INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

manu:script

Gläserne Bürger – transparenter Staat?

Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft

Peter Parycek

ÖAW
Österreichische Akademie der Wissenschaften

Wien, Mai/2007
ITA-07-04
ISSN 1681-9187

http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_04.pdf

Mai/2007
(ITA-07-04)

Gläserne Bürger – transparenter Staat?

Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft

Peter Parycek

Donau-Universität Krems − Zentrum für E-Government

Keywords

E-Government, Datenschutz, Informationsfreiheit, Register, Personenkennzeichen

Abstract

Der Umgang des öffentlichen Sektors mit seinen umfangreichen Informationssammlungen und oft sensiblen Daten ist entscheidend für moderne Verwaltung und rechtsstaatliche Demokratie. E-Government bedeutet ja Verknüpfung von Daten, Austausch von Informationen und im Stadium der E-Partizipation auch politischer Überzeugungen. Vernetzte E-Register und Informationsverbundsysteme etablieren sich heute in allen staatlichen Bereichen und stellen hohe Anforderungen an den Datenschutz. Zwar existieren bereits komplexe Regelungen wie etwa bereichspezifische Personenkennzeichen, doch wie sind diese mit kundenfreundlichem One-Stop-Government und der Amtshilfe zu vereinbaren? Hier sind laufende Kontrollen durch unabhängige Einrichtungen, effektiver Rechtsschutz und Nachvollziehbarkeit essentiell. E-Government kann und soll dem Individuum Zugang zu seinen eigenen Daten eröffnen – der Staat muss den Rahmen setzen, damit Bürgerinnen und Bürger ihr informationelles Selbstbestimmungsrecht wahrnehmen können. Ein verfassungsrechtlich gewährleisteter Informationszugang kann zugleich das Vertrauen in den Staat fördern und die Zivilgesellschaft stärken. Denn ein frühzeitiges elektronisches Transparenzgebot sowohl in der 'öffentlichen' Verwaltung als auch in der Gesetzgebung – wie es derzeit nur vereinzelt v. a. im Umwelt- und Raumplanungsbereich besteht – stärkt die demokratische Kontrolle, diskursive Meinungsbildung und mündige Bürgerbeteiligung, festigt die Legitimität und letztlich auch Akzeptanz von Entscheidungen. Dieser aktivierende E-Staat erfordert ein Zusammenspiel von Recht, Technik und Bewusstseinsbildung von Bevölkerung, öffentlichen Bediensteten und Verantwortlichen. Gerade jetzt bieten innovative E-Government-Projekte die Chance, neue IT-Systeme auf ein modernes Informationsrecht mit datenschutzgerechter Transparenz auszurichten.

Inhalt

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
http://www.oeaw.ac.at/ita

Die ITA-manu:scripts erscheinen unregelmäßig und dienen der Veröffentlichung von Arbeitspapieren und Vorträgen von Institutsangehörigen und Gästen.
Die manu:scripts werden ausschließlich über das Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
http://epub.oeaw.ac.at/ita/ita-manuscript

ITA-manuscript Nr.: ITA-07-04 (Mai/2007)
ISSN-online: 1818-6556
http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_04.pdf

1 Digitalisierungstendenzen

Die öffentliche Verwaltung verfügt über die umfangreichsten und vielfältigsten Wissensressourcen und Datensammlungen. Auch den herkömmlichen Staat der Prä-Wissensgesellschaft könnte man als ‚informationsverarbeitendes System' bezeichnen, doch waren diese Informationen damals eher abgeschlossen, schwer zugänglich für andere Amtsstellen und erst recht außenstehende BürgerInnen. Heute ist es prinzipiell technisch möglich, alles zu veröffentlichen. Bund, Länder und Gemeinden stellen auf Websites und Portalen eine nie dagewesene Informationsmenge zur Verfügung. Der öffentliche Sektor verwendet immer mehr elektronische Dokumente, Datensammlungen und Systeme mit Schnittstellen zum Internet; in verschiedenen E-Government Projekten wird das staatliche Wissen digitalisiert, koordiniert, vernetzt und dadurch extensiviert. Wir erleben einen epochalen Wandel staatlicher Informationskultur: Nicht mehr Papier ist das Original, sondern elektronische Gesetze, Register und Akten.

Einerseits eröffnen diese Digitalisierungstendenzen die Chance auf mehr Transparenz, andererseits können personenbezogene Daten leichter in ganz anderen Kontexten ge- und miss-braucht werden. Es entstehen neue Möglichkeiten, aber auch neue Risiken, die zeitgemäß geregelt werden müssen. Besteht die Beziehung zwischen Bürgern und Verwaltung primär aus Informationsaustausch,[1] so gilt das erst recht für E-Government.[2] Die Frage ist: Wer oder was kann und darf worauf zugreifen? Und wie sind diese Regelungen zu kontrollieren?

1.1 Vereinheitlichte Register – Ein einheitliches Personenkennzeichen?

Von den umfassenden Verwaltungsdatenbanken schwer abzugrenzen sind die vom Staat geführten Register, Listen, Verzeichnisse, etc. Sie sind zahlreich, wohl zu zahlreich,[3] auffallend heterogen und ihr Bestand dadurch unübersichtlich: Unterschiedliche (auch privatrechtliche) Stellen sind gesetzlich zuständig bzw. führen de facto die Register. Auch die Rechtswirkungen – ob konstitutiv, deklarativ oder rein informativ – und die daraus resultierenden Anforderungen sind oft unklar. Dazu kommen Inkonsequenzen wie unterschiedliche Schreibweisen und teils mangelnde Datenqualität durch fehlerhafte Altdatenbestände.

Aufgrund dieser Uneinheitlichkeiten und auch weil ab 2010/2011 eine Registerzählung die Volkszählung ersetzt, bestehen Bestrebungen, die Verzeichnisse zu verbessern und zu harmonisieren, und zwar durch Digitalisierung und Zentralisierung bzw. Standardisierung. Diese Tendenzen gibt

[1] Laut Oberndorfer (2006, 83) ein Informationsproblem „das weder die Verwaltung noch die Bürger gemeistert haben". Und für Pernthaler (2004, 208) „muss endlich die Absurdität ins Bewusstsein dringen, dass ‚öffentliche Verwaltung' – gleich in welchen Rechts- oder Organisationsformen – in Österreich nach wie vor prinzipiell nichtöffentlich geführt wird".

[2] „Im Behördenkontakt über das Internet stellt Informationsabruf die bei weitem häufigste Tätigkeit von Usern dar und Informationssysteme machen heute den größten Teil des E-Government Angebots aus" (Aichholzer/Spitzenberger 2005, 38).

[3] „Viele gesetzlich vorgesehenen Verzeichnisse sind überflüssig, etwa weil die darin enthaltenen Informationen nutzlos, banal oder schon in anderen Registern enthalten sind, oder weil sie von der Behörde entgegen ihrem gesetzlichen Auftrag gar nicht oder nur schlampig geführt werden" (Morscher/Christ 2005, 175). Vgl. deren Liste ohne Anspruch auf Vollständigkeit: http://www.uibk.ac.at/oeffentliches_recht/mitarbeiter/morscher_verzeichnis.pdf.

es auch international, etwa im EU-weit geregelten Firmenbuchregister und dem geplanten Unternehmensregister online. In allen staatlichen Bereichen werden sich E-Register und Informationsverbundsysteme etablieren. Das bringt gewichtige Vorteile, weil elektronische Datenbanken das Verwaltungswissen vernetzen und dadurch vermehren. Standards erhöhen die Benutzerfreundlichkeit und erleichtern Behördenwege (Stichwort: One-Stop-Government). Auch intern werden durch behördenübergreifende und interkommunale Zusammenarbeit Effizienzsteigerungen und Synergieeffekte erzielt. Dabei sind freilich personenbezogene Daten zu schützen.

Die älteste, umfangreichste und oft aktuellste Datensammlung zum Personenstand verwaltet der Hauptverband der Sozialversicherungen; darum ist er eine zentrale Auskunftsstelle für Behörden und Justiz. Diverse Institutionen in sozialversicherungsfremden Bereichen verwenden diese Daten, u. a. die Finanzämter bei der Prüfung und Berechnung von Abgaben, Steuern, Prämien und begünstigten Vorsorgen.[4] Doch nicht nur die Daten des Hauptverbandes werden außerhalb des Sozial- und Gesundheitswesens eingesetzt, sondern auch die Sozialversicherungsnummer (SVNr.). Während andere EU-Staaten einheitliche Personenkennzeichen zur Identifikation gebrauchen,[5] ist das in Österreich nicht vorgesehen. Die SVNr. ist als inoffizielle Ersatz-Personenkennzahl nicht nur aufgrund von Datenmängeln und vielfacher Doppelvergaben ungeeignet (Souhrada 2004), sondern insbesondere besteht ein Datenschutzrisiko, weshalb der Datenschutzrat immer wieder diese „schleichende Einführung eines Personenkennzeichens“ (BKA 1997) beanstandete. Auch das 2001 erlassene Bildungsdokumentationsgesetz verwendet zur Identifikation die SVNr.;[6] bis zu 20 personenbezogene Daten ihrer Schüler bzw. Studierenden müssen Bildungseinrichtungen an das Ministerium weiterleiten. Kritisiert wird, durch die geforderte Bekanntgabe der SVNr. seien die Daten leicht zurückzuverfolgen, zumal sie 60 Jahre lang verschlüsselt gespeichert werden – entscheidend ist also der Datenschutz.

1.2 Überwachung

Telekommunikationsdaten sind in Österreich traditionell durch das Fernmeldegeheimnis außerordentlich gut grundrechtlich geschützt. Als neue Grundlage zur Telekommunikationsüberwachung entstand im Mai 2006 die EU-’Richtlinie über die Vorratsdatenspeicherung[7] von Daten’. Der auffallend schnelle Prozess der Richtlinienerstellung ist auf den verstärkten Druck der USA zurückzuführen.[8] Es blieb wenig Zeit für einen Diskurs, bei dem sich beinahe einhellige Ablehnung durch die Wirtschaft im Bereich Informations- und Kommunikationstechnik (IKT) (wegen der enormen

[4] Das waren etwa 2002 über 1 Mio. Auskünfte an die Justiz und über 1,6 Mio. online an Behörden. Souhrada (2004) zählt dazu – ohne Anspruch auf Vollständigkeit – dutzende Verwaltungsabläufe auf.

[5] Z. B. wird die niederländische ‚SoFi-Nr.’ obligatorisch von öffentlichen Institutionen, Arbeitgebern, Banken, Schulen etc. verwendet (Auflistung: http://www.cbpweb.nl/downloads_wetten/WBP_besluit_sofinummer.pdf).

[6] Gemäß einer Verordnung ist ein Ersatzkennzeichen zuzuweisen, falls glaubhaft keine SVNr. vergeben wurde. Ein ministerielles Rundschreiben betont, der Schüler müsse das Fehlen der SVNr. plausibel machen, und erinnert an Verwaltungsstrafen im Weigerungsfall: www.bmbwk.gv.at/ministerium/rs/2004-07.xml.

