Widmung

Vorwort

XXX

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Ansicht
a. E.	am Ende
a. F.	alte Fassung
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz

BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
CC	Common Criteria
CR	Computer und Recht
DÖV	Zeitschrift für Öffentliches Recht und Verwaltungswissenschaften
DuD	Datenschutz und Datensicherheit
DV	Die Verwaltung
DVBl.	Deutsches Verwaltungsblatt
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EnWG	Energiewirtschaftsgesetz
ErwGr.	Erwägungsgrund
EU	Europäische Union
EUV	Vertrag über die Europäische Union
EVU	Energieversorgungsunternehmen
f./ ff.	folgende
Fn.	Fußnote
GPKE	Geschäftsprozesse zur Kundenbelieferung mit Elektrizität
HAN	Home Area Network/ Heimnetzwerk

Hrsg.	Herausgeber
Hs.	Halbsatz
i. d. R.	in der Regel
i. e. S.	im engeren Sinne
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
i. w. S.	im weiteren Sinne
IFE	Informatik - Forschung und Entwicklung
IKT	Informations- und Kommunikationstechnologie
InTeR	Zeitschrift zum Innovations- und Technikrecht
K&R	Kommunikation & Recht
KOM	Kommission
kW(h)	Kilowatt(stunde)
LF	Lieferant
LG	Landgericht
LMN	Local Metrological Network/ Lokales metrologisches Netz
Ls.	Leitsatz
m. w. N.	mit weiteren Nachweisen
MaBiS	Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom
MessZV	Messzugangsverordnung

MMR	Multimedia und Recht
MSB	Messstellenbetreiber
MsbG-E	Entwurf eines Messstellenbetriebsgesetzes
MSCONS	Metered Services Consumption report message
MsysV-E	Entwurf einer Messsystemverordnung
n. F.	neue Fassung
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OBIS	Object Identification System
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PP	Protection Profile
P3P	Platform for Privacy Preferences
PING	Policy Language Interest Group
PTB	Physikalisch-Technische Bundesanstalt
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer
SigG	Signaturgesetz
SMGW-Admin	Smart Meter Gateway-Administrator
StromNZV	Stromnetzzugangsverordnung
TKG	Telekommunikationsgesetz

TMG	Telemediengesetz
TR	Technische Richtlinie
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
ÜNB	Übertragungsnetzbetreiber
VerwArch	Verwaltungsarchiv
vgl.	vergleiche
VNB	Verteilnetzbetreiber
VO	Verordnung
VV	Verwaltungsvorschrift
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
W3C	World Wide Web Consortium
WAN	Wide Area Network
WiM	Wechselprozesse im Messwesen
XML	Extensible Markup Language
ZD	Zeitschrift für Datenschutz
ZNER	Zeitschrift für neues Energierecht

Im Übrigen wird auf die Abkürzungen nach Kirchner, Abkürzungsverzeichnis der Rechtssprache (8. Auflage, Berlin 2015), verwiesen.

Teil 1: Einleitung

A. Motivation

In der Energiewirtschaft hat in den letzten Jahren ein ***doppelter*** *bzw.* ***mehrschichtiger Paradigmenwechsel*** stattgefunden. Bedingt durch die europäischen Vorgaben zur Steigerung der Energieeffizienz[1] und der Etablierung eines intelligenten Energieinformationsnetzes (Smart Grid)[2] wurden sogenannte intelligente Messsysteme (Smart Meter)[3] eingeführt, um Netzbetreibern und Energieversorgungsunternehmen eine Optimierung des Stromverbrauchs zu ermöglichen sowie die aktive Beteiligung der Verbraucher am Stromversorgungsmarkt zu unterstützen. Durch die Einführung vernetzter Energiesysteme wurde auf die zunehmende Nutzung von Energie aus regenerativen aber auch fluktuierenden Quellen wie Wind und Sonne, welche im Gegensatz zu klassischen Kraftwerken nicht steuerbar sind, reagiert und somit die Voraussetzungen für eine bessere In-

---

1 Siehe ErwGr. 27, 55, Art. 3 Abs. 11, Anlage I Pkt. 2 Elektrizitätsbinnenmarkt-RL 2009/72/EG.

2 Unter dem Begriff „Smart Grid" wird ein „intelligentes" Netz verstanden, bei dem Stromerzeuger, Verbraucher, Speicher sowie Netzbetriebsmittel vernetzt werden, vgl. Wiesemann, MMR 2011, S. 355.

