Oliver Raabe

Datenschutz im SmartGrid

Anpassungsbedarf des Rechts und des Systemdatenschutzes

Zur optimierten Anpassung der Energieerzeugung an den tatsächlichen Bedarf werden zukünftig vernetzte „intelligente Stromzähler" (Smart Meter) nicht nur dem Verbraucher detaillierte Verbrauchskontrollen ermöglichen, sondern die Messdaten zyklisch an die jeweiligen Stromnetzbetreiber übermitteln. Der Beitrag analysiert die datenschutzrechtlichen Implikationen und den Handlungsbedarf des Gesetzgebers.

Einleitung

Mit der verbindlichen Einführung von sogenannten intelligenten Energiezählern (SmartMeter) ist der erste Schritt zur Integration von IKT in das Energienetz (SmartGrid) aus Gründen der Steigerung der Energieeffizienz getan. Derzeit werden im Rahmen der E-Energy-Initiative der Bundesregierung erste Realsierungen dieses Ansatzes im Rahmen von Modellprojekten untersucht.[1]

Der Sicherung datenschutzrechtlicher Aspekte wird im Rahmen der Erprobung eine Schlüsselrolle für die erfolgreiche Entwicklung des SmartGrid zugewiesen. Der Beitrag konkretisiert anhand von Beispielen die datenschutzrechtlichen Herausforderungen des SmartGrid und diskutiert den bereits heute absehbaren legislatorischen Handlungsbedarf zur Ausgestaltung des zukünftigen Rechtsrahmens. Dabei wird ein neues Verständnis des Systemdatenschutzes im Energiesektor durch die fakultative Verwendung von Mechanismen des technischen Zugriffsschutzes gefordert.

Dr. Oliver Raabe

ist als Forschungsgruppenleiter am Institut für Informations- und Wirtschaftsrecht (IIWR), Karlsruhe Institut of Technology (KIT) mit Fragen der rechtlichen Bewertung komplexer IT-Systeme befasst.
E-Mail: raabe@kit.edu

1 Vgl. http://www.e-energy.de [Abgerufen am 11.01.2010].

1 Vom SmartMeter zum SmartGrid

Im Jahr 2007 hat die Europäische Kommission ein integriertes Paket von Rechtsvorschriften zum Thema Energie/Klimawandel vorgelegt, das in der 10-Jahres Perspektive auf die Themen Energieversorgung, Klimawandel und industrielle Entwicklung eingeht. Im Ergebnis ist hiernach eine 20 %ige Steigerung der Energieeffizienz, eine 20 %ige Verringerung der Treibhausgasemissionen und ein Zielwert von 20 % für den Anteil erneuerbarer Energiequellen am Gesamtenergieverbrauch der EU im Jahr 2020 vorgesehen.

Zudem finden sich mit den europäischen Vorgaben zur Liberalisierung des Messwesens sowie der Richtlinie zur Endenergieeffizienz und Energiedienstleistungen auch schon kurzfristig wirkende Maßnahmen im Prozess der Umsetzung in nationales Recht, die das Thema Energie nicht mehr nur unter dem Aspekt der Gewährleistung des binnenmarktrelevanten ökonomischen Wettbewerbs adressieren.

Aus globaler Sicht geht es bei den vorgesehenen Maßnahmen um die Steigerung der Energieeffizienz durch die Nutzung einer Kommunikationsinfrastruktur zum Echtzeit-Informationsaustausch zwischen Akteuren des Energiemarktes. Man kann sich dieses Paradigma auch durch die Substitution von verlustbehafteten, weil unscharf prognostizierten, realen Stromflüssen durch Informationsflüsse verbildlichen. Hierdurch soll ermöglicht werden, dass Angebot und Nachfrage zeitnah und hochauflösend aufeinander abgestimmt werden. In einem ersten Schritt werden deshalb auf gesetzlicher Grundlage des § 21b Abs. 3a EnWG ab 2010 schrittweise bei Neubauten und bei Renovierungen von Gebäuden nur noch solche Energiezähler eingebaut, die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit zeigen. In der Folge können diese Zähler durch die Anbindung an die IKT-Infrastrukturen des Internet auch zur Weitergabe der Messdaten an Mehrwertdienste im Internet genutzt werden. Die insofern relevanten datenschutzrelevanten Gefahrenlagen des Einsatzes von SmartMeter hat das ULD-Schleswig-Holstein jüngst in einem Gutachten dargelegt.[2]

Die nicht so ferne Zukunft der angestrebten Energieeffizienzsteigerungen wird durch ein intelligentes Stromnetz, das so genannte SmartGrid, gekennzeichnet sein, das insbesondere auch bidirektionale Datenkommunikation zur Steuerung von Lasten erlauben und den Anforderungen für einen hochkomplexen Netzbetrieb genügen wird. Gerade die Potentiale zur Verbesserung des Klimaschutzes durch die Integration von Elektromobilität in den Energiemarkt liegen auf der Hand, wenn man neben der besseren CO_2-Bilanz

2 Vgl. https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.pdf [Abgerufen am 11.01.2010].

der klassischen Elektromobilitätsszenarien auch noch den Einsatz im Bereich der sog. Tertiärregelenergie in die Betrachtung einbezieht.

So liegt eines der wesentlichen Probleme bei der Verwendung von unsteten regenerativen Energieerzeugungsanlagen wie der Windkraft in dem Bedarf an (konventionellen) Reservekapazitäten. Durch die Nutzung der Batteriespeicher von Elektromobilen zur Aufnahme von Überkapazitäten und Einspeisung bei Lieferengpässen lassen sich diese Nachteile verringern. Im Hinblick z. B. auf den Ausbau von Offshore-Windparks ist dies sicher ein entscheidendes Argument für die Marktfähigkeit dieser Planungen.