[7] Für Heinrich Neisser (Diskussionsbeitrag in ÖJK 2005, 246) ist das liebenswerte Wort, mit dem man „Eichhörnchen assoziiert, die sozusagen das Fressen für die Winterzeit hinterlegen” nur ein Euphemismus für „gigantomanische” Speicherhypertrophie.

[8] Westphal (2006, 34 f.) lässt eine tragende Rolle der „eifrigen österreichischen Ratspräsidentschaft” anklingen. „Schließlich führte die österreichische Ratspräsidentschaft den zur Annahme der Richtlinie erforderlichen förmlichen Mehrheitsbeschluss des Rates der Justiz- und Innenminister am 21. Februar 2006 herbei.“

Kosten), Datenschützerinnen, NGOs und Öffentlichkeit abzeichnete. Hauptkritikpunkte sind die mögliche missbräuchliche Überwachung von aufgerufenen Websites bzw. Standorten der Mobiltelefone (wodurch ein Bewegungsprofil jeder Benutzerin erstellt werden kann).[9] Der Grundrechtseingriff sei unverhältnismäßig, ungeeignet (schon durch das Datenvolumen) und gerade durch die „Zielgruppe" Terroristen und Kriminelle leicht zu umgehen. Aufgrund unpräzise formulierter Regelungen bleibt es den einzelnen Mitgliedstaaten überlassen, was sie unter „schweren Straftaten" verstehen, wie kurz (sechs Monate) oder lang (zwei Jahre, mit vagen Verlängerungsoptionen) sie Daten speichern,[10] welche Behörden zugreifen etc. Konträr zur Harmonisierungsabsicht der Richtlinie lässt sich ironisch konstatieren: „solely intrusion into privacy has been harmonized" (Liebwald 2006, 56).

Diese Daten werden künftig auch die Rufdatenrückerfassung im Rahmen von Strafverfahren erleichtern. Andere strafgerichtlichen Informationseingriffe wie Rasterfahndung (offiziell ‚automationsunterstützter Datenabgleich'), Lausch- und Spähangriffe (‚optische und akustische Überwachung von Personen unter Verwendung technischer Mittel') werden zwar heftig diskutiert,[11] doch selten eingesetzt.[12] Sie bedürfen einer richterlichen Anordnung, nicht zuletzt weil die Betroffenen hier nicht wissen, dass sie überwacht werden. Die Eingriffsmöglichkeiten der Sicherheitsbehörden wurden in den letzten Jahren beachtlich erweitert, wie weit bleibt in mancher Hinsicht (bewusst?[13]) unklar. Unter anderem darf die Exekutive jetzt auch private Videoaufzeichnungen verwenden. Datenschutzbedenken bestehen auch angesichts der zunehmenden Überwachung öffentlicher Orte und Verkehrsmittel, nicht zuletzt, weil die Kamera automatisch ‚sensible' personenbezogene Daten wie Herkunft und Gesundheit mit aufzeichnet. Ob die „Section Control" verfassungswidrig ist, prüft zurzeit der Verfassungsgerichtshof, nach dessen „vorläufiger Auffassung" fehlen die gesetzlichen Grundlagen zur Kennzeichen-Speicherung.[14] Fraglich ist, ob die genannten Intentionen – vorwiegend Aufklärung von Straftaten und Hebung des subjektiven Sicherheitsgefühls – die Eingriffe rechtfertigen. Der Nutzen wird vielfach angezweifelt, die Aufzeichnung bringe bestenfalls eine temporäre Verlagerung der Kriminalität, also keinen nachhaltigen Sicherheitsgewinn verglichen mit der unbedenklichen Live-Kamera an Hot-Spots, die als ‚verlängertes Auge' schnelle Hilfe verschaffen könnte (Peissl 2003, 172 f.). Allgemein wird eine Tendenz zur vagen Ausweitung von Informationseingriffen bei eingeschränkten Kontrollmöglichkeiten konstatiert. Die Sicherheits-

[9] Zu speichern sind: Beginn und Endzeit des Telefongesprächs; Telefondienst; Rufnummern, IMSI und IMEI beider Teilnehmer; bei Erstaktivierung vorausbezahlter anonymer Dienste: Datum, Uhrzeit und Standortkennung (Cell-ID); bzw. Internetdienst, Datum und Uhrzeit der An- und Abmeldung; IP-Adresse, Benutzerkennung; Rufnummer des Anrufenden und DSL.

[10] „In Österreich hat man es mit der Umsetzung weniger eilig. [...] Die einjährige Speicherdauer für Telefonie-Verkehrsdaten könne frühestens im Sommer 2007 gesetzlich verankert werden. Für die Internet-Daten habe Österreich zusammen mit anderen EU-Staaten eine weitere Übergangsfrist von zusätzlichen 18 Monaten ausgehandelt" (E. Moechel, http://futurezone.orf.at/it/stories/101686).

[11] Z. B. Heinrich Neisser (in ÖJK 2005, 247) fordert regelmäßige Evaluation „die nicht nur darin bestehen kann, dass die Sicherheitsverwaltung uns erklärt, das ist ohnedies alles in Ordnung und wir brauchen das unbedingt" und einen Grundrechtsdiskurs zur Sensibilisierung der Öffentlichkeit.

[12] Insgesamt von 2000 bis 2005 nur in zwölf Gerichtsfällen große und in 18 kleine Lauschangriffe (BM für Justiz: ‚Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen im Jahr 2005' vom 06.11.2006).

[13] So etwa Funk (2006, 20): Er spricht von Placebo und Alibi-Ermächtigungen, einem „Wildwuchs an Ermächtigungen für Informationseingriffe […] deren unklar gehaltene Reichweite den Auf- und Ausbau dichter Informationsnetze ermöglicht". Anekdotisch erwähnt Gerhart Kunnert (ÖJK 2006, 47): „Es hat sich in der Praxis schon gezeigt, dass – gerade bei den Überwachungen auf öffentlichen Plätzen zum Teil, wenn wenig los ist – Beamte die Kamera nicht ganz zielgerichtet einsetzen und sich etwa in umliegende Wohnhäuser ein bisschen mit der Zoomfunktion hineinbegeben."

[14] Kunnert (2006, 18 f.) kritisiert v. a., dass Kennzeichen auch ohne Geschwindigkeitsübertretung aufgezeichnet werden; außerdem den Einsatz mindestens einer mobilen Anlage ohne Meldung ans Datenverarbeitungsregister (DVR).

behörden drängen verstärkt auf Dinge, die sie „gerne hätten, aber momentan eben nicht dürfen“ (Zwettler 2004, 51).[15] Letztlich passt sich so das Recht der herrschenden Praxis an:

> „Erfahrungen aus der Vergangenheit lehren uns, dass damit zu rechnen ist, dass die rechtlichen Befugnisse von Ermittlungsbehörden an die wachsenden technischen Möglichkeiten der Überwachung immer wieder angepasst werden“ (Čas 2005, 100).

1.3 Risiken

Absolute Datensicherheit kann es nicht geben und gerade in den letzten Jahren traten vermehrt Sicherheitsprobleme auf (DSK 2005, 38). Auch E-Government birgt die vom E-Business bekannten Gefahren. Einen Fall von Datenverlust beanstandet der Rechnungshofbericht 2006/3: Die Wiener Lehrpersonalplanung (im Gesamtumfang von jährlich 400 Mio. €) war teilweise kaum nachvollziehbar, denn leitende Mitarbeiter des Stadtschulrats hatten vor ihrem Pensionsantritt alle Computerdaten gelöscht und eine ordnungsgemäße Datensicherung gab es nicht.[16] Vereinzelt verursachte der Trend zum Outsourcing von IT-Dienstleistungen Datensicherheitsprobleme. So wurde eine aus dem Verkehrsministerium stammende Festplatte bei eBay versteigert und geheime Daten konnten rekonstruiert werden. Einhellige Reaktion der Ministerien auf parlamentarische Anfragen im Juni 2006: Festplatten werden jetzt vor ihrer Entsorgung zerstört. Teils wurden auch Verbesserungen angekündigt wie im Sozialministerium verstärkte Stichprobenkontrollen, im Außenministerium eine Spezial-Software, um Daten rückstandslos löschen zu können.

Zu diesem Restrisiko kommen beim E-Government noch spezifische Herausforderungen. Wenn elektronische Akten, Dokumente und Daten das Original darstellen, sind besonders hohe Ansprüche an ihre Authentizität zu stellen.[17] Darüber hinaus muss den potentiellen Nutzerinnen evident sein, dass ihre Daten sicher sind:

> „Technisch noch so durchdachte und ausgefeilte Sicherheitssysteme, welche auch bei internationalen Firmen im Einsatz sind, müssen nicht automatisch für e-Government Lösungen akzeptabel sein. Da im Gegensatz zu obigen Systemen im e-Government eine zusätzliche Anforderung hinzukommt: Das Vertrauen des Endbenutzers“ (Hof 2005, 110).

Je komplizierter die Sicherheitsmechanismen, desto umständlicher meist die Anwendung.[18] Externes E-Government sollte also möglichst ‚kundenfreundlich’ sein, sowohl für Servicekomfort, E-Inclusion und Akzeptanz als auch aus Sicherheitsgründen.[19]

[15] Genannt werden etwa vom Sektionschef im Innenministerium Mathias Vogl (ÖJK 2005, 249 f.) „die Ermittlung und Verarbeitung personenbezogener Daten für den Zweck der Gefährdungseinschätzung”, die „verpflichtende Einführung der Abnahme von Fingerabdrücken für alle Visa-Werber“ und die Teilnahme an internationalen Informationsverbundsystemen.

[16] Mittlerweile trägt der Wiener Stadtschulrat den Empfehlungen zur lückenlosen, unveränderbaren Speicherung wichtiger Daten und ordnungsgemäßen Dokumentation von Verwaltungsvorgängen bereits Rechnung.

[17] Hier setzt auch das Bürgerkartenkonzept an, das sowohl die Online-Identität als auch Authentizität von Urheber und Daten sicherstellt. Dafür erhielt Österreich 2005 den ersten Preis für Datenschutz in der europäischen öffentlichen Verwaltung.

[18] U. a. müssen bestimmte ‚sichere’ Signaturen bis Ende 2007 nachsigniert werden.

[19] Kritisch zum österreichischen Modell der abgestuften Signaturen etwa Forgó (2003) und Karning (2004, 85): „Eine weniger technokratische Lösung würde mM nicht nur mehr Datenschutz gewährleisten, sondern auch ein verstärktes Verständnis der Bürger für E-Government mit sich bringen.“

Neben der Datensicherheit ist der Schutz persönlicher Daten unabdingbar. Bei vielen staatlichen Datenanwendungen haben Betroffene keine Wahl, denn sie sind „Kunden" eines Monopolisten bzw. Rechtsunterworfene. Praktisch die ganze Bevölkerung ist in den umfangreichen Verwaltungsdatenbanken gespeichert. Und oft geht es in staatsnahen Institutionen um besonders problematische Daten (z. B. Vorstrafen, Sozialhilfe, Krankheiten, Aufenthaltsbewilligung).

