälfte der echten Wahlkosten ersetzt bekommen, ist Handlungsbedarf angesagt. Die rechtlichen Adaptierungen der Wahlgesetze sind längst überfällig. Um die Ignoranz in diesem Bereich zu verdeutlichen, ein kleines, aber typisches Detail: Obwohl die schriftlichen Zuzugsmitteilungen der Gemeinden aufgrund des ZMR seit bald 2 Jahren überflüssig geworden sind, ist diese Verpflichtung im Wählerevidenzgesetz nach wie vor aufrecht, und einige Gemeinden sind auch nicht davon abzubringen und füllen damit regelmäßig die Postmappen der Wahlämter.

3.5 ZENTRALES MELDEREGISTER (ZMR): WO BLEIBT DER E-GOVERNMENT-EFFEKT?

Die Etablierung des ZMR nach der Volkszählung 2001 hat im österreichischen Meldewesen einen radikalen Paradigmenwechsel bewirkt. Dass sich in den Gemeinden, insbesondere in den großen Städten, die Freude über das ZMR in Grenzen gehalten hat, ist wohl verständlich, weil damit ein beträchtlicher Ressourceneinsatz verbunden war und ist. Das ZMR ist primär auch nicht eingeführt worden, weil man den Gemeinden etwas Gutes tun wollte, sondern weil es von Haus aus in der österreichischen E-Government-Konzeption eine Schlüsselrolle spielen sollte. Das ZMR ist zwar noch jung, hat aber schon eine bewegte Geschichte hinter sich und so manchem Benutzer in den Meldeämtern die eine oder andere schlaflose Nacht beschert.

Dass es immer wieder zu Meinungsverschiedenheiten und auch Missverständnissen zwischen den Anwendern und den ZMR-Projektverantwortlichen gekommen ist, ist wohl nicht zuletzt darauf zurückzuführen, dass die Entwicklung der Applikation nicht immer unter der optimalen Beteiligung der Städte und Gemeinden vor sich gegangen ist. Nach Phasen mangelnder Stabilität und nervenaufreibenden Durchhängern scheint in den letzten Monaten eine gewisse Konsolidierung eingetreten zu sein. Nach wie vor gibt es jedoch programmtechnische Ungereimtheiten.

Nachdem das ZMR immer wieder als E-Government-Vorzeigeprojekt präsentiert wird (dies zurecht, weil es Vergleichbares im mitteleuropäischen Raum nur in Slowenien gibt), soll im Folgenden vom Standpunkt eines Städtevertreters doch aufgezeigt werden, wo es Defizite gibt, Prioritäten falsch gesetzt sind und der mit dem ZMR erwartete und erhoffte E-Government-Effekt nicht nur nicht eingetreten ist, sondern geradezu ad absurdum geführt wird.

- In so mancher Dienststelle der Länder und des Bundes hat sich noch nicht herumgesprochen, dass die Benutzung des ZMR bei allen Verwaltungsvorgängen absolute Priorität haben sollte und auf die Vorlage von Meldeauskünften bzw. Meldebestätigungen verzichtet werden kann. Eine besonders fragwürdige Rolle spielt in diesem Zusammenhang auch die österreichische Versicherungswirtschaft, die bei Kfz-Anmeldungen Meldebestätigungen von ihren Kunden einfordert. Das kann nur als Schikane in Reinkultur bezeichnet werden. Angemerkt sei, dass über 90 % aller Meldebestätigungen für öffentliche Dienststellen, oder solche, die im öffentlichen Auftrag tätig sind, ausgestellt werden. Wenn daher maßgebliche E-Government-Strategen die Meldebestätigung immer wieder als Beispiel für gelungene elektronische Transaktionen heranziehen, so wurde die Funktion des ZMR im Rahmen des E-Government bisher offensichtlich nicht richtig erkannt.

- Als Bürger darf man erwarten, dass sich Änderungen in der Wohnadresse automatisch auch in andere elektronische Verwaltungsregister (z. B. Kfz-Register, Waffenscheinregister, Führerscheinregister) durchziehen. Mit Ausnahme des in Planung begriffenen zukünftigen neuen Fremdenregisters gibt es derzeit keine konkreten diesbezüglichen Projekte für derartige informationstechnische Infrastrukturen. Meldepflicht durch den Bürger ist nach wie vor überall angesagt.

- § 4 Abs. 3 Rundfunkgebührengesetz 1999 schreibt vor, dass dem Gebühren-Inkasso-Service seitens der Gemeinde bestimmte Meldedaten zu übermitteln sind, und zwar in der dem jeweiligen Stand der Technik entsprechenden Form. Wer glaubt, dass anno 2005 diese Übermittlung durch das ZMR (tatsächlich in der dem jeweiligen Stand der Technik entsprechende Form) erfolgt, täuscht sich gewaltig. Der GIS besteht darauf, von 2.359 Gemeinden diese Daten übermittelt zu bekommen, um parallel zum ZMR eine riesige Einwohnerdatenbank zu generieren. Wie in solchen Fällen üblich, nimmt sich sofort ein EDV-Dienstleister der Sache an, und jede Gemeinde kann über diesem dem GIS die Meldedaten übermitteln. Hier werden primitivste E-Government-Grundsätze über Bord geworfen.

- Das Prinzip „Daten sind dort zu verarbeiten, wo sie entstehen“ sollte stärker forciert werden. Die Standesämter hat man konsequenterweise dazu verpflichtet, alle Meldevorgänge selbst durchzuführen, bei den Justizanstalten und Polizeianhaltezentren ist jetzt aber wieder Sendepause und Stöße von Haftzetteln werden in die Meldeämter transferiert.

- Die Einführung des Standarddokumentenregisters war gut gemeint. Ob der gewünschte Effekt jemals eintreten wird, bezweifeln viele, wenn nach 4 Jahren nicht einmal die Benutzung des ZMR obligatorisch ist. Zynisch gesprochen: der „E-Government-Faktor" für die Melde-, Standes- und Staatsbürgerschaftsämter liegt darin, dass dort durch die Eintragungen im Standarddokumentenregister der Zeitaufwand um fast 1/5 gestiegen ist.

Auch die Rechtslage ist in diesem Punkt akut verbesserungswürdig. So muss das Standesamt bei Sterbefällen wohl das entsprechende Standarddokument eintragen, die Abmeldung des Verstorbenen darf aber derzeit nicht vorgenommen werden.

- Im Bereich der Wählerevidenz ist die Erwartungshaltung der Kommunen noch lange nicht erfüllt. Es sind wohl de facto die Zuzugsmitteilungen weg (obwohl sie im Gesetz hartnäckig weiter bestehen), eine deutliche Entlastung würde aber auch ein Informationsverbund bei der Führung der Auslandsösterreicherevidenz und der EU-Wählerevidenz (viele Auslandsösterreicher sind mehrfach wahlberechtigt) bringen. Ein besonderes Kapitel ist die Registrierung jener Personen, die aufgrund strafrechtlicher Verurteilung von den Wahlen auszuschließen sind. Das automatische Übermitteln der Daten aus dem Strafregister in die Wählerevidenzen im Wege des ZMR wäre eigentlich die logische Vorgangsweise, um dieses Problem in den Griff zu bekommen. Dies ist derzeit weit und breit nicht in Sicht. Man nimmt lieber in Kauf, dass um die tausend Personen bei jeder Wahl in Österreich entgegen den Bestimmungen der Wahlgesetze wahlberechtigt sind.

- Was besonders erstaunt und vor allem die Frage nach den Prioritäten aufwirft, sind die Aktivitäten rund um das sogenannte „webbasierte lokale Meldewesen". Damit soll das bisherige von der Gemeinde erzeugte Lokale Melderegister (LMR) durch das ZMR geführt werden und die ausschließliche Verfügbarkeit der Gemeinden über ihre Daten im Melderegister aufgehoben werden. Viele Gründe sprechen meiner Ansicht nach gegen eine Teilnahme an einem webbasierten LMR. Die Entscheidung darüber sollten nicht allein die EDV-Verantwortlichen fällen. Jenseits der Kostenfrage ist die Aufgabe der Autonomie über die lokalen Meldedaten und die daraus resultierenden Folgen vor allem auch ein Thema der Verantwortlichen im Einwohnerwesen, der Wahlämter, der Statistik, der Stadtplanung und der gesamten politischen Verwaltung, die damit die für das Verwaltungshandeln wichtigste Datenbasis aus der Hand gibt. In diesem Zusammenhang wird immer wieder die Schnittstellenproblematik zwischen LMR und ZMR ins Spiel gebracht. Dazu ist festzustellen, dass die ZMR-Entwickler sich genau überlegen sollten, welche Auflagen sie den Anwendern noch aufhalsen wollen. Nach der jetzt schon existierenden Überfrachtung der Melde- und Standesämter kann sich dies aufgrund hochgradigen Ressourcenmangels nur kontraproduktiv auf die Qualität des ZMR auswirken.

3.6 STAATSBÜRGERSCHAFTSEVIDENZ

In der Öffentlichkeit hält sich der Bekanntheitsgrad dieses lokalen Registers in Grenzen. Dennoch ist diese Evidenz von entscheidender Bedeutung, ob jemand österreichischer Staatsbürger ist oder nicht. Viele Städte und Gemeinden (Staatsbürgerschaftsverbände) führen dieses Register elektronisch mit unterschiedlichem Nacherfassungsgrad. Die Karteikarten, die aber in diesem

Bereich noch in Verwendung sind, würden Räumlichkeiten beträchtlichen Ausmaßes füllen. Eine zentrale Staatsbürgerschaftsevidenz würde den Gemeinden die Ausstellung von Staatsbürgerschaftsnachweisen erleichtern bzw. dessen Vorlage bei bestimmten Verwaltungsvorgängen, wie z. B. im Personenstandswesen, erübrigen. Das Standarddokumentenregister wird gerade in diesem Bereich, wo eine besondere qualifizierte Beweiskraft erforderlich ist, die Rolle einer Staatsbürgerschaftsevidenz nicht übernehmen können.

3.7 PASSWESEN – IDENTITÄTSDOKUMENTENREGISTER (IDR)

Auf dem Weg zum neuen Hochsicherheitspass ist damit zu rechnen, dass auch die Applikation Identitätsdokumentenregister umgestaltet wird. Ein Direktzugang zum ZMR wäre dringend erforderlich. Ebenso sollte man nach technischen Möglichkeiten suchen, die Passarchive zu entlasten.

3.8 REGISTERZÄHLUNG

Das neue Volkszählungsgesetz, auch Registerzählungsgesetz genannt, ist sicherlich eines der wichtigsten E-Government-Projekte der letzten Jahre, das bereits mit Stichtag 31. Oktober 2006 seine Feuertaufe in Form einer Probezählung bestehen soll. Die statistischen Daten über Bevölkerung, Gebäude, Wohnungen und Arbeitsstätten sollen aus den bestehenden Registern generiert werden.

Soweit es die Städte und Gemeinden betrifft, sollten 2 Probleme aufgezeigt werden, die auf den ersten Blick wie vernachlässigbare Details wirken, die aber noch gehöriges Kopfzerbrechen bereiten werden.

3.8.1 Tür- oder Wohnungsnummer

Die Tür- oder Wohnungsnummer ist als Wohnungsadresse die Basis für das Wohnungsregister und der Schlüssel für wichtige statistische Auswertungen (z. B. Wohnungsstatistik, Haushaltsstatistik, leer stehende Wohnungen). Es war bis heute nicht möglich, die Türnummer österreichweit rechtlich so zu verankern, dass deren Führung für jeden Wohnungsbenutzer verpflichtend ist. Ob die in einer Novelle zum Postgesetz vorgesehene Regelung in Zusammenhang mit den Brieffächern die Anforderungen, die man in der Praxis an eine Wohnungsnummer als Basis für eine eindeutige Wohnungsadresse stellt, erfüllen wird, ist in höchstem Maße fraglich. Es zeichnet sich ab, dass die Letztverantwortung und damit ein exorbitant hoher Aufwand wieder bei den Gemeinden hängen bleibt - als Folge von zu spätem und zu wenig konsequentem legistischen Handeln. Im Übrigen kommt jede Regelung, damit sie auch registerwirksam wird, um mindestens 10 Jahre zu spät.

3.8.2 Registerabgleich (bereichsspezifisches Personenkennzeichen)

Ausgehend vom ZMR als führendes Register müssen für die Registerzählung alle Personen in anderen Registern identifiziert und für die Verknüpfung mit dem einheitlichen bereichsspezifischen Personenkennzeichen angereichert werden. Wie schon im Kapitel „Standesamt“ erwähnt, ist abzusehen, dass diese Identifizierung wegen der vernachlässigten einheitlichen Namensschreibweise in den verschiedenen Registern einen erheblichen zusätzlichen Arbeitsaufwand bedeuten wird. Eine dem Suchprozess vorgeschaltete Software soll Erleichterung bieten, Allheilmittel wird sie wohl keines sein.

3.9 FUNDWESEN

Mit Übernahme des Fundwesens durch die Städte hat in diesem Verwaltungsbereich auch der E-Government-Gedanke Fuß gefasst. Durch Initiative des Städtebundes wurde unter Hauptbeteiligung der großen Städte das österreichweite Fundinformationssystem „www.fundamt.gv.at“ in kürzester Zeit realisiert.

Dass sich das BMI immer noch weigert, die rund um die Uhr geöffneten Polizeiinspektionen mit einem Direktzugriff auszustatten, hat zwar direkt nichts mit E-Government zu tun, entspricht aber in keinster Weise dem vom Innenministerium propagierten „Rot-weiß-roten Bürgerministerium“.

3.10 E-GOVERNMENT IST KEIN SELBSTLÄUFER

Jeder Beteiligte erwartet sich vom E-Government etwas anderes. E-Government kann nur Erfolg haben, wenn es „von den Bürgern und Unternehmen als nutzenbringendes Kundenservice gesehen und von der Verwaltung als ressourcenschonende Verbesserung akzeptiert wird“ (Dipl.-Ing. Dr. Berthold Rauchenschwandtner, Städtetag 2005). So gesehen ist das Ergebnis der bisherigen E-Government-Strategie des Bundes aus der Sicht der Städte ein zwiespältiges.

Es ist sicher gelungen, die Wirtschaft zu gewinnen. Dass es sich für den einfachen Menschen von der Straße in Zukunft lohnt, eine Bürgerkarte zu erwerben und auch zu benutzen, wird man an den geschilderten Massenanwendungen praktisch demonstrieren müssen.

Was ist weiters zu tun?

- Die Nutzung der IT-Strukturen (Register) sollte in Hinkunft in allen Verwaltungsstellen verpflichtend sein.
- Strikte Vermeidung von Doppelgleisigkeiten aufgrund rechtlicher Bestimmungen (z. B. Rundfunkgebührengesetz, Wählerevidenzgesetz).
- Daten sind dort in die Register einzubringen, wo sie entstehen.
- Entlastung der Mitarbeiter durch Schaffung von Schnittstellen zu anderen Registern (laufende Überprüfung der Usability).
- Für verpflichtende Datenänderungen durch den Bürger ist die Durchgängigkeit der Register so rasch als möglich rechtlich und technisch zu realisieren.

- Leichterer Zugang der Verwaltungsstelle zu den für den Vollzug notwendigen Registern. Diese Zugangsmöglichkeiten sind rechtlich zu fixieren.
- Rasche Realisierung eines zentralen Personenstands- und Staatsbürgerschaftsregisters.
- Änderung von Materiengesetzen, um diese E-Government-tauglich zu machen.
- Permanente Konsultationen des Städte- und Gemeindebundes bezüglich der Umsetzung von E-Government-Projekten im Hinblick auf deren Priorität und Praktikabilität.

Soweit es bei den von den Gemeinden zu vollziehenden Angelegenheiten aus dem Bereich der Bundesverwaltung bisher überhaupt E-Government-Aktivitäten gegeben hat, waren diese vor allem für die Städte mit einem beträchtlichen zusätzlichen Aufwand an Ressourcen verbunden. Weiterhin erforderlich ist auch ein relativ hoher Grad an laufendem Wissensmanagement.

E-Government führt auch nicht zwangsläufig zur Reorganisation von Verwaltungsabläufen, da ja zusätzlich zur elektronischen Verwaltung die herkömmliche Verwaltung bedient werden muss.

Es ist unbestritten, dass in den letzten Jahren auf dem Gebiet des E-Government Hervorragendes geleistet wurde, sei es auf Bundesebene oder auf der Ebene der lokalen Anwendungen der Länder und Gemeinden. Eine Nachdenkpause ist aber dringend notwendig und wohl auch weitere finanzielle Ressourcen sowie auch eine (neue) Strategie, wie man nicht nur eine durchgehende elektronische Infrastruktur schafft, sondern wie diese auch in der Praxis gelebt wird.

„E-Government hängt entscheidend vom Bewusstseinsstand der Akteure ab. Die Zukunft hängt davon ab, wie sehr E-Government als Instrument und Motor von Verwaltungsmodernisierung wahrgenommen wird“ (Univ.-Prof. em. Dr. Klaus Lenk, Städtetag 2005).

Kapitel 4

VIRTUELLER ORTSNAMENS-SCHUTZ IN ÖSTERREICH – WWW.QUOVADIS-STADT.AT?*

Dr. Clemens Thiele

* RA Dr. Clemens Thiele, LL.M. Tax (GGU), *Anwalt.Thiele@eurolawyer.at,* Näheres unter *http://www.eurolawyer.at.*

4.1 ABSTRACT

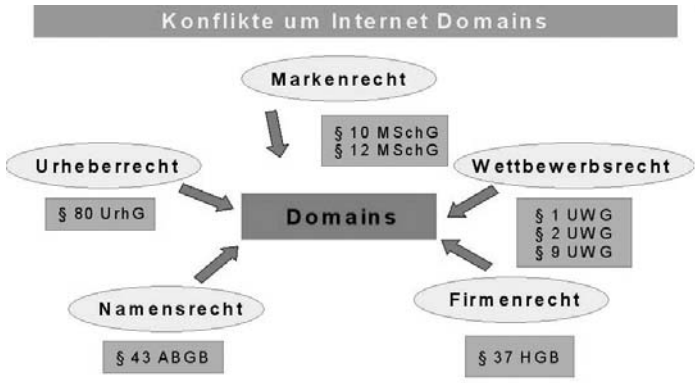
Mit zunehmender Durchdringung des Alltages durch das Internet kommt den Internetadressen – korrekt als „Internetdomains“ bezeichnet – steigende Bedeutung zu, was sich auch in verstärkten Rechtsstreitigkeiten niederschlägt. Die Probleme um bereits belegte Domänennamen machen auch nicht vor Städte- und Gemeindenamen Halt, weshalb es mittlerweile einige Musterentscheidungen in diesem Bereich gibt.

Grundsätzlich kommen im Bereich des „virtuellen Ortsnamenschutzes“ das ABGB (§ 43, Namensrecht) sowie das UWG (§ 1, Domaingrabbing, § 9, Kennzeichenmissbrauch) zum Tragen. Aus namensrechtlicher Sicht ist vorab eine „Identität der zu vergleichenden Bezeichnungen“ erforderlich, um überhaupt Rechtsansprüche aus diesem Titel heraus geltend machen zu können, wobei dies jedoch nur gilt, wenn einer Domain Namensfunktion zukommt und der Verkehr diese auch als Unterscheidungshinweis auffasst (was im Falle von Städtenamen in jedem Fall zutrifft). Eine Namensanmaßung im Sinne des § 43 ABGB tritt bereits mit der Registrierung einer namentlich gleichlautenden Domain ein, eine Namensverletzung kommt allerdings erst dann zum Tragen, wenn durch einen unbefugten Namensgebrauch das schutzwürdige Interesse des Namensträgers verletzt wird. Ein solches Interesse besteht darin, nicht mit anderen verwechselt zu werden oder mit anderen in eine nicht gegebene Beziehung gebracht zu werden. Für die Beurteilung des Verwechslungstatbestandes wird sowohl die Domain als auch der Inhalt der dazugehörigen Website herangezogen. Auf Städte und Gemeinden angewandt bedeutet dies, dass zwar aus dem Namensrecht heraus Unterlassungs- und Beseitigungsansprüche bestehen, eine Beurteilung derselben jedoch von der Verletzung schutzwürdiger Interessen der Stadt/-Gemeinde abhängt. Eine solche besteht jedenfalls nicht, wenn sich unter der strittigen Internetadresse Inhalte wieder finden, deren Verbreitung auch im Interesse der Stadt/-Gemeinde liegen, sodass Interessensgleichklang besteht.

Domaingrabbing nach § 1 UWG kommt nur dann zur Anwendung, wenn ungerechtfertigte Forderungen an die Herausgabe einer Internetdomain geknüpft wurden. Allein die Anmeldung eines Namens als Internetadresse (beispielsweise eines Stadtnamens) wird noch nicht als bereits bestehende Behinderungsabsicht des Namensträgers ausgelegt. Auch der Erwerb einer Domain von einem sogenannten Domaingrabber reicht nicht aus für den Tatbestand des „Domaingrabbers“, da bei der Beurteilung der Absichten des aktuellen Domainbesitzers jene des Vorbesitzers keine Rolle spielen.