3 Nach § 21d Abs. 1 EnWG a.F. wurde in Umsetzung der europäischen Vorgaben ein Messsystem definiert als eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt. Der Begriff des intelligenten Messsystems war gesetzlich noch nicht eingeführt. Nach § 2 Nr. 7 MsbG handelt es sich bei einem intelligenten Messsystem um eine über ein Smart-Meter-Gateway in ein Kommunikationsnetz eingebundene moderne Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt und den besonderen Anforderungen nach den §§ 21 und 22 MsbG genügt, die zur Gewährleistung des Datenschutzes, der Datensicherheit und Interoperabilität in Schutzprofilen und Technischen Richtlinien festgelegt werden können. Ein Messsystem wird in § 2 Nr. 13 MsbG hingegen lediglich als eine in ein Kommunikationsnetz eingebundene Messeinrichtung definiert.

tegration erneuerbarer Energien geschaffen. Hierfür wurde damit begonnen, erforderliche Mechanismen - wie sogenannte lastvariable und damit von der aktuellen Wetterlage abhängige Tarife - zur Anpassung des Stromverbrauchs an die jeweilige Erzeugungssituation zu etablieren. Die zeitnahe Übermittlung dieser sogenannten Anreiztarife dient dabei der Motivation von Kunden, einen möglichst großen Anteil ihres Stromverbrauchs in Zeiten zu verlagern, in welchen die Erzeugung aus regenerativen Quellen hoch und der Gesamtverbrauch niedrig ist. Gleichzeitig sollen die Messdaten die ***Prognosebasis*** der Energielieferanten für die Kraftwerkseinplanung verbessern. Diese Mechanismen erfordern in der Konsequenz eine vollelektronische Abrechnung mittels Messsystemen mit einer entsprechenden Kommunikationsschnittstelle. Damit wird nicht nur die Möglichkeit der elektronischen Übermittlung von Messwerten notwendig, sondern auch eine vollelektronische Abwicklung der übrigen (Mess-)Datenbedürfnisse der Akteure des klassischen Energiemarktes auf Basis einer Kommunikationsverbindung bis zum Letztverbraucher. Zugleich wird damit auch eine fernkommunikative Vernetzung der Messsysteme für die kommende Integration von Elektromobilität in das Energiesystem ermöglicht.[4]

…

[4] *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831, 839.

Teil 2: Wissensperspektiven zum Smart Grid

A. Legislative und behördliche Wissensdefizite zum Smart Grid

I. Einleitung

Wie bereits angedeutet, waren im Energiewirtschaftsrecht seit Einführung des Smart Meter zur Entwicklung eines Smart Grid nicht nur zahlreiche Gesetzesneuerungen zu verzeichnen, sondern es wurden auch Verfahren zur Digitalisierung des Energiemarktes, wie das bei der BNetzA angesiedelte Festlegungsverfahren implementiert, welche den Gesetzgeber entlasten sollten. Der energiewirtschaftsrechtliche Kontext kann aufgrund der Technisierung als dynamisch bezeichnet werden, weil dessen erforderliche Wissensgrundlage aus mehreren Quellen zusammengestellt werden müssen, wie beispielsweise dem Marktwissen von Verbänden und dem Technikwissen von Informatikern, wie auch dem Wissen um verbraucherschutzrechtliche oder datenschutzrechtliche Aspekte, welche bei Vereinigungen von Verbraucherschützern oder den Datenschutzaufsichtsbehörden vorhanden sind. Aus diesem Grunde konnte kaum auf vorhandenes **Erfahrungswissen** zum Zusammenwachsen von ehemals getrennten Sachdomänen zurückgegriffen werden, weil dieses Wissen aus anderen Netzwirtschaften - wie beispielsweise dem Telekommunikationssektor - nicht vollständig übertragbar war. Dies stellte und stellt Gesetzgeber und Verwaltung im Hinblick auf die Wissensgenerierung und -verarbeitung vor große Herausforderungen. Dass diese Prozesse der Wissensgenerierung und -verarbeitung als Vorstufe zu den rechtlich verbindlichen Entscheidungen wie den Erlass eines bestimmten Gesetzes oder eines bestimmten Standards oder Prozesses im Festlegungsverfahren teilweise nicht optimal funktionieren können, wurde bereits allgemein dargelegt. Im Folgenden sollen die konkreten Defizite in den historischen Wissensgenerierungs- und Wissensverabeitungsprozessen dargestellt werden, aufgegliedert in legislative Wissensdefizite und solche der Regulierungsbehörde