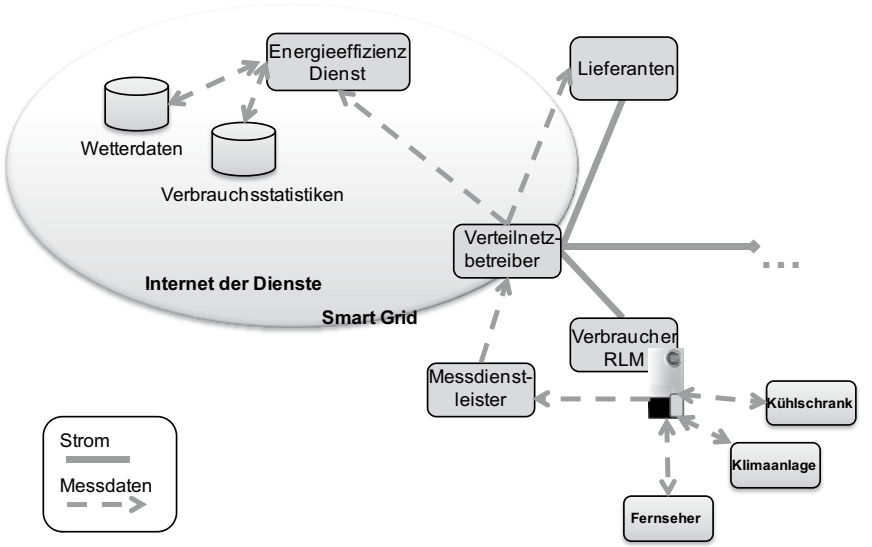
Daneben können auf Basis feingranular aufgelöster Sensordaten zukünftig auch neue Geschäftsfelder der internetbasierten Energieeffizienzberatung ermöglicht werden, die bis hin zum Steuern von Haushaltsgeräten reichen.

Nach jüngsten Aktivitäten in den USA wurde für die korrespondierenden datenschutzrechtlichen Problemlagen des SmartGrid insofern gerade der Begriff Smart Privacy[3] eingeführt. Allerdings motiviert die diesbezügliche Studie wegen des visionären Charakters des SmartGrid eher noch das Gefahrenpotential und beschränkt sich im Wesentlichen auf datenschutzrechtliche Allgemeinplätze. In verschiedenen Modellprojekten werden in Deutschland hingegen schon konkrete Anwendungsszenarien umgesetzt und erprobt. Angelehnt an diese Ansätze sollen im Folgenden zwei Beispiele betrachtet werden, welche die kommende Herausforderung modellhaft konkretisieren.

2 Elektromobilität, Effizienzberatung und das SmartGrid

Im Fall der Energieeffizienzberatung (Abbildung 1) können auf Basis gerätegenauer Stromverbrauchsprofile die Messdaten zur Auswertung durch einen externen Energieeffizienzberater übermittelt werden. Auf Basis dieser Daten sind eine Vielzahl von Angeboten, wie Vergleichsanalysen oder die Anreicherung mit weiteren

Abbildung 1 | Energieeffizienzberatung



Daten, im Rahmen des „*Internet der Dienste*“[4] *denkbar.*

In Abbildung 1 werden die typischen Messdatenflüsse gezeigt, wie sie einerseits aggregiert zur Abrechnung des normalen Haushaltsverbrauchs durch den Lieferanten übermittelt werden müssen, und auf der anderen Seite die Basis für die Energieeffizienzdienstleistung bilden. Aus Gründen der Komplexitätsreduzierung sollen die korrespondierenden, personalisierten Vertragsdatenflüsse hier nicht näher betrachtet werden.

Aus rechtlicher Sicht liegt dieser Gestaltung zugrunde, dass sie mit den in der Konsultation befindlichen zukünftigen Bestimmungen der Bundesnetzagentur zu Prozessen und Datenformaten im Strom und Gasbereich korrespondieren. Hier ist insbesondere ausdrücklich bestimmt, dass zukünftig der jeweilige Verteilnetzbetreiber die Stellung der zentralen „Datendrehscheibe“ einnehmen soll.[5]

Im zweiten Beispiel, der Integration von Elektromobilität (Abbildung 2), wird davon ausgegangen, dass Verbraucher auch zukünftig nur einen Stromlieferanten haben werden, der sowohl bei der Aufladung an der heimischen Steckdose als auch bei einem Ladevorgang an einer „mobilen“ Steckdose eine einheitliche Abrechnung stellt. Jedenfalls für den Fall der „mobilen Steckdose“ wird damit aus Gründen der eichrechtlich gebotenen Nachvollziehbarkeit der Rechnungsstellung aber eine Personalisierung der im Zähler erfassten und gespeicherten Messwerte unumgänglich.

Beiden Szenarien ist damit gemein, dass einerseits eine Übermittlung von aggregierten Verbrauchsdaten an den jeweiligen Lieferanten zu Zwecken der Haushaltsabrechnung erfolgen muss; auf der anderen Seite müssen zur Zweckerreichung hoch aufgelöste Profildaten über den Verteilnetzbetreiber geleitet werden. Im Fall der Elektromobilität findet notwendig eine Weitergabe der personalisierten Mess- und Standortdaten über eine Kette von weiteren Akteuren statt.

Soll gleichzeitig der mobile Stromspeicher auch noch im Bereich der Bereitstellung im Tertiärregelenergiemarkt[6] eingesetzt werden und sollen nicht mehr die Prozessdefinitionen für den Endkundemarkt gelten, können noch weitere, veränderte Informationsflüsse der Messdaten konstatiert werden. Damit stellt sich beim Verteilnetzbetreiber als Datendrehscheibe in jedem Fall der Übermittlungstätigkeit eine Entscheidungssituation, wie mit den Daten und einzelnen Datensegmenten zu verfahren ist. Aber auch bei den anderen Akteuren der Prozesskette wird es zu einer Reihe von Entscheidungssituationen über die zur jeweiligen Aufgabenerfüllung

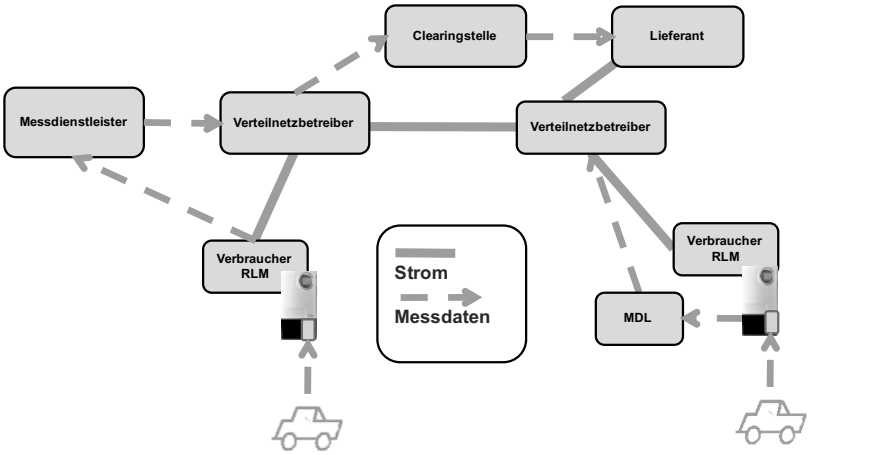
3 SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf [Abgerufen am 11.01.2010].

4 Zum Begriff „Internet der Dienste“ vgl. Heuser, Lutz; Alsdorf, Claudia; Woods, Dan (2008): International Research Forum 2007. Evolved Technologists Press, 2008, S. 100.