4.2 EINLEITUNG

Rechtsstreitigkeiten um Internet Domains beschäftigen nunmehr schon seit einem Jahrzehnt deutsche Gerichte[13] und seit Februar 1998 das österreichische Höchstgericht. Der virtuelle Ortsnamensschutz nimmt dabei eine prominente Rolle ein.[14] Der nachfolgende Beitrag gibt eine Zwischenbilanz und zeigt den Stand der Rechtsentwicklung anhand eines praktischen Ausgangsfalles auf.



4.3 AUSGANGSFALL UND PROBLEMSTELLUNG

Die Domain „stadtname.at" ist zugunsten von Herrn Franz Berger[15] bei der Österreichischen Domainvergabestelle, der nic.at – Internet Verwaltungs- und Betriebsgesellschaft m.b.H, mit Sitz in 5020 Salzburg, Jakob-Haringer-Straße 8, registriert. Dies seit ca. Anfang des Jahres 2003. Soweit recherchierbar, wurde die Domain erstmals Ende der 1990er Jahre vom zwischenzeitig zu trauriger Berühmtheit erlangten „Domain-Grabber" Dr. Bertram von Wittgenstein angemeldet, wobei weder dessen akademischer Titel noch seine Adeligkeit gewiss scheinen. Herr Wittgenstein hatte sich schon sehr früh auf Domainhandel spezialisiert. Er hatte zu diesem Zweck weltweit Firmen gegründet, anfangs auf den Kanalinseln, später in Florida, in Mittelamerika (Belize) und schließlich in Thailand.

Es ist sehr wahrscheinlich, dass der nunmehrige Inhaber die Domain Ende des Jahres 2002 von einer der Wittgensteinschen Firmen, z. B. der European Internet Foundation, käuflich erworben hat. Dies muss allerdings ohne Einsichtnahme in die Registerakte bei der nic.at letztlich Spekulation bleiben.

---

[13] Legendär mittlerweile die E des LG Mannheim 8.3.1996, 7 O 60/96 – *heidelberg.de,* CR 1996, 353 *(Hoeren)* = GRUR 1997, 377 = NJW 1996, 2736 = ZUM 1996, 705.

[14] Die ÖGZ hat immer wieder darüber berichtet: *Thiele,* Privatrechtlicher Schutz von Ortsnamen im Internet, ÖGZ 1999) H 11, 4; *Sampl,* „feldkirchen.at" gehört endlich Feldkirchen, ÖGZ 2003, H 6, 55; *Thiele,* Schutz virtueller Ortsnamen, ÖGZ 2003, H 6, 49.

[15] Der Name und Sachverhalt sind völlig frei erfunden und jede Ähnlichkeit mit lebenden oder verstorbenen Personen ist ungewollt und rein zufällig.

Frühestens mit April 2003 lässt sich eine Website in der nunmehr gehaltenen Präsentation durch Herrn Franz Berger an der Internetadresse *http://www.stadtname.at* nachweisen. Aus den bereits damals verwendeten Allgemeinen Geschäftsbedingungen sowie dem heutigen Impressum ergibt sich der Zweck dieser Website:

„… stellt unter www.stadtname.at eine Plattform zur Verfügung, welche zur raschen und effizienten Suche von Firmen, Unterkünften sowie Gastronomiebetrieben dient. Durch die Kategorisierung auf Basis einer innovativen Datenbanktechnologie ist eine einfache Suche für den potenziellen Kunden möglich."

Im Impressum findet sich folgende „Anmerkung des Inhabers": „Dieses Projekt ist politisch unabhängig und sieht sich als wertfrei an. Der Zweck der gesamten Anstrengungen dient zum Wohle der Stadt … Beachten Sie dabei, dass diese Seite eine Initiative eines Bürgers der Stadtgemeinde ist und nicht die offizielle Website der Stadt … darstellt!"

Darüber hinaus wird die Domain auch als E-Mail-Adresse, zumindest in der Form Franz.Berger@stadtname.at, genutzt.

Eine wie immer geartete Zustimmung der Stadtgemeinde, weder durch den Bürgermeister noch durch einen Stadtsenatsbeschluss zur Registrierung und Nutzung der Domain für Herrn Franz Berger, ist nicht bekannt.

An den Stadtamtsdirektor wurden die von einigen Gemeindebürgern, vor allem Innenstadtkaufleuten und Hoteliers, gestellten Fragen herangetragen, warum denn die „ureigenste" Domain „stadtname.at" nicht im Besitz der Stadt sei und ob Franz B. denn berechtigt sei, den Namen der Stadt so zu vermarkten?

4.4 RECHTLICHE BEURTEILUNG

4.4.1 Mögliche Anspruchsgrundlagen

Die Ansprüche der Stadtgemeinde sind gegenständlich auf § 43 ABGB (Namensrecht), § 9 UWG (Kennzeichenmissbrauch) sowie § 1 UWG (Domain-Grabbing) zu stützen. In der Bekämpfung von „Namenspiraten" kommt vor allem dem sittenwidrigen Domain-Grabbing und den namensrechtlichen Ansprüchen Bedeutung zu, die nachfolgend näher erörtert werden sollen. Zuvor bedarf allerdings die in der Praxis immer wieder Verwirrung stiftende Frage der Zeichenähnlichkeit einer genaueren Abklärung.

4.4.2 Zeichenähnlichkeit

Zunächst ist festzuhalten, dass im Kennzeichenstreit Identität der zu vergleichenden Bezeichnungen vorliegen muss. Dabei hat das zuständige zivile Höchstgericht[16] festgehalten, dass einer Domain Namensfunktion zukommt, wenn und weil der Verkehr diese auch als Unterscheidungshinweis auffasst. Die Netzbezeichnungen „WWW" und die Topleveldomains (TLDs) z. B. „.at" und „.com" sind namensrechtlich ohne Belang. Die TLDs geben einen Hinweis auf die sachliche oder geografische Herkunft des Angebots, nicht aber einen zwingenden Hinweis auf den Namensträger. „Die TLD tritt deshalb in ihrer Bedeutung für den der Second-Level-Domain (der eigentliche Domainname) bestimmten Gesamteindruck zurück."[17] Die Zeichenidentität ist also bei Verwendung der Domain „stadtname.at", sei es als Netzadresse oder als E-Mail-Kennung, zum gleich lautenden Namen der Stadt gegeben. Auf die allfällige Umschreibung der Umlaute durch „ae", „oe" oder „ue" bzw. die Verwendung von Bindestrichen kommt es nach der Rechtsprechung[18] nicht an.

4.4.3 Sittenwidriges Domain-Grabbing

In sämtlichen Gemeindedomains betreffenden Entscheidungen verneinte das Höchstgericht das Vorliegen einer bei Anmeldung der Domain bereits bestehenden Behinderungsabsicht, sohin das Domain-Grabbing. Lediglich im Falle einer „erpresserischen" Geldforderung durch den Domaininhaber gegenüber dem Bürgermeister, was in erster Instanz ausdrücklich festgestellt wurde, beließ es das Höchstgericht beim Zuspruch der Domain an die klagende Gemeinde[19]:

Die klagende Gemeinde Aistersheim in Oberösterreich beabsichtigte, eine Homepage unter der aus ihrem Namen gebildeten Domain „aistersheim.at" im Internet zu etablieren. Der nicht in Aistersheim wohnhafte Beklagte ließ sich die strittige Domain zuvor bei der „NIC.AT Internetverwaltungs- und Betriebs GmbH" auf seinen Namen registrieren und beteuerte im Prozess, die Domain in der Absicht erworben zu haben, den Sitz seiner Firma für die Zukunft wieder nach Aistersheim zu verlegen. Bislang hätten nur die finanziellen Mittel für die Realisierung einer Homepage gefehlt.

Das Erstgericht stellte den Inhalt eines Telefonats zwischen dem Bürgermeister der Klägerin und dem Beklagten im Wesentlichen dahingehend fest, dass der Beklagte eine Zahlungsaufforderung für die Freigabe der Domain gestellt hatte. Das Erstgericht stellte die Behinderungsabsicht des Beklagten zum Zeitpunkt der Domainregistrierung (richtig: der Domainanmeldung) fest und qualifizierte dieses Verhalten als sittenwidriges Domain-Grabbing nach § 1 UWG. Das Berufungsgericht bestätigte sowohl das klägerische Unterlassungs- als auch Löschungsbegehren.

---

[16] OGH 25.3.2003, 4 Ob 42/03k – *rtl.at,* ecolex 2003/317, 773 *(Schanda)* = ÖBl 2004/11, 35 *(Fallenböck)* = MR 2004, 63

[17] OGH 25.3.2003, 4 Ob 42/03k – *rtl.at,* ecolex 2003/317, 773 *(Schanda)* = ÖBl 2004/11, 35 *(Fallenböck)* = MR 2004, 63

[18] Vgl. OGH 3.4.2001, 4 Ob 73/01s – *pro-solution.at,* wbl 2001/266, 449 = ecolex 2001/281, 757 *(Schanda)* = EvBl 2001/176, 769 = RdW 2001/610, 592 = MR 2001, 258 = ÖBl 2001, 263 = JUS Z/3331

[19] OGH 20.1.2004, 4 Ob 258/03z – *aistersheim.at,* ÖBl-LS 2004/50, 114.

Der OGH wies die außerordentliche Revision des Beklagten zurück und bestätigte die Entscheidungen der Vorinstanzen als mit der Rechtsprechung des Senats zu Verstößen gegen § 1 UWG wegen Domain-Grabbings im Einklang stehend.

Nach den Feststellungen der Vorinstanzen war dem Beklagten **zum Zeitpunkt der Registrierung der Domain** sowie später bewusst, dass er die Klägerin durch die Belegung dieser Domain bei der Präsentation bzw. Bewerbung der Gemeinde behindern würde. Er ließ die Domain aus dem überwiegenden Motiv registrieren, diese in weiterer Folge mit finanziellem Vorteil an die Gemeinde zu vermarkten. Ein berechtigtes nachvollziehbares Eigeninteresse des Beklagten an der Domain konnten die Vorinstanzen nicht feststellen. Sowohl das auf Beseitigung gerichtete Löschungsbegehren als auch das für die Zeit danach formulierte Unterlassungsbegehren waren nach Auffassung des Höchstgerichtes nicht unschlüssig und daher ebenfalls zu bestätigen.

Auf den vorliegenden Fall angewandt, lässt sich für die Stadtgemeinde daraus allerdings nichts gewinnen. Dafür, dass Franz Berger bei Erwerb der Domain im Jahr 2002/2003 in Schädigungsabsicht zum Nachteil der Stadt handeln wollte, gibt es keine Anhaltspunkte. Dass er die Domain von einem „amtsbekannten Grabber" erwarb, reicht nicht aus, um sittenwidriges Domain-Grabbing zu begründen, weil es auf eine allfällige Bösgläubigkeit des Domain-Vorbesitzers nicht ankommt.[20] Schließlich hat Herr Berger auch nie ein Ablöseangebot an die Stadt für die Domain gestellt oder sich sonstige Sondervorteile gegenüber der Stadtgemeinde herauszuschlagen versucht.

Nach dem konkreten Sachverhalt müssen daher auf § 1 UWG gestützte Ansprüche scheitern.

4.4.4 Namensverletzung

Darüber hinaus geht der OGH in ständiger Rechtsprechung davon aus, dass eine so genannte „Namensanmaßung" im Sinne des § 43 ABGB bereits durch die Anmeldung einer gleich lautenden bzw. ähnlichen Second-Level-Domain erfolgt. Eine Namensverletzung tritt allerdings erst dann ein, wenn durch den unbefugten Namensgebrauch bzw. die Namensanmaßung das schutzwürdige Interesse des Namensträgers verletzt wird.[21]

In einer ersten Leitentscheidung zum „virtuellen Ortsnamensschutz" hielt der OGH[22] fest, dass keine Verletzung schutzwürdiger Interessen bei Verwendung eines Ortsnamens als Internetadresse bei Interessengleichklang vorliegt, was insbesondere dann anzunehmen ist, wenn die zugehörige Website Informationen im Interesse des Namensträgers enthält. Den Gebietskörperschaften wäre ein Ausweichen auf die ihnen vorbehaltene Second-Level-Domain „.gv" (hier: stadtname.gv.at) zumutbar. Die eindeutig zu Gunsten der Gemeinden bestehende Rechtsprechung in Deutschland und der Schweiz wären daher in Österreich nicht anwendbar.

---

[20] Vgl. BGH 22.11.2001, I ZR 138/99 - shell.de, MR 2001, 402 = MR 2002, 198 (Thiele); OGH 20.5.2003, 4 Ob 103/03f - centro-hotel.com, RdW 2003/471, 558 = ÖBl 2003/65, 241 (Fallenböck) = MR 2004, 67.

[21] OGH 29.1.2002, 4 Ob 246/01g - graz 2003.at, wbl 2002/230, 331 (Thiele) = RdW 2002/394, 403 = ecolex 2002/200, 524 (Fallenböck) = MR 2002, 342 = ÖBl 2002/63, 280 (Gamerith).

[22] Urteil vom 20.5.2003, 4 Ob 47/03w - adnet.at II, ÖGZ 2003 H 10, 84 = wbl 2003/308, 542 (Thiele) = RdW 2003/470, 558 = ÖBl 2003/74, 271 (Fallenböck) = MR 2004, 65.

Allerdings entwickelte der OGH seine Rechtsprechung in dem zuletzt zu dieser Thematik ergangenen Urteil[23] wesentlich fort. Im entschiedenen Fall betrieb der Beklagte in Serfaus das 4-Sterne-Hotel „Post". Er war Inhaber der strittigen Domain „serfaus.at", auf deren zugehöriger Website er sein Hotel vorstellte, die auf der Startseite den folgenden Hinweis trägt: „Das ist nicht die offizielle Seite der Gemeinde Serfaus, für diese klicken Sie **hier!**".

Die klagende Gemeinde Serfaus forderte – gestützt auf ihr Namensrecht – die Übertragung der Domain, hilfsweise die Unterlassung ihrer Verwendung durch den Hotelier und ihre Löschung. Die Gerichte hatten zu prüfen, ob die Domainverwendung durch den Beklagten die Namensrechte der klägerischen Gemeinde verletzt oder nicht.

Das Erstgericht wies das Hauptbegehren auf Herausgabe ab und gab dem Unterlassungs- und Löschungsbegehren statt. Das Berufungsgericht wies nach Berufung durch den Beklagten die Klage zur Gänze ab, da der Hotelier die Bezeichnung „Serfaus" bloß als geografische Ortsangabe im Internet nutzte, und ließ – dankenswerterweise – die ordentliche Revision an den OGH zu.

Das Höchstgericht stellte das Ersturteil wieder her und führte – in bewusster sachverhaltsmäßiger Abgrenzung zur früheren E *adnet.at II*[24] begründend aus, dass die berechtigten Interessen der klagenden Gemeinde bereits dadurch verletzt werden, dass der Beklagte den – jedenfalls bei einem Teil der Internetnutzer – durch die Domain serfaus.at erweckten Anschein, der Internetnutzer rufe durch die Eingabe dieser Internetadresse die Website der Gemeinde auf, ausnützt, um (auch) Internetnutzer auf seine Website zu bringen, die Informationen über die Gemeinde und nicht bloß Informationen über sein Hotel suchen.

[23] OGH 16.12.2003, 4 Ob 231/03d – *serfaus.at,* wbl 2004/95, 196 (Thiele) = RdW 2004/242, 269 = ecolex 2004/219, 464 (Schumacher) = ÖGZ 2004, H 5, 58 = ÖBl 2004/45, 171 (Fallenböck).

[24] OGH 20.5.2003, 4 Ob 47/03w, ÖBl 2003, 271 (zust *Fallenböck)* = ÖGZ 2003, H 10, 84 = RdW 2003/470, 558 = wbl 2003/308, 542 (krit *Thiele).*

Dem Beklagten wurde untersagt, die Domain für seinen Hotelbetrieb zu nutzen, und aufgetragen, die Domain bei der NIC.AT Internet-VerwaltungsGmbH löschen zu lassen. Dadurch, dass der Beklagte im Falle *serfaus.at* auf der zugehörigen Website lediglich sein eigenes Hotel Post vorstellte und keine weiteren Mitbewerber zuließ, musste sich die klagende Gemeinde Serfaus auch nicht auf die den Gebietskörperschaften vorbehaltene Second-Level-Domain „.gv.at“ verweisen lassen.

4.5 EIGENE STELLUNGNAHME

Positiv zu vermerken ist zunächst, dass auch einer Gemeinde als öffentlich-rechtlichem Namensträger ein berechtigtes Interesse daran zuerkannt wird, dass ihr Name nicht gebraucht wird, um die Aufmerksamkeit auf Aktivitäten zu lenken, mit denen sie nichts zu tun hat bzw. zu tun haben will. Die unbefugte Namensanmaßung beginnt aber mE nicht erst beim Unterlegen der Domain mit Inhalten im WWW, sondern bereits mit der Registrierung durch die Vergabestelle.[25] Dieser Gedanke des „leave me alone“ siedelt sich in der Dogmatik des Namensrechts im Bereich der Namensanonymität an. Der Oberste Gerichtshof hat mehrfach das Recht einer Person darauf anerkannt, dass ihr Name nicht von Dritten in Zusammenhängen erwähnt werden darf, zu deren Erwähnung sie keinen sachlichen Anlass gegeben hat.[26] Dieses Recht auf Namensanonymität ergibt sich aus einer Zusammenschau der §§ 16 und 43 ABGB und führt dazu, dass der rechtmäßige Namensträger ein Recht auf Nichtnennung seines Namens in bestimmtem Zusammenhang ohne Veranlassung des Genannten hat.[27]

Der „sachliche Anlass“ zur Namensnennung hat in der **erforderlichen Interessenabwägung** ein besonderes Gewicht.[28] Aufgrund der Doppelfunktion der Gemeinde als hoheitlicher und privater Rechtsträger ist dabei mE ein strenger Maßstab zugunsten der Kommunen anzulegen. Worin der sachliche Anlass im gegenständlichen Fall liegen soll, ist nicht zu erkennen, zumal der Beklagte sich die – namensrechtlich nicht zu beanstandende – Domain „hotel-post-serfaus.at“ hätte registrieren lassen können. Der Beklagte verfolgt mit dem Domaingebrauch eigene Interessen im geschäftlichen Verkehr und begnügt sich nicht mit einer bloß privaten Nutzung des Gemeindenamens oder einer solchen als regionaler Herkunftsbezeichnung. Ein derartiger Namensgebrauch verletzt daher die schutzwürdigen Interessen des Namensträgers.

Das österreichische Höchstgericht liegt mit der nunmehrigen E endlich auf der schon viel deutlicher namensbewahrenden Linie des deutschen Höchstgerichtes: der Träger eines bürgerlichen Namens kann gegenüber einem Dritten, der denselben Namen als Alias (oder Pseudonym) für seine Internet-Präsenz verwendet, beanspruchen, dass dieser den Namen nicht als Domain-Adresse verwendet. Der BGH bejaht – mE durchaus zutreffend – bereits die Möglichkeit einer Namensrechtsanmaßung durch die Registrierung (genauer: das Anmelden und Aufrechterhalten

[25] Ausführlich dazu bereits *Thiele,* Domainrecht „à la carte“ oder virtueller Ortsnamenschutz ade? MR 2004, 52, 56 ff mwN.
[26] OGH 17.12.1997, 7 Ob 329/97a – *Tiroler Rechtsanwälteverzeichnis,* EFSlg 83.025 = EvBl 1998/92 = MR 1998, 53.
[27] Deutlich OGH 18.12.1998, 6 Ob 306/98p, EFSlg 85.845.
[28] So *Aicher* in *Rummel* I3, § 43 ABGB Rz 12.

der Registrierung) einer Domain. Wie selbstverständlich geht der BGH schon davon aus, dass bereits die Anmeldung und (weitere) Verwendung eines bürgerlichen Nachnamens ohne eigene Rechte einen Eingriff in das von § 12 BGB geschützte zivile Namensrecht darstellt.[29]

Der OGH hält aber bei genauerem Hinsehen unter dem – nur schwer nachvollziehbaren – Hinweis auf den „grundlegenden Unterschied" zum Sachverhalt der adnet.at II-Entscheidung (bedauerlicherweise) großteils an seiner bisherigen, zurückhaltenden Judikaturlinie fest, wobei er allerdings bestrebt scheint, weiter zu differenzieren:

Der Namensschutz des § 43 ABGB begründet nur dann einen Abwehranspruch, wenn schutzwürdige Interessen des Namensträgers beeinträchtigt sind. Ein solches (ideelles) Interesse besteht vor allem darin, nicht mit anderen verwechselt und nicht in eine – tatsächlich nicht gegebene – Beziehung zum Unternehmen eines anderen gebracht zu werden; dabei genügt es, dass der Anschein erweckt wird, es bestünden ideelle oder wirtschaftliche Beziehungen zwischen dem Namensträger und dem Verletzer. Ob dieser Anschein erweckt wird, ist, ebenso wie bei der Beurteilung einer durch die Domain hervorgerufenen Verwechslungsgefahr, nicht allein nach der Domain, sondern auch nach dem Inhalt der dazugehörigen Website zu beurteilen. Der Gebrauch eines Ortsnamens als Domainname greift nur dann in die Rechte der jeweiligen Gemeinde ein, wenn deren schutzwürdige Interessen verletzt werden.