als Exekutive. Auch wenn ein Zusammenspiel mehrerer Faktoren und Komponenten zu den erläuterten Fehlern geführt hat, soll Anknüpfungspunkt für Problemlösungen bzw. Optimierungsvorschläge lediglich das Festlegungsverfahren[1] der BNetzA und die dazugehörigen Problemkreise sein. Grund hierfür ist, dass Herausforderungen und vor allem Lösungen in dem damit gewählten beschränkten Rahmen besser herausgearbeitet werden können und eine spätere Übertragbarkeit erleichtert wird. Zudem sind für die Zukunft mit der nun expliziten Zuweisung für ***produktbezogene Maßnahmen*** am Ende der Kommunikationsinfrastruktur an das BSI gleichwohl noch die Fragen von ***prozessbezogenen Maßnahmen*** der ***Marktkommunikation*** weitgehend ungelöst. Dabei handelt es sich um eine Sachmaterie, die wegen der *auch* wettbewerblichen Implikationen schon in klassischer Betrachtung in der Regulierungszuständigkeit der BNetzA verbleiben wird.

II. Einzelne legislative Wissensdefizite

1. Ausgestaltung des rechtlichen Rahmens

Mit der Novellierung des EnWG im Jahr 2011 wurde - motiviert durch die Einführung von kommunikativ vernetzen Messsystemen - mit den §§ 21g-i EnWG erstmals datenschutzrechtliche Regelungen in das EnWG aufgenommen. Bei der Konzeption der Normen wurden jedoch auf mehreren Ebenen die energiewirtschaftlichen Rahmenbedingungen nicht hinreichend zur Kenntnis genommen. Dies gilt insbesondere für die bestehenden verbindlichen ***Vorgaben der elektronischen Marktkommunikation***, aber teilweise auch hinsichtlich der ***klimapolitischen Zielsetzungen***, die seit

[1] Dies muss wiederum eine Eingrenzung finden, indem das Festlegungsverfahren nach § 29 EnWG i.V.m. § 27 Abs. 1 Nr. 11 StromNZV zur bundeseinheitlichen Regelung zum Datenaustausch zwischen den betroffenen Marktteilnehmern, insbesondere hinsichtlich Fristen, Formaten sowie Prozessen, die eine größtmögliche Automatisierung ermöglichen, Gegenstand der Arbeit ist.

der Einführung der Smart Meter beim Endkunden verfolgt werden sowie bezüglich der notwendigen ***verfahrensrechtlichen Gestaltungen***.

Im Rahmen einer Bestandsaufnahme defizitärer energiewirtschaftlicher Rahmenbedingungen wird im Folgenden zunächst das ***materielle datenschutzrechtliche Konzept*** mit seinen Schwerpunkten erläutert.

Daraufhin wird auf den ***technischen Datenschutz*** und damit auf das erstmals eingeführte materielle Prinzip der Datenhoheit und schließlich aus verfahrensrechtlicher Perspektive und dessen ***Sicherung durch technische Schutzprofile*** eingegangen.

a. Vier-Säulenmodell

Bei der Einführung der materiellen Datenschutzregelungen in das EnWG hatte sich der Gesetzgeber auf als zentralen Säulen konzipierte grundlegende Bestimmungen beschränkt, da angesichts der Fülle und des notwendigen Detaillierungsgrades erst die Verordnung die genannten Konkretisierungen in Form von speziellen technischen Vorgaben enthalten sollten.[2] Geplant war die Regelung der Mindestfunktionalitäten der Messsysteme, die Verpflichtung zum Einbau der Messsysteme in gesetzlich festgelegten Fällen sowie die bereichsspezifische Verankerung von Datenschutz und Datensicherheit zum Schutz der Verbraucherinteressen.[3]

