Stefan Strauß

Datenschutzimplikationen staatlicher Identitätsmanagement-Systeme

Fallbeispiel Österreich

Identitätsmanagement (IDM) gewinnt auch im staatlichen Kontext an Bedeutung. Der Beitrag befasst sich mit der Einführung nationaler IDM-Systeme und den möglichen Folgen für den Schutz der Privatsphäre. Neben grundlegenden Datenschutz-Anforderungen werden wesentliche Merkmale des österreichischen Systems erläutert und daraus datenschutzrelevante Aspekte abgeleitet.

Einleitung

Seit einigen Jahren ist ein globaler Trend im Bereich elektronisches IDM erkennbar. Zahlreiche Staaten sind im Begriff, elektronische Identitätsmanagementsysteme (eIDMS) auf Basis digitaler Ausweise in Form von Chipkarten (eID-Cards) einzuführen bzw. haben dies bereits getan [vgl. Aro08; CEN04]. Auf europäischer Ebene wird die Implementierung eines europaweit einheitlichen eIDMS als Schlüsselfaktor für die Nutzung von elektronischen Behördendiensten betrachtet [EUK06]. Die eID dient idR. zumindest zwei Funktionen: Der eindeutigen Identifizierung einer Person und der Bekundung ihres Willens für die Nutzung von Online-Transaktionen (Authentifizierung). Vordergründig geht es dabei um die Stärkung sicherer und vertrauenswürdiger Interaktion mit der öffentlichen Verwaltung (E-Government). Zudem sollen die Systeme im elektronischen Geschäftsverkehr (E-Commerce) zum Einsatz kommen, um die Sicherheit zu erhöhen und neue Geschäftsmodelle zu ermöglichen. Bestehende IDM-Ansätze basieren derzeit – je nach Dienst – meist auf sehr unterschiedlichen Technologien (Konzepten, Standards, etc.).

Mag. Stefan Strauß,

Wirtschaftsinformatiker, Institut für Technikfolgenabschätzung, Österreichische Akademie der Wissenschaften. Aktuelle Arbeitsschwerpunkte: E-Governance, Identitätsmanagement und Datenschutz, elektronische Demokratie.
E-Mail: sstrauss@oeaw.ac.at

Pläne zur Einführung von eIDMS bezwecken daher u. a., die für den Prozess der Identitätsfeststellung erforderlichen Abläufe stärker zu vereinheitlichen. Als Basis-Technologie setzen die meisten nationalen eIDMS Chipkarten ein, die gewissermaßen als „missing link" fungieren und in diesem Bereich zum Quasi-Standard wurden. Neben ihrer weiten Verbreitung im Alltag (EC-Karte, Kreditkarte usw.) ist das nicht zuletzt auf die verschiedenen Smartcard-Initiativen[1] zur Realisierung einer einheitlichen Infrastruktur (OSCIE[2]) zurückzuführen.

Chipkarten erlauben die Kombination von *Besitz* (Karte) und *Wissen* (PIN-Code) des Inhabers, wodurch ein höheres Sicherheitsniveau erzielt werden kann als bei den derzeit überwiegenden Konzepten, die nur auf Wissen (Benutzername/Passwort) basieren [SW08]. Dies erscheint daher grundsätzlich zweckmäßig, um Sicherheit und Rechtsverbindlichkeit von Anwendungen zu verbessern. Als weitere Gründe für die Entwicklung einer nationalen eID bzw. längerfristig einer europaweit interoperablen eID gelten die Bekämpfung von Identitätsbetrug und Terrorismus [CEN04]. Ein Teilziel des EU-Aktionsplans „i2010" im Kontext eID ist etwa „the Assertion of the authenticity of online identity (one safeguard against identity fraud): Easier ownership and management of personal/business data (…)" [EUK06]. Ein Grund hierfür liegt in der verzeichneten Zunahme potenzieller Bedrohungen durch Internet-Kriminalität (z. B. verschiedene Formen von Identitätsdiebstahl) als Folge der Verbreitung von IKT. Etwa sei in den letzten Jahren ein sprunghafter Anstieg von Phishing-Versuchen zu beobachten [OECD08]. Vor diesem Hintergrund gilt die Schaffung eines eIDMS auch als Maßnahme, um diesem erhöhten Gefahrenpotenzial entgegenzuwirken.