5 Vgl. Bundesnetzagentur, Entwurf zur Konsultation zu dem Beschluss BK7-09-001 / BK6-09-034, Wechselprozesse im Messwesen, S. 59 http://www.bundesnetzagentur.de/media/archive/16664.pdf [Abgerufen am 11.01.2010].

6 Die Batterien der Elektromobile werden hier als schaltbare Lasten verwendet, um im Fall der Überproduktion als Stromspeicher und im Fall der Unterproduktion als Stromerzeuger für die Netzstabilität zu sorgen.

Abbildung 2 | Elektromobilität



notwendigen Granularität und Personalisierung ggf. pseudonymisierter Messdaten kommen. Zugleich sind Entscheidungen über notwendige Übermittlungs- und Verarbeitungsschritte zu fällen. Diese Flexibilität ist dem bestehenden energiewirtschaftsrechtlichen Rechtsrahmen mit seinen klar formulierten Prozessstrukturen fremd, was im ersten Schritt erhebliche regulierungstheoretische und inhaltliche Anforderungen an die datenschutzrechtliche Anpassung dieses Rechtsrahmens stellt.

3 Personenbezug der Daten

Schon die derzeit gesetzlich vorgesehene, mögliche hohe Übermittlungsfrequenz von aggregierten Daten des Haushaltsverbrauchs lässt, im Gegensatz zur bislang üblichen jährlichen Übermittlung, sogar eine Profilbildung über Muster der Lebensgestaltung der Stromkunden zu. In den Fällen der zur Energieeffizienzberatung notwendigen ggf. geräte- und raumgenauen Auflösung der Messdaten können aus diesen Daten mit entsprechendem Zusatzwissen sogar konkrete Verhaltensprofile einzelner Familienmitglieder im innerhäuslichen Bereich ermittelt werden.[7] Im Elektromobilitätsszenario können, wegen der Abrechnungsrelevanz der Standortinformationen, durchaus auch Bewegungsprofile entstehen, wie sie schon für die Maut-Szenarien befürchtet wurden.

Im Beispiel der Energieeffizienzberatung (Abbildung 1) liegen aufgrund der jeweils notwendigen vertraglichen Bindungen der beteiligten Akteure die für die personale Zuordnung der Messdaten notwendigen Angaben zum Anschlussinhaber bei jedem Akteur der Prozesskette vor.[8] Im Elektromobilitätsszenario (Abbildung 2) wäre im Fall der entfernten Stromabnahme eine vorzugswürdige anonyme Nutzung bei Prepaid oder Barzahlung möglich. Sobald aber eine Abrechnung über den Heimlieferanten in Frage steht, muss auch hier eine Identifikation des Nutzers, z. B. über eine Vertrags-ID, bei der fremden Messstelle erfolgen. Es sind insofern Verfahren der pseudonymen Nutzung denkbar, da insofern nur der Heimlieferant zu Abrechnungszwecken eine Zuordnung der Messdaten zu den Vertragsdaten vornehmen muss. Dem stehen aber nach den bisher geplanten Festlegungen der Bundesnetzagentur zum Messwesen noch grundlegende Standardisierungsentscheidungen auf der Ebene der gewählten Nachrichtenformate zur Messdatenübermittlung entgegen.

Spätestens mit dem Einsatz von Elektromobilen im Bereich der Tertiärregelenergie müssen regelmäßig die personalisierten Einspeise-, Entnahme- und Standortdaten bei allen Akteuren der diesbezüglichen Prozesskette zu Abrechnungszwecken bekannt sein.

4 Anforderungen an den Rechtsrahmen

Schon in der Vergangenheit wurde im Hinblick auf die bereichsspezifische Regulierung des Datenschutzes bei deutlich weniger komplexen Technikgestaltungen festgestellt, dass der klassische ordnungsrechtliche Ansatz und die Überwachung des entsprechenden Pflichtenkanons versagen bzw. wenig effektiv sind. Über die richtige Strategie zur legislativen Auflösung des Spannungsfeldes von Datenschutz und technischer Innovationsoffenheit unter der Bedingung, dass die Entwicklungslinien komplexer Systemgestaltungen für den Gesetzgeber zunehmend schwerer zu prognostizieren sind, herrscht keine Einigkeit.

Für den hier interessierenden Fragenkreis muss zudem konstatiert werden, dass im Gegensatz zu den vergleichbaren Problematiken der Verwendung von RFID-Techniken[9] dem grundrechtlichen Schutz der informationellen Selbstbestimmung bei der Entscheidung über die richtige Gestaltung des bereichsspezifischen Datenschutzes mit dem angestrebten Klimaschutzziel eine Grundbedingung menschlichen Lebens in verhältnismäßiger Weise in Einklang gebracht werden muss.

5 Regulierungstheoretische Fragen

In regulierungstheoretischer Sicht ist damit zum einen die Frage nach dem systematisch richtigen normativen Rahmen der Datenschutzregelungen zum Smart-Grid betroffen. Es kommt insofern grundsätzlich in Betracht, es bei den allgemeinen Regelungen des BDSG zu belassen, oder ein neues bereichsspezifisches Schutzprogramm (z. B. nach telekommunikationsrechtlichem Vorbild) im Energiewirtschaftsrecht zu verankern.

Im Spannungsfeld von Datenschutz, Rechtssicherheit für die Marktakteure und Innovationsoffenheit zur bestmöglichen Erreichung der Effizienzziele stellt

7 Ein Aspekt der offensichtlich übersehen wird, wenn solche Profile zur entfernten Ablesung durch den Anschlussinhaber getwittert werden sollen. Insofern muss wegen der Möglichkeit einer verdeckten innerfamiliären Überwachung in Frage gestellt werden, ob die Privilegierung des familiären Bereiches in § 1 Abs.2 Nr.3 BDSG nicht einer bereichsspezifischen Konkretisierung bedarf.

8 Das gilt für den Verteilnetzbetreiber allerdings nur insofern, als er auch gleichzeitig Messdienstleister ist.

9 Friedewald M., Raabe O., Koch D., Georgieff P., Neuhäusler P., Ubiquitäres Computing – Zukunftsreport für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag, TAB Arbeitsbericht 113, 2009

sich zudem noch die Frage nach der Ausgestaltung der positiven Regulierungstiefe im Optionenraum von ordnungspolitischen bis zu kooperativen, selbstregulierenden Maßnahmen.