Als wichtigstes Verwaltungsregister ermöglicht das Zentrale Melderegister (ZMR) unzählige E-Government-Anwendungen.[20] Es ist nur insofern öffentlich als der aktuelle Hauptwohnsitz einer bestimmten Person abgefragt werden kann; erweiterte Möglichkeiten haben Verwaltungsstellen, der dritte Sektor und „Business-Partner" (wie etwa Rechtsanwälte, Inkassobüros, Banken, Verkehrsbetriebe). Einige dieser Abfrageberechtigten hatten Daten an Unbefugte weiterverkauft. Als Reaktion auf „Empfehlungen" der Datenschutzkommission musste das Innenministerium Zugriffsberechtigungen entziehen und den Abfragemodus umstellen. Darüber hinaus bergen insbesondere vernetzte E-Register und Informationsverbundsysteme spezielle Risiken, in erster Linie ein gewisses Missbrauchspotenzial. Das ‚Elektronische Kriminalpolizeiliche Informationssystem' (EKIS) umfasst etwa ein Dutzend Anwendungen mit teils sensiblen Daten.[21] Daneben besteht die Gefahr, dass verfassungsrechtliche Prinzipien aufgeweicht werden: Die Zentralisierung lokaler Register schwächt den Föderalismus als gewaltenteilendes Element. Und durch die Vernetzung und Vereinheitlichung der Systeme werden Daten aus ihrem ursprünglichen Kontext gelöst und verwaltungsübergreifend zu andersartigen Zwecken abgerufen – insbesondere wenn verschiedene Datenbanken mit einer Personenkennung verbunden werden. Eine Machtkonzentration des Staates im elektronischen Bereich zuungunsten des Einzelnen könnte zu Vertrauensverlust führen, die E-Government-Akzeptanz gefährden und in Verbindung mit steigenden Überwachungsmaßnahmen letztlich Fortschritt und Entwicklung hemmen (vgl. Peissl 2003).[22]

[20] Z. B. im Jahr 2005 wurden 23.607.849 Abfragen durch Behörden durchgeführt (Parlament. Anfragebeantwortung des BMI, 20.4.2006).

[21] In der sog. Spitzel-Affäre wurden illegal abgefragte Daten politisch missliebiger Personen an Unbefugte weitergegeben und öffentlich präsentiert (vgl. u. a. Nationalratsdebatten 22.11.2000, 28.03.2001; A. Medosch: Grundrechtlicher Super-GAU in Österreich kontaminiert die EU: http://www.heise.de/tp/r4/artikel/8/8992/1.html).

[22] Auch Funk (2006, 21) konstatiert „ein rechtsstaatliches Untermaß, das die Entwicklung eines Eingriffs-Übermaßes begünstigt". Es „könnte vom Rechtsstaats-Placebo über den Überwachungsstaat zum Sicherheitsdefizit reichen."

2 Datenschutz

E-Government bringt nicht nur Risiken mit sich, sondern auch Sicherheitsgewinne: Papierbasierte Übertragungsfehler wurden reduziert, und in erster Linie ist jetzt leicht zu protokollieren und nachzuvollziehen, wer auf welche Daten zugegriffen hat. Datenschutz umfasst technische, organisatorische und nicht zuletzt personelle Maßnahmen (wie Schulungen von MitarbeiterInnen bzw. NutzerInnen),[23] und geht als normativ-regulative Aufgabe darüber hinaus. Viele rechtliche und organisatorische Schritte zum Schutz personenbezogener Daten wurden schon gesetzt. Die Europäische Menschenrechtskonvention garantiert die Achtung des Privatlebens; der Europäische Datenschutzbeauftragte kontrolliert als unabhängige Instanz die Einhaltung der relevanten Rechtsquellen. Wie der Europäische Gerichtshof 2003 feststellte, gilt die Datenschutzrichtlinie bei abweichenden staatlichen Bestimmungen auch für personenbezogene Daten des öffentlichen Sektors, im Anlassfall Österreichs.[24]

2.1 Regelungen und Datenschutzkommission

In Österreich wurde die Datenschutzrichtlinie durch das Datenschutzgesetz 2000 (DSG) umgesetzt; das Grundrecht auf Geheimhaltung personenbezogener Daten steht sogar im Verfassungsrang. In anderen Gesetzen verstreut finden sich unterschiedliche Regelungen, insbesondere für die Sicherheitsbehörden und Gerichte; das österreichische Datenschutzrecht und damit seine Durchsetzung sind sehr komplex.

Im DSG gibt es einige spezielle Bestimmungen für den öffentlichen Sektor, d. h. sowohl für öffentlich-rechtliche Institutionen als auch für private Unternehmen, die Hoheitsverwaltung betreiben (z. B. Parkraumüberwachung oder Kfz-Zulassung).[25] Amtliche Datenverarbeitungen müssen prinzipiell von einer gesetzlichen Ermächtigung gedeckt sein. Wenn sie indes für bestimmte staatliche Zwecke benötigt werden, müssen sie weder der Datenschutzkommission (DSK) gemeldet werden, noch brauchen sie temporär eine gesetzliche Grundlage.[26] Prinzipiell dürfen personenbezogene Daten gemäß dem Zweckbindungsgebot weder für einen anderen als den ursprünglichen Aufgabenbereich selbst verwendet noch einer anderen Stelle weitergeleitet werden. Demgegenüber werden durch Amtshilfe einer Behörde für eine andere keine schutzwürdigen Geheimhaltungsinteressen verletzt. Die in der Verfassung verankerte Amtshilfe zählt darüber hinaus zu den 13 Ausnahmen vom grundsätzlichen Verwendungsverbot sensibler Daten (betreffend Herkunft, Überzeugung, Gesundheit etc.).

[23] Z. B. empfiehlt Forgó (2003, 27) zur Sensibilisierung des Datenschutzbewusstseins, Bürgerkarten-User zu schulen; Aichholzer/Spitzenberger (2005, 39) schlagen dafür E-Learningsysteme vor.

[24] Leitende ORF-Angestellte hatten sich gegen die Veröffentlichung ihrer Einkommen gewandt (Rs. C-465/00).

[25] Der Dritte Sektor ist oft schwer abzugrenzen, angesichts zunehmender Ausgliederungen und bei bestimmten Berufsgruppen wie Notaren. Vgl. Mayer-Schönberger/Brandl (2006), Janel (2006, 338). So ist die Datenschutzkommission z. B. unzuständig für Beschwerden gegen die Österreichischen Bundesbahnen (K121.150/0014 vom 26.9.2006).

[26] Diese Zwecke sind (bis Ende 2007) der Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen Österreichs oder der EU, die Vorbeugung, Verhinderung oder Verfolgung von Straftaten; darüber hinaus (bis zur allfälligen Erlassung eines Gesetzes, also womöglich unbeschränkt!) die Sicherung verfassungsmäßiger Einrichtungen, der Einsatzbereitschaft des Bundesheeres und der Interessen der umfassenden Landesverteidigung. Diese problematische Übergangsbestimmung steht im Verfassungsrang (vgl. Mayer-Schönberger/Brandl 2006, 148; Jahnel, 2006, 336).

Da Datenschutzverstöße im Unterschied zu anderen Grundrechtverletzungen kaum wahrnehmbar sind, sind hier effektive Kontrolleinrichtungen essentiell. Zu diesen gehört, neben dem Datenschutzrat (der im Wesentlichen beratende Funktion hat und Stellungnahmen zu relevanten Vorhaben abgeben kann) und dem Rechtsschutzbeauftragten im straf- und sicherheitspolizeilichen Bereich (dessen Effektivität häufig hinterfragt wird),[27] in erster Linie die DSK. Datenverarbeitungen sind gewöhnlich der DSK zu melden und von dieser im Datenverarbeitungsregister (DVR) zu registrieren. Nicht meldepflichtig sind u. a. ‚Standardanwendungen' (z. B. Personenstandsbücher, Staatsbürgerschaftsevidenz, Wähler- und Stimmlisten).

Prinzipiell kann die DSK ausschließlich bei begründetem Verdacht auf rechtswidrige Datenverwendung überprüfen, doch Informationsverbundsysteme und Anwendungen mit ‚sensiblen' oder strafrechtlich relevanten Daten unterliegen sogar einer Vorabkontrolle und dürfen erst nach Genehmigung betrieben werden. Auch dem Innenministerium als EKIS-Betreiber wurde keine Ausnahme zugestanden sondern empfohlen, die notwendigen Meldungen unverzüglich nachzuholen (DSK 2005, 53). Weiters behandelt die DSK Beschwerden über Verletzungen des Auskunftsrechts und – im öffentlichen Bereich – hinsichtlich Geheimhaltung, Richtigstellung und Löschung. In den letzten Jahren häufen sich Beschwerden von Eltern in Vertretung minderjähriger Schüler gegen das Bildungsdokumentationsgesetz bzw. dessen Verwendung der SVNr. Und etliche Betroffene beantragten die Löschung ihrer Daten im EKIS oder anderen Verzeichnissen der Sicherheitsbehörden.[28]

Angesichts der Risiken von Datenverknüpfungen mittels einer einheitlichen Personenkennung wie der SVNr. fungiert die DSK auch als Stammzahlenbehörde. Sie erzeugt nämlich aus der ZMR-Zahl (Zentrales Melderegister) die verschlüsselte ‚Stammzahl' und damit die Personenbindung.[29] Aus dieser Stammzahl werden von der DSK oder mittels Bürgerkarte durch nicht-umkehrbare Kryptographie bereichspezifische Personenkennzeichen (bPK) abgeleitet. Nur diese bPK dürfen verwendet werden, die Verwendung der ZMR-Zahl oder der virtuellen Stammzahl ist unzulässig. Sie sind auf einen von 26 Tätigkeitsbereichen (von ‚Arbeit' bis ‚Zur Person') beschränkt und entsprechen damit prinzipiell dem Zweckbindungsgebot des DSG. Daneben bestehen allerdings auch neun bereichsübergreifende Kennungen (wie ‚Öffentlichkeitsarbeit' und ‚Zustellungen').

Besonders für die Kommunen und die Länder ist die Bereichsbeschränkung aufwändig, denn gerade im Sinne des One-Stop-Governments gibt es in der Verwaltung viele Querschnittsverfahren und -anwendungen. Um nun bereichsübergreifenden Datenaustausch und Amtshilfe zu erleichtern, errechnet die DSK für öffentliche Stellen bPK aus anderen Bereichen. Diese ‚Fremd-bPK' werden

[27] U. a. zumal die meisten Datenverwendungen nicht zu seiner Kenntnis gelangen und er nicht verfassungsgemäß weisungsfrei gestellt ist (Wiederin 2003, 146 f., 222 f.); weitergehend Bernd-Christian Funk (Diskussionsbeitrag in ÖJK 2006, 56): „Man kann ihn noch so sehr weisungsfreistellen, wenn die Einrichtung selbst von Anfang an eine Alibieinrichtung ist, weil es an den Kompetenzen fehlt." Und Hannes Tretter vom Ludwig Boltzmann Institut für Menschenrechte (in ÖJK 2006, 48): „Ich weiß nicht, wo Daten und Bildaufzeichnungen, auch wenn sie offiziell nach 48 Stunden gelöscht werden, versteckt werden, wo sie weitergeleitet werden, wo irgendwelche Datenmengen weggeschnitten werden, um irgendwie in einem anderen Zusammenhang wieder aus dem Koffer hervorgezaubert zu werden. Ich bezweifle, dass das Institut des Rechtsschutzbeauftragten ohne gerichtliche Kontrolle derzeit effektiv genug ist, hier zumindest stichprobenartig ständig nachzuprüfen."