Dementsprechend lassen sich zwei grundlegende Ziele für die Einführung eines nationalen eIDMS nennen: Die Vereinheitlichung von Identifizierungsprozessen und die Erhöhung der Sicherheit von Online-Diensten. Datenschutz und -sicherheit, Schutz der Privatsphäre und informationelle Selbstbestimmung sind dabei grundsätzlich von zentraler Bedeutung. Wie und in welchem Ausmaß diese Aspekte berücksichtigt werden, hängt naturgemäß von der konkreten Gestaltung des Systems und der entsprechenden Rahmenbedingungen ab. Dieser Beitrag[3] geht näher auf diese Aspekte ein und fragt nach möglichen Folgen, die nationale eIDMS

1 Z. B. www.smartis.org, www.eurosmart.com
2 Open Smart Card Infrastructure for Europe

3 Diese Arbeit knüpft an Ergebnisse einer Länderstudie über den Einführungsprozess des österreichischen Systems an.

für den Schutz der Privatsphäre mit sich bringen. Nach einer kurzen Erläuterung von IDM im Datenschutzkontext werden Grundcharakteristika des österreichischen eIDMS erklärt, um im Anschluss mögliche Auswirkungen für den Datenschutz durch ein solches System zu skizzieren.

1 Datenschutz-Relevanz von IDM

Allgemein wird IDM als „representation, collection, storage and use of identity information" definiert [LP08]. „Privacy-enhancing identity management" ist ein Konzept, das Privatsphäre und Authentizität kombiniert [CPHH05]. Das impliziert natürlich die Wahrung fundamentaler Datenschutzprinzipien (Verhältnismäßigkeit, Zweckbindung, Datensparsamkeit, Transparenz etc.) als grundsätzliche Voraussetzung für die informationelle Selbstbestimmung [vgl. Deh08; RBBN08].

Konkret sind u. a. folgende Aspekte bei Privatsphäre-unterstützendem IDM von zentraler Bedeutung: Nutzerzentrierung und die weitgehende Kontrolle der betroffenen Person über ihre Identität(en) (bzw. personenbezogenen Daten). Benutzer sollen weitgehend selbst kontrollieren können, welche Daten sie preis geben und in welchen unterschiedlichen Kontexten diese Daten verwendet und verkettet werden dürfen. In jenen Bereichen, wo dies nicht möglich ist, sollte zumindest für sie nachvollziehbar dargestellt sein, welche Stellen auf welcher Grundlage und zu welchem Zweck personenbezogene Daten verarbeiten [vgl. Deh08; HKRG03; CPHH05].

Im alltäglichen Leben werden Individuen i. d. R. nicht durch eine „universale" Identität repräsentiert, sondern durch mehrere unterschiedliche Teilidentitäten für verschiedene Zwecke. „There is no such thing as ‚the identity' but several of them" [PH08]. Allerdings besteht die Tendenz, diesen Umstand zu übersehen [Sch03]. Die Bündelung zu einer zentralen Identität wäre problematisch, da Betroffene in ihrem Recht auf informationelle Selbstbestimmung eingeschränkt wären, wonach jedes Individuum selbst über Preisgabe und Verwendung ihrer persönlichen Daten bestimmen darf.

Datenschutzkonformes IDM schließt daher auch die Verwaltung von kontextbezogenen Teilidentitäten mit ein. Benutzer sollen demnach je nach Erfordernis verschiedene Rollen respektive Teilidentitäten verwenden können, über die nur die jeweils unbedingt für den Kontext erforderlichen Daten verarbeitet werden. Damit verbunden ist die anonyme und pseudonyme Nutzung. Im Zusammenhang mit staatlichem eIDMS ließe sich daraus schließen, in jenen Bereichen, wo keine Identifizierung nötig oder Anonymität sogar geboten ist, das System gar nicht einzusetzen. In Hinblick auf die Tendenz zu einem „Ubiquitous Computing", das potenziell einen deutlichen Rückgang von anonymen Bereichen bedeutet [vgl. Roß06; RBBN08], greift dieser Schluss mitunter jedoch zu kurz. Es erscheint daher zweckmäßig, die Möglichkeit zur anonymen Nutzung als fixen Bestandteil in das eIDMS zu integrieren.

Eine große Bedrohung für die Privatsphäre des einzelnen stellt die Verkettung von personenbezogenen Daten zur Erstellung umfassender Profile dar, die insbesondere aus der Verwendung eindeutiger Personenkennzeichen resultiert. Unverkettbarkeit („unlinkability") ist daher eine entscheidende Eigenschaft, die gegeben sein muss, um den Schutz der Privatsphäre zu gewährleisten [FIDIS07]. Die Umsetzung der Unverkettbarkeit authentifizierter Daten ist nur dann möglich, wenn Benutzer im eIDMS die Möglichkeit haben, verschiedene Pseudonyme zu verwenden, die selbst nicht verkettbar sind [CPHH05].