Diese Fragen unterscheiden sich insofern nur unwesentlich von den zuletzt in den Szenarien der Nutzung von RFID angeführten Problemlagen. Dies gilt insbesondere unter der Prämisse der in den Beispielen gezeigten unsicheren Prognoselagen zur tatsächlichen Entwicklung des SmartGrid. Mit den im Fragenkreis des Einsatzes von RFID gewonnenen datenschutzrechtlichen Erfahrungen, können sich damit Anhaltspunkte für eine sinnvolle Ausgestaltung im Hinblick auf die neue Herausforderung gewinnen lassen.

5.1 Bereichsspezifische Regelung

Grundsätzlich ist zu bejahen, dass eine bereichsspezifische Anreicherung des Energiewirtschaftsrechts um Datenschutzaspekte erforderlich ist. Dem könnte allerdings wie schon bei der RFID-Problematik grundsätzlich entgegengehalten werden, dass das die Flexibilität von Selbstverpflichtungen im Bereich moderner Technikgestaltung, im Gegensatz zu starren gesetzlichen Regelungen, differenziertere Lösungen ermögliche. Für den Verzicht auf ordnungsrechtliche Eingriffe könnte auch hier ins Feld geführt werden, dass die Selbstverpflichtung offener für neue datenschutzrelevante Entwicklungen sei und dadurch die Wettbewerbsfähigkeit und das Innovationspotential der betroffenen Unternehmen weniger einschränke.[10]

Dieser pauschalen Aussage kann allerdings nicht gefolgt werden. Es ist das Wesen moderner Technikgestaltung, dass sie mit prognostischen Unsicherheiten belastet ist. Damit wird die gesetzliche Ex-Ante-Steuerung der Datenverarbeitung angesichts der dynamischen Entwicklung von Technik und Anwendungen zunehmend schwierig.[11] Eine mit einem umfassenden Verweis auf eine wie auch immer geartete Selbstverpflichtung einhergehende pauschale Verlagerung der Prognoserisiken auf den Grundrechtsträger der informationellen Selbstbestimmung, durch eine totale Verweigerung normativer Grundsatzentscheidungen, ist aber aus verfassungsrechtlicher Sicht unzulässig. Auf der anderen Seite ist im Bereich des Energiewirtschaftsrechts das marktliche Wissen um notwendige Geschäftsprozesse des Kernmarktes schon im bestehenden Rechtsrahmen verankert. So sind im Bereich des Messwesens die damit verbunden Verarbeitungsschritte und Legitimationstatbestände schon heute weitgehend energiewirtschaftsrechtlich normiert. Auch wenn die Komplexität der Marktprozesse zukünftig deutlich steigen wird, handelt es sich gleichwohl um ein auch zukünftig einheitlich zu betrachtendes Marktsystem, bei dem aus Gründen der Versorgungssicherheit eine enge normative Verortung neuer Marktakteure und Prozesse zu erwarten steht.

Insofern bietet es sich an, bei der notwendigen Anreicherung des materiellen Rechts auch zugleich die datenschutzrechtlichen Implikationen zu gestalten.

5.2 Regulierungsinstrumente

Auf einem anderen Blatt steht allerdings die Frage nach den dann sinnvoll zu verwendenden verfahrensrechtlichen und materiellen datenschutzrechtlichen Regulierungsinstrumenten. Es steht also in Frage, was in datenschutzrechtlicher Hinsicht auf das SmartGrid wie geregelt werden soll.

Im Gegensatz zu der vorhandenen gesetzlichen Marktgestaltung, welche einen überschaubaren Kreis von Akteuren mit klaren Rollenzuweisungen und Kommunikationsbedürfnissen abbildet, ist die Prognose im Hinblick auf die zur Energieeffizienzsteigerung notwendige Öffnung des Marktes und mithin datenschutzrelevanter neuer Rollen, Kommunikationsbeziehungen und Verarbeitungsschritte nur schwer vorhersagbar. Da die diesbezügliche rechtswissenschaftliche Diskussion um die Realisierung von regulierter Selbstregulierung im Datenschutz[12] bislang keine konkrete Ausgestaltung oder gar eine gesetzliche Normierung erfahren hat, kann insofern nicht auf Erfahrungswissen zurückgegriffen werden.

Als Besonderheit für die hier gegenständliche Sachgestaltung ist festzuhalten, dass der Begriff der Innovationsoffenheit für zukünftige Technikgestaltungen nicht nur abstrakte Dimension besitzt, sondern im Hinblick auf die Effektivierung von Klimaschutzaspekten eine auch legislativ zwingende Größe darstellt. Dies kann am Beispiel der Energieeffizienzberatung (Abbildung 1) verdeutlicht werden. In diesem Bereich ist davon auszugehen, das entsprechend den neueren Trends zu Service Orientierten Architekturen auch innovative Modelle kombinatorischer Energieeffizienzdienstleistungen kostengünstig zu gestalten[13] sind und einen erheblichen Beitrag zum Klimaschutz leisten können.

5.3 Ordnungsrecht

Für die Absicherung der datenschutzrechtlichen Prinzipien ist deshalb zukünftig von einem Maßnahmenbündel auszugehen, welches einerseits im sicher erschlossenen Bereich der energiewirtschaftsrechtlichen Kernmärkte einen unbedingten, ordnungsrechtlich normierten Bestand an materiellen Vorgaben zur Datenverarbeitung enthält. Auf der anderen Seite dürften im Bereich der prognostisch nicht sicher erfassbaren System- und Technikgestaltungen ein selbstregulativer Ansatz erfolgversprechend sein, welcher allerdings nicht die Fehler der bestehenden Systeme der Selbstregulierung wiederholt.

Diese Fehler sind, wie die RFID-Thematik zeigt, einerseits auf das Fehlen von Sanktionsmechanismen bei Verweigerung des privaten Tätigwerdens zurück zu führen. Auf der anderen Seite bedarf es einer Neubewertung des Verständnisses, dass selbstregulative Maßnahmen lediglich dann greifen können, wenn sie über das bestehende Schutzprogramm hinausgehen.[14] Die Frage nach sinnvollen Datenschutzmechanismen in zukünftigen Sachgestaltungen der Technikentwicklung im SmartGrid sollte vielmehr, wegen der größeren Nähe der betroffenen Kreise zur

10 So für RFID, Bundesregierung, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie. Deutscher Bundestag, Drucksache 16/789, S. 13.

11 Ladeur, K.-H. (2000): Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur „objektiv-rechtlichen Dimension" des Datenschutzes. In: DuD – Datenschutz und Datensicherheit 24(1), S. 16

12 Siehe nur: Hoffmann-Riem, W. , Informationelle Selbstbestimmung in der Informationsgesellschaft – auf dem Wege zu einem neuen Konzept des Datenschutzes. In: Archiv des öffentlichen Rechts 123(4), 1998, S. 513-540; Roßnagel, A. , Konzepte der Selbstregulierung. In: Roßnagel, A. (Hg.): Handbuch des Datenschutzrechts, München, 2003, S. 387-436.