[28] Die DSK hatte vorzeitige Löschungsbegehren regelmäßig abgelehnt, doch nach einer Entscheidung des Verfassungsgerichtshofs muss sie im Einzelfall prüfen, ob die gespeicherten Daten aktuell und korrekt sind und noch für den vorgesehenen Zweck benötigt werden.

[29] Laut der Regierungsvorlage zum E-Government-Gesetz (Art. 1 § 7, 252 Beil XXII. GP) empfehle sich die DSK auch als Stammzahlenregisterbehörde, weil sie beim DVR bereits „mit Aufgaben der Registerführung vertraut ist, was eine Minimierung der erforderlichen Zusatzkosten erwarten lässt." Diese Zuständigkeiten weichen jedoch deutlich voneinander ab. Im Übrigen müsste die DSK als Stammzahlenbehörde bei etwaigen Beschwerden im Zusammenhang mit bereichsspezifischen Personenkennzeichen (bPK) gegen sich selbst ermitteln und entscheiden.

auch verschlüsselt auf Vorrat gespeichert.[30] So kann etwa „sichergestellt werden, dass auch dann, wenn z. B. für ein anfragendes Finanzamt nur das finanzbereichsspezifische Personenkennzeichen bekannt ist, dennoch Auskünfte aus den Datenbeständen der Sozialversicherung möglich bleiben" (Souhrada 2004, 528 f.) Letztlich kann exzessiver Gebrauch oder Missbrauch von Fremd-bPK jedoch Datenschutzregelungen aushebeln und die Idee der Bereichszuordnung ad absurdum führen.[31]

2.2 Reformvorschläge

Die EU-Kommission hat 2005 ein Vertragsverletzungsverfahren gegen Österreich eingeleitet: Die erforderliche völlige Unabhängigkeit der Datenschutzkommission sei nicht gewährleistet. Schon 2003 hatte die ‚ARGE Daten' Beschwerde wegen mangelhafter Umsetzung der EU-Richtlinie eingelegt, u. a. wegen „unvereinbarer Aufgaben" als Datenschutz- und Stammzahlenbehörde und „unzulässiger personeller Verflechtungen". Auch die DSK selbst moniert immer wieder Engpässe bei Personal, Infrastruktur und Finanzen (kein eigenes Budget!) trotz immer komplexeren Datensystemen (DSK 2005, 56). In der Praxis verursachen diese Ausstattungsdefizite oft jahrelang verzögerte Entscheidungen und dadurch Säumnisbeschwerden – das ist besonders gravierend, da die DSK hier oberste und einzige Instanz ist. Der Ressourcenmangel verhindert die regelmäßige Herausgabe der Datenschutzberichte und in erster Linie die gesetzlich vorgesehenen Kontrollen ohne Beschwerdefall. Das begünstigt auch Nachlässigkeiten von Stellen, die ihrer Registrierungspflicht nur unvollständig oder schleppend nachkommen.

Gefordert ist eine laufende, umfassende Kontrolle der Register und personenbezogenen Daten, auch von Organisationen des Dritten Sektors (wie Sozialversicherungen). Diese Prüfungen sind präventiv durchzuführen statt nur anlassbezogen als Reaktion auf einzelne Beschwerden und die Prüfungsorgane sind verfassungsrechtlich weisungsfrei zu stellen.[32] Damit die Kontrollinstanz de lege und de facto unabhängig von den kontrollierten Stellen agieren kann, sollte sie nicht der Exekutive unterstehen sondern direkt dem Parlament,[33] selbstverständlich mit geeigneten Rahmenbedingungen, ausreichender Ausstattung und einem eigenen Budget. Denkbare Varianten sind stark erweiterte Kompetenzen für die DSK, wie sie auch selbst fordert,[34] oder eine permanente aktive Kontrolle durch einen „Datenschutzhof" analog zum Rechnungshof im Bereich der Gesetzgebung.

30 Vgl. die 2006 eingerichtete Webseite der Stammzahlenregisterbehörde: www.stammzahlenregister.gv.at/bpk.htm.

31 Karning (2004, 83 f.) sieht weitere Gefahren: „Man kann trotz der technisch versiert anmutenden Methoden der Nichtrückführbarkeit der Stammzahl sowie der bereichsspezifischen Personenkennzeichen nicht sicher sein, dass dadurch nicht doch der ‚gläserne Bürger' geschaffen wurde". Er bezweifelt „dass vor allem im Hinblick auf die rasant fortschreitende Entwicklung der Technik es absolut nicht möglich sein soll, Rückschlüsse auf die ZMR-Zahl ziehen zu können."

32 Vgl. Mayer-Schönberger/Brandl (2006, 122).

33 Auch für Simitis (2004, 77) erfordert „ernst genommene und wirklich resistente Unabhängigkeit eine Ausgliederung aus den Hierarchien der jeweiligen Behördenstrukturen […] und eine direkte Kooperation mit dem Parlament".

34 „Gerade die Einführung eines umfassenden e-Government-Konzeptes in Österreich verschafft der Stellung der DSK als Stammzahlenregisterbehörde und damit Hüterin der elektronischen Identitäten der Bürger besondere Bedeutung. Wenn die Bevölkerung nicht den Eindruck gewinnt, dass sich eine kompetente und wachsame Stelle um die Datenschutzinteressen der Bürger gegenüber der fortschreitenden Elektronisierung des öffentlichen Lebens erfolgreich annimmt, wird der dringend notwendige Innovationsschub in der öffentlichen Verwaltung auf Akzeptanzprobleme stoßen. Diese Wachsamkeit muss dauernd, allgemein und auch unabhängig vom Vorliegen einer konkreten Beschwerde ausgeübt werden" (DSK 2005, 15).

Neben den vorhandenen gesetzlichen Bestimmungen zum Schutz persönlicher Daten sind demnach weitere Maßnahmen notwendig, vor allem zur Kontrolle ihrer Einhaltung in der Praxis. Angesichts der durchaus wünschenswerten Tendenzen zur Standardisierung bzw. Zentralisierung und der möglichen Verknüpfung bisher getrennter Systeme sind die Zuständigkeiten neu zu überdenken, auch ob die Registerführung überhaupt an beliehene Unternehmen delegiert werden kann oder vielmehr zu den staatlichen Kernaufgaben gehört. In Frage kommen weisungsfreie Behörden, zumindest für neu entstehende zentrale Register und sensible Daten. Dafür würde sich die Gerichtsbarkeit anbieten, aufgrund ihrer verfassungsgemäß strikten Trennung von der Exekutive. Die Gewaltenteilung im Sinne der Verfassung ist auf jeden Fall auch im elektronischen Bereich zu erhalten. Denkbar sind weiters getrennte registerführende Stellen für bundes- und landesrechtliche, öffentliche bzw. gerichtliche Verzeichnisse (Morscher/Christ 2005) und zentrale/dezentrale Portale.

Voraussetzung ist als erster Schritt die vollständige Nachvollziehbarkeit (die als Nebeneffekt datenverarbeitende Stellen vor unzutreffenden Vorwürfen schützt). E-Government bietet technische Möglichkeiten, den gesetzeskonformen Umgang mit personenbezogenen Daten zu dokumentieren und zu kontrollieren, u. a. durch fälschungssichere Protokolle der abgelaufenen Prozesse und regelmäßige, zyklische Auditverfahren. In einem serviceorientierten One-Stop-System könnte jeder in seinem eigenen Online-Account seine Daten selbst abrufen und überprüfen ‚Wer hat wann und warum welche meiner Daten verarbeitet?' und so seine Rechte geltend machen. Schließlich bedeutet E-Government die Datenhoheit der Bürgerinnen und Bürger.

3 Informationspotenziale

Die Informationsbestände des öffentlichen Sektors reichen weit über personenbezogene Daten hinaus. Verschiedenste Angaben zu sammeln, reproduzieren und weiterzugeben gehört sozusagen zum staatlichen Kerngeschäft. Information ist heute die Schlüsselressource und zu erfolgreichem staatlichem Wissensmanagement gehört die Einsicht, dass sich Wissen durch Teilung vermehrt. Das bedeutet im Idealfall „Förderung des Austauschs von Wissen mit der Öffentlichkeit bei gleichzeitiger Beachtung des Datenschutzes", denn „das öffentliche Gedächtnis garantiert durch verbesserte Transparenz und erweiterten Zugang zu Bürger- und Staatswissen, dass relevante Informationen und zu behaltendes Wissen nicht verloren gehen" (Thom/Ritz 2006, 158, 208). Doch wenn Wissen Macht ist, ist ein Wissensgefälle auch ein Machtgefälle.

> „Die Asymmetrie im Informationsaustausch liegt darin, dass die Verwaltung sehr viel an Informationen vom Bürger fordert, ohne dass dieser oftmals einzusehen vermag, wozu eine bestimmte, ihm abverlangte Information von der Verwaltung benötigt wird. Dem steht umgekehrt ein sehr geringer Informationsstandard des Bürgers über seine Handlungschancen in der Verwaltung gegenüber" (Oberndorfer 2006, 84).

Hier verstärkt die IKT den Druck auf Zugangsansprüche und Beteiligung. Dass eine generellere elektronische Öffnung bereits technisch machbar ist, forciert die Frage ‚Wem gehören öffentliche Informationen? Und wer kann sie nutzen?' Der mit dem technischen Fortschritt forcierte Paradigmenwechsel verlangt auch einen Mentalitätswandel. Ein signifikantes Beispiel für die Umbruchphase, in der sich der Staat befindet: Wurde die Online-Publikation des Kunstberichts 2003 noch entschieden abgelehnt,[35] sind die Kunstberichte 2004 und 2005 schon problemlos im Internet abzurufen.

Heute sind schon viele Informationen des öffentlichen Sektors online zugänglich. Österreich ist besonders im Bereich der Gesetzgebung vorbildlich. Das Parlament und der Steirische Landtag veröffentlichen Dokumente wie Protokolle aus durchgängig elektronischen Gesetzgebungs-Workflows. Im Rechtsinformationssystem des Bundeskanzleramts (RIS) finden sich neben der authentischen Online-Kundmachung des Bundesgesetzblatts auch Landes- und Gemeinderecht, Erlässe und Judikatur. Weiters gibt es zahlreiche Bürgerservice-Angebote, die meist lokal oder thematisch bestimmt sind.[36] Dies birgt zugleich das Risiko der Informationsflut, denn ungeregelt führt die Multiplizierung der Kommunikationswege mit der Vielzahl von Behörden zu unkoordiniertem Auftreten von Portalen unterschiedlicher Qualität, darunter auch bloßes „digitales Hochglanzpapier" (Dix 2002, 90). Status quo ist demnach Informations(über)angebot bei mangelnder Transparenz, denn auch interessierte Bürgerinnen und Unternehmen haben nur selektiv eingeschränkten Zugang zu Verwaltungswissen.