Das impliziert eine Trennung in unterschiedliche Bereiche und die Vermeidung eines für alle Bereiche eindeutigen Personenkennzeichens. Um „privacy-destroying linkage and aggregation of identity information across data contexts" zu verhindern, sollten daher für jeden Bereich unterschiedliche Identifikatoren in Form von lokalen Pseudonymen eingesetzt werden [vgl. RBBN08].

Eng mit der Unverkettbarkeit verbunden ist die Wichtigkeit einer dezentralen Datenhaltung sowie der Separierung unterschiedlicher Kontexte. Identitätsdaten sollen demnach in so viele Bereiche wie sinnvoll möglich getrennt werden, um eine Daten-Verkettung verhindern zu können [RBBN08]. Dem Grundsatz der Datensparsamkeit entsprechend sollen dabei jeweils nur unbedingt erforderliche Daten verarbeitet werden.[4] Es gilt daher, nicht unbedingt nötige zusätzliche Informationen zu vermeiden, die eine Verkettung „über Umwege" ermöglichen (z. B. Name, Geburtsdatum, Adresse).

In Summe bedeutet privacy-enhancing IDM eine Förderung der informationellen Selbstbestimmung, die Benutzern die Steuerung und Darstellung der Verwendung ihrer personenbezogenen Daten unterstützt und ihnen mehr Transparenz (im Sinne von Nachvollziehbarkeit) im Hinblick auf die Verwendung ihrer Daten bietet [HKRG03].

2 eIDM in Österreich

Österreich war eines der ersten europäischen Länder, das ein eIDMS für die Verwendung im E-Government eingeführt hat. Das Kernstück des Systems bildet die sog. Bürgerkarte (BK), die zwei zentrale Funktionen vereint: Als elektronisches Ausweisdokument ermöglicht sie die Identifizierung der betroffenen Person und die elektronische Signatur dient zur Leistung einer rechtsgültigen Unterschrift (Authentifizierung). Eine Zusatzfunktion ist die Verschlüsselung von Inhalten (Dokumenten, E-Mails etc.). Die BK selbst ist keine spezifische Chipkarte, wie die Bezeichnung vermuten lässt, sondern ein virtuelles Konzept, das weitgehend technologie-neutral ist und prinzipiell auf verschiedenen Trägermedien angebracht werden kann. Das können neben gängigen Chipkarten wie z. B. EC-Karten, Kreditkarten, Studenten-/Dienst-Ausweisen usw. auch Mobiltelefone oder USB-Geräte sein. Aufgrund ihrer weiten Verbreitung wurden jedoch (seit 2005) die elektronische Sozialversicherungskarte (eCard) und die EC-Karte zu den Hauptträgermedien. Für die Nutzung als BK bedarf es zunächst der Aktivierung durch den Karteninhaber bei einer Registrierungsstelle, wobei die nötigen Komponenten (Signatur-Zertifikat und Personenbindung) auf der Karte gespeichert werden. Die Nutzung selbst erfordert einen Card-Reader und eine spezielle Software – die sog. Bürgerkartenumgebung (BKU). Diese gibt es in verschiedenen Varianten (meist kostenfrei) und seit 2008 auch als reine Online-Anwendung ohne lokalen Installationsbedarf.

2.1 System-Infrastruktur

Die Verwendung der e-Signatur beruht auf asymmetrischer Verschlüsselung (Pu-

4 Beispielsweise erfordert eine Altersüberprüfung keine Kenntnis des Geburtsdatums. Es genügt eine Abfrage, ob es über oder unter einem bestimmten Referenzdatum liegt.