13 Die deutet sich beispielsweise beim Google PowerMeter an. Siehe: http://www.google.org/powermeter/ [Abgerufen am 11.01.2010].

14 Bizer, J. (2003): Mut zur Selbstregulierung. In: DuD – Datenschutz und Datensicherheit 27(7), S. 394.

Technik, gerade Gegenstand von kooperativ gestalteten Erkenntnisprozessen sein.

Schließlich bedarf es zu einer sinnvollen Durchsetzung der kooperativ gewonnen Vorgaben aber noch eines imperativ wirkenden und ordnungsrechtlich sanktionierten Befehls. Die insofern bislang gelegentlich im Bereich der datenschutzrechtlichen Selbstregulierung angestrebte Verweisung auf eine privatrechtliche Durchsetzung der Sanktionsmechanismen muss im Rahmen der sich aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG ergebenden Schutzpflichten, gerade im Bereich unsicherer Prognoselagen, im Kern beim Staatssouverän verbleiben, weil er ansonsten das Risiko, welches mit solchen Prognosen verbunden ist, auf den sachunkundigen Bürger abwälzte.

Die in der Diskussion um die Selbstregulierung vertretene zivilistisch geprägte Position, welche aus Gründen einer eigentumsrechtlich motivierten Betrachtung[15] des Gegenstandes „Information" eine durch Art. 14 GG (analog)[16] terminierte Betrachtung aller diesbezüglichen Sachgestaltungen in den Markt weisen will, verkennt die Reichweite dieser auch bei privatem Handeln bestehenden Prognoseverantwortung des Staates. Dies zeigt sich gerade bei der Entwicklung komplexer, die Daseinsvorsorge stützender, privater Informationssysteme wie dem SmartGrid.

Auf der anderen Seite erfordert die Ausgestaltung von Kommunikationsinfrastrukturen des Energiemarktes erhebliche Investitionen, die letztlich auch aus Gründen der Rechtssicherheit eine verbindliche staatliche Abschlussentscheidung verlangen.

5.4 Kooperative Verfahren

Um die vorgenannte Anforderung zu erfüllen, muss damit im Hinblick auf die einzelnen normierungsbedürftigen materiellen Tatbestände einerseits das Wissen aller betroffenen Kreise bestmöglich in den Prozess der legislativen Erkenntnisgewinnung eingebracht werden. Auf der anderen Seite ist aus Gründen des notwendigen Investitionsschutzes und der im Energiesektor grundlegenden Gewährleistung von Versorgungssicherheit ein Höchstmaß an Rechtssicherheit bei hinreichender Flexibilität zur Anpassung an zukünftige Technik- und Geschäftsmodellentwicklungen, mithin Innovationsoffenheit, zu realisieren.

Im einschlägigen Sachbereich liegt es insofern nahe, dass später noch wegen seiner kritischen Vorwirkungen aus anderer Perspektive zu betrachtende Festlegungsverfahren der §§ 21b i. V. m. § 29 EnWG als Schema auch für die Auflösung der Zielkonflikte zu betrachten.

Das nach §§ 21b Abs. 4 i. V. m. 29 EnWG eingeführte Festlegungsverfahren im Messwesen ist so ausgestaltet, dass die Bundesnetzagentur im Rahmen von Konsultationen der betroffenen Kreise gesetzlich geforderte Zielvorgaben formuliert. Von den Verbänden der Marktakteure werden sodann konkrete technische Spezifikationen erarbeitet, welche nach weitergehenden Konsultationen dann von den Beschlusskammern der BNetzA als allgemeinverbindlich erklärt werden. Rechtstechnisch handelt es sich bei der Festlegung um einen allgemeinverfügenden Verwaltungsakt. Dieser Akt steht allerdings unter der Prämisse eines gesetzlich angeordneten Änderungsvorbehaltes. Durch diese Verfahrengestaltung können also die Kenntnisse der betroffenen Kreise um eine sinnvolle Sachgestaltung sehr frühzeitig in den Entscheidungsprozess eingebracht und gleichzeitig unter der Ägide der sachgerechten Ermessensausübung eine im Vergleich zur unmittelbaren gesetzlichen Normierung flexible Änderung herbeigeführt werden, wenn sich innovationshemmende Wirkungen der Festlegungen zeigen. Gleichzeitig verbleiben die Sanktionsmechanismen und die Bestimmung der Umsetzungsfristen allein beim staatlichen Souverän. Im Hinblick auf das weitgehend zu konstatierende Versagen der bisherigen ordnungsrechtlichen Ansätze des Datenschutzes in Bereichen weniger komplexer Technikgestaltungen, dürfte diesem Ansatz aus Gründen der Effektivierung des Grundrechtsschutzes auch nicht das Wesentlichkeitsprinzip entgegenzuhalten sein, als die Formulierung der (neutral formulierten) Zielvorgaben beim Gesetzgeber verbleiben kann.

6 Materiellrechtliche Fragen

Da in Ermangelung bereichsspezifischer Datenschutzregelungen des Energiewirtschaftsrechts eine Analyse der Legitimation einzelner Verarbeitungsschritte und verfahrensrechtlichen Absicherungen der Messdatenübermittlung nur auf Basis des Bundesdatenschutzgesetzes erfolgen kann, ist es müßig über die zukünftige Rechtskonformität einzelner Datenflüsse und die erforderlichen Legitimationstatbestände zu spekulieren. Dass aber die allgemeinen Prinzipien des positiven Datenschutzrechts einer Überprüfung im Hinblick auf die zukünftige gesetzliche Ausgestaltung bedürfen, ist leicht ersichtlich. Insofern werden hier insbesondere die allgemeinen Begleitprinzipien des Datenschutzes einer Würdigung unterzogen.

7 Datensparsamkeit/ Pseudonymisierung

Aus globaler Perspektive ist insbesondere für die Elektromobilitätsszenarien das Gebot des § 3a BDSG dahingehend zu konkretisieren, als auch immer die Möglichkeit einer Inanspruchnahme von Ladestationen im Barverkehr erforderlich sein sollte.