Wenn der Internetnutzer auf der Website des Beklagten Informationen erhält, deren Verbreitung auch im Interesse der Klägerin liegt, besteht kein Interessenkonflikt, sondern ein Interessengleichklang. Wird unter der Domain eine Website betrieben, auf der nur das Hotel des Beklagten vorgestellt wird, wird der Beklagte nicht im Interesse der Gemeinde, sondern ausschließlich in seinem eigenen Interesse tätig. Er erlangt mit der Verwendung der Domain vielmehr einen Vorteil, der ihm nicht zukommt.

Der OGH nimmt damit ein Schwinden der Rechtssicherheit in Kauf. Denn wo hört das „regionale Informationsportal, das ganz allgemein über das touristische Angebot einer Region informiert", auf, und wo beginnt „nur die Vorstellung des eigenen Hotels"?

Das vom Höchstgericht herangezogene Kriterium des „bloßen Informationsportals" vermag nicht zu überzeugen. Es ist unehrlich, den Namen eines anderen ohne Zustimmung für die Eigenwerbung zu benutzen. Ist es nicht (mehr) unehrlich, wenn diese Werbemöglichkeit einer Vielzahl von gleich (schlecht) Gesinnten zur Verfügung gestellt wird? Der Ruf nach dem (Landes-)Gesetzgeber wird unvermeidlich immer lauter, in den einzelnen Gemeindeordnungen entsprechende Schutzbestimmungen zugunsten der „virtuellen Gemeindebezeichnungen" vorzusehen, wie dies derzeit schon für den Gemeindenamen, das Gemeindewappen und die Gemeindefarben vorgesehen ist.[30]

[29] Urteil 26.6.2003, I ZR 296/00 – *maxem.de,* CR 2003, 845 *(Eckhardt)* = JurPC Web-Dok 258/2003 Abs 14.
[30] Vgl. z. B. §§ 4, 5 OÖ GemO 1990, OÖ LGBl 1990/91 idF LGBl 2001/152.

6.6 ZUSAMMENFASSUNG

Unter Zugrundelegung der teilweise einander widersprechenden höchstgerichtlichen Entscheidungen zum „virtuellen Ortsnamensschutz“ lässt sich zusammenfassend festhalten, dass Städte an den aus ihrer Bezeichnung und der Top Level Domain .at gebildete Domain, z. B. „stadtname.at“ namensrechtliche Unterlassungs- und Beseitigungsansprüche gegen unbefugte Domaininhaber geltend machen können. Ob sie damit gerichtlichen Erfolg haben, hängt nach der kaum vorhersehbaren zivilen Rechtsprechung in Österreich davon ab, ob der Betreiber der zugehörigen Website in der Art eines regionalen Informationsportals ganz allgemein über die Region berichtet oder bloß seinen eigenen (Hotel-)Betrieb bewirbt. Im letzteren Fall schützt auch ein Disclaimer auf der Startseite nicht vor der Domainlöschung.

Langfristig bietet nur eine gesetzliche Regelung Abhilfe. Ein Ausweichen auf die Second-Level-Domain „.gv.at“ ist schon jetzt möglich.

Kapitel 5

RECHTLICHE ASPEKTE KOMMUNALER INTERNETAUFTRITTE: E-COMMERCE/ E-BUSINESS[31]

Prof. Dr. Andreas Wiebe, LLM.

[31] Für die Vorarbeiten bei der Erstellung des Beitrags danke ich meinem Mitarbeiter, Herrn Mag. Heidinger.

5.1 ABSTRACT

Mittlerweile gibt es kaum noch eine Stadt oder Gemeinde, die nicht über eine eigene Internetpräsentation verfügt. In diesem Zusammenhang sind jedoch einige rechtliche Grundvoraussetzungen zu beachten, die auch für Gebietskörperschaften gelten. Bei der Beurteilung der Anwendbarkeit von gesetzlichen Bestimmungen ist eine Differenzierung zwischen Hoheitsverwaltung und Privatwirtschaftsverwaltung erforderlich, die auf der Ebene der rechtstechnischen Umsetzung des Verwaltungshandelns erfolgt. Dies bedeutet, dass alle jene Teile eines kommunalen Internetauftritts, die der unmittelbaren Durchführung der Hoheitsverwaltung dienen, diesem zuzuordnen sind. Elektronische Formulare beispielsweise fallen zwar nicht unter den Begriff der „unmittelbaren Ausübung von Hoheitsgewalt", wären aber als hoheitliche „Hilfsmittel" zu qualifizieren.

Unter diesem Aspekt kommt das E-Commerce-Gesetz, das auf Grundlage einer E-Commerce-Richtlinie der EU erlassen wurde, bei Städten und Gemeinden kaum zum Tragen, da es vor allem dann zur Anwendung kommt, wenn „ein Dienst der Informationsgesellschaft" vorliegt, der „im Regelfall gegen Entgelt" bereitgestellt wird. Internetauftritte von Städten und Gemeinden fallen somit nicht unter diese Regelungen, es sei denn, es werden Dienste in Erwerbsabsicht erbracht. Dies kann vor allem im kulturellen (z. B. Verkauf von Eintrittskarten für eine von der Stadt organisierte Kulturveranstaltung) und touristischen (z. B. Plattform für Hotel- und Privatzimmervermittlung) Bereich der Fall sein. In diesem Fall besteht eine normierte Informationspflicht nach § 5 ECG und es sind bestimmte Regeln beim Vertragsabschluss (§ 9 ECG) einzuhalten.

Für alle Betreiber von Webseiten – also auch Städte und Gemeinden – gelten hingegen die im Mediengesetz geregelten Verpflichtungen zur Offenlegung (§ 25 MedienG) und im Falle von Newsletter auch eine Impressumspflicht (§ 24 MedienG).

Bei Verkäufen über das Internet (z. B. Tickets) kommt weiters auch das Konsumentenschutzgesetz zur Anwendungen, das z. B. gesonderte Informationspflichten vorschreibt.

Auch Werbung im Internet wird mittels E-Commerce-Gesetz geregelt. Da Werbung mittlerweile auch auf Seiten von Gebietskörperschaften zu finden ist, kommt gegebenenfalls der Trennungsgrundsatz nach § 6 ECG zum Tragen, der besagt, dass Werbung klar als solche zu kennzeichnen ist und sich überdies vom „echten" Inhalt deutlich erkennbar abheben muss. Weiters muss auch der Auftraggeber der Werbung identifizierbar sein.

In diesem Zusammenhang wirkt auch das Wettbewerbsrecht, das vor allem Verstöße im Bereich der Werbung ahndet. Hievon betroffen sind auch beliebte „Hintertüren" zur Verbesserung der Reihung in Suchmaschinen (Index Spamming), da solche als Absatzbehinderung nach § 1 UWG interpretiert werden.

Ein leidiges Dauerthema war in der Vergangenheit die Haftungsfrage für die Inhalte von Webseiten. Im Falle von Städten und Gemeinden ist bei Haftungsfragen der Wirkungskreis von Bedeutung: Im hoheitlichen Bereich kommt das Amtshaftungsgesetz (AHG) zum Tragen,

wohingehend im privatwirtschaftlichen Bereich das allgemeine Zivilrecht Anwendung findet. Im Falle verlinkter Inhalte auf fremden Webseiten bringt das E-Commerce-Gesetz eine gewisse Entspannung, da unter bestimmten Umständen Haftungsbeschränkungen gelten. So kommt eine Haftung beispielsweise nur bei Kenntnis von rechtswidrigen Informationen oder Tätigkeiten in Betracht. Gleiches gilt auch für das Setzen von Hyperlinks. Allerdings ist zu bedenken, dass Links auf fremde Seiten auch urheberrechtliche oder wettbewerbsrechtliche Konsequenzen nach sich ziehen können.

Als Besonderheit ist zu beachten, dass auch im Rahmen der Privatwirtschaftsverwaltung durch die Stellung von Städten und Gemeinden als Körperschaften des öffentlichen Rechts eine Bindung an die Grundrechte (Fiskalgeltung der Grundrechte) besteht. Diese umfassen den Gleichheitsgrundsatz und auch ein Diskriminierungsverbot, was beispielsweise von Bedeutung wäre, wenn eine Gemeinde z. B. nur (selbst) ausgewählte Wirtschafts- oder Tourismusbetriebe in einen Werbeprospekt o. Ä. aufnehmen würde, ohne dies mit sachlichen Argumenten begründen zu können.

5.2 EINLEITUNG

Das Internet und seine verschiedenen Dienste haben sich in den letzten Jahren als neues Medium für geschäftliche ebenso wie private Kommunikation etabliert. Der Einsatz neuester elektronischer Mittel ist heute aber auch aus der öffentlichen Verwaltung nicht mehr wegzudenken. Dies zeigt sich vor allem bei den verschiedenen Maßnahmen zur Etablierung eines funktionierenden E-Government. Internetauftritte von Gemeinden stellen einen wesentlichen Punkt einer effizienten und bürgernahen Verwaltung dar. Allerdings sind auch beim Betrieb einer gemeindeeigenen Internetpräsenz die rechtlichen Rahmenbedingungen zu beachten. Zwar richten sich jene speziellen Bestimmungen, die den E-Commerce regeln, nicht primär an öffentlich-rechtliche Körperschaften, sondern an Unternehmen. Dennoch können Normen wie zum Beispiel das E-Commerce-Gesetz (ECG) von Gemeinden nicht vollständig ignoriert werden, insbesondere dann nicht, wenn erwerbswirtschaftliche Interessen verfolgt werden. Im Folgenden sollen zunächst die für die Internetpräsenz von Gemeinden relevanten Bestimmungen dargestellt werden, wobei ein besonderer Schwerpunkt auf den Besonderheiten liegen soll, die sich aus der öffentlich-rechtlichen Stellung von Gemeinden ergeben.

5.3 ABGRENZUNG VON PRIVATWIRTSCHAFTS- UND HOHEITSVERWALTUNG

Die Internetpräsenz eines öffentlichen Rechtsträgers kann nicht einheitlich der Hoheits- oder Privatwirtschaftsverwaltung zugeordnet werden. Vielmehr sind die einzelnen Unterbereiche voneinander abzugrenzen. Dies erscheint insbesondere im Hinblick darauf angebracht, dass die Rechtsprechung im Bereich des Amtshaftungsrechts eine umfangreiche Differenzierung im Hinblick auf die unterschiedlichen Tätigkeiten einzelner Staatsorgane vorgenommen hat.[32]

[32] Ähnlich *Schlägel,* AHG[3], Rz 81 im Bezug auf die Zuordnung von Dienstfahrten.

Grundsätzlich gilt, dass die Abgrenzung[33] zwischen Hoheitsverwaltung und Privatwirtschaftsverwaltung ausschließlich aufgrund der rechtstechnischen Umsetzung des Verwaltungshandelns erfolgt, d. h., es wird lediglich auf formelle Kriterien abgestellt.[34] So ist beispielsweise die Kundmachung von Verordnungen im Internet zur Hoheitsverwaltung einer Gemeinde zuzurechnen. Allerdings zählt nicht nur die unmittelbare Ausübung von Hoheitsgewalt (z. B. Bescheiderlassung) zur Hoheitsverwaltung, sondern auch jenes Verwaltungshandeln, dass zwar selbst nicht „normativer Art" ist, das aber im unmittelbaren Zusammenhang mit der Hoheitsverwaltung steht (sogenannte „schlichte Hoheitsverwaltung").[35] All jene Teile einer Internetpräsenz, die der unmittelbaren Durchführung der Hoheitsverwaltung einer Gemeinde dienen müssen daher selbst als hoheitlich qualifiziert werden. Zu denken ist dabei vor allem an E-Government-Applikationen, die der Durchführung von Verwaltungsverfahren dienen (z. B. bei der Durchführung von Bauverfahren).

Jene Teile der Webpräsenz einer Gemeinde, die keinen Zusammenhang zum hoheitlichen Wirkungsbereich einer Gemeinde aufweisen sind demnach der Privatwirtschaftsverwaltung zuzurechnen. Nach ständiger Rechtsprechung ist überdies im Zweifelsfall immer Privatwirtschaftsverwaltung anzunehmen.[36]

5.4 E-COMMERCE-GESETZ UND INTERNETANGEBOT VON GEMEINDEN

5.4.1 Einleitung

Die EU hat mit der E-Commerce-Richtlinie[37] wichtige rechtliche Rahmenbedingungen gesetzt, die für Österreich im E-Commerce-Gesetz (kurz: ECG) umgesetzt wurden. Etliche Vorschriften des ECG sind nur dann anwendbar, wenn ein „Dienst der Informationsgesellschaft" vorliegt. Darunter wird ein „in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst verstanden". Grundsätzlich ist davon auszugehen, dass es sich bei Internetangeboten von Gemeinden um keinen Dienst der Informationsgesellschaft handelt. In den erläuternden Bemerkungen zum ECG wurde zu dieser Thematik ausgeführt:

---

[33] Vgl. *Raschauer,* Allgemeines Verwaltungsrecht[2], 200 ff; *Novak,* Hoheitsverwaltung und Privatwirtschaftsverwaltung: Eine Abgrenzung im Spannungsfeld zwischen Verfassungsrecht und Verfassungsreform, JBl 1979, 1.

[34] VfSlg 3262/1957: *„Für die Abgrenzung des Gebietes der Privatwirtschaftsverwaltung von der Hoheitsverwaltung kommt es auf die Motive und den Zweck der Tätigkeit nicht an, entscheidend ist vielmehr, welche rechtstechnischen Mittel die Gesetzgebung zur Verwirklichung der zu erfüllenden Aufgaben bereitstellt. Hat der Gesetzgeber den Verwaltungsträger mit keinen Zwangsbefugnissen ausgerüstet, so liegt keine Hoheitsverwaltung, sondern Privatwirtschaftsverwaltung vor."*

[35] *Raschauer,* Verwaltungsrecht[3], 203.

[36] *Raschauer,* Verwaltungsrecht[3], 203; *Schlägel,* AHG3, Rz 81; vgl. zum Beispiel OGH 30.01.2001, 2 Ob 257/00a wonach die Vermittlung Arbeitsloser durch das AMS nicht dem hoheitlichen Bereich zuzuordnen ist.

[37] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG Nr. L 178 v. 17.7.2000, S. 1 ff.

„Bei den von der Richtlinie geregelten Diensten der Informationsgesellschaft handelt es sich – grob gesagt – um kommerzielle elektronische Dienste, um Dienste, die in Ertragsabsicht erbracht werden. Nach der Rechtsprechung des Europäischen Gerichtshofs muss das Entgelt die wirtschaftliche Gegenleistung für die bereitgestellte Leistung darstellen (vgl. EuGH 7.12.1993, Rs C-109/92-Wirth, Slg. 1993, I-6447). An dieser Voraussetzung fehlt es bei Tätigkeiten, die die öffentliche Hand ohne wirtschaftliche Gegenleistung im Rahmen ihrer Aufgaben, vor allem in den Bereichen Soziales, Kultur, Bildung und Justiz, ausübt. Solche Dienstleistungen zählen nicht zu den Diensten der Informationsgesellschaft. Dies gilt auch dann, wenn diese Aktivitäten von Selbstverwaltungskörpern (etwa einer Kammer oder einem Sozialversicherungsträger) ausgeübt werden. Über ein Extranet abgewickelte Serviceleistungen einer Kammer für ihre Mitglieder sind damit kein Dienst der Informationsgesellschaft, auch wenn die Kammermitglieder diese Leistungen mittelbar über die Beiträge finanzieren. Auch sind – private oder staatliche – Dienste, die keinen ökonomischen Hintergrund aufweisen (wie etwa von Universitäten betriebene und der Öffentlichkeit zur Verfügung stehende Datenbanken), keine Dienste der Informationsgesellschaft.“

Etwas Anderes gilt dann, wenn Dienste in Erwerbsabsicht erbracht werden. Auch bei einer durch einen Sponsor finanzierten unentgeltlich abrufbaren Webseite kann Erwerbsabsicht vorliegen. Erwerbsabsicht im Kontext von Gemeinden ist beispielsweise dann anzunehmen, wenn touristische Dienstleistungen (z. B. eine Hotelzimmervermittlung) auf einer Gemeindehomepage betrieben wird (auch dann, wenn die allenfalls vorgesehenen Entgelte von den vermittelten Betrieben bezahlt werden und nicht von den Kunden).

5.4.2 Informationspflichten

Bei Vorliegen eines Dienstes der Informationsgesellschaft müssen vor allem die Informationspflichten nach § 5 ECG erfüllt werden. Dabei sind den Nutzern folgende Informationen (falls vorhanden) leicht und unmittelbar zu Verfügung zu stellen:

- Name
- geographische Anschrift
- Kommunikationsadressen (z. B. Telefonnummer), vor allem aber eine E-Mail-Adresse
- Firmenbuchnummer und -gericht
- allfällige Aufsichtsbehörde
- eindeutige Preisauszeichnung

Ist es in der Praxis nicht möglich, eindeutig zu klären, ob ein Dienst der Informationsgesellschaft vorliegt oder nicht, so ist es ratsam, die entsprechenden Informationen der Einfachheit halber bereitzustellen. Auf diesem Weg können im Einzelfall schwierige Abgrenzungsfragen vermieden werden. Ein Verstoß gegen die im ECG vorgesehenen Informationspflichten stellt eine Verwaltungsübertretung dar, die mit einer Geldstrafe bis zu 3000 Euro bestraft werden kann. Daneben kommen wettbewerbsrechtliche Ansprüche in Frage (Rechtsbruch, § 1 UWG).

5.4.3 Regeln zum Vertragsschluss

Wird ein Vertrag vom Nutzer mit einem Dienst der Informationsgesellschaft online geschlossen, müssen die Schritte zum Vertragsschluss gem. § 9 ECG dem Verbraucher klar dargelegt werden. Weiter müssen technische Mittel zur Erkennung und Berichtigung von Eingabefehlern bereitgestellt und er darüber unterrichtet werden. Nach Eingang einer Erklärung muss dem Nutzer unverzüglich eine elektronische Empfangsbestätigung übersandt werden. Eine Einbeziehung von AGB über Hyperlink ist bei Webangeboten möglich. § 12 enthält im Übrigen eine wichtige Regel für den Zugang von Vertragserklärungen im digitalen Bereich. Dieser erfolgt mit Abrufbarkeit. Dazu gehört etwa das Einlangen in die Mailbox des Empfängers, jedenfalls während der Geschäftszeiten.

5.5 WEITERE INFORMATIONSPFLICHTEN

5.5.1 Mediengesetz

Neben den Informationspflichten des ECG sieht auch das Mediengesetz eine Pflicht zur Offenlegung des Betreibers einer Webseite vor, und zwar unabhängig davon, ob Entgeltlichkeit vorliegt. Auch bei Gemeindewebseiten ist daher die Offenlegungspflicht nach § 25 MedienG zu beachten. Dabei sind zumindest der Name des Betreibers und der Sitz zu nennen. Werden die Informationspflichten nach den ECG erfüllt, so ist auch dem § 25 MedienG in der Regel genüge getan.[38] Eine Impressumspflicht besteht nach § 24 MedienG nur für mindestens viermal jährlich erscheinende Newsletter.

5.5.2 Informationspflichten nach §§ 5a ff. KSchG

Im Bereich der Privatwirtschaftsverwaltung unterliegen juristische Personen des öffentlichen Rechts nach § 1 II 2 KSchG als Unternehmer den Regeln des KSchG. Dazu gehören die Informationspflichten im Fernabsatz nach §§ 5c und 5d KSchG, die recht umfangreich und weitgehend sind. Neben Informationen, die vor Vertragsschluss zu liefern sind, müssen bestimmte Informationen mit einer schriftlichen Bestätigung übersandt werden. Dies kann allerdings auch per E-Mail, nicht aber über eine Webseite erfolgen.

Hinzu kommt nach § 5e KSchG das Recht, innerhalb von sieben Werktagen ohne Angabe von Gründen vom Vertrag zurückzutreten. Besondere Probleme entstehen bei Vertragsschlüssen über Handy, bei denen die Erfüllung der Informationspflichten schon technisch an ihre Grenzen

[38] Anderes gilt nach § 25 MedienG nur dann, wenn die Webseite geeignet ist, die öffentliche Meinung zu beeinflussen. Dies wird vor allem bei Gemeindewebseiten anzunehmen sein, die auch politische Inhalte enthalten (z. B. bei Kampagnen). In diesem Fall sind folgende Informationen anzugeben: Name oder Firma, Unternehmensgegenstand, Wohnort oder Sitz (ohne genaue Anschrift), Art und Höhe der Beteiligung der Medieninhaber, bei einer Gesellschaft deren Organe und Gesellschafter, Beteiligung der Medieninhaber an anderen Medienunternehmen, die grundlegende Richtung des Mediums.

stößt und durch Verweis auf eine Webseite mit den entsprechenden Informationen rechtlich nicht wirksam durchführbar ist.[39] Dagegen wird das Versenden einer entsprechenden SMS oder das Setzen eines WAP-Links ausreichen.