[35] Parlamentarische Anfragebeantwortung (1897/AB XXII. GP, 16.08.2004): „Die jährlichen Kunstberichte, die jeweils rund 180 Seiten umfassen, sind als Printmedium konzipiert. Die Printversion vermittelt übersichtlich und klar strukturiert die wesentlichen Informationen. Es erscheint nicht zweckmäßig, lange Textdokumente und umfangreiche Listen, wie sie im Kunstbericht zu finden sind, im Internet zu veröffentlichen, da diese am Bildschirm nur schwer und umständlich zu lesen sind." Deshalb sei trotz Kostenargument (für Satz, Grafik, Druck und Versand rund 20.000 €) keine Online-Publikation vorgesehen.

[36] Neben dem bekannten ‚Amtshelfer' (www.help.gv.at) z. B. das Bundesländer-Geodatenportal www.geoland.at oder www.verkehrslage.at der Stadt Wien.

3.1 Von der Auskunftspflicht …

Im österreichischen Recht existieren zwar diverse Offenlegungspflichten und Einsichtsrechte, denen jedoch zahlreiche Einschränkungen gegenüberstehen. Laut DSG müssen Organisationen auf Anfrage die Betroffenen über deren gesammelte personenbezogene Daten informieren. Nur falls das „öffentliche Interesse“ an der Geheimhaltung überwiegt, erfolgt die doppeldeutige Auskunft „dass keine der Auskunftspflicht unterliegenden Daten verwendet werden“. In der Praxis sind Auskünfte oft mangelhaft, laut einer Fallstudie (Reichmann 2004) nur in 13 % der Fälle korrekt. Besonders im öffentlichen Bereich ist die Beantwortung selten verständlich und wird gerne die Herkunft der Daten verschwiegen; die Behörden brauchten außerdem doppelt so lange wie private Unternehmen.

In der Verfassung findet sich eine Auskunftspflicht für öffentliche Organe, „soweit eine gesetzliche Verschwiegenheitspflicht dem nicht entgegensteht“. Diese Bestimmung gewährt jedoch nach einem (umstrittenen) Erkenntnis kein verfassungsrechtlich gesichertes subjektives Recht und ist deshalb nicht beim Verfassungsgerichtshof (VfGH) einklagbar. Aus ihr wurden elf Auskunftsgesetze für Bund und Länder abgeleitet, was den Zugang zu dieser komplexen Materie zusätzlich erschwert. In der Praxis gravierender sind Einschränkungen, die letztlich die Intention des Gesetzes aushebeln können. Zunächst ist die Auskunftspflicht auf das örtlich und sachlich zuständige Verwaltungsorgan limitiert – dessen Zuständigkeit ist allerdings für die Bürger nicht leicht festzustellen.[37] Die Antwort ist binnen acht Wochen zu erteilen, es fehlen Regelungen für den Fall einer zeitlich prekären Anfrage oder der Verweigerung durch die Behörde. Beispielsweise hatte der Verfassungsrechtler Feik (2006b) ein Auskunftsbegehren an das „geheimniskrämernde” Wissenschaftsministerium gerichtet. Erst nach über 10 Monaten erhielt er den (letztlich vom Verwaltungsgerichtshof wegen Rechtswidrigkeit aufgehobenen) Bescheid, es könne keine Auskunft erteilt werden.

Dazu kommen diverse Ausnahmen, deren Ermessensspielraum kaum einzuschätzen ist: „Auskünfte sind nur in einem solchen Umfang zu erteilen, der die Besorgung der übrigen Aufgaben der Verwaltung nicht wesentlich beeinträchtigt […] Sie sind nicht zu erteilen, wenn sie offenbar mutwillig verlangt werden.“[38] Das ist wohl als Nachrangigkeit der Auskunftspflicht nach anderen Verwaltungsagenden zu interpretieren.[39] Im Fall einer Anfrage für illegitime Zwecke – etwa „den Kenntnisstand von Behörden gleichsam ‚abzuprüfen’, die Behörden zu belehren und sie zu logischem Denken ‚anzuleiten’“ (VwGH 97/19/0022) – kann sogar eine Mutwillenstrafe verhängt werden. Letztlich ist ein Auskunftsrecht das sich auf die bloße Mitteilung des Inhalts von Aktenteilen beschränkt „als Instrument der Informationssicherung und Mitwirkung der Bürger im Planungsverfahren fast wertlos” (Pernthaler 2004, 206).

Des Weiteren ist die Antwort nur zu erteilen „soweit eine gesetzliche Verschwiegenheitspflicht dem nicht entgegensteht“. Die Informationsrechte werden hauptsächlich von der ausgeprägten Amtsverschwiegenheit konterkariert, die in Österreich – als einzigem EU-Land – sogar in der Verfassung verankert ist (unmittelbar vor der Auskunftspflicht). Insoweit die Grenze zwischen Informationsfreiheit und Geheimhaltung das Transparenzniveau mitentscheidet, zählt Österreich zu den

[37] Oberndorfer (2006, 82) konstatiert sogar „ein völliges Unverständnis für die Verwaltungszuständigkeiten“.

[38] § 1 Abs 2 Auskunftspflichtgesetz des Bundes. Pernthaler (2004, 206) beanstandet diese unbestimmte Einschränkung, denn „die ausreichende Information der Öffentlichkeit kann in bestimmten Planungsphasen zur Hauptaufgabe der Verwaltung werden.”

[39] „Jedes auskunftspflichtige Organ soll aber ganz allgemein darauf Bedacht nehmen, dass ein Zuviel an Engagement in Auskunftsfragen zu einer Gefährdung der herkömmlichen Verwaltungsabläufe führen könnte, und daher jedem einzelnen Auskunftsbegehren, ungeachtet der momentanen sonstigen Belastung, nur soweit zu entsprechen trachten, als die Beschaffung und Weiterleitung der gewünschten Informationen ohne besonderen Aufwand zu bewerkstelligen ist“ (Janko 2003, 16).

tendenziell restriktiven Staaten. In dieser althergebrachten Mentalität wurzelt die übersteigerte Geheimhaltungspraxis vieler Behörden, die von Fall zu Fall willkürlich entscheiden, ob sie Auskunft gewähren (Aichholzer/Tang 2004). Der Verfassungskonvent hat im sog. ‚Fiedler-Entwurf' die Amtsverschwiegenheit auf ein notwendiges Minimum reduziert und im Ausschuss sogar einstimmig einen überparteilichen Konsens erreicht: Die Auskunftspflicht sollte als subjektiv einklagbares Recht auch für Gerichte gelten und ist (als Regel) der Amtsverschwiegenheit (als Ausnahme) überzuordnen.[40] Entscheidend ist die Klärung der Verschwiegenheitspflichten, kann doch ein rigides Amtsgeheimnis selbst das modernste Informationsgesetz untergraben.

3.2 … zur Informationsfreiheit

Auf dem Weg zur Informationsfreiheit lassen sich verschiedene Stufen unterscheiden:

- Als Vorstufe kann im Auskunftsrecht nach dem DSG der Betroffene sein informationelles Selbstbestimmungsrecht über seine eigenen Daten geltend machen.
- Österreichischer Status quo ist die Auskunftspflicht, allerdings unterminiert von Einschränkungen. Diese Holschuld ist schwer durchzusetzen, schon weil Bürgerinnen mangels Informationszugang kaum wissen oder belegen können, dass ihnen Informationen (und von welcher Stelle) vorenthalten werden, bzw. ob die erhaltenen Auskünfte womöglich inkorrekt oder unvollständig und damit tendenziös sind. Unbewusste oder gar absichtliche Manipulation durch Teilinformation ist nicht auszuschließen, zumal für Verwaltungsmitarbeiter eine womöglich unzulässige Auskunftserteilung wegen ihrer Endgültigkeit deutlich riskanter ist als deren Ablehnung (Hart et al. 2004, 219). Die Holschuld verändert generell nichts an der staatlichen Wissensüberlegenheit gegenüber der Antragstellerin, kurz: „ein Auskunftsrecht ist lediglich eine abgeschwächte und nicht mehr zeitadäquate Variante eines Informationsrechts."[41]
- Die nächste Stufe ist Information als Bringschuld der Verwaltung, wobei die österreichische Praxis hier auf halber Höhe stehenbleibt, da Wissenswertes (bzw. was die Behörden dafür halten)[42] in der Regel nur selektiv, als freiwilliges Service angeboten wird: „Informationen erreichen den Bürger mehr oder minder zufällig, oft zu spät, unvollständig und zu wenig kontinuierlich. Problematisch ist ferner, dass besonders wichtige Informationen (z. B. Planungsvorhaben) vielfach überhaupt nicht mitgeteilt werden, andere Aussagen eher unverbindlich formuliert werden und insgesamt die Informationsmaßnahmen großen Quantitäts- und Qualitätsschwankungen unterliegen" (Oberndorfer 2006, 66).
- Als rechtsstaatliche Minimalforderung wären obligatorisch solche Fakten und Meta-Verzeichnisse online zu stellen, die dem Einzelnen überhaupt die Entdeckung ermöglichen, wo sich für ihn Relevantes verbirgt, um daraufhin seine Auskunftsrechte wahrzunehmen; ferner eine Publikationspflicht für Dokumente, die Einblick in Verwaltungsprozesse mit externen Auswirkungen gewähren: Werden meine Anträge und Anliegen korrekt erledigt? Nach welchen Regeln, auf-

[40] Ausschuss 8 ‚Demokratische Kontrollen', 27. Sitzung des Präsidiums, 14.07.2004.

[41] Feik in der Ausschussvorlage 303/AVORL-K zum Verfassungskonvent.

[42] Vgl. die Erfahrungen Großbritanniens, wo ebenfalls ursprünglich vorgesehen war „dass die Verwaltung auf freiwilliger Basis Information selbst zugänglich macht. Dies scheiterte letztlich, weil die Verwaltung die Informationen so selektierte, dass nur ‚Erfolge' veröffentlicht wurden" (Rohde-Liebenau 2003, 114).

grund welcher internen Dienstvorschriften fallen (Ermessens-)Entscheidungen? Gerade solche „Interna“ werden in Österreich oft gut gehütet.[43]

- Letztlich garantiert nur eine staatliche Bringschuld echte Informationsfreiheit, und zwar eine generelle elektronische Publikationspflicht, jedenfalls für neu entstehende Dokumente. Ältere Unterlagen könnten in der Übergangszeit schrittweise digitalisiert werden (beginnend mit den erfahrungsgemäß nachgefragten). „Das entscheidend Neue: die ‚Obrigkeit’ fragt nicht mehr, aus welchen Gründen sich jemand für die Verwaltungsunterlagen interessiert; das tiefsitzende Misstrauen der ‚Wissenden’ gegenüber dem – meist für unvernünftig gehaltenen – Volk findet keinen Ansatzpunkt im Gesetz mehr“ (Bull 2005, 103).