Sofern aber eine Abrechung über den Heimatlieferanten gewünscht ist, oder eine Teilnahme am Tertiärregelenergiemarkt in Frage steht, scheidet eine Anonymisierung der Daten nach § 3 Abs. 6 BDSG aus, da die Personalisierung für Abrechnungszwecke möglich sein muss. Zumutbar wäre aber eine Systemgestaltung, welche eine pseudonyme Inanspruchnahme der Ladestation ermöglichte. Im Beispiel der Abbildung 2 würde für den Netzbetreiber eine Berechnung der anteiligen Netznutzungsentgelte und eine Saldierung gegen den Stromverbrauch des Anschlussinhabers auch auf Basis pseudonymisierter Daten ermöglicht werden. Die Bereitstellung und Auflösung des Pseudonyms und die Speicherung der Messdaten hätte allein durch den Rechnung stellenden Lieferanten zu erfolgen. Allerdings würde dem Lieferanten bei dieser Systemgestaltung bei der ihm technisch möglichen Depseudonymisierung nicht nur eine Auswertung der Messdaten, sondern auch die Auswertung der standortbezogenen Informationen ermöglicht werden. Da dem Lieferanten bis zum Ablauf der Frist zum Widerspruch gegen die Rechnung

15 Kilian, W. (2002): Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? In: Bizer, J., Lutterbeck, B., Rieß, J. (Hg.): Umbruch von Regelungssystemen in der Informationsgesellschaft – Freundesgabe für Alfred Büllesbach, 2002, S. 152.

16 Vesting, T. : Das Internet und die Notwendigkeit der Transformation des Datenschutzes. In: Ladeur, K.-H. (Hg.): Innovationsoffene Regulierung des Internet, Baden-Baden, 2003, S. 189.

auch die Archivierung der Daten obläge, würde hier einer weitgehenden Möglichkeit des Missbrauchs und einem Informationspool möglicher sicherheitspolitisch motivierter Begehrlichkeiten der Weg geebnet. Beide Aspekte kumulieren vor diesem Hintergrund zu einer starken Forderung nach einem technisch realisierten Zugriffsschutz hinsichtlich der Mechanismen zur Auflösung der Pseudonyme und der inhaltlichen Daten, dessen Einhaltung ggf. durch eine neutrale dritte Partei überprüfbar sein müsste.

8 Einwilligung

Das Beispiel der Energieeffizienzberatung zeigt wegen der vielfältig möglichen Kombination von Teildiensten, dass eine vollständige gesetzliche Antizipation der möglichen Rollen und Prozesse nicht möglich sein wird. Insofern ist es naheliegend, dass – sofern keine hinreichende vertragliche Legitimation besteht – die informierte Einwilligung eine Aufwertung in diesem Bereich erfahren kann. Die personenbezogenen Verbrauchs- und Gerätedaten der Nutzer einer solchen Effizienzberatung könnten auf den ersten Blick als Nutzungsdaten i. S. d. Telemediengesetzes (TMG) angesehen werden. Unter dessen Ägide könnte eine an den Vorgaben des § 13 Abs. 2 TMG orientierte medienbruchfreie elektronische Einwilligung auf der Dienstplattform realisiert werden. Allerdings findet das TMG und damit seine Einwilligungsregelung nur im Hinblick auf die Bestands- und Nutzungsdaten der Dienstnutzer Anwendung. Hierzu zählen die Verbrauchsdaten nicht.

Im Gegensatz zur Regelung des TMG stellt sich die Möglichkeit einer medienbruchfreien elektronischen Einwilligung unter der Ägide des Bundesdatenschutzgesetzes als problematisch dar. Die Formulierung „Schriftform" in § 4a Abs. 1 S. 3 BDSG bedeutet nach § 126 Abs. 1 BGB, dass die Erklärung vom Aussteller eigenhändig durch Namensunterschrift unterzeichnet werden muss. Daraus würde im konkreten Fall folgen, dass die Teilnehmer einer entsprechenden Dienst-Plattform einen Medienbruch durch Versand von entsprechend verkörperten, unterschriebenen Erklärungen hinzunehmen hätten. Zwar ist anerkannt, dass die Einwilligung unter der Voraussetzung einer qualifizierten elektronischen Signatur nach dem Signaturgesetz auch elektronisch erklärt werden kann.[17] Aus praktischer Sicht stellt sich für Dienste im zukünftigen Internet der Energie trotzdem das Problem, dass die vom Gesetz geforderte qualifizierte elektronische Signatur bislang nur einen äußerst geringen Verbreitungsgrad gefunden hat.[18] Zu den Gründen ist schon hinreichend ausgeführt worden.[19] De lege ferenda scheint es daher geboten, für den Energiesektor eine vereinfachte elektronische Einwilligung nach dem Vorbild des § 13 Abs. 2 TMG zu schaffen.

9 Systemdatenschutz

Neben dem Datenschutz muss im Energiemarkt auch aus Gründen der informationellen Entflechtung und des Schutzes von Geschäftsgeheimnissen gewährleistet werden, dass bei einer Übermittlung der Messdaten nur der berechtigte Empfänger Kenntnis von diesen Daten erlangen kann. Die Notwendigkeit eines entsprechenden Geheimnisschutzes lässt sich dadurch illustrieren, dass im Falle einer IKT-gestützten Energieberatung die gerätegenaue Verteilung der Stromflüsse in einem Unternehmen auch Rückschlüsse auf die Unternehmenstätigkeit zulassen kann.

Sowohl der Geheimnisschutz als auch die datenschutzrechtlichen Obliegenheiten konnten im Rahmen des Systemdatenschutzes im klassischen Energiemarkt noch durch organisatorische Maßnahmen sichergestellt werden. Einerseits wird dem Geheimnisschutz für die hier interessierenden Fälle schon mittelbar durch organisatorische Maßnahmen im Rahmen der informatorischen Entflechtung beim Netzbetrieb nach § 9 Abs. 1 EnWG Rechnung getragen.[20] Auf der anderen Seite konnte mit organisatorischen Maßnahmen nach § 9 BDSG, wie Instruktionen zum zulässigen Datenumgang, auch den datenschutzrechtlichen Obliegenheiten genügt werden, da aufgrund der langfristigen Ableseintervalle ein geringes Missbrauchsrisiko bestand. Wegen der geringen Anzahl möglicher Empfänger der Messdaten und der gesetzlich fixierten Verarbeitungsschritte war dies nicht grundlegend in Frage zu stellen.

Zukünftig stellt sich wegen des hohen Datenaufkommens und der Datenübermittlung an weitere Akteure allerdings die Frage, ob es zur Sicherung der vorgenannten Aspekte nicht generell einer zusätzlichen Sicherung durch die Implementierung von Mechanismen des technischen Zugriffsschutzes bedarf. In der Tat dürfte sich die Abwägung zwischen den berechtigten Schutzinteressen der Endkunden und den Interessen der Daten verarbeitenden Stellen an einer möglichst ungehinderten Verwendung der Daten für eine Vielzahl von möglichen Auswertungen und Übermittlungen, vor dem Hintergrund der gesteigerten Sensibilität der Messdaten, verschieben. Die Bereitstellung von Mechanismen des technischen Zugriffsschutzes erfordert zwar einen anfänglichen Implementierungsaufwand, meidet aber die Schwächen des organisatorischen Datenschutzes, wie personelle Diskontinuität, fehlendes Rechtswissen und bewusste Ausnutzung von Schutzlücken.