5.6 WERBUNG AUF WEBSEITEN

5.6.1 Trennungsgrundsatz § 6 ECG

Bei der Gestaltung von Internetauftritten ist darauf zu achten, dass die redaktionellen Inhalte deutlich von allfälligen Werbeeinschaltungen getrennt werden.

Werbeeinschaltungen sollen im Interesse des Verbraucherschutzes und der Lauterkeit des Geschäftsverkehrs als solche erkennbar sein. Nach § 6 ECG ist Werbung klar und transparent zu gestalten. Insbesondere ist darauf zu achten, dass Einschaltungen, die nicht eindeutig als Werbung erkennbar sind, mit Hinweisen wie „Werbung“ oder „bezahlte Anzeige“ gekennzeichnet werden. Die Trennung von Werbung und redaktionellen Inhalten gilt grundsätzlich auch für Werbebanner. Eine ausdrückliche Kennzeichnung ist allerdings in diesem Fall nicht erforderlich, da für den durchschnittlichen Internetuser zumeist erkennbar ist, dass es sich dabei um eine Werbeeinschaltung handelt.

Nach § 6 ECG muss des Weiteren der Auftraggeber der Werbung identifizierbar sein. Ein entsprechender Trennungsgrundsatz ist auch in § 26 MedienG verankert, sodass das Trennungsgebot unabhängig davon beachtet werden muss, ob eine konkrete kommunale Internetpräsenz auch ein Dienst der Informationsgesellschaft ist. Für die Einhaltung des Trennungsgebotes sind sowohl der Webseitenbetreiber als auch der Werbende verantwortlich.[40]

5.6.2 Wettbewerbsrecht

Werbemaßnahmen dürfen nicht gegen das Wettbewerbsrecht verstoßen, dessen Zweck es ist, unlautere Geschäftspraktiken zu verhindern. Werbemaßnahmen dürfen nicht irreführend (vgl. § 2 UWG) oder herabsetzend gegenüber Mitbewerbern sein (vgl. § 7 UWG). Zudem ist vergleichende Werbung nur unter bestimmten Umständen zulässig (vgl. § 2 Abs. 2 UWG). Im Internet hat sich eine Fülle neuartiger Werbeformen entwickelt, von denen viele kritisch zu betrachten sind.[41] So wird das „Kaufen“ von Listenplätzen in Ergebnislisten von Suchmaschinen als irreführend bewertet, da der Nutzer von einer Reihung nach thematischer Relevanz ausgeht.[42] Aus Sicht von konkurrierenden Anbietern kann in der „Überschwemmung“ von Suchmaschinen mit bestimmten, in der Webseite „versteckten“ Begriffen („Index Spamming“) eine Absatzbehinderung nach § 1 UWG liegen, da diese ihre Leistung nicht mehr ungehindert dem Kunden anbieten

[39] OGH 4 Ob 149/03w, ecolex 2004, 101.
[40] *Seidelberger* in Brenn, ECG, S. 214.
[41] *Bräutigam*/*Leupold*/*Pfeiffer,* WRP 2000, 1 ff.
[42] Vgl. *Ernst,* WRP 2004, 278, 280.

können. Eine genaue wettbewerbsrechtliche Prüfung von Werbemaßnahmen ist jedoch nur dann erforderlich, wenn eigene Werbung auf der Webseite einer Gemeinde veröffentlicht wird.

Bei fremder Bannerwerbung haftet der Inhaber einer Webseite für den Banner nur dann, wenn es sich um offensichtlich wettbewerbswidrige Werbung handelt.[43] Nach der Rechtsprechung des OGH[44] ist dies nur dann gegeben, wenn die Rechtsverletzung für einen juristischen Laien ohne weitere Nachforschungen offenkundig ist. Dies ist beispielsweise dann der Fall, wenn in einer Bannerwerbung ein Mitbewerber beschimpft wird.

5.7 HAFTUNG FÜR INHALTE

Im Bezug auf die Haftung für Inhalte, die auf einer gemeindeeigenen Webseite veröffentlicht werden, ist die Unterscheidung zwischen Hoheits- und Privatwirtschaftsverwaltung von großer Bedeutung. Für hoheitliches Handeln richten sich die Ersatzansprüche nach dem Amtshaftungsgesetz (AHG), für die Privatwirtschaftsverwaltung hingegen nach dem allgemeinen Zivilrecht.

Soweit eine Haftung für fremde Inhalte begründet ist, können die Haftungsbeschränkungen nach §§ 13–17 ECG eingreifen. Relevant ist vor allem die Beschränkung der Haftung von Host-Providern nach § 16 ECG. Eine Haftung kommt nur bei Kenntnis von der rechtswidrigen Information oder Tätigkeit in Betracht. Ob Unterlassungsansprüche überhaupt von den Haftungsprivilegierungen erfasst werden, ist aber streitig.[45] Das Setzen von Hyperlinks wird nach § 17 ECG dem Host Providing gleichgestellt. Danach ist die Haftung für verlinkte rechtswidrige Inhalte auf Kenntnis beschränkt. Noch weitergehender ist die Haftungsbeschränkung für die Anbieter von Suchmaschinen nach § 14 ECG. Eine allgemeine Überwachungspflicht besteht für Host Provider ebenso wenig wie für Access Provider.

Das Setzen von Links kann auch unabhängig von einer Haftung für den Inhalt der verlinkten Seite eine Haftung wegen Urheberrechts- oder Wettbewerbsrechtsverletzung auslösen. Diese wird aber von der Judikatur in den Hintergrund gedrängt und demgegenüber die Bedeutung von Links für die Kommunikation im Internet betont.[46]

5.8 BESONDERE OBLIEGENHEITEN VON GEMEINDEN IM VERGLEICH ZU „REIN PRIVATEN“ WEBSEITEBETREIBERN

Bei der Gestaltung von Internetpräsenzen haben Gemeinden aufgrund der aus ihrer Stellung als Körperschaften des öffentlichen Rechts resultierenden Bindung an die Grundrechte im Rahmen der Privatwirtschaftsverwaltung („Fiskalgeltung der Grundrechte“) einige Besonderheiten zu

[43] *Seidelberger* in Brenn, ECG, S. 73.
[44] Vgl. OGH vom 6.7.2004, 4 Ob 66/04s.
[55] Vgl. OLG Wien 15.12.2003, 4 R 186/03g.
[46] OGH 4 Ob 248/02b, MR 2003, 36 – METEO-DATA.

beachten. Der Staat ist nämlich auch dann an die Grundrechte gebunden, wenn er nicht hoheitlich, sondern in der Rechtsform des Privatrechts handelt. Von besonderer Bedeutung in diesem Zusammenhang ist der Gleichheitsgrundsatz. Danach besteht auch in Bereich der Privatwirtschaftsverwaltung ein Diskriminierungsverbot.[47]

Bedeutung kommt dem Gleichheitsgrundsatz vor allem dort zu, wo Werbung für Unternehmen auf der Webseite einer Gemeinde zu finden ist. Besonders relevant ist dies im Hinblick auf Tourismusbetriebe. Denkbar wäre zum Beispiel, dass eine Gemeinde bestimmte Hotels auf ihrer Webseite auflistet. Um dem Gleichheitssatz genüge zu tun, wäre es in diesem Fall notwendig, alle Hotelbetriebe, die dies wünschen, auf die Webseite aufzunehmen. Die (unsachliche) Bevorzugung einzelner Mitbewerber kann auch einen Verstoß gegen § 1 UWG[48] darstellen. Auch die Gemeinde kann allerdings aus sachlich gerechtfertigten Gründen die Aufnahme eines Unternehmens in ein Webverzeichnis ablehnen. So hat beispielsweise der OGH in einem ähnlichen Fall entschieden, dass ein Fremdenverkehrsverband bei überdurchschnittlicher Häufung sachlich begründeter Beschwerden gegen ein Beherbergungsunternehmen nicht verpflichtet ist, dieses in einen Prospekt aufzunehmen.[49]

[47] Vgl. OGH vom 24.2.2003, 1 Ob 272702k – *„Bundesbetreuung“.*
[48] Vgl. OGH vom 16.7.2002, OGH 4 Ob 71/02y – *„Thermenhotel“*
[49] Vgl. OGH vom OGH 10.9.1991, 4 Ob 538, 539/91 in RdW 1992, 108.

Kapitel 6

URHEBERRECHT[50]

Dr. Albrecht Haller[51]

[50] Überarbeitete Fassung eines auf der Städtebund-Fachtagung „Internet, E Government & Recht“ am 25. Oktober 2005 im Rathaus Wien gehaltenen Referates.

[51] MMag. Dr. Albrecht Haller, Rechtsanwalt und Universitätslektor in Wien (office@netlaw.at).

6.1 ABSTRACT

Bei der Gestaltung kommunaler Internet-Auftritte birgt das Urheberrecht zahlreiche Fallstricke und Unsicherheitsfaktoren, die bei Rechtsstreitigkeiten zu unangenehmen Folgen für eine Stadt als Betreiber der Internet-Seiten führen können. Daher sollten bereits bei der Vergabe von Aufträgen an Webdesigner, Grafiker und andere Dienstleister im Umfeld des Internet ganz klar die Rechte an den neu geschaffenen bzw. veränderten Werken eindeutig geklärt bzw. seitens der Stadt gesichert werden.

Das Urheberrechtsgesetz definiert „Werke" als eigentümliche geistige Schöpfungen auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst, wobei der Begriff „eigentümlich" auf die Originalität von Schöpfungen im Sinne einer Unterscheidbarkeit abstellt. So ist auch das Layout einer Web-Seite als Gebrauchsgrafik und damit als Werk der bildenden Künste urheberrechtlich geschützt, außer es handelt sich um ein „Standardlayout", das beispielsweise der Vorlagensammlung einer HTML-Design-Software entnommen wurde. Der für die Beurteilung der Schutzwürdigkeit ausschlaggebende Faktor ist eben die Originalität. Auch einer Schlagwortsammlung mit rund 250 individuell ausgewählten und angeordneten Einträgen wird im Sinne des Urheberrechtsgesetzes Werkcharakter zuerkannt.

Zu beachten sind nicht nur Urheberrechte an Werken, sondern auch sogenannte verwandte Schutzrechte an bestimmten anderen künstlerischen oder auch nur organisatorisch-wirtschaftlichen Leistungen. Als Beispiele mögen die verwandten Schutzrechte der Hersteller von einfachen Lichtbildern (Photos) und von Datenbanken dienen.

Unter Datenbanken versteht das Urheberrechtsgesetz Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind. Das Urheberrechtsgesetz bietet einen zweigliedrigen Schutz: Erstens genießen Datenbanken unter der allgemeinen Voraussetzung von Originalität urheberrechtlichen Schutz (als Datenbankwerke). Wenn für die Beschaffung, Überprüfung oder Darstellung des Datenbank_inhaltes eine wesentliche (nicht notwendigerweise finanzielle) Investition erforderlich war (z. B. Zusammenstellung Hunderter Links zu einer Linksammlung), dann ist die Datenbank – gegebenenfalls zusätzlich zum Urheberrechtsschutz – durch ein verwandtes Schutzrecht geschützt.

Werden urheberrechtlich geschützte Werke von Dritten weiter bearbeitet, so darf der Bearbeiter seine Bearbeitung nur verwerten, wenn er vorher die Zustimmung des Originalurhebers eingeholt hat.

Zu beachten ist weiters der sogenannte Bildnisschutz, d. h. das Recht jeder natürlichen Person am eigenen Bild. Hier gilt, dass eine Veröffentlichung grundsätzlich zulässig ist, sofern sie nicht berechtigte Interessen des Abgebildeten verletzt. Diese werden insbesondere bei Bloßstellung, Preisgabe des Privatlebens, Anlass zur Missdeutung und entwürdigenden oder herabsetzenden Abbildungen verletzt. Die nicht vom Abgebildeten

bewilligte Verwendung von Personenbildnissen zu Werbezwecken ist nach ständiger Rechtsprechung nicht zulässig, weil der Abgebildete damit dem Verdacht ausgesetzt wird, sein Bildnis entgeltlich für Werbezwecke zur Verfügung gestellt zu haben. Vor diesem Hintergrund wäre auch die Zulässigkeit der Abbildung von Mitarbeitern auf der Web-Site der Stadt kritisch zu hinterfragen. Kriterium für eine Beurteilung wäre in diesem Fall das Verhältnis zwischen „Veröffentlichungsinteresse" und „Persönlichkeitsschutz".

Eine Besonderheit des Urheberrechtes besteht darin, dass es unter Lebenden grundsätzlich nicht übertragen werden kann. Stattdessen kann der Urheber jedem beliebigen Dritten nicht-ausschließliche Lizenzen (Werknutzungsbewilligungen) oder ausschließliche Lizenzen (Werknutzungsrechte) erteilen.

6.2 EINLEITUNG

Hand aufs (kommunale) Herz: Welche Stadt oder welche Gemeinde kommt bei ihrem Web-Auftritt ohne urheberrechtlich geschützte Inhalte aus? Keine. Denn wessen Internetpräsenz über eine bloße virtuelle Visitkarte hinausgeht, der nutzt fast immer geschützte Werke und Leistungen – sei es in Wort, Bild, Ton oder einer beliebigen Kombination dieser Elemente. Die Bedeutung des Urheberrechtes für Städte und Gemeinden kann also kaum unterschätzt werden.

Im Folgenden soll nicht eine systematische Einführung ins Urheberrecht geboten werden. Vielmehr mögen drei in der Praxis häufig auftauchende Fragen veranschaulichen, was unter urheberrechtlichem Blickwinkel zu bedenken ist und welche urheberrechtlichen Fallen sich auftun können.

6.3 WAS ALLES IST URHEBERRECHTLICH GESCHÜTZT?

Inhalte werden entweder selber geschaffen oder von Dritten beschafft – wobei sich „Beschaffung" nicht auf den Schlachtruf „Woher nehmen, wenn nicht stehlen?", sondern auf den ordnungsgemäßen Erwerb einer Nutzungserlaubnis bezieht.

Egal, ob man selber schafft oder von Dritten beschafft: In beiden Fällen stellt sich die Frage, welche Inhalte denn überhaupt urheberrechtlich geschützt sind. Bei der Beantwortung dieser Frage sollte man nicht übersehen, dass das Urheberrecht **verschiedene Arten von Schutzgegenständen** kennt: Denn wie schon der volle Titel des Urheberrechtsgesetzes – „Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte" – zum Ausdruck bringt, werden im Rahmen des Urheberrechtes (im weiteren Sinn) nicht nur **Werke** geschützt (durch das Urheberrecht im engeren Sinn), sondern auch bestimmte dem Urheberrecht im engeren Sinn benachbarte **Leistungen** (durch verwandte Schutzrechte). Zwei Beispiele: Wer im World-Wide Web Musikdateien anbietet, hat nicht nur die Urheberrechte der Autoren, sondern auch die verwandten Schutzrechte der Interpreten und der Produzenten zu beachten. Wer Fotos in urheberrechtlich relevanter Weise nutzen will, muss sich nicht nur um das Urheberrecht (des Fotografen als einer natürlichen Person), sondern auch um das verwandte

Schutzrecht des Lichtbildherstellers (vielleicht eines Fotostudios) kümmern; bei Personenbildnissen ist außerdem das Recht des Abgebildeten am eigenen Bild (dazu später) zu beachten.

Das Urheberrechtsgesetz definiert Werke als **eigentümliche geistige Schöpfungen** auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst. Wie jeder unbestimmte Gesetzesbegriff bedarf auch die Formulierung „eigentümliche geistige Schöpfung" der Konkretisierung durch die Rechtsprechung. Die Gerichte stellen darauf ab, ob ein Ergebnis menschlichen Schaffens den Stempel der persönlichen Eigenart seines Schöpfers trägt. Mit anderen Worten: Auf Originalität im Sinne von Unterscheidbarkeit kommt es an.

Unter der Voraussetzung, dass es sich um eine originelle Schöpfung handelt, ist etwa auch das **Layout einer Web-Seite,** und zwar als Gebrauchsgrafik und damit als Werk der bildenden Künste, urheberrechtlich geschützt. Im ersten vom OGH entschiedenen Fall bestand der Schutzgegenstand in jener konkreten Ausdrucksform, die Gestaltungselemente wie Banner und Navigationsleisten im Layout der Homepage eines Unternehmens gefunden hatten; die abstrakten Gestaltungsideen und -techniken sind vom Urheberrecht nach ständiger Rechtsprechung nie umfasst. Wenn es einer Web-Seite dagegen schon an Individualität fehlt, dann bleibt natürlich auch die konkrete Formgebung schutzlos: etwa bei einer rein handwerklichen, routinemäßigen Leistung, die sich im Rahmen des Alltäglichen und Üblichen bewegt, indem sie sich zum Beispiel auf die Standard-Layouts der Erstellungs-Software beschränkt und keine individuellen Gestaltungselemente einsetzt (OGH 24. 4. 2001, 4 Ob 94/01d – www.telering.at).

In einer anderen, ganz jungen Entscheidung hat der Oberste Gerichtshof (OGH) einer **Sammlung von rund 250 Schlagwörtern,** die auf der Homepage eines Online-Shop „suchmaschinenoptimiert" dessen Sortiment beschreiben, Werkcharakter zuerkannt. Denn bei der nach verschiedenen Auswahl- und Ordnungskriterien zusammengestellten Schlagwortsammlung handelt es sich um das originell gegliederte Ergebnis einer gedanklichen Durchdringung des verarbeiteten Materials, das den Stempel der persönlichen Eigenart trägt und damit unterscheidbar im urheberrechtlichen Sinn ist (OGH 12. 7. 2005, 4 Ob 58/05s – Schlagwortsammlung).

Die vom Werkbegriff vorausgesetzte Eigentümlichkeit kann auch überhaupt nur in der Auswahl und/oder Anordnung einzelner Elemente liegen: „Sammlungen, die infolge der Zusammenstellung einzelner Beiträge zu einem einheitlichen Ganzen eine eigentümliche geistige Schöpfung darstellen, werden als **Sammelwerke** urheberrechtlich geschützt; die an den aufgenommenen Beiträgen etwa bestehenden Urheberrechte bleiben unberührt." Wenn ein Sammelwerk zugleich unter die **Datenbank-**Definition fällt – „Datenbanken im Sinn dieses Gesetzes sind Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind." – spricht man von einem **Datenbankwerk.**

Der OGH vertritt zumindest an einer Stelle die Auffassung, eine einzelne Web-Seite könne kein Datenbankwerk sein; denn ihre Elemente seien nicht voneinander unabhängig, sondern von vornherein aufeinander bezogene Teile eines einheitlichen Werkes. Sind jedoch mehrere Web-Seiten ihrem Inhalt nach voneinander unabhängig, aber miteinander durch Hyperlinks verbunden und bilden sie zusammen einen **systematisch angeordneten Internet-Auftritt** (Website), so liegt –

eine eigentümliche geistige Schöpfung vorausgesetzt – ein Datenbankwerk vor (OGH 10. 7. 2001, 4 Ob 155/01z – C-Villas).

Geschützt sind nicht nur Originalwerke, sondern – soweit sie eine eigentümliche geistige Schöpfung des Bearbeiters sind – auch **Bearbeitungen,** zum Beispiel Übersetzungen. Die Grenze der schutzwürdigen Bearbeitung verläuft einerseits dort, wo es sich bloß um handwerkliche Veränderungen handelt; anderseits, wo ein im Vergleich zum benutzten Werk selbständiges neues Werk, eine sogenannte freie Bearbeitung entsteht (Stichwort Inspiration). Was immer wieder vergessen wird und häufig Anlass zu Streit gibt: Der Urheber einer Bearbeitung darf diese nur so weit verwerten, als ihm der Urheber des bearbeiteten Werkes dies erlaubt (Bearbeitungsrecht).

Wie gesagt: Unter dem Dach des Urheberrechtes im weiteren Sinn werden nicht nur Urheber hinsichtlich ihrer Werke (Urheberrecht im engeren Sinn), sondern auch einige andere Personengruppen hinsichtlich bestimmter urheberrechtsnaher Leistungen geschützt. Diese **verwandten Schutzrechte** werden auch Leistungsschutzrechte oder Nachbarrechte genannt. Die durch verwandte Schutzrechte geschützten Objekte sind: Vorträge und Aufführungen (zusammenfassend: Darbietungen) von Werken der Literatur oder Tonkunst, Lichtbilder und Laufbilder (kinematographische Erzeugnisse), Schallträger, Rundfunksendungen, nachgelassene Werke und Datenbanken. Die geschützten Subjekte sind: ausübende Künstler, Veranstalter, Lichtbildhersteller, Schallträgerhersteller, Rundfunkunternehmer, Erstherausgeber nachgelassener Werke und Datenbankhersteller.