3.3 Desideratum Informationsfreiheitsgesetz

Viele Staaten weltweit haben die Freedom of Information bereits gesetzlich verankert, darunter ein Großteil Europas. Die EU hat schon Anfang der 90er-Jahre mit dem Aufkommen der neuen Medien eine aktive Informationspolitik gestartet. Trotz gewisser Einschränkungen bei Dokumenten, die sich auf Strafverfolgung und Antiterror-Maßnahmen beziehen, sind die Online-Publikationspraxis ihrer Organe und besonders die Umweltrichtlinie wegweisend. Die Mitgliedsstaaten werden sich dieser Entwicklung kaum entziehen können, weil sich auf Dauer schwer Argumente für eine Schlechterstellung der eigenen Bevölkerung aufrechterhalten lassen. So insistierte der Datenschutzbeauftragte Brandenburgs (Dix 2002, 95): „In der zivilen Informationsgesellschaft ist ein allgemeines Recht auf Zugang zu den Informationen der öffentlichen Verwaltung dringend notwendig. Es wird Zeit, dass Deutschland die rote Laterne in der internationalen Entwicklung zu mehr Verwaltungstransparenz abgibt.“ Seit 1.1.2006 hat Deutschland ein Informationsfreiheitsgesetz und damit das Schlusslicht weitergegeben.

Österreich bleibt hier anachronistisch. Immerhin auf dem Umweltgebiet ist die Informationsfreiheit schon verwirklicht: In Umsetzung der vorbildlichen EU-Umweltinformationsrichtlinie werden zahlreiche Daten (Umweltzustand, Maßnahmen, Analysen, Satellitenbilder…) online präsentiert.[44] Umgesetzt wurde auch eine ökonomisch orientierte Richtlinie zur kommerziellen Nutzung öffentlicher Dokumente, mit dem Hauptziel gleicher Marktchancen im interkontinentalen Wettbewerbsdruck. Auch das zugehörige österreichische Informationsweiterverwendungsgesetz öffnet nicht die Schleusen der staatlichen Wissensspeicher – die Behörde kann weiterhin entscheiden, was sie veröffentlichen will – sondern reguliert nur den nichtdiskriminierenden Informationsfluss zu den verschiedenen Akteuren auf dem Content-Markt, zwecks Veredelung und Vertrieb der Rohdaten. Die Wirtschaft ist auch treibende Kraft in der Forderung nach Informationszugang:

> „As democratic movements have been rather weak, the early improvement to access was not the result of strong bottom-up pressure from civil society or the media, as in the US or the UK. A major discourse on information rights did not take place in Austria. More recently, the private information industry and its collective association have been the most active force urging policy formulation on PSI issues” (Aichholzer/Tang 2004, 319).

[43] Mit dieser prinzipiellen Öffentlichkeit aller Verfahren der Entscheidungsfindung „wäre erst der – seit mehr als 150 Jahren geltende Standard an Öffentlichkeit in der Justiz für diese Bereiche der Verwaltung und der Regierung erreicht!“ (Pernthaler 2004, 209).

[44] www.umweltbundesamt.at/umweltinformation/.

Nachgefragt wird also zunächst wirtschaftlich Verwertbares – was im Idealfall letztlich nicht nur einzelnen Unternehmen dient.[45] Von allgemeinem Interesse sind oft Großprojekte wie Bauvorhaben und andere regionale Pläne. Hier sollten nicht nur gegebene Sachverhalte publiziert werden, sondern ebenso die Intentionen der Behörde und nicht zuletzt, welche Optionen Bürgerinnen haben, sich am Prozess zu beteiligen. Die Bereiche Verkehrs- und Geodaten sind zugleich generell und ökonomisch relevant (z. B. für Unternehmen zur Standortauswahl). Benachrichtigungen über temporäre Maßnahmen wie Baustellen oder Verkehrseinschränkungen sind vorzugsweise technologieneutral in Form mobiler Dienste (M-Government) umzusetzen,[46] wofür etwa beim Handyparken schon lokale Ansätze existieren. Erfahrungsgemäß von vitalem öffentlichem Interesse sind weiters Konsumenteninformationen, Wartelisten für Gemeindebauten, Kindergärten und Betreuungsheime − die einzelnen Belange sind äußerst vielfältig und nicht vorherzusagen.[47] Schon deshalb ist es von eminenter Bedeutung, dass prinzipiell alles Wissen des öffentlichen Sektors veröffentlicht wird. Selbstverständlich ist der Datenschutz sicherzustellen, personenbezogene Daten sind heute leicht zu anonymisieren. Andere Ausnahmen sind schwerwiegende Angelegenheiten der öffentlichen Sicherheit (wie militärische Geheimnisse, die ohnehin ausreichend geschützt sind) und laufende Verfahren (etwa polizeiliche Ermittlungen oder unangekündigte Untersuchungen; sie müssen jedenfalls nachträglich nachvollziehbar sein.)

Das wäre ein Paradigmenwechsel: Die allgemeine Publikationspflicht wird zur Regel, die allfällige Geheimhaltung im Einzelfall zur begründungsbedürftigen Abweichung. In einer Umkehrung von Begründungslast und Aufwand, die derzeit beim Antragssteller liegen, müsste dann die Behörde detailliert belegen, warum sie bestimmte Informationen nicht publizieren kann. Eine Ablehnung wäre aufwändiger als die vorgesehene Veröffentlichung und durch eine neutrale unabhängige Instanz mit Einblick in „geheime“ Dokumente zu überprüfen. Denkbar wären abgestufte Verfahren, die mehrere Instanzen und Gewalten involvieren (Rösch 1999), eine parlamentarische Kontrollkommission oder der schon erwähnte „Datenschutzhof“. Jedenfalls sind Ausnahmen im Gesetz präzise festzulegen; den Bürgerinnen muss klar sein, was warum geheimgehalten wird. Kein Bereich ist pauschal von der Informationsfreiheit auszunehmen und damit von Transparenz und demokratischer Kontrolle.

[45] So kann (neben den konkurrierenden Unternehmen) indirekt die Allgemeinheit profitieren, wenn öffentliche Genehmigungs- bzw. Vergabeverfahren tatsächlich öffentlich gemacht werden: Ausschreibungsunterlagen, wer warum den Auftrag erhält, der Vertrag und allfällige nachträgliche Änderungen – „ein hinlänglich bekanntes Einfallstor für Korruption“ (Rohde-Liebenau 2003, 118).

[46] Feik (2006a, 449 f.) nennt „Routenplaner mit Einbahnstraßen, Höhen- und Gewichtsbeschränkungen, temporalen oder sektoralen Fahrverboten, dh also mit Daten, die aus einem normalen Stadtplan nicht ablesbar sind [...] die regionale SMS-Warnung vor einem entflohenen Häftling, eine SMS-Sturmwarnung für die Seglerinnen und Segler am Bodensee, eine SMS-Stauwarnung oder eine SMS-Warnung vor einer Straßensperre nach einer Mure”.

[47] „Gefragt wurde nach einfachen Bauakten und komplexen Straßenplanungen, nach dem Wirtschaftlichkeitsgutachten einer Kurverwaltung, dem Protokoll einer Gemeindevertretersitzung, den Akten einer Tierschutzbehörde, verkehrsrechtlichen Anordnungen und dem Verkehrsgutachten für ein Gewerbegebiet, den Unterlagen über die Vergabe von Kindergartenplätzen, Ausschreibungsunterlagen und einer Stadtchronik, bei Landesbehörden u. a. nach Organisationsakten der Polizei, Lärmschutzunterlagen, Auskünften über Altlasten, Entnazifizierungsakten und der Pensenbelastung beim Oberlandesgericht“ (Bull 2005, 99).

3.4 Vision: der transparente E-Staat

Letztlich geht es essenziell um die Qualität unserer Demokratie. Denn ein Informationsfreiheitsgesetz erleichtert nicht nur den einzelnen Informationssuchenden die Verfolgung ihrer jeweiligen Interessen (Bürgerinnen, Intermediären, NGOs, Medien…). Von der Offenheit profitiert indirekt die gesamte Öffentlichkeit. Ein modernes Informationsrecht gehört zu den vordringlichsten demokratiepolitischen Maßnahmen, ist umfassende authentische Information doch der Grundstein für fundierte Meinungsbildung und Meinungsäußerung. Der öffentliche Diskurs (etwa in moderierten Online-Diskussionsforen) ist wiederum eine notwendige Voraussetzung der Mitbestimmung von Bürgerinnen und Bürgern. Die aktive staatliche Informationspflicht ist demnach ein Schritt zum aktivierenden Staat, der die Zivilgesellschaft integriert.

> „Private werden auf diese Weise, ohne im formalen Sinn die Grenzen zwischen dem administrativen Binnen- und Außenbereich zu verwischen, Teil einer als sachgerecht empfundenen Entscheidungs- oder in gewissem Sinne sogar Organisationsstruktur, die auf das Erreichen öffentlicher Zwecke zielt" (Mehde 2004, 338).

Durch diese Durchlässigkeit wird das Wissensgefälle zwischen Verwaltung und Verwalteten abgebaut. Die Transparenz von Entscheidungen eröffnet Kontrollpotenzial, zumal Mängel oft erst durch den Informationszugang entdeckt werden;[48] sie dient der Prävention von Missständen wie Datenmissbrauch und Korruption, und fördert dadurch angemessenes, effektives und zügiges Verwaltungshandeln. Die Informationsfreiheit bringt so indirekt auch Vorteile im Sinne der Verwaltungsmodernisierung: Auf Seite der Behörde könnte die zunehmende Durchsichtigkeit zur verstärkten Wahrnehmung der „Außenwelt" beitragen. Die lernfähige Verwaltung erfährt (aus Zugriffen, Feedback, etc.), welche Informationen für ihre Kundinnen relevant bzw. welche noch nicht ausreichend zugänglich sind.[49] Durch diesen positiven Rückkopplungseffekt könnte die Publikationspflicht als ein integraler Bestandteil das verbesserungsfähige[50] interne Wissensmanagement unterstützen. Dies führt im Idealfall zum „Impuls, über die ordnungsmäßige Abwicklung des Verfahrens hinaus nach weiterem Nutzen zu suchen. Oft stehen Daten nur dort zur Verfügung, wo sie ursprünglich erhoben wurden, obwohl sie in anderen Verwaltungsbereichen ebenfalls produktiv genutzt werden könnten."[51] Wird die Informationsbereitstellung als genuine Verwaltungsaufgabe begriffen und ‚öffentlicher Dienst' beim Wort genommen, als öffentliches Service für die Öffentlichkeit, dann unterstützt diese Auffassung den klimatischen Mentalitätswechsel vom statischen Beamtentypus zum dynamischen Verwaltungsmanager (Makolm, Wimmer, Parycek 2005).

Geboten ist also ein modernes, verfassungsrechtlich gewährleistetes Informationsrecht mit aktivem Publikationsgebot und Recht auf elektronische Akteneinsicht. Der Staat soll seine Informationen

[48] Z. B. konnte so 2002 die irrtümliche Patentierung menschlicher Stammzellen verhindert werden (Redelfs 2003, 104). Er schildert auch die rührend aufrichtige Reaktion eines Ministeriums, das zugibt, die obligatorischen Störfallmeldungen gar nicht zu kennen, und seinerseits den Anfragenden um Hinweise bittet.