blic Key Infrastruktur). Die Identifizierungsfunktion basiert auf dem Zentralen Melderegister (ZMR), das die Daten aller in Österreich meldepflichtigen Personen beinhaltet. Welche Daten auf der BK gespeichert sind, hängt vom Trägermedium ab. Jede BK beinhaltet aber zumindest folgende Daten des Karteninhabers: Vor- und Zuname, Geburtsdatum, die sog. Stammzahl als Identifikator und je einen öffentlichen Schlüssel für Signaturfunktion und Inhaltsverschlüsselung. Diese Daten befinden sich in einer eigenen XML-basierten Datenstruktur, der sogenannten Personenbindung. Die privaten Schlüssel sind getrennt davon in einem eigenen Bereich auf dem Chip der Karte gespeichert, der nur über korrekte PIN-Eingabe zugänglich ist. Kernelement der Personenbindung ist die Stammzahl (SZ), eine verschlüsselte Variante der ZMR-Zahl, die ein einheitliches Identifizierungsmerkmal für jede Person im ZMR darstellt. Alle technischen Vorgänge zur Erzeugung und Verarbeitung der elektronischen Identität finden im sog. Stammzahlenregister (SZR) statt, einem rein virtuellen, an das ZMR gekoppelten Datenverbund. Daten werden im SZR also nur im Bedarfsfall erzeugt und nicht dauerhaft gespeichert. Die Datenschutzkommission verwaltet das SZR in ihrer Funktion als Stammzahlenregisterbehörde (SZRB), wobei die technischen Abläufe vom Bundesministerium für Inneres (BMI) als Dienstleister der SZRB erbracht werden [BKA08, AS09].

2.2 Bereichsspezifische Personenkennzeichen

Da die SZ dennoch ein einheitliches Personenkennzeichen darstellt, wird sie nicht direkt zur Identifikation verwendet. Stattdessen werden sog. bereichsspezifische Personenkennzeichen (bPK) generiert, die für eine definierte Anzahl von Bereichen (derzeit 26) jeweils unterschiedlich sind und die keine Rückschlüsse auf die SZ ermöglichen. Die Erzeugung ist zulässig, wenn die eindeutige Identifikation notwendig ist. Ein bPK darf nur innerhalb des Bereichs verwendet werden, für den es erzeugt wurde und nur von jenen Stellen, die rechtlich determiniert in diesem Bereich agieren.

Die Generierung von bPK kann auch ohne BK des Betroffenen erfolgen. Dazu werden Daten der betroffenen Person (Name, Geburtsdatum) benötigt. Bei behördenübergreifenden Verfahren dürfen bPK (im anfordernden Bereich) nur verschlüsselt verarbeitet werden (sog. Fremd-bPK). Um den Aufwand bei der Verwendung von bPK zu verringern, besteht für Behörden auch die Möglichkeit, die Kennzeichen auf Vorrat zu berechnen und zu speichern.

Für den Einsatz im privatwirtschaftlichen Bereich (E-Commerce) werden ebenfalls bPK erzeugt [BKA08, AS09]. Bislang gibt es jedoch neben E-Banking, das von einigen österr. Banken optional auch mit BK angeboten wird, kaum weitere Anwendungen in der Privatwirtschaft.

2.3 Datenschutzaspekte

Datenschutz war ein wesentliches Kriterium bei der Gestaltung des österreichischen eIDMS. Das Spannungsfeld zwischen möglichst einfacher praktischer Handhabung und der Gewährleistung von Datenschutzkonformität wurde in den Entscheidungsgremien im Zeitraum von über einem Jahr diskutiert. Einwände des Datenschutzrates gegen die anfangs bevorzugte Variante der direkten Verwendung der ZMR-Zahl führten zum gegenwärtigen ID-Konzept mit SZ und bPK, das von den Entscheidungsträgern als gangbarer Kompromiss akzeptiert und beschlossen wurde.

Dennoch wurde das eIDMS immer wieder von verschiedenen Stellen als zu komplex und intransparent kritisiert. Das System sei dadurch für Benutzer nicht nachvollziehbar und folglich auch die Datenverarbeitung nicht kontrollierbar. Daher bringe es weitere Bedrohungen für die Privatsphäre mit sich [AS09]. Für einige dieser Kritikpunkte gibt es durchaus Evidenz. 2006 zeigten Sicherheitsforscher der TU Wien einige Schwachstellen des Systems auf. U. a. gelang es, eine Session zu entführen („Session Hijacking“) und eine Komponente der BKU zu manipulieren.[5]

Hinsichtlich der Realisierung wesentlicher Datenschutzanforderungen ergibt sich folgendes Bild: Das komplexe ID-Konzept verwendet bPK und *kein einheitliches Personenkennzeichen*, wodurch der *Unverkettbarkeit* grundsätzlich Rechnung getragen wird. Nach den unterschiedlichen Arten von Pseudonymen entspricht ein bPK in etwa einem Beziehungspseudonym [vgl. PS03], da einer Person immer die gleiche bPK für einen bestimmten Bereich zugewiesen ist. Die Verwaltung von Teilidentitäten ist demnach prinzipiell möglich. De facto kann das bPK zwar als Pseudonym verstanden werden. Allerdings werden i. d. R. dennoch Identitätsdaten (Name, Anschrift, Geburtsdatum) verarbeitet. Bei Transaktions-Diensten im E-Government ist das meist notwendig, nicht jedoch per se bei allen Diensten (Informationsdienste erfordern z. B. keine Identifizierung).