Im Hinblick auf das verwandte Schutzrecht des Lichtbildherstellers hatte sich der OGH bereits mit dem Thema **Web-Cam und Live-Bilder** zu befassen. Er stellte klar, dass auch mittels computergesteuerter Digitalkameras aufgenommene und gespeicherte „Standbilder" Leistungsschutz genießen. Im konkreten Fall kam der OGH nach gründlicher Auseinandersetzung mit dem einschlägigen Schrifttum zum Schluss, dass der klagende Online-Dienst-Betreiber gegenüber der Tätigkeit der Bedienung des von ihm installierten Systems mehr als eine reine Hilfsleistung erbrachte: „Die Klägerin ist deshalb jedenfalls (Mit-)Herstellerin der Standbilder […], allenfalls zusammen mit demjenigen, der in Ansehung der installierten Kameraanlage die Verfügungsbefugnis darüber besitzt, das aufzunehmende Motiv sowie den Zeitpunkt seiner Aufnahme durch Bedienung des Systems zu bestimmen." (OGH 1. 2. 2000, 4 Ob 15/00k - Vorarlberg Online)

Im Zusammenhang mit dem Internet hat von allen verwandten Schutzrechten wahrscheinlich jenes des **Datenbankherstellers** die größte Bedeutung. Während Datenbanken früher in Österreich und den meisten anderen Mitgliedstaaten der Europäischen Union nur dann sonderrechtlich geschützt waren, wenn sie zugleich Sammelwerke waren, besteht seit 1998 ein zweigliedriger Schutz: der (bloß modifizierte) urheberrechtliche Schutz für Datenbankwerke und – gegebenenfalls kumulativ – ein neuer leistungsschutzrechtlicher Schutz für Datenbanken, wenn für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts eine (nach Art oder Umfang) wesentliche Investition erforderlich war; diese Investition muss nicht in Geld, sondern kann auch in Mühe oder Zeit bestehen. Unter der genannten Voraussetzung können also nach neuer Rechtslage auch bloße **Link-Sammlungen,** bei denen weder die Auswahl noch die Anordnung eigentümlich ist, sonderrechtlich geschützt sein.

8.4 DARF MAN FOTOS AUCH OHNE ZUSTIMMUNG DER ABGEBILDETEN VERWENDEN?

Der Bildnisschutz – auch **Recht am eigenen Bild** genannt – ist in § 78 des Urheberrechtsgesetzes (UrhG) geregelt. Der Kern dieser Bestimmung lautet: „Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden."

Die Veröffentlichung eines Personenbildnisses ist also grundsätzlich erlaubt, außer es würden berechtigte Interessen des Abgebildeten verletzt. Der Zweck der Bestimmung ist der **Schutz** der abgebildeten Person **gegen** den **Missbrauch** ihrer Abbildung **in der Öffentlichkeit.** Der Schutz gilt also dem Aussehen einer natürlichen Person als einem wesentlichen Teil ihrer Persönlichkeit. § 78 UrhG schützt nicht davor, fotografiert zu werden, sondern verbietet erst bestimmte Verwendungen eines bereits hergestellten Bildnisses.

Nach § 78 UrhG dürfen „Bildnisse von Personen" unter bestimmten Umständen nicht verbreitet werden. Als Eingriffsgegenstand kommen alle Arten von Personenbildnissen in Betracht. Auf die verwendete Technik kommt es nicht an; ebenso wenig darauf, ob das beanstandete Bild urheberrechtlich oder leistungsschutzrechtlich geschützt ist. Obwohl es in Praxis und Rechtsprechung meistens um Fotos geht, kann der Abgebildete unter denselben Voraussetzungen etwa auch gegen Karikaturen vorgehen. Die Rechtsprechung bezieht sogar **Bildunterschriften, Begleittexte und Ähnliches** in ihre Prüfung ein.

Nach § 78 UrhG dürfen Personenbildnisse unter bestimmten (in zwei verschachtelten Konditionalsätzen zusammengefassten) Voraussetzungen „weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden". Die Eingriffshandlung besteht also in einem veröffentlichenden Verbreiten, kurz: im Veröffentlichen.

Der Gesetzgeber hat den Begriff der berechtigten Interessen bewusst nicht näher festgelegt, um einen weiten Spielraum zu eröffnen, der es ermöglicht, den Verhältnissen des Einzelfalls gerecht zu werden. Zur Erleichterung der Entscheidung, ob im konkreten Einzelfall berechtigte Interessen verletzt würden, hat die Rechtsprechung ein **Prüfungsschema** entwickelt. In einem ersten Schritt wird überprüft, ob ein (objektiv) schutzwürdiges Interesse des Abgebildeten vorliegt, das verletzt sein könnte. Ist dies zu bejahen, ergibt sich entweder schon daraus die Verletzung berechtigter Interessen oder es ist in einem zweiten Schritt zu prüfen, ob ein (objektives) Veröffentlichungsinteresse vorliegt, sofern der Veröffentlicher ein solches behauptet. Das schutzwürdige Interesse des Abgebildeten ist dann gegen das Veröffentlichungsinteresse abzuwägen. Überwiegen die Interessen des Abgebildeten, liegt eine Verletzung berechtigter Interessen vor.

Voraussetzung jeder Bildnisschutzverletzung ist naturgemäß, dass die abgebildete Person e**rkennbar** ist. Die Erkennbarkeit muss sich nicht aus den Gesichtszügen, sondern kann sich auch aus dem sonstigen Erscheinungsbild des Abgebildeten oder einem Begleittext ergeben. Maßgebend ist nach der Rechtsprechung nicht der Familien- und Freundeskreis, sondern der Bekanntenkreis.

Die meisten der vom OGH entschiedenen Fälle lässt sich einer, zwei oder mehreren von vier **Fallgruppen** zuordnen, in denen eine Bildnisveröffentlichung rechtswidrig ist: Bloßstellung; Preisgabe des Privatlebens; Anlass zu Missdeutungen; entwürdigende oder herabsetzende Abbildung.

Die Fallgruppe **„Anlass zu Missdeutungen"** zeigt, dass sich niemand gefallen lassen muss, durch eine bestimmte Veröffentlichung seines Bildnisses in einen nicht den Tatsachen entsprechenden Zusammenhang gestellt zu werden. Schon die bloße Möglichkeit von Missdeutungen reicht. Das klassische Beispiel ist die Verwendung von Personenbildnissen (ohne Zustimmung der Abgebildeten) zu Werbezwecken. Der OGH begründet diese Entscheidungspraxis damit, der Abgebildete werde dem Verdacht ausgesetzt, sein Bildnis entgeltlich zu **Werbezwecken** zur Verfügung gestellt zu haben. Im Hinblick auf den verstärkten und heutzutage kaum mehr als anrüchig empfundenen Einsatz von haupt- und nebenberuflichen Fotomodellen wäre es allerdings zeitgemäßer zu argumentieren, dass es dem Abgebildeten vorbehalten ist zu entscheiden, ob beziehungsweise zu welchen Bedingungen seine Persönlichkeitsmerkmale den Geschäftsinteressen Dritter dienstbar gemacht werden sollen.

In eine ähnliche Richtung geht die erste Bildnisschutz-Entscheidung des OGH mit Internet-Bezug: Der OGH hat auch – in diesem Fall allerdings ohne Bezugnahme auf eine Fallgruppe – das Abrufbarhalten des **Fotos einer Arbeitnehmerin** auf der nicht zugangskontrollierten Website des Arbeitgebers gegen den Willen der Arbeitnehmerin als Bildnisschutzverletzung beurteilt; eine entsprechende Duldungspflicht könne auch nicht aus der arbeitsrechtlichen Treuepflicht abgeleitet werden (OGH 5. 10. 2000, 8 Ob A 136/00h – Arbeitnehmerfoto). Ähnlich zu beurteilen wäre wohl auch das Abrufbarhalten von Fotos der Gemeindebediensteten auf der Website einer Gemeinde.

In zwei Fällen sind ansonsten unzulässige Veröffentlichungen von Personenbildnissen doch rechtmäßig: wenn der Abgebildete der Veröffentlichung **zugestimmt** hat **oder** wenn das **Veröffentlichungsinteresse** den Persönlichkeitsschutz **überwiegt.** Zunächst zur allfälligen Zustimmung des Abgebildeten: Liegt eine Zustimmung des Abgebildeten zur Veröffentlichung vor, entfällt ein allfälliges schutzwürdiges Interesse. Die Zustimmung kann ausdrücklich oder stillschweigend (zum Beispiel beim Posieren für Presse- oder Werbeaufnahmen) erfolgen. Die Reichweite und der Zweck der erteilten Zustimmung sind zu berücksichtigen. So ist etwa die Zustimmung zur Veröffentlichung eines Bildes in medizinischen Fachzeitschriften nicht auch eine Zustimmung zur Veröffentlichung in der auflagenstärksten österreichischen Tageszeitung.

Die vom Gesetzgeber gebotene Abwägung der beiderseitigen Interessen wirft die Frage nach allfälligen Interessen des Veröffentlichers auf. Als verfassungsrechtliche Grundlage dient die **Meinungsäußerungsfreiheit** (Artikel 10 der Europäischen Menschenrechtskonvention), die sich nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte auch auf bildliche Kommunikation erstreckt. Das verfassungsgesetzlich und völkerrechtlich gewährleistete Recht auf freie Meinungsäußerung rechtfertigt aber nicht jede Bildnisveröffentlichung, sondern ist mit dem ebenfalls verfassungsgesetzlich und völkerrechtlich geschützten **Recht auf Achtung des Privat- und Familienlebens** (Artikel 8 EMRK) in Einklang zu bringen.

Die Veröffentlichung von Bildern einer **Person,** deren Aussehen **allgemein bekannt** ist (zum Beispiel eines Spitzenpolitikers), verletzt in der Regel wegen des Überwiegens des Veröffentlichungsinteresses keine berechtigten Interessen der abgebildeten Person, insbesondere wenn die Person in jener Funktion in Erscheinung tritt, der sie ihre Bekanntheit verdankt. Die schutzwürdigen Interessen der abgebildeten Person werden aber wohl dann überwiegen, wenn die veröffentlichten Bilder zum Beispiel die Intimsphäre verletzen oder für Werbung verwendet werden, entstellen, die Person der Neugierde und Sensationslust aussetzen, sie mit Vorgängen in Verbindung bringen, mit denen sie nichts zu tun hat, oder sie in peinlichen Situationen zeigen.

6.5 WAS IST BEIM ABSCHLUSS VON LIZENZVERTRÄGEN ZU BEACHTEN?

Das Urheberrecht ist zwar vererblich, aber unter Lebenden **grundsätzlich nicht übertragbar.** Umso wichtiger ist die Möglichkeit des Urhebers, einem Dritten eine Lizenz (Erlaubnis) zur Nutzung seines Werkes zu erteilen. Lizenzverträge können ausdrücklich oder stillschweigend, **mündlich oder schriftlich** abgeschlossen werden. Zwecks besserer Beweisbarkeit empfiehlt es sich, Lizenzverträge ausdrücklich und schriftlich abzuschließen. Anders als etwa Mietverträge unterliegt die Beurkundung von Lizenzverträgen keiner Rechtsgeschäftsgebühr.

Lizenzen werden entweder **umfassend oder** (sachlich, örtlich und/oder zeitlich) **beschränkt** erteilt. Lizenzen können den Lizenznehmer nicht-ausschließlich oder ausschließlich berechtigen; je nachdem spricht man von **Werknutzungsbewilligungen** oder **Werknutzungsrechten.** Wichtig ist auch zu klären, ob Lizenzen übertragbar sind oder nicht. Und schließlich sollte der Lizenznehmer, wenn er das betroffene Werk nicht nur in ursprünglicher, sondern auch in bearbeiteter oder sonst veränderter Form nutzen will, die Lizenz ausdrücklich auf solche Nutzungen erstrecken lassen.

Das größte urhebervertragsrechtliche Problem stellt sich im Verhältnis von alten Verträgen und neuen Medien. Mit anderen Worten: Deckt ein alter, schon vor dem „Internet-Zeitalter“ abgeschlossener Lizenzvertrag auch moderne Nutzungen, insbesondere im World-Wide Web?

Zur Illustration ein Vergleich mit der Rechtslage in Deutschland: Nach deutschem Urheberrecht bestimmt sich der Umfang eines Nutzungsrechtes, bei dessen Einräumung die Nutzungsarten, auf welche sich das Recht erstrecken soll, nicht einzeln bezeichnet sind, nach dem mit der Rechtseinräumung verfolgten Zweck. Dem österreichischen Urheberrechtsgesetz dagegen mangelt es an einer ausdrücklichen Bestimmung dieses Inhalts; einmal hat der OGH die sogenannte **Zweckübertragungstheorie** (besser: Einräumungszwecktheorie) sogar ausdrücklich als „in Österreich nicht herrschend“ bezeichnet.

Nichtsdestoweniger anerkennt der OGH in ständiger Rechtsprechung den allgemeinen Grundsatz, dass das Ausmaß der Befugnisse, die der Werknutzungsberechtigte durch den Werknutzungsvertrag erhält, im Zweifel nicht weiter reicht, als es für den praktischen Zweck der ins Auge gefassten Werknutzung erforderlich erscheint. Der OGH gewinnt diesen Grundsatz im Wege der Rechtsanalogie aus den urheberrechtlichen Auslegungsregeln, den im Urheberrechtsgesetz geregelten weiteren Vorbehalten zugunsten des Urhebers und dem im Urheberrechtsgesetz enthaltenen Hinweis auf die Grenzen des Werknutzungsrechtes.

Zwischen diesen beiden Positionen besteht ein wesentlicher Unterschied: Während die deutsche Regelung bei Verletzung der **Spezifizierungsobliegenheit** zur Reduktion auch eindeutiger Formulierungen (wie etwa einer pauschalen Einräumung sämtlicher Nutzungsrechte) führt, ist der vom OGH anerkannte Grundsatz nicht mehr als eine am Vertragszweck orientierte **Zweifelsregel**.

Und noch ein ganz wesentlicher Umstand, den man beim Abschluss von Lizenzverträgen nicht aus den Augen verlieren darf: Im Urheberrecht und auch im sonstigen Immaterialgüterrecht (insbesondere Marken-, Muster- und Patentrecht) gibt es **keinen Gutglaubenserwerb vom Nichtberechtigten.** Das heißt: Wer einen Lizenzvertrag mit jemandem schließt, der keine Rechte am vertragsgegenständlichen Werk (oder sonstigen Schutzgegenstand) hat, der kann durch diesen Lizenzvertrag auch selbst keine Rechte erwerben. Man tut also gut daran, sich seine Lizenzgeber sorgfältig auszusuchen – und Verträge so abzuschließen, dass man auch bei bösen Überraschungen bestmöglich geschützt ist.

Kapitel 7

SPAM: VOM UMGANG MIT UNERWÜNSCHTER ELEKTRONISCHER KOMMUNIKATION

Prof. DDr. Walter Blocher

7.1 ABSTRACT

E-Mail bildet einen – wenn nicht sogar den wichtigsten – Dienst des Internets, der auch von Behörden intensiv genützt wird. Aufgrund seiner enormen Verbreitung ist dieser Dienst auch eines der Hauptziele von Attacken, vor allem in Form von Viren und SPAM. Im Umfeld von E-Mail gibt es einige rechtliche Regelungen, die bei der Nutzung dieses Dienstes zu beachten sind. Ein Teil dieser gesetzlichen Bestimmungen umfasst analog dem Briefgeheimnis den Schutz der Inhalte von E-Mails in Form neuer Tatbestände im StGB. Es sind dies der „Widerrechtliche Zugriff auf ein Computersystem" (§ 118a), die „Verletzung des Telekommunikationsgeheimnisses" (§ 119) und das „Missbräuchliche Abfangen von Daten (§ 119a). Das Telekommunikationsgesetz 2003 untersagt ein „Verfälschen, Verändern, Unterdrücken oder unrichtiges Wiedergeben von Nachrichten", und auch das unerlaubte Vorlesen oder sonstige Verbreiten des Inhalts von Briefen, Tagebüchern und ähnlichen vertraulichen Aufzeichnungen wird ganz generell im Urheberrechtsgesetz (§ 77 UrhG) untersagt. Das ABGB sieht sogar die Möglichkeit von Schadenersatzforderungen vor, wenn jemand „rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet" (§ 1328a ABGB).

Neben dem Zugriff auf Mailboxen und E-Mail-Inhalte stellt SPAM, also der unaufgeforderte Massenversand von E-Mails, einen zweiten Problembereich der elektronischen Post dar; die Bandbreite der Belästigungen reicht von der unaufgeforderten Übermittlung von Newslettern bis hin zu regelrechten Attacken mit Müll-E-Mails. Auch gegen solchen SPAM gibt es mittlerweile eine rechtliche Handhabe, auch wenn diese gerade im Umfeld von Unternehmen (und öffentlichen Rechtsträgern) etwas zu kurz greift: Das E-Commerce-Gesetz berührt nicht die Zulässigkeit der Übermittlung elektronischer Post, sondern schreibt lediglich vor, dass kommerzielle E-Mails, die ohne Zustimmung des Empfängers an diesen gerichtet werden, eindeutig als solche erkennbar sein müssen. Der gesamte Bereich des „privaten" SPAM wird vom E-Commerce-Gesetz somit nicht erfasst. Hier greift das Telekom-

munikationsgesetz (TKG), das „Zusendungen zu Zwecken der Direktwerbung" oder „an mehr als 50 Empfänger gerichtete Sendungen ohne vorherige Einwilligung des Empfängers" untersagt. Im Falle von unaufgeforderten Newslettern oder Massenmails durch eine Gemeinde sind daher diese gesetzlichen Vorgaben jedenfalls zu beachten. ***Durch die am 1.März 2006 in Kraft getretene Novelle des §107 TKG 2003 besteht nun auch für Unternehmer der gleiche Schutz vor Spam wie für Verbraucher.***

In Zusammenhang mit den Auswirkungen von SPAM, nämlich einem Ausfall von Computersystemen bei massiver Belastung, sieht das StGB im § 126b überdies Strafbestimmungen vor, wenn jemand die „Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt".

7.2 E-MAIL ALS „KILLER-APPLICATION"

Allen „Internet-Hypes" wie Peer-to-Peer-Dateienaustausch, Voice over IP, Blogging etc. zum Trotz gilt E-Mail nun schon seit Jahren unangefochten als die „Killer-Application"[52]. Inzwischen ist der seit Mitte der Sechzigerjahre des vorigen Jahrhunderts verfügbare elektronische Nachrichtenaustausch längst zum wichtigsten Kommunikationsmedium geworden und wird im Geschäftsleben bereits dem Telefon vorgezogen[53]. Die wichtigsten Gründe dafür sind wohl darin zu sehen, dass E-Mail archivier- und damit nachvollziehbar ist, dass mehrere Personen auf einmal erreicht werden können und dass die Kommunikationspartner nicht zeitgleich online sein müssen. Sogar bei den mobilen Diensten hat E-Mail inzwischen nach Einschätzung von Führungskräften deutscher Telekommunikationsunternehmen SMS auf Platz zwei verdrängt, während Sprachtelefonie und Internet erst weit abgeschlagen auf den Rängen drei und vier folgen[54].

7.3 E-MAIL UND E-GOVERNMENT

Im Zusammenhang mit E-Government kann man sich dem Thema „E-Mail" unter verschiedensten Aspekten nähern. Im Kernbereich der Hoheitsverwaltung geht es vorrangig um sichere und beweisbare Kommunikation mit Bürgerinnen und Bürgern. Daher haben hier elektronische Signaturen und Zustelldienste größte Bedeutung. Sie werden in diesem Heft von *Wilfried Connert* erläutert.

Neben den genannten technischen und organisatorischen Maßnahmen schützt eine ganze Reihe gesetzlicher Bestimmungen den Inhalt elektronischer Kommunikation. Nach h.M. ist zwar der mit „Verletzung des Briefgeheimnisses und Unterdrückung von Briefen" übertitelte § 118 StGB nicht

---

[52] Vgl. *Hudetz*/*Mörsheim*/*van Baal,* Elektronischer Geschäftsverkehr in Mittelstand und Handwerk (2005) [http://www.ec-net.de/downloads/files/Studien/ElektronGeschaeftsprozesse.pdf] 20, wonach die E-Mail-Kommunikation sowohl heute als auch in den kommenden zwei Jahren den intensivsten Nutzungsgrad sämtlicher Internet-Anwendungen aufweist bzw. aufweisen wird.

[53] *Cain,* Enterprise Approaches to E-Mail Hygiene, Meta Practice, 18 August 2004 [http://www.proofpoint.com/downloads/WP-Proofpoint-META-Enterprise-Approaches-to-Email-Hygiene.pdf].