[49] Das wäre die Umkehrung des unter der Auskunftspflicht herrschenden Status quo: „Selbst potentiell vorhandenes Wissen verpflichtet dann nicht zur Auskunftserteilung, wenn es mit unvertretbarem Aufwand verbunden wäre, die nötigen Daten aufzufinden bzw. zusammenzutragen; dass die Ursache hierfür in den konkreten Gegebenheiten der Verwaltungsorganisation liegt, schadet nicht" (Janko 2003, 28).

[50] Dearing beklagt „oft fehlende Durchlässigkeit von Informationen innerhalb von Ministerien und Dienststellen, die Informationen bleiben bei den Führungskräften hängen, ein funktionierendes Wissensmanagementsystem gibt es kaum" (Verwaltung Innovativ, 12.04.2006, 11).

[51] Beyer (2004, 381 ff.) schlägt deshalb vor, Elemente aus dem Behörden-Intranet ins externe Internetangebot einzubauen: „die Qualität der öffentlichen Angebote wird steigen, wenn sie von möglichst vielen eigenen Mitarbeitern immer wieder gesehen, genutzt und damit auch getestet werden. Zugleich nimmt der Kreis der Personen zu, die fähig und bereit sind, Beiträge zur Pflege und Weiterentwicklung dieser Angebote zu leisten."

digitalisiert und strukturiert online stellen, mit der unersetzlichen Metainformation: ‚Wo ist was wie zu finden?' Verschiedenste Lösungen stehen hier zur Verfügung, etwa Ontologien als Basis, alphabetische und thematische Indices oder eine Public-Sector-Suchmaschine, Kunden-Feedbackschleifen (mit verstärkten Vorinformationsmöglichkeiten bei festgestellten Informationsdefiziten) etc. Angebracht wären zusätzlich Hinweise, die z. B. die Herkunft, Entstehung und Rechtswirkungen der Daten bzw. Dokumente erklären.

In Zusammenarbeit aller Ebenen können konsolidierte Lösungen entwickelt werden, die sowohl verfassungskonform mit Föderalismus und Gewaltenteilung im Einklang stehen, als auch im Sinne des serviceorientierten One-Stop-Government die einzelnen NutzerInnen ins Zentrum stellen. Für ein zielgruppengerecht strukturiertes Portal empfiehlt sich das Lebenslagenmodell, an die jeweiligen User adaptiert: BürgerInnen und Unternehmen erhalten auch Zugang zu ihren eigenen Daten (Steuer- und Pensionskonto etc., Intermediäre wie AnwältInnen oder SteuerberaterInnen auf die Online-Accounts ihrer KlientInnen). Also nicht (nur) die Verwaltung, sondern die BürgerInnen verwalten ihren Datenpool selbst.

Bei der Verwirklichung ist der Datenschutz ebenso sicherzustellen wie der Informationszugang für alle.[52] Gerade jetzt eröffnen innovative E-Government-Projekte die Chance, neue Systeme auf ein modernes Informationsrecht mit erhöhter Transparenz auszurichten.[53] Letztendlich führen durchgehende elektronische Vernetzung und Informationsdurchlässigkeit zum transparenten E-Staat.

[52] Im Sinne der „E-Inclusion" sind zielgruppengerechte Lösungen und Erklärungen bereitzustellen; die „digitale Kluft" erfordert Mehrkanallösungen wie (aus)gedruckte Informationen und Dokumenteneinsicht in den Amtsräumen mithilfe von Verwaltungsbediensteten. Für Vorschläge zum Datenschutz vgl. Schäfer (2003, 139 f.).

[53] Die elektronische Aktenführung ermöglicht unaufwändig die separate Verarbeitung sensibler Daten und Schnittstellen zu Content-Management-Systemen bzw. Internet. Die Publikationspflicht verursacht so kaum Mehrkosten und macht zudem viele potenzielle Anfragen und Anträge auf Akteneinsicht obsolet.

4 Ausblick

Bei der rasanten technischen Beschleunigung sind alle Prognosen unzuverlässig. Mit hoher Wahrscheinlichkeit werden in Zukunft fast unbeschränkte Speicherkapazität, unbegrenzte Übertragungsreichweite und vollständige Vernetzung möglich und voraussichtlich wird der Staat verstärkt biometrische Daten und RFID-Technologie (Radio Frequency Identification) verwenden. Schon jetzt wird Biometrie als Zugangskontrolle[54] und v. a. zur Identifikation eingesetzt: seit Jahrhunderten in der Strafverfolgung, heute in DNA-Datenbanken und den EU-Reisepässen. RFID-Chips findet sich z. B. auf der 'edu.card'[55]; und seit 2004 erhalten Wiener Hunde verpflichtend einen Chip unter die Haut implantiert, womit sich über das Hunderegister im Bedarfsfall die Besitzerin ermitteln lässt. Die spezifischen Herausforderungen beim derzeit diskutierten E-Voting liegen in der Sicherstellung des geheimen und freien Wahlrechts.[56] Welchen technischen und gesellschaftlichen Entwicklungen die Zukunft gehört, ob verstärkter Auswertung genetischer Daten, Pervasive Computing bis zu unsichtbaren Lügendetektoren (Čas 2005) oder gar futuristisch anmutende Gehirn-Scans in der Strafverfolgung… Maßgeblich sind in jedem Fall das Ausloten alternativer Gestaltungsoptionen und wirksame Kontrollmechanismen.

Sind wir auf dem Weg zum gläsernen Bürger? Beim transparenten Staat stehen wir erst am Anfang des Weges. Der öffentliche Sektor agiert zwischen Informationsdefizit und -überschuss, Sicherheit und Freiheit, Datenschutz und Transparenz, zwischen den komplementären Menschenrechten Schutz der Privatsphäre (Art. 8 EMRK) und Informations- bzw. Meinungsfreiheit (Art. 10). Dieses dialektische Spannungsverhältnis ist breit zu diskutieren und durch rechtliche, soziopolitische und technische Maßnahmen auszubalancieren. Als verbindendes Prinzip lässt sich das informationelle Selbstbestimmungsrecht sehen; sowohl auf individueller Ebene (der Einzelne als Souverän seiner Daten) als auch auf staatlicher (das Volk als Souverän des öffentlichen Wissens). In einem liberalen Rechtsstaat bildet es die Voraussetzung für (E-)Demokratie und (E-)Government: bürgernah, datenschutzgerecht und transparent.

[54] So wurden in Justizanstalten Gesichtserkennungssysteme installiert, um das Betreten und Verlassen zu überprüfen (vgl. http://futurezone.orf.at/it/stories/83820/).

[55] Das Pilotprojekt „gewann" (ohne überzeugende Begründung) den Big-Brother-Award 2006: http://www.bigbrotherawards.at/2006/Preistraeger.

[56] Status quo ist teils die elektronische Beantragung von Wahlkarten (vgl. http://steiermark.orf.at/stories/139343/).

5 Literatur

Aichholzer, G., Tang, P. (2004): Harnessing public sector information for greater accessibility – Austria and the UK. In: G. Aichholzer, H. Burkert (Hg.): Public Sector Information in the Digital Age − Between Markets, Public Management and Citizens' Rights, Cheltenham, Northampton: Edward Elgar, 275-286.

Aichholzer, G., Spitzenberger, M. (2005): Anwendungsfelder für Wissensmanagement im E-Government. In: J. Makolm, M. Wimmer (Hg.): Wissensmanagement in der öffentlichen Verwaltung – Konzepte, Lösungen und Potentiale, Wien: OCG − Oesterreichische Computer Gesellschaft, 105-116.

Beyer, L. (2004): Aus dem Aktenkeller in die Wissensspirale – Brauchen öffentliche Verwaltungen ein neues Wissensmanagement? In: P. Collin, T. Horstmann (Hg.): Das Wissen des Staates − Geschichte, Theorie und Praxis, Baden-Baden: Nomos, 361-387.

BKA (1997): Österreichisches Bundeskanzleramt: Datenschutzbericht; http://www.dsk.gv.at/Datenschutzbericht1997.pdf.

Bull, H.P. (2005): Datenschutz, Informationsrecht und Rechtspolitik – Gesammelte Aufsätze, Berlin: Duncker & Humblot.

Čas, J. (2005): Privacy in einer Zukunft mit allgegenwärtigen Informationstechnologien – Ein Widerspruch in sich? In: M. Nentwich, W. Peissl (Hg.): Technikfolgenabschätzung in der österreichischen Praxis, Wien: ÖAW − Österreichische Akademie der Wissenschaften, 91-112.

Dix, A. (2002): Informationszugang und politische Mitgestaltung in der elektronischen Demokratie In: K. P. Möller, F. von Zezschwitz: Verwaltung im Zeitalter des Internet, Baden-Baden: Nomos, 85-95.

DSK (2005): Österreichische Datenschutzkommission: Datenschutzbericht – 1. Jänner 2002 bis 30. Juni 2005; http://www.dsk.gv.at/Datenschutzbericht2005.pdf.

Feik, R. (2006a): Zugang zu Informationen als Voraussetzung für Content-Produkte, ÖJZ − Österreichische Juristen-Zeitung 06/28, 449-454.

Feik, R. (2006b): Zugang zu Verwaltungswissen, ZfV – Zeitschrift für Verwaltung 06/330, 187-195.

Forgó, N. (2003): e-Mail und elektronische Signatur. In: IT-LAW.AT (Hg.): E-Mail − elektronische Post im Recht, Wien: Manz, 13-28.

Funk, B.-C. (2006): Schutzzonen und Bildaufzeichnung − Sicherheits-Placebo oder Dammbruch zum Überwachungsstaat? In: Österreichische Juristenkommission (Hg.): Sicherheit im öffentlichen Raum, Wien, Graz: NWV − Neuer Wissenschaftlicher Verlag, 10-21.

Hart, T., Welzel, C., Garstka, H. (2004): Informationsfreiheit − Die ‚gläserne Bürokratie' als Bürgerrecht, Gütersloh: Bertelsmann Stiftung.

Hof, S. (2005): Alternative Security Approaches in E-Government, Linz: Trauner − zugl. Diss., Univ. Linz.

Jahnel, D. (2006): Das Grundrecht auf Datenschutz nach dem DSG 2000. In: M. Akyürek et al. (Hg.): Staat und Recht in europäischer Perspektive, Wien: Manz, C.H.Beck, 313-341.

Janko, A. (2003): Auskunftspflichten im österreichischen öffentlichen Recht. In: A. Hauer (Hg.): Die Verwaltung zwischen Verschwiegenheit und Transparenz, Linz: Trauner, 1-31.

Karning, B. (2004): Rechtliche Aspekte des E-Government in Österreich, Berlin: WiKu.

Kunnert, G. (2006): Die abschnittsbezogene Geschwindigkeitsüberwachung (Section Control) aus datenschutzrechtlicher Sicht, ZVR − Zeitschrift für Verkehrsrecht, 06/17, 78-88.

Liebwald, D. (2006): The New Data Retention Directive, MR-Int – Medien und Recht International 1/06, 49-56.

Makolm, J., Wimmer, M., Parycek, P. (2005): Zielsetzung und Motivatoren für Wissensmanagement in der öffentlichen Verwaltung. In: J. Makolm, M. Wimmer (Hg.): Wissensmanagement in der öffentlichen Verwaltung – Konzepte, Lösungen und Potentiale, Wien: OCG − Oesterreichische Computer Gesellschaft, 3-18.