Zudem könnten technische Mechanismen des Zugriffschutzes eine unmittelbare Repräsentation des Nutzerwillens in dem technischen System und die zwingende Durchsetzung gesetzlicher Vorgaben wie Transparenz der Datenverarbeitung oder die Durchsetzung von gesetzlichen Nutzerrechten effektivieren.

Ob und inwieweit sich ein legislativer Handlungsauftrag für einen ggf. bereichsspezifisch geregelten Zwang zur Verwendung von technischen Mechanismen des Systemdatenschutzes aus den grundrechtlichen Schutzpflichten des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verdichtet, muss noch weitergehend untersucht werden. Allerdings kann an dieser Stelle angemerkt werden, dass sich bei einer Gesamtschau der Regelungen des § 40 Abs. 3, 21b EnWG mit der Einführung der SmartMeter eine Sachgestaltung ergibt, die in ihrer praktischen Konsequenz auf die Pflicht zur Verwendung von IKT-Infrastrukturen im Hausanschlussbereich hinausläuft. Es ist nicht fernliegend, dem damit staatlich gesetzten Risiko einen korrespondierenden

17 Gola/Schomerus, Bundesdatenschutzgesetz Kommentar, zu § 4a BDSG Rn. 13. Allerdings ist auch die Verwendung von signaturgesetzkonformen PIN-Verfahren im Hinblick auf den besonderen Rang des Schriftformerfordernisses im Datenschutzrecht in der Literatur in Abrede gestellt worden, vgl. Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, S. 100.

18 Die elektronische Einwilligung hat nach Schleipfer, RDV 2005, 56, im Rahmen des BDSG noch eher theoretische Natur.

19 Siehe nur Bizer, DuD 2002, 276 f.

20 Vgl. BNetzA, Gemeinsame Richtlinien der Regulierungsbehörden des Bundes und der Länder zur Umsetzung der Informatorischen Entflechtung nach § 9 EnWG, S. 16, 2007. Abrufbar unter: http://www.bundesnetzagentur.de/media/archive/10485.pdf [Abgerufen am 11.01.2010].

Sicherungsauftrag für die informationelle Selbstbestimmung zuzumessen. Im europäischen Kontext des Datenschutzes ist dabei zu beachten, dass das niederländische Parlament im April 2009 der im Gesetzentwurf enthaltenen Verpflichtung zur Verwendung von SmartMetern durch Endkunden gerade im Hinblick auf Datenschutzaspekte nicht zugestimmt hat.[21]

Ein Datenschutzkonzept, welches in diesem grundrechtsrelevanten Bereich einen angemessenen Ausgleich im Sinne der Verwirklichung praktischer Konkordanz herstellen will, muss aber, wie schon die Erfahrungen bei der Einführung der RFID-Technologie zeigen, einen deutlichen Schwerpunkt in den Bereich des technischen Datenschutzes legen.[22]

Zusammenfassend lässt sich also als erste Herausforderung festhalten, dass insbesondere technische Maßnahmen des Zugriffsschutzes anhand technisch formaler, das Gesetz repräsentierender Verarbeitungsregeln, bei allen Akteuren der zukünftigen Prozessketten der Mess- und Vertragsdatenverarbeitung im Smart Grid gesetzlich als pflichtig normiert sein müssen.

10 Protokolle und Nachrichtenformate

Neben den durch gesetzliche Vorgaben terminierten Verarbeitungsregeln müssen aber im SmartGrid auch die Entscheidung des Betroffenen zu erlaubten oder verbotenen Verwendungen der Mess- und Vertragsdaten in jeder Entscheidungssituation zwingend berücksichtigt werden. Insofern muss in den hier behandelten Beispielfällen die Nutzerentscheidung schon an der Quelle, dem Messgerät, den Messdaten beigefügt und wiederum als zwingende technische Regel im System des Zugriffsschutzes berücksichtigt werden. Dies bedeutet aber, dass die verwendeten Nachrichtenformate und Sicherungsmechanismen für die Messdatenübermittlung eine entsprechende Repräsentation des Nutzerwillens unterstützen müssen.

Eine technische Kapselung und Zugriffssteuerung, wie sie im Markt bereits entwickelt ist, muss also in unserem Beispiel durch alle Protokolle und Datenmodellierungsstandards der Marktkommunikation unterstützt werden.

10.1 Standardisierung

In diese Richtung sind auf europäischer Ebene die Bemühungen des ebIX[23] angelegt. Im RFC „Exchange of metered data" findet sich der Use Case „Apply Confidentiality Rules".[24] Der ebIX ist zwar noch nicht ausdefiniert, aber es zeigt sich, dass auf europäischer Ebene davon ausgegangen wird, dass Meter Data Informationen künftig technisch geschützt werden sollen. Die „European Federation of Energy Traders (EFET)" hat folgerichtig in der Spezifikation für den Datenaustausch im Energiehandel EFET eCMim Rahmen der ebXML-Standardisierung die vorgenannten Aspekte ebenfalls standardisiert[25], um die erforderliche Ende-zu-Ende-Sicherheit zu gewährleisten.

Ergänzend kommt hinzu, dass aus dem Eichrecht erwachsene beweisrelevante Vertrauenstatbestände für die Richtigkeit der Messdaten in die digitale Welt transformiert werden müssen. Im Hinblick auf die vielfältigen zukünftigen Messdatenempfänger, die in besonderer Weise auf die Sicherstellung der Herkunft und Unverfälschtheit der Messdaten angewiesen sind, ist eine elektronische Signierung und Sicherung vor Verfälschung der relevanten Verbrauchsdaten am Ort der Entstehung notwendig. Die einmal generierten Vertrauenstatbestände müssen auch auf dem Energiekernmarkt transparent Ende-zu-Ende gewährleistet werden.

Insofern gewinnt aber das schon angeführte Festlegungsverfahren der BNetzA vorwirkendes Gewicht, als hier hinsichtlich der zur Messdatenübermittlung notwendigen Nachrichtenformate eine Entscheidung getroffen wird.