[54] Vgl. *Mummert Consulting,* „TELCO Trend"-Berichtsband März 2005.

auf E-Mails anwendbar, weil diese unkörperlich und damit weder Schriftstücke noch Briefe sind[55], wobei eine analoge Anwendung wegen des strafrechtlichen Analogieverbots nicht in Betracht kommt. In jüngerer Zeit – insbesondere im Zuge der Umsetzung der „Cyber-Crime-Konvention"[56] – wurden aber folgende u.U. einschlägigen Tatbestände neu in das StGB aufgenommen bzw. entsprechend adaptiert: „Widerrechtlicher Zugriff auf ein Computersystem" (§ 118a), „Verletzung des Telekommunikationsgeheimnisses" (§ 119) und „Missbräuchliches Abfangen von Daten" (§ 119a). Das Telekommunikationsgesetz 2003 pönalisiert u.a. das Verfälschen, Verändern, Unterdrücken oder unrichtige Wiedergeben von Nachrichten (§ 108), während der in § 77 UrhG geregelte Briefschutz das Vorlesen oder sonstige Verbreiten des Inhalts von Briefen, Tagebüchern und ähnlichen vertraulichen Aufzeichnungen verbietet. Schließlich kann seit dem 1. 1. 2004 nach dem durch das ZivRÄG 2004 neu in das ABGB eingefügten § 1328a Schadenersatz von demjenigen begehrt werden, der „rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet".

Beim Versand von Newsletters oder der Beteiligung an Newsgroups schließlich besteht auch für eine Gemeinde die Gefahr, sich als „Newbie" zu outen, durch den Verstoß gegen die sog. „Netiquette"[57] oder sonstige Gepflogenheiten Reputation einzubüßen oder gar durch die Verletzung einschlägiger Gesetze mit unangenehmen Sanktionen konfrontiert zu werden. Um derartiges zu vermeiden, sollten neben den anwendbaren Rechtsvorschriften auch „Best Practices" der Direktmarketing-Branche berücksichtigt und z.B. (mindestens) die „Richtlinie für erwünschtes Online-Direktmarketing"[58] des Verbands der deutschen Internetwirtschaft e.V. eingehalten werden.

7.4 SPAM ALS „APPLICATION-KILLER"?

Dieser Beitrag konzentriert sich jedoch auf ein sattsam bekanntes Phänomen, das sich als „Application-Killer" erweisen könnte, wenn es nicht gelingt, ihm Herr zu werden. Die unter dem Markennamen „Spam"[59] vertriebene seltsame Masse aus Schweinefleisch, Wasser und Kartoffelstärke hat bisher (zum Glück) nur den Weg in die u.s.-amerikanische und allenfalls noch in die britische Küche gefunden. Von den unverlangten E-Mails dagegen, denen ein Spaßvogel vielleicht auch wegen des beim Empfänger ausgelösten Ekels den Namen der kulinarischen Verirrung gab[60], blieben auch heimische Internet-Nutzer nicht verschont.

---

[55] Vgl. *Lewisch* in *Höpfel/Ratz* (Hrsg.), Wiener Kommentar zum Strafgesetzbuch², 30. Lfg., § 118 StGB Rz. 5.

[56] Convention on Cybercrime, European Treaty Series No 185 vom 23. 11. 2001.

[57] Siehe z.B. Die Netiquette für AT.*: [http://www.usenet.at/netiquette.html].

[58] [http://www.eco.de/servlet/PB/show/1075685_l1/Richtlinie_OM_121.pdf].

[59] Dabei handelt es sich um ein Kunstwort aus „spiced pork and ham" bzw. aus den beiden ersten und letzten Buchstaben von „spiced ham".

[60] Der Legende nach geht die Bezeichnung auf einen Klassiker der englischen Komikertruppe Monthy Python zurück. Der Sketch aus dem Jahr 1970 spielt in einem Restaurant, das ausschließlich Speisen mit Frühstücksfleisch anbietet. Mrs. Bun, die mit Ihrem Mann zu Gast ist, bittet flehentlich um eine Mahlzeit ohne Spam, doch ihr akuter Widerwille wird von einem Wikinger-Chor erstickt, der immer lauter den Gesang von „Spam, lovely spam, wonderful spam" anstimmt. (*Schneider,* Werde reich, glücklich und satt!!! – SPAM: Die Schattenseite des E-Commerce, [http://www.heise.de/tp/r4/artikel/9/9110/1.html].)

7.5 SPAM FACTS

Man schätzt, dass weltweit etwa 65 % aller Mails in die Kategorie „Spam“ fallen[61]. In Österreich sind es nach einer jüngsten Untersuchung 48,8 %[62]. Die für die europäischen Unternehmen durch Spam-bedingten Produktivitätsverlust entstehenden Kosten werden in einer Mitteilung der EU-Kommission mit mehreren Milliarden Euro beziffert[63]. Anschaulicher wird das Ausmaß des Problems, wenn man z.B. in einer Gemeinde mit 150 Bediensteten mit je 10 Spams pro Tag und Mitarbeiter rechnet. Werden je Spam-Mail für das Anlesen und Löschen nur 10 Sekunden benötigt, bedeutet das bei 220 Arbeitstagen einen Zeitverlust von 611 Stunden und bei einem Brutto-Stundensatz von durchschnittlich 40,– Euro einen verdeckten Schaden von insgesamt 36.000,– Euro pro Jahr[64]. Aus solchen Zahlen lässt sich nicht zuletzt für Behördenleiter, die dem Grundsatz der zweckmäßigen und sparsamen Mittelverwendung verpflichtet sind, unmittelbarer Handlungsbedarf ableiten.

7.6 ORGANISATORISCHE UND TECHNISCHE MASSNAHMEN ZUR SPAM-BEKÄMPFUNG

7.6.1 Spam vermeiden

Die bessere Alternative zur Bekämpfung von Spam ist zweifellos dessen Vermeidung. Das „Geschäftsmodell“ der Spammer besteht darin, mit minimalem eigenem Kostenaufwand eine riesige Anzahl von Empfängern zu erreichen, sodass es für den wirtschaftlichen Erfolg völlig genügt, wenn nur ein verschwindend geringer Bruchteil davon Interesse am Spam-Inhalt zeigt oder gar darin angebotene Waren oder Dienstleistungen ordert. Die von Spammern genutzten Adressen werden von einfach „gestrickten“ Software-Robots (sog. „Harvester“) aus Web-Seiten, Mailinglist-Archiven und Newsgroups gefiltert und in der Regel wiederum durch Spam („100 Millionen Adressen um 100 Dollar“) an den Mann oder die Frau gebracht. Wenn auf dem kommunalen Web-Angebot im Sinne der Bürgernähe die E-Mail-Adressen der Ansprechpartner im Klartext angegeben werden, öffnet das zuallererst dem E-Mail-Spam Tür und Tor. Dabei ist es einfach, die Adressen sammelnden Harvester zu überlisten. Gewöhnlich sind diese nämlich ziemlich „einfältig“ und interpretieren keinen HTML-Code, sondern suchen lediglich nach Zeichenketten, die wie E-Mail-Adressen „aussehen“: Text, evtl. gefolgt von einem Punkt und weiterem Text, gefolgt von „@“, gefolgt von weiterem Text, der von ein, zwei Punkten unterbrochen wird. Eine einfache aber dennoch wirksame „Verschlüsselung“ bewirkt man z.B. dadurch, dass E-Mail-Adressen im HTML-Text als ASCII-Code-Folge notiert werden:

[61] Vgl. *MassageLabs,* Average global ratio of spam in email scanned by MessageLabs (July 2005).
[62] Vgl. *MassageLabs,* Monthly Report: August 2005.
[63] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über unerbetene Werbenachrichten (Spam) KOM(2004) 28 endg., 7.
[64] Vgl. (Deutsches) *Bundesministerium für Wirtschaft und Arbeit,* e-facts, Ausgabe 17 (November 2004) 2.

Statt

post@staedtebund.gv.at

kodiert man gleichbedeutend

<A HREF="mailto:
post@stb.or.at">
post@stb.or.at</A>

Wer zusätzlich das verräterische „mailto:“ maskieren möchte, kann es wie folgt kodieren:

mailto:

Jeder Browser interpretiert eine dreistellig Zahl hinter „&#“ und gefolgt von einem Strichpunkt als ASCII-Code und stellt das diesem entsprechende Zeichen dar. Der menschliche Leser der Web-Seite erhält also dasselbe Ergebnis auf seinem Bildschirm wie bei Verwendung einer nicht-kodierten Adresse, wogegen die meisten Harvester mit der Zeichenfolge nichts anfangen können und die E-Mail-Adresse daher ignorieren[65]. Eine simple, manche Benutzer aber vielleicht überfordernde, jedenfalls aber nicht so elegante Methode besteht darin, die E-Mail-Adresse so zu verändern, dass sie nur mit ein wenig Intelligenz gelesen werden kann: „post AT staedtebund Punkt gv Punkt at“. Etwas aufwendiger aber am sichersten ist es, E-Mail-Adressen oder jedenfalls den darin enthaltenen „Klammeraffen“ als Bild darzustellen und auf den „Mailto:“-Link zu verzichten. Möchte man den Benutzern jedoch den gewohnten Komfort bieten, kann dies mit – relativ geringem – zusätzlichem Aufwand mittels eines Scripts erreicht werden, das auf einen „Mailto:“-URL umleitet: Per Mausklick wird die Adresse in das sich öffnende Mail-Programm übertragen, einem Harvester bleibt sie dagegen verborgen[66].

Ein weiterer Spam-Magnet ist die Verwendung von E-Mail-Adressen in öffentlichen Chat-Rooms und in Newsgroups, aber auch bei der Bestellung von Waren oder der Inanspruchnahme diverser Internet-Dienste, die eine Registrierung erfordern, wie z.B. Web-Communities, Download-Bereiche, Newsletters etc. Daher sollten Mitarbeiter dazu angehalten werden, für die genannten Zwecke keinesfalls ihre „amtliche“ E-Mail-Adresse zu benutzen, sondern sich dafür alternativer Adressen (z.B. von einem der zahlreichen Gratis-E-Mail-Anbieter) oder sog. „Einmaladressen“[67] zu bedienen. Als effiziente „Spam-Bremsen“ fungieren auch Dienste, die dem Benutzer nach einmaliger Anmeldung anzahlmäßig beliebig begrenzbare Umleitungen auf seine Standard-E-Mail-Adresse erlauben, wobei sich die Anzahl jeweils aus der dem Gegenüber mitgeteilten

[65] Wer sich die Mühe des händischen Kodierens der E-Mail-Adressen sparen möchte, kann dafür z.B. folgenden Dienst in Anspruch nehmen: http://www.wbwip.com/wbw/emailencoder.html.

[66] [http://jamesthornton.com/software/redirect-mailto.html].

[67] So kann man z.B. ohne vorherige Anmeldung (!) als Empfänger-Adresse ein frei gewähltes Adress-Präfix gefolgt von „@trash-mail.de“ (etwa staedtebund@trash-mail.de) angeben und darunter eingelangte E-Mails im Web unter <http://www.trash-mail.de/> abrufen.

„Wegwerf-Adresse“ ergibt[68]. In Kombination mit einem Script[69], das bei jedem Anklicken des Kontakt-Links unter Verwendung der jeweiligen Systemzeit eine nur einmal benutzbare „Wegwerf-Adresse“ (worauf natürlich hingewiesen werden sollte) erzeugt, können auf Web-Seiten für Spammer unbrauchbare Kontaktadressen angegeben werden, die aber für Anfragen von Bürgern, denen eventuell in der Antwort für die weitere Kommunikation unbegrenzt (oder z.B. zehnmal) verwendbare Adressen mitgeteilt werden, bestens geeignet sind.

Wer sich vor SMS-Spam schützen möchte, sollte in Web-Formulare auch keine Mobiltelefonnummern eingetragen. Selbst bei der Verwendung von Web-SMS-Diensten ist Vorsicht geboten: Handelt es sich nicht um einen seriösen Dienst, kann in diesem Fall zwar nicht das eigene Handy, wohl aber jenes des SMS-Empfängers zum Spam-Ziel werden.

7.7 ZWECKMÄSSIGE „BEHANDLUNG“ VON SPAM

Das oberste Gebot für den Umgang mit Spam[70] lautet schlicht: „Ignorieren!“ Dass jemand, der mit seinem Geld besseres anzufangen weiß, keine in einer Spam-SMS angegebene („Mehrwert“)Telefonnummer wählen bzw. an diese Nummer eine Antwort-SMS senden darf, hat sich inzwischen herumgesprochen. Aber auch Spam-E-Mails sollten auf keinen Fall beantwortet werden. Die eigentliche Wurzel des Spam-Übels besteht bekanntlich darin, dass ein ausreichender Anteil unbedarfter Empfänger Interesse an den Spam-Angeboten zeigt. Strenge Strafen für derartiges Verhalten wären daher die wirksamste Form, die Spam-Flut mit rechtlichen Mitteln zu bekämpfen. Da dies aus nahe liegenden Gründen nicht opportun ist, müssen die Gesetzgeber- wie unten noch erörtert wird - am weniger greifbaren anderen Ende der „Spam-Kette“ ansetzen. Aber auch von negativen Reaktionen auf Spam ist dringend abzuraten: Der in vielen Spam-E-Mails enthaltene Hinweis, dass man sich auf Wunsch von der Versand-Liste streichen lassen könne, ist meist nur eine List des Spam-Versenders, der herausfinden möchte, welche der von ihm verwendeten Adressen noch „aktiv“ und daher für weitere Spam-Attacken prädestiniert bzw. auf dem Markt für Spam-Adressen besonders wertvoll sind.

Aus dem gleichen Grund sollten keine in Spam-E-Mails enthaltenen Links aufgerufen werden. Sie sind häufig „personalisiert“ und zeigen dem Betreiber der Web-Site, welche E-Mail-Adresse zu diesem „Spam-Erfolg“ beigetragen hat. Besonders zu warnen ist in diesem Zusammenhang vor E-Mails im HTML-Format. Abgesehen davon, dass durch das bloße Aufrufen entsprechend kodierter HTML-Seiten Schadprogramme wie Viren, Würmer, Trojaner etc. auf dem Client-PC eingeschleust werden können, ist „Lazy HTML“ ein beliebtes Spammer-Instrument. Es handelt sich dabei um per E-Mail versandten HTML-Code, der, wenn er auf dem Empfänger-PC inter-

[68] So leitet z.B. der Dienst <www.spamgourmet.com> genau drei E-Mails mit der Adresse <irgendetwas.3.staedtebund@spamgourmet.com> an die vom Benutzer mit der Kennung „Staedtebund“ angegebene E-Mail-Adresse weiter, während er alle folgenden Mails kommentarlos „verschluckt“.

[69] <http://www.meinwebworker.de/index.php?rubrik=knowhow&thema=einwegemail>.

[70] Umfassende Informationen zur Spam-Bekämpfung bietet das kürzlich veröffentlichte Dokument „Antispam-Strategien – Unerwünschte E-Mails erkennen und abwehren“ des deutschen Bundesamtes für Sicherheit in der Informationstechnik: <http://www.bsi.de/literat/studien/antispam/antispam.pdf >.

pretiert wird, über das Internet Elemente nachlädt, um diese gemeinsam mit dem in der E-Mail versandten Inhalt am Bildschirm darzustellen. Das Element muss dabei aber gar nicht sichtbar sein. So kann es sich z.B. um eine Grafik handeln, die aus einem einzigen weißen Pixel auf weißem Grund besteht. Ihr einziger Zweck besteht dann darin, dem Spam-Versender aus dem Umstand, welche (wiederum „personalisierte") Grafik-Datei aufgerufen wurde, eindeutige Rückschlüsse auf die E-Mail-Adresse zu erlauben, die zur Anzeige der Spam-E-Mail führte. Überdies lassen sich auf diese Art und Weise noch Daten darüber gewinnen, wann die Spam-E-Mail angezeigt wurde, welche IP-Adresse dem aufrufenden Client-Rechner zugeordnet ist, welche Browser-Software und welche Betriebssystem-Version darauf laufen etc. Da solche Grafiken ähnliche Aufgaben wie Abhör-Wanzen erfüllen, werden sie als „Web Bugs" bezeichnet[71]. Übrigens ist es für ihr Funktionieren nicht einmal nötig, eine entsprechend präparierte Spam-E-Mail bewusst anzeigen zu lassen. Vielmehr genügt es, dass in der E-Mail-Client-Software die HTML-Vorschau-Funktion aktiviert ist. Aber davon ist schon wegen der damit verbundenen Viren-, Würmer- und Trojaner-Gefahr dringend abzuraten!

Da die immer noch (bei ihren Absendern) beliebten „Out of Office Messages" automatisch jede eingehende E-Mail-Nachricht beantworten und damit weiteren Spam anziehen können, sollte vor ihrer Aktivierung eine „Kosten/Nutzen-Überlegung" angestellt werden. Vielleicht genügt es auch, diesen Dienst so einzustellen, dass nur Teilnehmer des eigenen „Post Office" bzw. der eigenen Domain, aber keine Externen über die voraussichtliche Dauer des Karibikurlaubs informiert werden.

Wer sich mit Don Quixote seelenverwandt oder aus altruistischem Antrieb zur Spam-Bekämpfung berufen fühlt, kann sich darüber beim eigenen Provider oder beim Provider des Spam-Versenders beschweren[72]. Dadurch können z.B. unbedarfte System-Administratoren darauf aufmerksam gemacht werden, dass einer ihrer Server als „Open Relay" oder „Open Proxy" konfiguriert ist und daher für Spam-Zwecke missbraucht wird. Die Beschwerde kann aber auch dazu führen, dass der verantwortliche Provider wegen seines offensichtlichen Verstoßes gegen die „Accaptable Use Policy" den Account des Spammers sperrt. Eine Häufung von Beschwerden bewirkt überdies eine Aufnahme in sog. „Blacklists". Diese enthalten IP-Adressen von Computern, die von Spammern verwendet werden, und ermöglichen es Mail-Server-Betreibern, Internet-Verbindungen mit derartigen IT-Systemen zu verweigern. Auch wenn es dem Spammer nicht allzu schwer fallen wird, seine Aktivitäten unter ständig wechselnden Accounts bei unterschiedlichsten Providern fortzusetzen, erzeugen Beschwerden doch einen gewissen Druck und können dadurch zur Eindämmung des gemeinschaftsschädigenden und daher schändlichen Treibens beitragen.

Zur Vermeidung des Empfangs von Spam wurden von Unternehmen, aber auch von Verwaltungsdienststellen[73] einige Zeit lang „Whitelists" eingesetzt. Dabei verlangt der empfangende Mail-Server von einem ihm bislang unbekannten Absender einer E-Mail eine Bestätigungs-Mail, bevor von derselben Adresse versandte E-Mails zugestellt werden. In der Praxis hat sich das jedoch

[71] Details unter <http://www.eff.org/Privacy/Marketing/web_bug.html>.
[72] Kostenlose Unterstützung bieten Dienste wie SpamCop http://www.spamcop.net/ an, die an Hand übermittelter Spams den zuständigen Provider ermitteln
[73] Z.B. vom deutschen Bundeskriminalamt und von Universitäten.

nicht bewährt. Zum einen misstrauen die Absender automatisch generierten E-Mail-Nachfragen, zumal wenn sie sich auf ihre „Identität“ beziehen. Zum anderen sind unerfahrene Benutzer oft überfordert, wenn sie den Anweisungen in der vom Mail-Server versandten Nachricht folgen sollen. Beides resultiert im Verlust von E-Mails, die nicht als Spam zu klassifizieren und daher zuzustellen gewesen wären.

Am einfachsten und sichersten ist es allemal, offensichtlichen Spam zu löschen. Dies kann „händisch“ oder – effizienter – unter Zuhilfenahme von Filter-Software erfolgen.

7.8 SPAM-FILTER

Nach dem Aschenputtelprinzip versucht Spam-Filter-Software die guten E-Mails „ins Töpfchen“ und die schlechten Spam-Mails „ins Kröpfchen“ bzw. in den elektronischen Orkus zu befördern. Dies erfolgt auf der Grundlage von Regeln und kann beim Provider, am evtl. von der Gemeinde bzw. im Unternehmen betriebenen Mail-Server oder am Mitarbeiter-PC erfolgen. Üblicherweise wird nicht nur nach einzelnen Schlüsselwörtern gesucht, da diese auch in „harmlosen“ E-Mails enthalten sein können, sondern der heuristische Ansatz verfolgt, Spam typische Kombinationen solcher Wörter zu finden und derartige Nachrichten auszusortieren[74]. Zu den bekanntesten und leistungsfähigsten Open-Source-Produkten dieses Genres gehört zweifellos SpamAssassin[75].

Da Provider zu Recht keine Kunden-E-Mails löschen wollen, lassen sie vermutliche Spam-Mails bloß entsprechend markieren (meist durch Einfügen einer Zeile in den „Header“), sodass der Empfänger entscheiden kann, wie weiter damit verfahren werden soll. So kann er seine E-Mail-Client-Software durch die Definition einfacher Regeln z.B. dazu bringen, markierte Mails sofort zu löschen oder in einen besonderen Spam-Ordner zu verschieben, der gelegentlich durchgesehen werden sollte. Letzteres ist gerade im Kontakt mit Bürgerinnen und Bürgern unbedingt anzuraten, da auch der beste heuristische Spam-Filter nicht vor sog. „False Positives“ gefeit ist, also ab und an „ordentliche“ E-Mails als Spam markieren wird, was im Fall einer irrtümlichen Löschung wesentlich gravierendere Folgen nach sich ziehen kann als alle „False Negatives“ zusammen.