Während das BDSG für die Gewährleistung eines prozessbezogenen Datenschutzes die notwendigen Schutzprinzipien entlang der gesetzlich vorgegebenen Prozesskette vollständig implementiert, wird im EnWG als der spezielleren Regelung der Fokus lediglich auf den Datenschutz des Produktes Smart Meter und seiner technischen Komponenten gelegt. Grund hierfür ist, dass ausweislich der Gesetzesmaterialien die gesetzlichen Regelungen im Wesentlichen als stark nutzerzentriertes Schutzkonzept kon-

2 BR-Drs. 343/11, S. 193 f.

3 BR-Drs. 343/11, S. 193 f.

zipiert wurden.[4] Dieses baut auf dem neuen Prinzip der „Datenhoheit des Anschlussnutzers“ auf, mit dessen gesetzlicher Umsetzung der Gesetzgeber seiner aus dem verpflichtenden Einbau von Smart Metern resultierenden Folgen- bzw. Gewährleistungsverantwortung gerecht werden wollte.

Kernelement der datenschutzrechtlichen Regelungen stellte § 21g EnWG dar. Der **Zweck** der einzelnen materiellen Normierungen des § 21g EnWG erschloss sich in weiten Teilen erst aus einer **Gesamtschau** der datenschutzrechtlich wirkenden Normen, welche das gesetzliche Schutzkonzept des novellierten EnWG [5] bildeten. Letzteres ließ sich, wie dargelegt, im Wesentlichen in vier Säulen aufgliedern, welche den Teilbereichen der materiell-rechtlichen Regelungen, der Rechtsverordnungsermächtigungen sowie den datensicherheitsrechtlichen Vorgaben untergeordnet werden konnten.[6] Veranschaulichend stellt sich das Modell folgendermaßen dar.

i. Erste Säule – materieller Grundbestand datenschutzrechtlicher Regelungen

Im Gesetz selbst war in den §§ 21g und h EnWG neben der Statuierung eines neuen, grundlegend nutzerzentrierten Schutzkonzeptes ein materieller Grundbestand an datenschutzrechtlichen Minimalregelungen und insbesondere zulässigen Zwecken der Datenverwendung normiert.[7] § 21g Abs. 1 EnWGstellte dabei die materielle Grundnorm für Datenverwendungen im EnWG dar. Sie bestimmte, unter welchen materiellen Voraussetzungen und für welche Zwecke die zum Datenumgang berechtigten Stellen mit personenbezogenen Daten im Kontext des Messsystems um-

4 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1 Teil 1, § 21 g Rn. 2. *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831, 832.

5 BGBl. I 2011, S. 1554.

6 Nach *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831, 831.

7 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 832.

gehen durften.[8] Indem § 21g EnWG das Prinzip des Verbots mit Erlaubnisvorbehalt konstituierte (vgl. § 4 Abs. 1 BDSG), stellte er die zentrale Vorschrift des bereichsspezifischen Datenschutzrechts des EnWG dar.[9] Dieser besagte, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem grundsätzlich verboten sei, sofern für die Datenverwendung keine Legitimationsgrundlage vorliege.[10] Aus diesem Grund wurden in § 21g Abs. 1 EnWG zur Ausgestaltung des Prinzips der Zweckbindung abschließend legitimierende Zwecke enumerativ aufgezählt, welche sich jedoch in ihrem Detaillierungsgrad erheblich unterschieden. Zur Konkretisierung des personellen Anwendungsbereich wurden in § 21g Abs. 2 EnWG *„zum Datenumgang berechtigte Stellen"* legal definiert. Dies waren neben dem MSB der Netzbetreiber (NB), der Lieferant (LF) sowie eine dritte Stelle, die eine schriftliche Einwilligung nach den Voraussetzungen des § 4a BDSG nachweisen konnte.