Aus datenschutzrechtlicher Sicht ist im eIDMS die Möglichkeit zur pseudonymen Nutzung derzeit nicht hinreichend realisiert [vgl. CP02]. Das wirkt sich auch auf die Nutzerzentrierung aus. Nutzer haben so nur wenig Kontrolle über die Verwendung ihrer Daten. Eine stärkere Differenzierung und Beachtung von Bereichen ohne Identifizierungserfordernis erscheint daher notwendig. Das gilt insbesondere auch für Anwendungen im E-Commerce. Die Bereichsabgrenzung der bPK impliziert eine Separierung unterschiedlicher Kontexte und z. T. eine dezentrale Datenhaltung. Zudem gibt es viele verschiedene Dienste-Anbieter. Die elektronische Identität als Ganze wird jedoch von staatlicher Seite zentral verwaltet (im ZMR), wobei das BMI als zentraler Identity-Provider agiert.

3 Mögliche Folgen von eIDMS

Der sich verändernde Umgang mit Identitätsdaten durch wachsende Bedeutung von eID und Systemen zu ihrer Verwaltung bringt naturgemäß neue Chancen wie auch Spannungen für den Schutz der Privatsphäre mit sich. Wobei die Systemgestaltung sowie die Einbettung im gesellschaftlichen Gesamtkontext definieren, was jeweils überwiegt.

3.1 Privatsphäre-fördernde Aspekte

Die Beachtung zentraler Datenschutzanforderungen bei der Systemgestaltung vorausgesetzt sind Verbesserungen der informationellen Selbstbestimmung vorstellbar. Ein vereinheitlichtes System könnte die derzeit bestehenden Schwierigkeiten aufgrund der Vielzahl unterschiedlicher Systeme entschärfen und IDM erleichtern. Die aktive Unterstützung der Nutzer bei der selbstbestimmten Verwaltung ihrer Identität(en) kann zu einem

5 „Practical Security Aspects of Digital Signature Systems“ http://tinyurl.com/ykwb9lu

stärkeren Bewusstsein („Awareness") für Datenschutz beitragen [vgl. CPHH05]. Die Möglichkeit zur Steuerung und Darstellung ihrer personenbezogenen Daten verleiht Nutzern mehr Kontrolle sowie Transparenz über die Datenverarbeitung.

Mit entsprechenden Diensten auf Basis der eID wäre eine Förderung der Informationsfreiheit denkbar, etwa durch Schaffung und Ausbau von Zugängen für BürgerInnen zu Verwaltungsdaten (z. B. Zugriff auf die eigenen Datensätze in den verschiedenen Verwaltungsregistern, Abruf von Verwaltungsakten, Information über laufende Verwaltungsverfahren oder dergleichen), sowie Zugang zu öffentlich relevanten Informationen, die ein höheres Sicherheitsniveau erfordern.

Das österreichische System unterstützt bereits einige solcher Anwendungen. Mit der Möglichkeit, auch Datenzugriffe einzusehen, könnten Betroffene zudem unmittelbar nachvollziehen, wer wann und zu welchem Zweck auf ihre Verwaltungsdaten zugegriffen hat (Eine ähnliche Option bietet z. B. das belgische eIDMS). Ein weiteres Argument für Informationsfreiheit im Kontext elektronischer Identität geht aus dem Umstand hervor, dass Überwachung nur dann effektiv kontrollierbar sein kann, wenn Informationen über Verwendungszwecke der eID eindeutig geregelt und frei zugänglich sind [vgl. Poun08].