Bei Spam-Filter-Software für den PC setzt sich mehr und mehr das „Bayesian Filtering“ durch. Dabei wird mittels des Bayes'schen Theorems auf Basis des Inhalts einer E-Mail die Wahrscheinlichkeit dafür ausgerechnet, dass es sich um Spam handelt[76]. Die Software „lernt“ durch Korrekturen seitens ihres Benutzers ständig dazu, erstellt sich dadurch – anders als heuristische Filter – ihre Liste mit Schlüsselwörtern selbst und passt sich rasch an die besonderen E-Mail-Gewohnheiten des Benutzers an. Daher kommen schon nach relativ kurzer Zeit kaum mehr

[74] Für eine Übersicht siehe *Harris,* Dronwning in Sewage – SPAM, the curse of the new millennium: an overview and white paper (2003), 20 ff. [http://www.internetnz.net.nz/public/committee-reports/ctte-legal-and-regulatory-affairs/larac030820spam-white-paper.pdf].

[75] [http://spamassassin.apache.org/].

[76] Eine detaillierte Erklärung findet sich hier: [http://spambayes.sourceforge.net/background.html].

„False-Positives“ vor[77]. Sehr gute Ergebnisse liefert eine Kombination aus heuristischen Tests mittels vordefinierter Regeln oder Listen beim Provider bzw. auf dem hauseigenen Mail-Server mit nachfolgendem „Bayesian Filtering“ am Benutzer-PC.

Allerdings passen Spammer laufend ihre Taktik an verbesserte Anti-Spam-Prozeduren an. So fügen sie seit kurzem zufällige Wörter in ihre Texte ein, die gewöhnlich nicht für Spam charakteristisch sind. Damit gelingt es ihnen zumindest einige Zeit lang, beim „Bayesian Filtering“ durchzurutschen. Es ist abzusehen, dass es niemals eine „wasserdichte“ technische Lösung geben wird, mit der man die Spam-Flut per Knopfdruck abstellen kann. Realistischer scheint vielmehr die Einschätzung zu sein, dass sowohl technologische als auch rechtliche Mittel nötigt sind, um das Problem auf ein erträgliches Ausmaß zu reduzieren.

7.9 RECHTSLAGE

Für die gesetzliche Regulierung von UBE (= Unsolicited Bulk E-Mail) bzw. UCE (= Unsolicited Commercial E-Mail), wie Spam in englischsprachigen amtlichen Texten häufig genannt wird, gibt es prinzipiell zwei Möglichkeiten: Aufgrund von Opt-In-Regelungen dürfen entsprechende E-Mails nur an Empfänger versandt werden, die zuvor zugestimmt haben, während Opt-Out-Bestimmungen die Zusendung an solche Adressaten erlauben, die sich bisher nicht dagegen ausgesprochen haben.

7.9.1 E-Commerce-Richtlinie

Die E-Commerce-RL[78] und in ihrer Umsetzung das ECG[79] lassen Rechtsvorschriften über die Zulässigkeit und Unzulässigkeit der Übermittlung kommerzieller Kommunikation im Weg der elektronischen Post unberührt. Gem. Spiegelstrich 8 des Anhangs zur E-Commerce-RL bzw. § 21 Z. 8 ECG wird diese Problematik überdies vom Anwendungsbereich des Binnenmarktprinzips ausgenommen. Art. 7 E-Commerce-RL und § 7 ECG sehen lediglich vor, dass zulässigerweise ohne Zustimmung versandte elektronische Post bei ihrem Eingang beim Nutzer klar und unzweideutig als solche erkennbar sein muss. Diese Vorschrift richtet sich jedoch lediglich an den „Diensteanbieter“ i.S.d. ECG[80] und bezieht sich überdies nur auf kommerzielle Kommunikation, sodass sie jedenfalls auf nichtkommerzielle Massen-E-Mails kommunaler Einrichtungen nicht anwendbar ist. Gleiches gilt für die Verbindlichkeit der gem. § 7 Abs. 2 ECG von der RTR-GmbH einzurichtenden (und nur von der E-Commerce-RL so genannten) „Robinsonliste“. Darin können sich Personen und Unternehmen kostenlos eintragen lassen, „die für sich die Zusendung kom-

[77] Bewährt haben sich insbesondere folgende Open-Source-Produkte: SpamBayes [http://spambayes.sourceforge.net/], POPfile [http://popfile.sf.net/] und PASP [http://sourceforge.net/projects/pasp].

[78] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) ABl. Nr. L 178 vom 17.07.2000, 1.

[79] Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt (E-Commerce-Gesetz - ECG) und das Signaturgesetz sowie die Zivilprozessordnung geändert werden, BGBl I Nr. 152/2001.

[80] Vgl. dazu in diesem Heft die Ausführungen von *Andreas Wiebe.*

merzieller Kommunikation im Weg der elektronischen Post ausgeschlossen haben." Die gesetzlich zur Führung dieser Liste verpflichtete RTR-GmbH hält aber – zu Recht – wenig von dieser Einrichtung und mit ihrer diesbezüglichen Einschätzung auch nicht hinter dem Berg. So heißt es in einer ihrer Publikationen[81] wörtlich:

„Aufgrund der bisherigen Erfahrungen kann klar festgehalten werden, dass eine Eintragung Ihrer E-Mail-Adresse in die Liste keinen ausreichenden Schutz vor Spam darstellt und die Anzahl der von Ihnen erhaltenen Spam-Mails sich nicht verringern wird."

Zutreffend wird dies damit begründet, dass die überwiegende Masse an Spam aus dem Ausland von Unternehmen versandt wird, die ihre Identität verschleiern, um einer Rechtsverfolgung zu entgehen. Es steht sogar zu befürchten, dass die in der Liste eingetragenen Adressen für professionelle Spammer besonders interessant erscheinen, da sie für seriöse inländische Werbung nicht erreichbar sind. Wer sich die aktuelle „Robinsonliste" künftige durch eine E-Mail an die Adresse <abrufen@ecg.rtr.at> automatisch zusenden lassen möchte, muss sich dazu lediglich durch ein per Fax zu übermittelndes Antragsformular anmelden.

Wie wenig die RTR-GmbH von der Sinnhaftigkeit dieser gesetzlich vorgesehenen „Anti-Spam-Maßnahme" überzeugt ist, lässt sie schon durch deren wenig ambitionierte Umsetzung erkennen: Die derzeit ca. 1400 regelmäßigen Abrufer erhalten die „Robinsonliste" im Klartext und damit in für weitere Spam-Aktivitäten idealer Form zugesandt. Dass es auch anders geht, zeigt der Interessenverband Deutsches Internet e.V. Seine freiwillig eingerichtete[82] „Robinsonliste"[83] wird interessierten deutschen Direct-Marketing-Unternehmen verschlüsselt übermittelt. Den Abgleich der „Robinsonliste" mit der im ASCII-Code vorliegenden Adressenliste des jeweiligen Unternehmens übernimmt eine ebenfalls mitgeschickte Spezial-Software. Danach ist die Adressenliste um Spam-Verweigerer bereinigt, obwohl wegen der Verschlüsselung kein direkter Zugriff auf die gesamte „Robinsonliste" besteht. Wer allen Warnungen zum Trotz immer noch die Absicht hegt, sich in die österreichische „§ 7 ECG-Liste" eintragen zu lassen (z.B. um als Anwalt mit Umsatz steigernden Abmahnungen gegen inländische Ignoranten vorzugehen), sende dazu eine E-Mail an eintragen@ecg.rtr.at.

7.9.2 TKG

Rechtslage ab 20. August 1999

„Heimstatt" der eigentlichen Anti-Spam-Bestimmungen unserer Rechtsordnung ist das Telekommunikationsgesetz (TKG). In Gestalt des § 101 TKG 1997[84] verfügte Österreich exakte vier Jahre lang (vom 20. 8. 1999 bis zum 19. 8. 2003) über eine der restriktivsten und damit fortschrittlichsten Regelungen zur Spam-Bekämpfung in Europa[85]. Danach bedurfte jede „Zusen-

[81] *RTR-GmbH,* Informationen betreffend unerwünschte Werbung mittels elektronischer Post (Spam) (Juni 2005), 11.

[82] Wegen des mit Blick auf die Rsp. de facto bestehenden Spam-Verbots wurde vom deutschen Gesetzgeber bei der Umsetzung der E-Commerce-RL in das TDG kein diesbezüglicher Umsetzungsbedarf gesehen.

[83] <http://www.erobinson.de/>.

[84] BGBl. I Nr. 100/1997 i.d.F. I Nr. 188/1999.

[85] Zur österr. Rechtslage vor dem In-Kraft-Treten dieser Bestimmung siehe *Blocher,* Gewerblicher Rechtsschutz und Urheberrecht, in *Jahnel*/*Schramm*/*Staudegger (Hrsg.),* Informatikrecht1 (2000) 90 f.

dung einer elektronischen Post als Massensendung oder zu Werbezwecken“ der vorherigen – jederzeit widerruflichen – Zustimmung des Empfängers. In einer im Auftrag der EU-Kommission erstellten und im Februar 2001 (also zu einem Zeitpunkt, zudem Österreich mit Lob aus Brüssel nicht gerade überhäuft wurde) veröffentlichten Studie über Spam und Datenschutz[86] wurde der von Österreich (sowie Dänemark, Finnland, Italien und Deutschland) gewählte Weg des „Opt-in“ als richtig und vorbildlich für eine gesamteuropäische Regelung dargestellt.

Dieser Empfehlung wurde mit Art. 13 der „Datenschutzrichtlinie für elektronische Kommunikation“[87] (DSRLeK) Folge geleistet, wonach die Mitgliedstaaten unerwünschte Werbung per E-Mail an natürliche Personen untersagen müssen, sofern nicht der Teilnehmer zuvor seine Zustimmung erteilt hat. Lediglich wer im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung von seinem Kunden dessen E-Mail-Adresse erhalten hat, darf diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, wenn der Kunde weder seinerzeit noch in der Folge eine derartige Nutzung seiner E-Mail-Adresse abgelehnt hat. Man kann diese Lösung daher als Mischung von „Opt-in“- und „Opt-out“-System oder – wohl treffender – als abgeschwächtes „Opt-in“-System zum Schutz natürlicher Personen bezeichnen.

Rechtslage ab 20. August 2003

Bis heute ist unklar, welcher Teufel den österreichischen Gesetzgeber ritt[88], die Umsetzung der DSRLeK zum Anlass zu nehmen, von seiner strikten „Opt-in“-Bestimmung wieder abzugehen! § 107 des seit 20. August 2003 in Kraft befindlichen TKG 2003 schießt zwar einerseits und wohl überflüssigerweise über die Vorgabe der DSRLeK hinaus, indem er nicht nur „Zusendungen zu Zwecken der Direktwerbung“ sondern auch „an mehr als 50 Empfänger“ gerichtete Sendungen ohne vorherige Einwilligung des Empfängers verbietet. Andererseits werden nicht sämtliche natürlichen Personen sondern „nur Verbraucher im Sinne des § 1 Abs. 1 Z. 2 Konsumentenschutzgesetz“ geschützt und damit die Richtlinienziele nicht vollständig erreicht[89]. Auch die Anordnung des Art. 13 Abs. 5 DSRLeK, wonach die Mitgliedstaaten dafür Sorge zu tragen haben, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf unerbetene Nachrichten ausreichend geschützt werden, verhallte – abgesehen von der schon durch die E-Commerce-RL vorgesehenen und wenig effektiven „elektronischen Robinsonliste“ – zunächst vom österreichischen Gesetzgeber ungehört. Der richtlinienwidrige nationale Alleingang lässt sich auch kaum rational begründen. Gerade bei Unternehmern bewirkt die Spam-Flut durch Pro-

[86] Unsolicited Commercial Communications and Data Protection (Internal Market DG - Contract n° ETD/99/B5-3000/E/96) [http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/spamstudy_en.pdf].

[87] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002.

[88] „Gewöhnlich gut informierte Kreise“ vermuten, dass sich die Lobbyisten des Fachverbands Werbung und Marktkommunikation der Wirtschaftskammer im Gesetzgebungsverfahren durchsetzten (vgl. ARGE Daten-Newsletter vom 28.06.2005).

[89] Vgl. *Mosing*/*Otto,* Spamming neu! MR 2003, 267; Burgstaller, E-Mail-Werbung zu Zwecken der Direktwerbung – Auch im B2B-Bereich vorherige Zustimmung notwendig? ecolex 2004, 905; *Kraft,* Unzureichender Unternehmerschutz gegen unerbetene Werbemails, ecolex 2004, 907; Fraiss, Das österreichische Spam-Verbot 2003 – Ein (gemeinschafts)rechtlich bedenkliches Kuriosum, RdW 2004/5; Stomper, Folgen der richtlinienwidrigen Umsetzung des Spam-Verbots – Was Disclaimer in Spam-Mails (nicht) bringen, MR 2005, 267.

duktivitätsverluste massive Schäden. Allerdings kommt – wie das HG Wien[90] bereits zutreffend feststellte - zwar ein Vertragsverletzungsverfahren sowie allenfalls eine Staatshaftung für legislatives Unrecht, nicht aber eine horizontale Drittwirkung der DSRLeK in Betracht, da diese zwar hinreichend bestimmt ist, aber dem Einzelnen nicht nur Rechte verleiht, sondern ihn (als Absender der E-Mails) teils auch belastet.

Zu allem Überfluss ist die Verweisung auf § 1 KSchG denkbar unglücklich: Dessen Verbraucherbegriff ist funktionaler bzw. dynamischer Natur, da er als „Verbraucher" eine Person definiert, für welche ein konkretes Geschäft, an welchem sie beteiligt ist, nicht zum Betrieb ihres Unternehmens gehört. Nun haben aber werbefreie Massen-E-Mails mit solchen Geschäften gar nichts am Hut, und sogar Direct-Marketing-E-Mails wollen geschäftliche Beziehungen in der Regel erst anbahnen, sodass noch kein konkretes Rechtsgeschäft als Beurteilungsmaßstab existiert. Damit die missglückte Bestimmung nicht den Großteil des intendierten Anwendungsbereichs verliert, wird man sie wohl so zu verstehen haben, dass der jeweilige Inhalt der Werbe- oder Massen-E-Mail als Richtschnur gilt: Berührt er die Unternehmersphäre des Empfängers, gilt dieser als Unternehmer, andernfalls als „Verbraucher" i.S.d. § 107 TKG. So betrifft einer instanzgerichtlichen Entscheidung des HG Wien[91] zu Folge das an eine Rechtsanwaltskanzlei gerichtete Angebot zur Schaltung von Stelleninseraten die unternehmerische Tätigkeit und ist – bei Vorliegen der weiteren Voraussetzungen des § 107 Abs. 4 und 5 TKG – zulässig[92]. Gem. § 1 Abs. 2, letzter Satz KSchG gelten juristische Personen des öffentlichen Rechts immer als Unternehmer. Daraus ist aber nicht abzuleiten, dass an sie gerichtete Massen- oder Werbe-E-Mails keinesfalls der vorherigen Zustimmung bedürfen. Zumeist werden E-Mails nämlich nicht an allgemeine Adressen des „Unternehmers", wie etwa <post@m48.magwien.gv.at>, sondern an einzelne Mitarbeiter, also z.B. an <franz.maier@m48.magwien.gv.at>, geschickt. Dann ist weiters zu entscheiden, ob der Inhalt der E-Mail die Sphäre des „Unternehmers" oder die persönliche Sphäre des Mitarbeiters betrifft[93]. Erhält eine Rathausmitarbeiterin per E-Mail an ihre Dienstadresse Ferienreisen angeboten, ist im Zweifel die Verbrauchersphäre betroffen.

Die alles andere als leicht zu handhabende und noch bis zum 28. Februar 2006 geltende österreichische Anti-Spam-Regelung kann vereinfachend wie folgt zusammengefasst werden:

- E-Mails und SMS, welche die Verbrauchersphäre des Empfängers betreffen, sind ohne dessen vorherige Einwilligung unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt oder sich an mehr als 50 Empfänger richtet.

- Eine Zustimmung ist nicht erforderlich, wenn der Absender die Adresse im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und die nunmehrige

[90] GZ 1 R 33/05g vom 08.04.2005.
[91] MR 2005, 269.
[92] Verfehlt war die E. des BGHS Wien (1 C 1050/03y vom 30.06.2004), wonach das von einem Reiseveranstalter an eine Rechtsanwaltskanzlei gerichtete Angebot zur Durchführung von Veranstaltungen wie Weihnachtsfeiern den Empfänger als Verbraucher anspreche, da dies nicht zum gewöhnlichen und typischen Betrieb einer Kanzlei gehöre. Der Unternehmerbegriff des § 1 KSchG begnügt sich schlicht damit, dass das Geschäft „zum Betrieb" des Unternehmens gehört.
[93] In (Ausnahme-)Fällen, in denen der Mitarbeiter nebenbei auch selbst unternehmerisch tätig ist, muss wohl wiederum zwischen dessen Unternehmer- und Verbrauchersphäre unterschieden werden.

Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und der Kunde überdies klar und deutlich die Möglichkeit erhalten hat, derartige Zusendungen von vornherein und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen.

- Die Unternehmersphäre betreffende Zusendungen sind zulässig, wenn sich der Empfänger nicht gegen weitere Zusendungen ausgesprochen hat und wenn der Versender dem Empfänger in der E-Mail oder in der SMS ausdrücklich die Möglichkeit einräumt, den Empfang weiterer Nachrichten abzulehnen.

- Beim Versand nicht zustimmungsbedürftiger kommerzieller E-Mails haben Diensteanbieter i.S.d. § 3 Z. 2 ECG die „elektronische Robinsonliste" gem. § 7 ECG zu beachten. Derartige E-Mails müssen überdies bei ihrem Empfang klar und deutlich als solche erkennbar sein.

- Unzulässig sind Direktwerbe-Sendungen jedenfalls dann, wenn die Identität des Absenders verschleiert oder verheimlicht wird oder wenn keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

Um damit nicht einen gegenteiligen Effekt zu bewirken, sollte aus den schon genannten Gründen von der gesetzlich vorgeschriebenen Möglichkeit, den Empfang weiterer Nachrichten abzulehnen, freilich nur dann Gebrauch gemacht werden, wenn die Sendung von einem als seriös bekannten Unternehmer stammt.

Rechtslage ab 1. März 2006

Das von den zahlreichen Kritikern der eigenwilligen „2. Auflage" der österreichischen Anti-Spam-Regelung erwartete Vertragsverletzungsverfahren ließ nicht allzu lange auf sich warten: Am 16.März 2005 stellte die Europäische Kommission fest, dass Österreich mit § 107 TKG 2003 gegen die DSRLeK verstoße, weil durch die Unterscheidung zwischen Verbrauchern und Business-Empfängern die Reichweite des Spam-Verbots gegenüber dem EU-Recht unzulässig eingeschränkt werde.

Am 28. September 2005 brachten die Regierungsparteien im Nationalrat einen Initiativantrag für eine Novelle des TKG 2003 ein, mit dem insb. § 107 „repariert" werden sollte. Die Beschlussfassung im Nationalrat erfolgte bereits am 19. Oktober 2005 mit den Stimmen sämtlicher im Parlament vertretener Parteien. Das Vertragsverletzungsverfahren gegen Österreich wurde daraufhin von der Kommission im Dezember 2005 eingestellt[94].

Die am 1. März 2006 in Kraft tretende Novellierung des § 107 TKG 2003 besteht im Wesentlichen in der Streichung des bisher in Abs. 4 verankerten „Opt-out"-Prinzips für Unternehmer, sodass diese nun den gleichen Schutz vor Spam genießen wie Verbraucher[95]. In der Abs. 3 hinzugefügten Z. 4 wird nun ausdrücklich auf die Liste gem. § 7 ECG verwiesen.

[94] IP/05/1585 vom 14.12.2005.

[95] Dass sich Bundesrat *Günter Molzbichler* ausweislich des Sten. Prot. zur 727. Sitzung des Bundesrates, S. 78, darüber freut, dass dieses Gesetz „vor allem für die Konsumentinnen und Konsumenten in Österreich eine Verbesserung" bedeutet, ist weder im Hinblick auf den Text der Novelle noch auf deren Intention nachvollziehbar.

Das Zusenden unverlangter elektronischer Post ist daher künftig in Österreich für Erstkontakte wieder generell unzulässig. Lediglich im Rahmen des „Customer Relationship Managements" (CRM) darf jene Kontaktinformation, die der Absender im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat, zu Zwecken der Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwendet werden. Auch im „B2B-Verhältnis" kommt es also nicht mehr darauf an, ob die Werbung die Unternehmersphäre betrifft. Vielmehr darf auch hier unverlangt nur mehr in Folge einer bereits bestehenden Geschäftsbeziehung und auch dann nur unter Verwendung der für die jeweilige Produkt- oder Dienstleistungsart „einschlägige(n)" (weil im Zusammenhang mit früheren derartigen Geschäften erhaltenen) Adresse(n) geworben werden. Selbst dies ist unzulässig, wenn sich der Empfänger beim konkreten Geschäftskontakt bzw. in der Folge gegen eine derartige Verwendung der Kontaktinformation ausgesprochen hat oder seine E-Mail-Adresse in die „elektronische Robinsonliste" gem. § 7 ECG eintragen ließ.