Flankiert wurden die Vorschriften durch Regelungen über die rechtswidrige Inanspruchnahme von Messsystemen und Diensten (§ 21g Abs. 3 EnWG) und zur Auftragsdatenverarbeitung (§ 21g Abs. 4 EnWG).[11] Des Weiteren wurden in Abs. 6 einzuhaltende nicht abschließende Grundsätze wie Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung und insbesondere ein Koppelungsverbot aufgestellt, welchen die Rechtsverordnung gerecht werden musste.[12]

§ 21h EnWG normierte in Abs. 1 schließlich - trotz der Beschränkung der amtlichen Überschrift auf „Informationspflichten" - in der datenschutz-

---

8 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 832.

9 *Lorenz/Raabe*, in: Säcker, Energierecht, Band 1 (Teil 1), EnWG, § 21g Rn. 17.

10 *Weis/Pallas/Lorenz/Raabe*, in: Boesche/Franz/Fest/Gaul, Berliner Handbuch zur Elektromobilität, S. 304.

11 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 64 und 81.

12 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 96 und 97.

rechtlichen Terminologie Auskunftsrechte des Betroffenen gegenüber dem Messstellenbetreiber (MSB).[13] Diese gehören zu den unabdingbaren Rechten von Betroffenen, da sie die Betroffenen erst in die Lage versetzen, weitere Rechte geltend zu machen.[14] Die tatsächliche Informationspflicht in Abs. 2 zielte hingegen auf eine Rechtspflicht der zum Datenumgang berechtigten Stelle, ohne dass es einer Initiative des Betroffenen bedurfte.[15] Wie auch im Rahmen des § 42a BDSG räumte der Gesetzgeber mit dieser Pflicht zur Publizität dem „informationellen Selbstbestimmungsrecht des Betroffenen Vorrang vor den Geheimhaltungsinteressen des Datenverarbeiters ein“. [16]

ii. Zweite Säule - Ermächtigung für konkretisierende datenschutzrechtliche Rechtsverordnungen

Daneben wurde in § 21i EnWG die Ermächtigung für Rechtsverordnungen geschaffen, welche verbindliche Vorgaben zu Mindestanforderungen datenschutzrechtlicher Prinzipien enthalten sollten.[17] In einem umfangreichen Katalog, adressiert an die Bundesregierung, wurden „verbindliche Vorgaben zu Mindestanforderungen datenschutzrechtlicher Prinzipien“ gemacht.[18] Eine weitere Konkretisierung fand sich in § 21g Abs. 6 S. 1 EnWG. Darin waren Vorschriften zum Schutz personenbezogener Daten der an der Energieversorgung Beteiligten enthalten, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regelten (§ 21g Abs. 6 S. 2 EnWG). Ferner hatten die zu erlassenden Vorschriften den Grundsätzen der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung,

---

13 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 h Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 837.

14 *Gola/Schomerus*, § 34 Rn.1.

15 *Lorenz/Raabe* , in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 h Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 838.

16 *Dix* in: Simitis, § 42a Rn. 1.

17 *Lorenz/Raabe*, in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 832.

18 *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831, 831.

Verarbeitung und Nutzung auf das Erforderliche, sowie dem Grundsatz der Zweckbindung Rechnung zu tragen (§ 21g Abs. 6 S. 3 EnWG).[19] [20]

iii. Dritte Säule – Datenhoheit und Technischer Datenschutz

Schließlich wurden in § 21e EnWG verbindliche, am „*Stand der Technik*" orientierte Schutzmaßnahmen für das eigentliche Messsystem eingeführt, die in Schutzprofilen und Technischen Richtlinien konkretisiert werden sollten.[21] Damit wurde das Prinzip der Datensparsamkeit durch Einführung von Maßnahmen des Systemdatenschutzes verwirklicht, indem in Schutzprofilen und Technischen Richtlinien verbindliche am Stand der Technik orientierte Schutzmaßnahmen für das Messsystem vorgeschrieben wurden.

Da der Anschlussnutzer durch die gesetzliche in §§ 21c Abs. 4 EnWG verankerte Einbaupflicht die Installation eines Messsystems nicht verhindern konnte, sollte dieser bereits ab Einbau eines Messsystems unter das besondere Schutzprogramm des EnWG zu stellen sein.