3.2 Spannungsfelder

Mit der Zunahme zentral geführter Register (wie dem ZMR), die u. a. zur Erzeugung und Verwaltung von Identitätsdaten dienen, ist ein Paradigmenwechsel zu einer Zentralisierung bei der Verarbeitung personenbezogener Daten erkennbar. „[T]he introduction of IDM layer components tends to centralise (…) identity-related data flows through a small number of standardised infrastructure components" [RBBN08]. Eine solch standardisierte Form von IDM für eine Vielzahl unterschiedlicher öffentlicher und privater Anwendungsfelder bietet eine potenziell höhere Angriffsfläche für Datenmissbrauch „than without the pervasive IDM layer" [RBBN08]. Es wird also „potenziell die Datenerfassung, Verknüpfung von Datenbanken, Datenvereinigung und Profilerstellung durch kommerzielle wie staatliche Stellen" vereinfacht [Cent03].

Auf das österreichische eIDMS bezogen sind u. a. folgende Aspekte relevant: Das ID-Konzept und der Einsatz von bPK dient grundsätzlich der Verhinderung einer Datenverkettung. Dennoch könnten sich bPK, sofern sie bereichsübergreifend verwendet werden (wie das bPK für den Bereich Zustellung), „zu einem alle Verwaltungsbereiche umfassenden Personenkennzeichen" entwickeln [RTR03]. Zudem ist eine Verkettung anhand „semi-identifizierender" Daten (z. B. Name, Geburtsdatum, Adresse), die bei praktisch jedem BK-Dienst verwendet werden, trotz bPK nach wie vor möglich [Pri08]. Oder allgemeiner formuliert: Es besteht die Gefahr, dass aus dem „Datenschatten"[6] – jenen Daten, die bei der Interaktion mit dem eIDMS „nebenbei" anfallen und eine Verkettung der Daten ermöglichen – eine Art „Schattenidentität" entsteht, die ohne Wissen des Betroffenen verarbeitet wird. Das eIDMS selbst kann so zu einem Risiko für die Privatsphäre der Benutzer werden.

In diesem Zusammenhang können auch Protokolldaten problematisch sein, die bei der Erzeugung der für die eID erforderlichen Elemente (SZ, bPK) entstehen. Wenngleich die Protokollierung im Grunde zur Überprüfung der Rechtmäßigkeit dient, können diese Protokolldaten auch detailliert Aufschluss über die Nutzung der elektronischen Identität(en) einer bestimmten Person geben [RTR03]. Die Problematik droht sich zu verschärfen, wenn die eID auch im Privatwirtschaftsbereich verstärkt Anwendung findet. Will eine öffentliche oder private Einrichtung Dienste mit BK anbieten, muss sie um Erzeugung der dazugehörigen bPK bei der SZRB ansuchen. Da diese Ansuchen beim BMI als Dienstleister der SZRB protokolliert werden müssen, wird hier (zumindest theoretisch) Wissen darüber generiert, in welchen Stellen die eID einer Person genutzt wird. Mit anderen Worten: Der Staat wäre durch das eIDMS anhand dieser Information in der Lage, für jede Person ein Profil zu erstellen, das offenbart, in welchen Bereichen sie ihre elektronische Identität verwendet. Bedenkt man die potenziell breite Palette an eID-Anwendungen, besteht so die Gefahr eines umfassenden Bewegungsprofils im virtuellen Raum.

Eng damit verbunden ist die Gefahr einer schrittweisen Ausdehnung der Verwendungszwecke für das eIDMS (sog. „function creep") [vgl. Poun08; HB08]. Durch eine solche „schleichende" Zunahme von Identifizierung können neue Bedrohungen für die Privatsphäre des Einzelnen entstehen. Der Einsatz von eID in der Privatwirtschaft ist etwa bewusst gewünscht. Es ist denkbar, dass die eID neue Geschäftsmodelle hervorbringt. Verlangen eID-Dienste die Feststellung der Identität, selbst wenn dies nicht notwendig wäre (z. B. bei Informationsdiensten), oder wenn eine anonyme Nutzung aufgrund der Art des Dienstes besonders wichtig wäre, ginge das auf Kosten zentraler Datenschutzprinzipien wie Verhältnismäßigkeit, Zweckbindung usw.

Gleiches gilt für den staatlichen Bereich. Es gibt bereits Dienste, die eine BK erfordern und wo der Grund dafür nicht eindeutig nachvollziehbar ist. Etwa zählen zu den verfügbaren BK-Diensten derzeit auch Meldungen von NS-Wiederbetätigung oder Kinderpornographie über das Web. Ein weiteres Beispiel, das sich zwar nicht unmittelbar, aber zumindest indirekt auf das eIDMS bezieht, ist eine Erweiterung der Nutzungsmöglichkeiten des ZMR, zu der es kurz nach dessen Einführung (2001) kam: Seitdem dürfen Unternehmen unter bestimmten Voraussetzungen Daten des ZMR auch für wirtschaftliche Zwecke nutzen. Diese sog. „Businesspartner" sind z. B. Banken, Versicherungen, Inkasso-Büros usw.