Ärgerlicherweise wird der klare Wortlaut der TKG-Novelle 2005 durch die dem Initiativantrag beigefügten Erläuterungen[96] wie folgt konterkariert:

„Unternehmen sind überwiegend an verhältnismäßiger Kontaktaufnahme durch Geschäftspartner im jeweiligen Geschäftsbereich interessiert. Daher ist sicherzustellen, dass der Erstkontakt zwischen Unternehmen im Wege des elektronischen Geschäftsverkehrs im jeweiligen Geschäftsbereich nicht verunmöglicht oder unverhältnismäßig eingeschränkt wird. Das Interesse eines Unternehmens, im jeweiligen Geschäftsbereich in verhältnismäßiger Art und Weise kontaktiert zu werden, wird insbesondere durch die willentliche Veröffentlichung eigener Kontaktinformationen auf Websites oder in anderer öffentlich zugänglicher Form bekundet. Daher ist anzunehmen, dass ein Unternehmen, welches seine eigenen Kontaktinformationen willentlich auf seiner Website oder in anderer öffentlich zugänglicher Form veröffentlicht, durch diese Veröffentlichung eine Einwilligung im Sinne des § 107 Abs. 2 TKG 2003 zur Zusendung elektronischer Post in seinem jeweiligen Geschäftsbereich erteilt.

Ebenso kann die Einwilligung im Sinne des § 107 Abs. 2 TKG 2003 durch die Mitgliedschaft in einem Verein oder einer politischen Partei als gegeben angesehen werden."

In dieses Bild passt, dass sich mit der NR-Abgeordneten Karin Hakl immerhin eine der Proponentinnen des Initiativantrags in der Debatte vor dessen 3. Lesung bemüßigt fühlte, zuzugeben, dass sie die Änderung des § 107 TKG „bis zu einem gewissen Grad bedauere", was sie u.a. damit begründete, dass diese „dem österreichischen und dem europäischen Wirtschaftswachstum im Verhältnis nicht gut" täten[97]. Mit dem gewagten Auslegungsvorschlag der Erläuterungen wurde versucht, den Werbetreibenden das wieder zu ermöglichen, was der Wortlaut der Novelle mit dem Ziel einer Beendigung des Vertragsverletzungsverfahrens gerade abstellen sollte.
Dieser gesetzgeberische Taschenspielertrick war aber schon dem Verkehrsausschuss[98] zu weit gegangen, der immerhin feststellte, dass

[96] 711/A XXII. GP, 4 f.
[97] Sten. Prot., 125. Sitzung, XXII GP, 220.
[98] 1127 der Beil. XXII. GP, 3 f.

„eine Veröffentlichung der Kontaktinformationen auf Grund einer gesetzlichen Verpflichtung, z.B. im Impressum einer Website, nicht als Zustimmung angesehen werden kann, da sie in diesem Zusammenhang offensichtlich nicht als Einwilligung zum Empfang von Nachrichten im jeweiligen Geschäftsbereich gewertet werden kann."

Auch die unglückliche Formulierung der Erläuterungen, welche Vereins- und Parteimitglieder zu schutzlosen Spam-Opfern erklärte, wurde vom Verkehrsausschuss insofern relativiert, als „die Erläuterungen zu Z. 5 des Entwurfes dahingehend zu verstehen sind, dass ein Schutzbedürfnis des Empfängers auch dann nicht anzunehmen sein wird, wenn das Senden der Nachricht auf einer anderen als einer geschäftlichen Rechtsbeziehung zwischen Absender und Empfänger, z. B. auf Grund einer Mitgliedschaft in einem Verein oder in einer politischen Partei, erfolgt."

M.E. lässt eine richtlinienkonforme Interpretation der novellierten Fassung des § 107 TKG 2003 – zumal vor dem Hintergrund des damit abgewendeten Vertragsverletzungsverfahrens – keinerlei Raum für eine neuerliche Benachteiligung Spam-geplagter Unternehmer. Zwar hat sich jüngst auch der OGH[99] der im Schrifttum mehrheitlich vertretenen Meinung angeschlossen, wonach hinsichtlich der Zustimmungserklärung für den Empfang von Werbung keine besonderen Formerfordernisse bestehen, sodass sich eine Zustimmung auch aus AGB ergeben könne. Selbst gegen die Möglichkeit einer schlüssigen Einwilligung scheint nichts zu sprechen, allerdings ist dafür gem. § 863 Abs. 1 ABGB zu fordern, dass die entsprechenden Handlungen mit Überlegung aller Umstände keinen vernünftigen Grund, daran zu zweifeln, übrig lassen. Und dass ein Unternehmer, auch wenn er es „willentlich" und nicht nur in Befolgung einer gesetzlichen Verpflichtung tut, mit der Veröffentlichung einer E-Mail-Adresse eine Einladung an Spammer aussprechen möchte, darf mit Fug und Recht bezweifelt werden.

Aus dem gleichen Grund bringt die TKG-Novelle 2005 für Direktwerber, die Werbeaussendungen, Newsletter etc. bisher mit der Opt-Out-Regel des ab 1. März 2006 ersatzlos gestrichenen § 107 Abs. 4 TKG rechtfertigen konnten, die Notwendigkeit einer intensiven Reduktion bzw. Überarbeitung ihrer Adressendatenbank mit sich. Aus der Tatsache alleine, dass ein bisher zulässigerweise beworbener Unternehmer nicht von der Möglichkeit Gebrauch machte, den Empfang weiterer Nachrichten abzulehnen, kann nicht auf seine künftig erforderliche Zustimmung geschlossen werden. So kann ein Grund dafür darin liegen, dass – ebenso wie auch oben, im Abschnitt „Zweckmäßige Behandlung von Spam" – in der Literatur zumeist selbst von negativen Reaktionen auf Spam abgeraten wird. Überdies spricht auch die Systematik des § 107 TKG 2003 gegen die Annahme einer konkludenten Einwilligung: Für die Zulässigkeit der Zusendung elektronischer Post unterscheidet die Bestimmung penibel zwischen der Möglichkeit der vorherigen Einwilligung (Abs. 2) und jenen Umständen, unter denen eine vorherige Zustimmung nicht notwendig ist (Abs. 3). Für letztere wird als unabdingbare Voraussetzung gefordert, dass „der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen". Der Gesetzgeber sieht offensichtlich gerade keine Zustimmung darin, wenn der Emp-

[99] 1 Ob 104/05h vom 02.08.2005 zum diesbezüglich wortgleichen § 101 TKG 1997.

fänger die Nutzung seiner E-Mail-Adresse bisher nicht abgelehnt hat. Auch den Weg, eine derartige Zustimmung zu fingieren, hat er nicht gewählt. Unter den genannten Bedingungen ist eine Zustimmung bloß „nicht notwendig". Es sind keine Anhaltspunkte dafür ersichtlich, den bisher durch einen Unternehmer gem. dem insofern ganz ähnlich konstruierten und ab 1. März 2006 obsoleten Abs. 4 nicht abgelehnten Empfang weiterer Nachrichten anders zu werten.

Einen pragmatischen Ansatz scheinen der Initiatoren der TKG-Novelle 2005 mit der folgenden Erläuterung zu verfolgen:

„Sofern nach der bisherigen Rechtslage die Kontaktinformation des Teilnehmers rechtmäßig, jedoch ohne die (damals noch nicht erforderliche) Möglichkeit der kostenfreien Ablehnung schon bei der Erhebung der Kontaktinformation ermittelt wurde, ist – ungeachtet des § 107 Abs. 3 Z 3 – die Zusendung elektronischer Post dennoch zulässig, wenn die sonstigen Voraussetzungen des § 107 Abs. 3 erfüllt sind."

Eine derartige Übergangsregelung könnte jenen Unternehmern helfen, die nach der bis zum 28. Februar 2006 geltenden Rechtslage zulässigerweise bei bestehenden Kundenbeziehungen im B2B-Verhältnis die seinerzeit anlässlich eines Verkaufs oder der Erbringung einer Dienstleistung erhobenen Kontaktinformationen für Direktwerbung nutzen, obwohl sie – anders als ab 1. März 2006 erforderlich – den Kunden bei der Datenerhebung keine „Opt-Out"-Möglichkeit anboten. Allerdings hätte die Regelung dazu in den novellierten Gesetzestext und nicht bloß in die Erläuterungen aufgenommen werden müssen. Da der Wortlaut des neu gefassten § 107 Abs. 3 TKG 2003 eine derartige Ausnahme auch bei extensiver Interpretation nicht „hergibt", wird auch dieser (halbherzige) Wunsch der Initiativantragsverfasser von der Praxis unberücksichtigt bleiben müssen.

Zur abschließenden Bewertung der in unauflöslichem Widerspruch zum Wortlaut und zur „richtlinienkonformen" Intention des § 107 TKG i.d.F. der Novelle 2005 stehenden Erläuterungen zum Initiativantrag sei nochmals aus dem Stenographischen Protokoll[100] zitiert:

„Die Ausweitungen durch die Erläuterungen werden nicht funktionieren. Sie gehen über die Gesetzesmaterie hinaus und werden in dieser Form in der Praxis nicht möglich sein."

7.9.3 StGB

So manchem Spammer unbekannt ist vermutlich die Tatsache, dass krasse Spam-Attacken auch gerichtlich strafbar sein können: Gem. § 126b StGB drohen demjenigen bis zu sechs Monate Freiheitsstrafe, der „die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt"[101]. Diese Bestimmung ist u.U. auch dann einschlägig, wenn jemand z.B. die Mailbox eines missliebigen Politikers „bombardiert" und damit den empfangenden Mail-Server zum Absturz bringt.

[100] Abgeordneter *Kai Jan Krainer,* Sten. Prot., 125. Sitzung, XXII GP, 219.

[101] Vgl. *Jaschke,* „Frühstück ohne SPAM": Fortschritte im Kampf gegen unerwünschte E-Mail-Werbung Zugleich eine Anmerkung zum Urteil des deutschen BGH vom 11. 3. 2004, ÖJZ 2005, 26.

7.9.4 Privatrechtliche Anti-Spam-Vereinbarungen

Als mindestens so effektiv wie die eben dargestellten Bestimmungen erweisen sich in jüngster Zeit auch privatrechtliche Vereinbarungen zur Spam-Bekämpfung. So wurde von der Vereinigung der österreichischen Internet-Service-Provider (ISPA) ein entsprechender „Code of Conduct“[102] beschlossen, wonach ISPs gegen aktive Spammer in ihrem jeweiligen Netzbereich (auch durch Open Relays und Open Proxys) vorzugehen haben.

Dabei ist zunächst das gelindeste Mittel, nämlich in der Regel eine Aufforderung an den Kunden, sein Treiben sofort einzustellen bzw. die Fehl-Konfiguration des Servers zu korrigiern, zu wählen. Wenn dies nicht fruchtet bzw. bei Gefahr im Verzug hat der ISP zunächst den verwendeten Port, dann den Mail-Transport-Agent, schließlich die IP-Adresse oder gar den gesamten Adressraum des spammenden Kunden zu sperren.

Wesentlich für die Effektivität dieses „Code of Conduct“ ist nicht zuletzt der Umstand, dass damit nicht auf die Rechtswidrigkeit der Spam-Aktivität abgestellt, sondern jede Form von UBE und UCE geahndet wird. Die ISPs sind freilich gut beraten, wenn sie die im „Code of Conduct“ vorgesehenen Maßnahmen per AGBs mit ihren Kunden vereinbaren, um nicht vertragsbrüchig und damit schadenersatzpflichtig zu werden.

7.10 RECHTSDURCHSETZUNG

Wie schon ausgeführt, besteht die effizienteste Behandlung von Spam-E-Mails darin, diese einfach zu löschen. Wer dennoch und über eine eventuelle Beschwerde bei den Providern hinaus aktiv zu Bekämpfung dieser Plage beitragen möchte, hat dazu auf Grund der eben dargestellten Rechtslage folgende Möglichkeiten:

7.10.1 Anzeige

Gem. § 109 Abs. 3 Z. 20 und 21[103] TKG ist eine Verletzung der in § 107 Abs. 2, 4[104] und 5 geregelten Spam-Verbote als Verwaltungsübertretung zu ahnden und mit einer Geldstrafe bis zu 37.000,– Euro zu bestrafen. Zuständige Behörden I. Instanz sind die in Wien, Graz, Linz und Innsbruck eingerichteten Fernmeldebüros bzw. – im Fall der Spam-Werbung für bestimmte Finanzmarktinstrumente – die FMA.

Dem Vernehmen nach haben sich diese Behörden wegen der offenbaren Aussichtslosigkeit des Unterfangens schon nach der früheren Rechtslage (§ 101 TKG 1997) geweigert, gegen aus dem Ausland agierende Spammer vorzugehen. Nun fühlen sie sich wegen der etwas unglücklichen Regelung des § 107 Abs. 6 TKG 2003 in der bis 28. Februar 2006 geltenden Fassung in ihrer Ansicht gestärkt. Sie sieht ausdrücklich nur für unerlaubte Telefon- bzw. Fax-Anrufe vor, dass

[102] „Verhaltensrichtlinie für ISP für die Behandlung von Spam“ vom 03.12.2003.
[103] Diese Ziffer entfällt gem. der TKG-Nov. 2005 ab 01.03.2006.
[104] Dieser Absatz und damit auch der zitierte Verweis entfallen gem. der TKG-Nov. 2005 ab 01.03.2006.

nicht im Inland begangene Verwaltungsübertretungen als an jenem Ort begangen gelten, an dem der Anruf den Anschluss des Teilnehmers erreicht. Daraus den Umkehrschluss zu ziehen, „dass E-Mails und SMS, die aus dem Ausland gesandt werden, straffrei bleiben“[105], ist m.E. aber nicht haltbar. Gem. § 2 VStG ist nämlich eine Übertretung schon dann „im Inland begangen“ (und daher die Fiktion des § 107 Abs. 6 entbehrlich), wenn der zum Tatbestand gehörende Erfolg im Inland eingetreten ist. Letzteres wird bei im Inland zugestellten bzw. abrufbaren Spam-Sendungen – trotz dabei insbesondere wegen des globalen Zugriffs gewiss diskutierbarer Einzelfragen – nicht ohne weiteres von der Hand zu weisen sein. Die TKG-Novelle 2005 nimmt den zuständigen Behörden ab 1. März 2006 dadurch die Möglichkeit, ihre Untätigkeit bei aus dem Ausland stammenden Spam-Sendungen mit der unklaren Rechtslage zu begründen, dass sie die Fiktion des § 107 Abs. 6 ausdrücklich auf unerlaubte elektronische Post erstreckt. Freilich bleiben die Erfolgsaussichten in solchen Fällen gering, da zum einen der ausländische Spam-Absender meist nicht eindeutig identifizierbar sein wird und zum anderen selbst bekannte Täter mangels zwischenstaatlicher Amts- und Rechtshilfeabkommen in der Regel nicht grenzüberschreitend verfolgt werden können.

Wie schon dargestellt, ist in extremen Spam-Fällen sogar eine Strafbarkeit gem. § 126b StGB nicht ausgeschlossen, sodass auch eine Anzeige bei der Polizei in Betracht kommt.

7.10.2 Unterlassungsklage

Konkurrenten eines mit verbotener Direktwerbung agierenden Unternehmers können ihre Unterlassungsklage auf § 1 UWG stützen. Nach ständiger Rechtsprechung handelt sittenwidrig, wer sich durch planmäßigen Rechtsbruch einen Wettbewerbsvorsprung vor gesetzestreuen Mitbewerbern verschafft[106].

Aber selbst dem in keinerlei Wettbewerbsverhältnis zum Absender stehenden Spam-Empfänger hat der OGH eine Tür zur Unterlassungsklage geöffnet: In einer Entscheidung[107] zur Stammfassung des § 101 TKG 1997, die m.E. vollinhaltlich auf § 107 TKG 2003 übertragbar ist, stellte er fest, dass die Bestimmung zwar zweifellos zum öffentlichen Recht zähle, dass sie aber dennoch ein subjektives Recht des verbotenerweise Beworbenen begründe, dieses Verhalten zu untersagen und daher auf Unterlassung bzw. gegebenenfalls auch auf Schadenersatz zu klagen[108].

Ein Spam-Opfer sollte sich jedoch gut überlegen, ob auch eine individuelle „Kosten/Nutzen-Analyse“ ein gerichtliches Vorgehen gegen den Täter rechtfertigt. Abgesehen vom Prozessrisiko ist jedenfalls mit nicht zu unterschätzendem Zeitaufwand zu rechnen, sodass selbst bei von anwaltlicher Seite angebotener kostenloser Rechtsverfolgung Vorsicht geboten ist. Zum „Geschäft“

[105] So nunmehr sogar die *RTR-GmbH* in *dieselbe,* Informationen betreffend unerwünschte Werbung mittels elektronischer Post (Spam) (Juni 2005), 10.
[106] E Vgl. *Handig,* Ist unerbetene E-Mail-Werbung sittenwidrig? ecolex 2003, 425.
[107] ÖBl 1999, 248 = ecolex 1999/271 = JBl 1999, 809.
[108] Unter bestimmten, hier nicht näher zu erörternden Umständen könnte ein Spam-Empfänger seine Unterlassungsklage auch auf die §§ 16 bzw. 354 ABGB stützen (vgl. zur Telefax- bzw. Telefonwerbung z.B. die Entscheidung OGH, MR 1998, 31).

wird die Spam-Bekämpfung nämlich allenfalls für Rechtsanwälte, die insbesondere durch kostenpflichtige Abmahnungen auf Umsatzsteigerungen hoffen dürfen. Manche von ihnen sollen zur „Belebung“ dieses Geschäftszweigs gar in der „Robinsonliste“ lauern und studentische Mitarbeiter damit beschäftigen, die dort registrierten E-Mail-Adressen zur Optimierung des Spam-Aufkommens möglichst flächendeckend im Internet zu verbreiten.

7.10.3 Verbandsklage

Auch für die Spam-geplagte Allgemeinheit Erfolg versprechend erscheint dagegen ein jüngst in Deutschland entwickeltes Modell zur Bekämpfung des Werbemülls: Dort haben sich der Verbraucherzentrale Bundesverband (vzbv), die Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ) sowie der Verband der deutschen Internetwirtschaft (eco) zu einem „Aktionsbündnis zur Bekämpfung von Spam“ zusammengeschlossen. Auf Initiative des Bundesverbraucherministeriums bündeln die drei Verbände ihre technische Expertise und ihre rechtlichen Befugnisse. Der eco-Verband soll dabei für die Ermittlung der gewerblichen Spammer samt ladungsfähiger Anschrift sorgen, sodass der Verbraucherzentrale Bundesverband und die Wettbewerbszentrale anschließend mit Hilfe von Verbandsklagen gegen Spam-Versender und deren Auftraggeber vorgehen können[109].

[109] Pressemitteilung vom 22.09.2005 <http://www.vzbv.de/go/presse/608/>.

BISHER ERSCHIENENE PUBLIKATIONEN IN DER SCHRIFTENREIHE DES ÖSTERREICHISCHEN STÄDTEBUNDES

1. 2003 **Bundesvergabegesetz 2002**
Claus Casati, Michael Holoubek

2. 2003 **Leitfaden zum Fundwesen**

3. 2003 **E-Government – Chance für Österreichs Städte und Gemeinden**
Elisabeth Dearing, Bernhard Krabina, Alexander Maimer, Otmar Pilgerstorfer, Thomas Prorok, Ronald Sallmann

4. 2003 **Statuten des Österreichischen Städtebundes**

1. 2004 **Leitfaden zu den Europäischen Wettbewerbsregeln für staatliche Beihilfen**
Renate Schohaj

2. 2004 **Open Source Software – Einsatz in der öffentlichen Verwaltung**
Emil Georgiev, Gottfried Haber, Julia Reifensteiner, Ronald Sallmann

1.2005 **Der Österreich-Konvent aus Sicht des Österreichischen Städtebundes**
Mag. Ulrike Huemer

2.2005 **Daseinsvorsorge – Dienstlesitungen von allgemeinem Interesse**
Mag. Renate Schohaj
Mag. Angelika Koman (D.A.E.S. Brügge)

3.2005 **Facility Management – ein Leitfaden für die Praxis**
Mag. Alexander Maimer, Mag. (FH) Markus Hödl,
Dr. Helmut Schuchter, Univ.-Prof. Dr. Christian Nowotny

ueber:reuter the new art of printing

für manche zu nah an der realität. www.ueberreuter.com

ISBN: 3-9502038-3-4

Österreichischer Städtebund
1082 Wien, Rathaus
Telefon: 01/4000-89980
Telefax: 01/4000-7135
E-Mail: post@staedtebund.gv.at
Internet: http://www.staedtebund.gv.at