Matscher, F. (2004): Die erweiterte Gefahrenerforschung aus der Sicht des Rechtsschutzbeauftragten im BM.I. In: BMI (Hg.): Terror – Prävention – Rechtsschutz. Wien, Graz: NWV − Neuer Wissenschaftlicher Verlag, 59-70.

Mayer-Schönberger, V., Brandl, E.O. (2006): Datenschutzgesetz − Grundsätze und europarechtliche Rahmenbedingungen, Wien: Linde.

Mehde, V. (2004): Rechtliche Deutungsmuster des Wissensgefälles zwischen Politik und Verwaltung. In: P. Collin, T. Horstmann (Hg.): Das Wissen des Staates − Geschichte, Theorie und Praxis, Baden-Baden: Nomos, 335-359.

Meltzian, D. (2004): Das Recht der Öffentlichkeit auf Zugang zu Dokumenten der Gemeinschaftsorgane, Berlin: Duncker & Humblot.

Morscher, S., Christ, P. (2005): Öffentliche Bücher, Evidenzen, Listen, Register, Verzeichnisse; ZfV – Zeitschrift für Verwaltung 05/267, 158-175.

Oberndorfer, P. (2006): Die Verwaltung im politisch-gesellschaftlichen Umfeld. In: G. Holzinger, P. Oberndorfer, B. Raschauer (Hg.): Österreichische Verwaltungslehre, Wien: Verlag Österreich.

ÖJK (2005): Podiumsdiskussion − Grundrechte in Gefahr? In: ÖJK − Österreichische Juristenkommission (Hg.): Aktuelle Fragen des Grundrechtsschutzes. Wien, Graz: NWV − Neuer Wissenschaftlicher Verlag, 227-266.

ÖJK (2006): Diskussionsbeiträge. In: ÖJK − Österreichische Juristenkommission (Hg.): Sicherheit im öffentlichen Raum, Wien, Graz: NWV − Neuer Wissenschaftlicher Verlag, 44-66.

Peissl, W. (2003): Privacy in Österreich − Eine Bestandsaufnahme. In: W. Peissl (Hg.): Privacy − Ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte, Wien: ÖAW − Österreichische Akademie der Wissenschaften.

Pernthaler, P. (2004): Österreichisches Bundesstaatsrecht – Lehr- und Handbuch, Wien: Verlag Österreich.

Redelfs, M. (2003): Umweltschutz durch Informationszugang – Erfahrungen mit dem Umweltinformationsgesetz (UIG). In: M. Kloepfer (Hg.): Die transparente Verwaltung − Zugangsfreiheit zu öffentlichen Informationen, Berlin: Duncker & Humblot, 85-108.

Reichmann, G. (2004): Das Auskunftsrecht nach dem Datenschutzgesetz 2000 – Eine Fallstudie, ZfV – Zeitschrift für Verwaltung 1529/04, 752-757.

Rohde-Liebenau, B. (2003): Korruptionsprävention durch Informationszugang. In: M. Kloepfer (Hg.): Die transparente Verwaltung − Zugangsfreiheit zu öffentlichen Informationen, Berlin: Duncker & Humblot, 109-122.

Rösch, U. (1999): Geheimhaltung in der rechtsstaatlichen Demokratie − Demokratietheoretische Überlegungen zum Informationsverhältnis zwischen Staat und Bürger sowie zwischen den Staatsgewalten, Baden-Baden: Nomos.

Schäfer, G. (2003): Sicherheitsbelange eines Electronic Government. In: A. Roßnagel (Hg.): Sicherheit für Freiheit? Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft, Baden-Baden: Nomos, 135-141.

Simitis, S. (2004): Der verkürzte Datenschutz − Versuch einer Korrektur der Defizite und Diskrepanzen im justitiellen und Sicherheitsbereich der Europäischen Union, Baden-Baden: Nomos.

Souhrada, J. (2004): Sozialversicherungsdaten in der staatlichen Verwaltung. In: R. Traunmüller et al. (Hg.): Von der Verwaltungsinformatik zum E-Government – FS Arthur Winter, Wien: ADV − Arbeitsgemeinschaft für Datenverarbeitung.

Thom, N., Ritz, A. (2006): Public Management – Innovative Konzepte zur Führung im öffentlichen Sektor, Wiesbaden: Gabler.

Westphal, D. (2006): Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, Juridikum 06/1, 34-42.

Wiederin, E. (2003): Privatsphäre und Überwachungsstaat − sicherheitspolizeiliche und nachrichtendienstliche Datenermittlungen im Lichte des Art 8 EMRK und der Art 9-10a StGG, Wien: Manz.

Zwettler, E. (2004): Videoüberwachung in der kriminalpolizeilichen Praxis. In: BMI (Hg.): Videoüberwachung zu sicherheits- und kriminalpolizeilichen Zwecken. Wien, Graz: NWV − Neuer Wissenschaftlicher Verlag.

Bisher erschienene manu:scripte

ITA-01-01 Gunther Tichy, Walter Peissl (12/2001): Beeinträchtigung der Privatsphäre in der Informationsgesellschaft. <http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf>

ITA-01-02 Georg Aichholzer(12/2001): Delphi Austria: An Example of Tailoring Foresight to the Needs of a Small Country. <http://www.oeaw.ac.at/ita/pdf/ita_01_02.pdf>

ITA-01-03 Helge Torgersen, Jürgen Hampel (12/2001): The Gate-Resonance Model: The Interface of Policy, Media and the Public in Technology Conflicts. <http://www.oeaw.ac.at/ita/pdf/ita_01_03.pdf>

ITA-02-01 Georg Aichholzer (01/2002): Das ExpertInnen-Delphi: Methodische Grundlagen und Anwendungsfeld „Technology Foresight". <http://www.oeaw.ac.at/ita/pdf/ita_02_01.pdf>

ITA-02-02 Walter Peissl (01/2002): Surveillance and Security – A Dodgy Relationship. <http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf>

ITA-02-03 Gunther Tichy (02/2002): Informationsgesellschaft und flexiblere Arbeitsmärkte. <http://www.oeaw.ac.at/ita/pdf/ita_02_03.pdf>

ITA-02-04 Andreas Diekmann (06/2002): Diagnose von Fehlerquellen und methodische Qualität in der sozialwissenschaftlichen Forschung. <http://www.oeaw.ac.at/ita/pdf/ita_02_04.pdf>

ITA-02-05 Gunther Tichy (10/2002): Over-optimism Among Experts in Assessment and Foresight. <http://www.oeaw.ac.at/ita/pdf/ita_02_05.pdf>

ITA-02-06 Hilmar Westholm (12/2002): Mit eDemocracy zu deliberativer Politik? Zur Praxis und Anschlussfähigkeit eines neuen Mediums. <http://www.oeaw.ac.at/ita/pdf/ita_02_06.pdf>

ITA-03-01 Jörg Flecker und Sabine Kirschenhofer (01/2003): IT verleiht Flügel? Aktuelle Tendenzen der räumlichen Verlagerung von Arbeit. <http://www.oeaw.ac.at/ita/pdf/ita_03_01.pdf>

ITA-03-02 Gunther Tichy (11/2003): Die Risikogesellschaft – Ein vernachlässigtes Konzept in der europäischen Stagnationsdiskussion. <http://www.oeaw.ac.at/ita/pdf/ita_03_02.pdf>

ITA-03-03 Michael Nentwich (11/2003): Neue Kommunikationstechnologien und Wissenschaft – Veränderungspotentiale und Handlungsoptionen auf dem Weg zur Cyber-Wissenschaft. <http://www.oeaw.ac.at/ita/pdf/ita_03_03.pdf>

ITA-04-01 Gerd Schienstock (1/2004): Finnland auf dem Weg zur Wissensökonomie – Von Pfadabhängigkeit zu Pfadentwicklung. <http://www.oeaw.ac.at/ita/pdf/ita_04_01.pdf>

ITA-04-02 Gunther Tichy (6/2004): Technikfolgen-Abschätzung: Entscheidungshilfe in einer komplexen Welt. <http://www.oeaw.ac.at/ita/pdf/ita_04_02.pdf>

ITA-04-03 Johannes M. Bauer (11/2004): Governing the Networks of the Information Society – Prospects and limits of policy in a complex technical system. <http://www.oeaw.ac.at/ita/pdf/ita_04_03.pdf>

ITA-04-04 Ronald Leenes (12/2004): Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality. <http://www.oeaw.ac.at/ita/pdf/ita_04_04.pdf>

ITA-05-01 Andreas Krisch (01/2005): Die Veröffentlichung des Privaten – Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip. <http://www.oeaw.ac.at/ita/pdf/ita_05_01.pdf>

ITA-05-02 Petra Grabner (12/2005): Ein Subsidiaritätstest – Die Errichtung gentechnikfreier Regionen in Österreich zwischen Anspruch und Wirklichkeit. <http://www.oeaw.ac.at/ita/pdf/ita_05_02.pdf>

ITA-05-03 Eva Buchinger (12/2005): Innovationspolitik aus systemtheoretischer Sicht – Ein zyklisches Modell der politischen Steuerung technologischer Innovation. <http://www.oeaw.ac.at/ita/pdf/ita_05_03.pdf>

ITA-06-01 Michael Latzer (06/2006): Medien- und Telekommunikationspolitik: Unordnung durch Konvergenz – Ordnung durch Mediamatikpolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_01.pdf>

ITA-06-02 Natascha Just, Michael Latzer, Florian Saurwein (09/2006): Communications Governance: Entscheidungshilfe für die Wahl des Regulierungsarrangements am Beispiel Spam. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_02.pdf>

ITA-06-03 Veronika Gaube, Helmut Haberl (10/2006): Sozial-ökologische Konzepte, Modelle und Indikatoren nachhaltiger Entwicklung: Trends im Ressourcenverbrauch in Österreich. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_03.pdf>

ITA-06-04 Maximilian Fochler, Annina Müller (11/2006): Vom Defizit zum Dialog? Zum Verhältnis von Wissenschaft und Öffentlichkeit in der europäischen und österreichischen Forschungspolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_04.pdf>

ITA-06-05 Holger Floeting (11/2006): Sicherheitstechnologien und neue urbane Sicherheitsregimes. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_05.pdf>

ITA-06-06 Armin Spök (12/2006): From Farming to "Pharming" – Risks and Policy Challenges of Third Generation GM Crops. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_06.pdf>

ITA-07-01 Volker Stelzer, Christine Rösch, Konrad Raab (3/2007): Ein integratives Konzept zur Messung von Nachhaltigkeit – das Beispiel Energiegewinnung aus Grünland. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_01.pdf>

ITA-07-02 Elisabeth Katzlinger (3/2007): Big Brother beim Lernen: Privatsphäre und Datenschutz in Lernplattformen. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_02.pdf>

ITA-07-03 Astrid Engel, Martina Erlemann (4/2007): Kartierte Risikokonflikte als Instrument reflexiver Wissenspolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_03.pdf>

ITA-07-04 Peter Parycek (5/2007): Gläserne Bürger − transparenter Staat? Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_04.pdf>