Unter Betrachtung der potenziell breiten Anwendungsfelder der eID im Zusammenhang mit aktuellen Entwicklungen wie die Einführung der verdachtsunabhängigen Vorratsdatenspeicherung und Bestrebungen, das Internet zur Bekämpfung von Straftaten (z. B. von Kinderpornographie, Urheberrechtsdelikten)[7] nach bestimmten Inhalten zu filtern, erscheint die evidente Gefahr eines function creep zusätzlich erhöht. Durch die Tendenz zu solchen präventivstaatlichen Maßnahmen kann etwa nicht ausgeschlossen werden, dass die Anwendungsbereiche der eID und eine verpflichtende Authentifizierung bei elektronischen Diensten künftig schrittweise erweitert werden. Wenngleich die gegenwärtig geringen Nutzungszahlen[8] von eIDMS nicht unmittelbar auf das Eintreten eines solchen Szenarios in absehbarer Zeit hindeuten.

6 Der Begriff „Data Shadow" wurde von Alan Westin, „Privacy and Freedom", 1967, geprägt.

7 Siehe z. B. Golem Special: Internetsperren http://tinyurl.com/d6kpyc

8 In Österreich sind ca. 120.000 aktivierte Bürgerkarten in Umlauf http://tinyurl.com/pmtg57

Fazit

Derzeit kommen staatliche eIDM-Systeme vor allem im E-Government zum Einsatz, wurden jedoch über diesen Bereich hinausgehend auch für weitere Anwendungsfelder geschaffen. Gegenwärtige Ansätze für nationales eIDM konzentrieren sich überwiegend auf die Gewährleistung sicherer Authentifizierung bei elektronischen Transaktionen mit dem Zweck, Identifizierungsprozesse zu vereinheitlichen, und Online-Dienste sicherer zu gestalten. Bislang befassen sich erst wenige davon mit der generellen Problematik der Identitätsfeststellung in einem breiteren Kontext. Insbesondere datenschutzrelevante Aspekte wie Nutzerzentrierung, Anonymität und Pseudonymität spielen gegenüber eindeutiger Identifizierung eher eine untergeordnete Rolle.

Es ist anzunehmen, dass eIDM weiter an Bedeutung gewinnt. Dieser Umstand und die hohe Komplexität der Materie verlangen einmal mehr nach modernisierten Ansätzen zum Schutz der Privatsphäre, die über geltende Rechtsnormen hinaus gehen; Denn „Lawful collection and processing of personal data does not prevent per se unethical practices deployed in the name of security, or unjust decisions based on them" [Deh08]. Das wurde u. a. durch die Datenskandale der jüngsten Zeit[9] drastisch verdeutlicht. Es besteht daher Bedarf nach effektiveren Instrumenten, um Datenmissbrauch möglichst zu verhindern, wirksam zu ahnden und einen ordnungsgemäßen Einsatz der eID zu gewährleisten [vgl. CPHH05]. Künftig sollten bei der Umsetzung von eIDMS deshalb noch genauer als bislang datenschutzrelevante Faktoren und mögliche Auswirkungen in einem breiteren Kontext berücksichtigt werden.

Um die genannten Spannungsfelder einzugrenzen, gilt es vor allem, die Systeme stärker als bisher für pseudonyme und anonyme Nutzung zu gestalten. Mit entsprechenden Diensten könnte mit der eID auch die Informationsfreiheit gestärkt werden. Die Vorstellung einer übergreifenden Infrastruktur für eine standardisierte Form von IDM wirft viele Fragen auf, die es noch genauer zu untersuchen gilt. Etwa, inwieweit die Verwaltung von (e)Identitäten der BürgerInnen eine Aufgabe des Staates ist bzw. sein sollte und welche Konsequenzen daraus resultieren.

9 Siehe u.a. MDR.de 18.04.2009: „Von Lidl bis Müller – Datenskandale" http://tinyurl.com/yznj865

Literatur

[Aro08] S. Arora, 2008, *National eID card schemes: A European overview*, Information Security Technical Report Volume 13 (2), 43-53.

[AS09] G. Aichholzer und S. Strauß, 2009, *Understanding a complex innovation process: identity management in Austrian e-government*, in: ACM International Conference Proceeding Series, vol. 390, 230-239.