10.2 Festlegungen der BNetzA

Die zuständigen Beschlusskammern der Bundesnetzagentur haben zur Erfüllung ihrer energiewirtschaftsrechtlichen Verpflichtungen zur Schaffung eines liberalisierten Marktes des Zähl- und Messwesens gemäß den §§ 29 EnWG, 13 MessZV im Jahr 2009 ein Festlegungsverfahren zur Standardisierung von Verträgen und Geschäftsprozessen im Bereich des Messwesens eröffnet und auf der Grundlage eines Verbändeentwurfs eine gemeinsame Beschlussvorlage erarbeitet. Neben vertragsrechtlichen Fragen stehen dabei auch Festlegungen zu den verbindlich durch die Marktakteure zu verwendenden Datenformate bei der Übermittlung der Messdaten zur Entscheidung an.

10.3 Formelle Aspekte

Wie bereits ausgeführt ist wegen der Unwägbarkeiten heutiger Festlegungen für die Zukunft die Festlegung mit einem Änderungsvorbehalt ausgestattet. Dieser ermöglicht es der BNetzA, unter Anwendung pflichtgemäßen Ermessens die hier relevanten Festlegungen zu den Datenformaten zukünftig zu ändern. Trotz dieses Vorbehaltes ist im Hinblick auf die erforderliche Ermessensbetätigung fraglich, ob im Hinblick auf höherrangiges Recht und die bei einer Änderung vorzunehmende Verhältnismäßigkeitsprüfung eine nachträgliche Anpassung der Datenformate in Betracht kommt.

Mit der verbindlichen Festlegung von Datenformaten werden bei den betroffenen Akteuren unmittelbare Investitionsentscheidungen hinsichtlich der verwendeten Software ausgelöst. Daneben werden auch im Bereich der Softwareentwicklung entsprechende Anwendungsimplementierungen veranlasst. Anders als bei den Festlegungen zur Netzentgeltregulierung und den hier gegenständlichen Prozessformalisierungen ist eine Anpassung nur mit erheblichen, aber zwingenden, Folgeinvestitionen möglich.

10.4 Materielle Aspekte

Nach den vorhandenen Prozessbeschreibungen ist für die hier interessierenden Messdaten zukünftig der Netzbetreiber für die Anforderung von Messwerten beim Messdienstleister zuständig. Er fungiert damit als Datendrehscheibe zwi-

21 Vgl. http://vortex.uvt.nl/TILTblog/?p=54 [Abgerufen am 11.01.2010].

22 vgl. nur für den insofern vergleichbaren Bereich die „Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" (KOM(2007) 96) , ABl. C 101/1 S.7.

23 European forum for energy Business Information eXchange (ebIX)

24 Exchange of metered data v0.9, S. 32 http://ebix.neonoesis.de/documents/ebIX_model_Measure_Introduction_0_9.doc [Abgerufen am 11.01.2010].

25 Vgl. Electronic Confirmation Matching Standards Version 3.3.1 Final, February 2009, S. 127 – 129.

schen dem Messdienstleister und den anderen Marktbeteiligten.[26] Als Nachrichtentyp für die Übermittlung der Messdaten vom Netzbetreiber an die anderen Marktakteure ist insofern das Format EDIFACT/MSCONS bestimmt[27], ein Nachrichtenformat, das für die klassischen B2B-Strukturen des Energiekernmarktes noch keine sinnvolle Etablierung gefunden hat.

Nicht zu erkennen ist aber, dass sich der Regulierer im Rahmen des laufenden Festlegungsprozesses sich den hier annoncierten Paradigmenwechsel im gedanklichen Vorgriff vergegenwärtigt hat. Die Bundesnetzagentur hatte zwar in ihren Erwägungen zu den GPKE-Festlegungen im Jahre 2006 selbst eine Abwägung zwischen den auf EDIFACT basierten Kommunikationsverfahren und dem XML-Pendant angestellt, aber eine Verwendung wegen mangelnder Marktdurchdringung von XML-Derivaten abgelehnt.

Die neuen Rollen und Kommunikationsprozesse im SmatGrid erfordern hingegen flexible Datenstandards, die eine Trennung von Datenstrukturen und semantischen Inhalten ermöglichen. Grundlegende Eigenschaften dieser Verfahren sind standardisierte Transformationsverfahren, Selbstbeschreibung und einfache formale grammatikalische Validierbarkeit. EDIFACT ist hingegen nicht selbstbeschreibend, d. h. es gibt in EDIFACT kein Konzept eines externen, beschreibenden Schemas, das auch zur Validierung (und Erzeugung) der Nachrichten eingesetzt werden kann.

Es gibt damit keine Möglichkeit, bei bestehenden Implementierungen die EDIFACT-Formate anzupassen oder auszutauschen. Die Spezifikation von EDIFACT existiert nur als textuelle Dokumentation. Die Spezifikation unterstützt damit nicht ihre eigene Implementierung; zudem ist auch der Änderungszyklus im Prozess von EDIFACT schwerfällig.

Aus datenschutzrechtlicher Sicht entscheidend ist aber, dass aus der Dokumentation zu MSCONS weder eine Unterstützung z. B. für fortgeschrittene Signaturverfahren nach dem Signaturgesetz noch ein dezidiertes Schema für die Kennzeichnung von datenschutzrechtlichen Zugriffsberechtigungen ersichtlich ist.[28]

Vor diesem Hintergrund besteht zusammenfassend die Gefahr, dass sich im Hinblick auf den oben adressierten Systemdatenschutz durch die zwingende Integration von technischen Mechanismen des Zugriffsschutzes zukünftig Parallelinfrastrukturen entwickeln, die einer Steuerung durch den Regulator nur noch schwer zugänglich sind.

11 Fazit

Aus datenschutzrechtlicher Sicht bedarf es zur Sicherung der informationellen Selbstbestimmung einer frühzeitigen Integration von bereichsspezifischen Regelungen zum Datenschutz in das Energiewirtschaftsgesetz. Zur Sicherung der notwendigen Flexibilität und Rechtssicherheit sollten hierbei nach dem Schema des energiewirtschaftsrechtlichen Festlegungsverfahrens kooperative Mechanismen zur materiellen Ausgestaltung von Anforderungen an den Systemdatenschutz etabliert werden. Wegen der langfristigen Vorwirkungen von kommenden Festlegungen im Rahmen des Messwesens ist eine frühzeitige Antizipation der zukünftigen Belange des Systemdatenschutz im SmartGrid durch die Bundesnetzagentur notwendig.

26 http://www.bundesnetzagentur.de/media/archive/16664.pdf (S. 59) [Abgerufen am 11.01.2010].

27 http://www.bundesnetzagentur.de/media/archive/16664.pdf (S. 64) [Abgerufen am 11.01.2010].

28 Siehe http://www.edi-energy.de/files2/EDI@Energy_MSCONS_AHB_2.1a_20081001.pdf [Abgerufen am 11.01.2010].