[BKA08] Österreichisches Bundeskanzleramt 2008, *Behörden im Netz - Das österreichische E-Government ABC*. Neuauflage 2008, Wien.

[CP02] J. Cas, W. Peissl, 2002, *Datenvermeidung in der Praxis - Individuelle und gesellschaftliche Verantwortung*. Studie im Auftrag der Bundeskammer für Arbeiter und Angestellte.

[CEN04] Commité Européen Normalisation 2004, *CEN/ISSS Workshop eAuthentication - Towards an electronic ID for the European Citizen, a strategic vision*, 03.10.2004, Brüssel. http://tinyurl.com/loq82p

[Cent03] C. Centeno 2003, *Zukunft der elektronischen Identifikation: Herausforderungen und Chancen für den öffentlichen Sektor*, No. 79, Institute for Prospective Technological Studies (IPTS) http://tinyurl.com/ljdehm

[CPHH05] S. Clauß, A. Pfitzmann, M. Hansen, E. V. Herreweghen, 2005, *Privacy-Enhancing Identity Management*, No. issue 67, Institute for Prospective Technological Studies (IPTS) http://tinyurl.com/mh6lrd

[Deh08] P. De Hert, 2008, *Identity management of e-ID, privacy and security in Europe. A human rights view*, Information Security Technical Report 13 (2008), 71-75.

[EUK06] EU-Kommission, 2006, *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, No. SEC (2006) 511, 25.04.2006, Brüssel.

[FIDIS07] Future of Identity in the Information Society, 2007, *D13.6: Privacy modelling and identity*. http://tinyurl.com/dcxc9v.

[HKRG03] M. Hansen, H. Krasemann, M. Rost, R. Genghini, 2003, *Datenschutzaspekte von Identitätsmanagementsystemen. Recht und Praxis in Europa*, Datenschutz und Datensicherheit 27 (9) 2003, 551-555.

[LP08] M. Lips, C. Pang, 2008, *Identity Management in Information Age Government. Exploring Concepts, Definitions, Approaches and Solutions*. Research Report, Victoria University of Wellington, New Zealand. http://tinyurl.com/kqgclb

[OECD08] Organisation for Economic Co-operation and Development 2008, *Scoping Paper on Online Identity Theft*, No. DSTI/CP (2007) 3/FINAL, Juni 2008, Seoul.

[PH08] A. Pfitzmann, M. Hansen, 2008, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology* version 0.31. http://tinyurl.com/2ys9fx

[PS03] A. Pfitzmann, S. Steinbrecher, 2003, *Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft*, in: Klumpp, D. Kubicek, H., Roßnagel, A. (Eds): next generation information society? Notwendigkeit einer Neuorientierung., Mössingen-Talheim, 290-299.

[Poun08] C. N. M. Pounder, 2008, *Nine principles for assessing whether privacy is protected in a surveillance society*, Identity in the information society (IDIS) Volume 1 (1) 2008, 1-22.

[Pri08] S. Priglinger, 2008, *Auswirkungen der EU-DL Richtlinie auf die E-Gov-Welt*, Jahnel, Dietmar (Hrsg.): Datenschutzrecht und E-Government, Graz, 267-283.

[Roß06] A. Roßnagel, 2006, *Datenschutz im 21. Jahrhundert*, Aus Politik und Zeitgeschichte Band 5-6 2006, 9-15.

[RTR03] 2003, *Stellungnahme der Rundfunk und Telekom Regulierungs-GmbH zum Entwurf des E-Government-Gesetzes* http://tinyurl.com/yc2hgyb

[RBBN08] M. Rundle, B. Blakley, J. Broberg, A. Nadalin, D. Olds, M. Ruddy, M.T.M. Guimarares, P. Trevithick, 2008, *At a crossroads: „Personhood" and digital identity in the information society*, 29.02.2008. http://tinyurl.com/cwpeec

[HB08] R. Halperin, J. Backhouse 2008, *A roadmap for research on identity in the information society, Identity in the information society*, Volume 1 (1) 2008.

[Sch03] M. Schnyder, 2003, *Die sogenannte digitale bzw. elektronische Identität. Bemerkungen eines Datenschützers*, TILT 2003 112. Jahresbericht, Berner Fachhochschule, März 2003, 81-85.

[SW08] C. Sorge, D. Westhoff, 2008, *eIDs und Identitätsmanagement*, Datenschutz und Datensicherheit 32 (5) 2008, 337-341.