---

19 Hierzu *Wieczorek,* in: Taeger, Big Data & Co – Neue Herausforderungen für das Informationsrecht, S. 448 ff.

20 Bezüglich der Verabschiedung der erforderlichen Verordnungen legte die Bundesregierung im Februar 2015 das Verordnungspaket Intelligente Netze vor. Darin wurden drei konkrete Verordnungsvorhaben angeführt: Eine Messsystemverordnung als technische Grundlagenverordnung, welche schon in einer Entwurfsfassung als MsysV-E seit längerer Zeit vorlag, eine Datenkommunikationsverordnung, die den zulässigen Datenumgang regeln soll, sowie eine „Rollout"-Verordnung zu den Fragen der tatsächlichen Umsetzung und Finanzierung der intelligenten Messsysteme. Vgl. BMWi, Verordnungspaket Intelligente Netze, S. 2.
Da jedoch in der Vielzahl der Verordnungsermächtigungen nach § 21i EnWG die Gefahr vermutet wurde, dass das Energiewirtschaftsrecht hierdurch zu komplex und zersplittert geregelt würde, wurde in Art. 1 des Entwurfs eines Gesetzes zur Digitalisierung der Energiewende das MsbG als „Stammgesetz" vorgeschlagen. Darin sollen nunmehr die grundrechtsrelevanten Regelungen des Energierechts im Sinne der Verfahrensklarheit einheitlich geregelt werden.

21 *Lorenz/Raabe* in: Säcker, Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 2; *Raabe/Lorenz/Pallas/Weis*, CR 2011, S. 831, 832.

Dies konnte für das Messsystem als zentralem Bestandteil der IKT-Infrastruktur nur durch die in § 21e EnWG normierten technische Anforderungen in Form von Schutzprofilen verwirklicht werden, welche dem jeweiligen „*Stand der Technik*“ entsprechende Schutzmaßnahmen zur Sicherstellung von Datenschutz und Datensicherheit vorsehen mussten. Mit § 21e EnWG wurde eine bereichsspezifische Regelung geschaffen, die dazu verpflichtet, „datenschutzfördernde Technik“ einzusetzen.[22] In § 21e Abs. 1 EnWG a.F. wurde neben der Einhaltung eichrechtlicher Vorschriften die Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität in Messsystemen zwingend vorgeben. Detaillierte Regelungen dazu fanden sich in den Absätzen 2 bis 4. Demnach mussten Messsysteme den Anforderungen aus Schutzprofilen entsprechen und Interoperabilität gewährleisten (Abs. 2), dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit treffen (Abs. 3) sowie festgelegte Zertifizierungsverfahren einhalten (Abs. 4). Für die praktische Umsetzung waren die Anforderungen der Schutzprofile[23] und der Technischen Richtlinie[24] des BSI zu berücksichtigen, die ihrerseits rechtlich verbindlich umgesetzt werden sollen.[25]

iv. Vierte Säule – Einbaupflicht für Smart Meter

Mit Einführung des § 21c Abs. 1 EnWG hatte der Gesetzgeber erstmals für den Letztverbraucher die Pflicht zur Nutzung von Smart Metern verankert. Dies begründete gleichzeitig die staatlich gesetzte Pflicht der be-

22 *Jandt/Roßnagel/Volland*, ZD 2011, 99, 101.

23 Siehe *BSI* Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073) sowie BSI Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0077).

24 *BSI*, Technische Richtlinie (TR-03109-1): Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.

25 Die Vorgaben des BSI sollen nach den §§ 19-28 MsbG-E verbindlich umgesetzt werden; siehe auch Begründung zu § 22 MsbG-E (Mindestanforderungen an das Smart Meter Gateway durch Schutzprofile und Technische Richtlinien), BR-Drs. 543/15, S. 128.

troffenen Haushalte, zukünftig eine technische Kommunikationsschnittstelle in ihrem Haushalt zu dulden. Ein Vorgang, der potentiell die Grundlage für erhebliche Eingriffe in das informationelle Selbstbestimmungsrecht der Bürger darstellte.[26] Damit diese Regelung im Rahmen der Verhältnismäßigkeit als verfassungskonform gelten konnte, wurde § 40 Abs. 5 EnWG eingeführt. Durch § 40 Abs. 5 EnWG wurde in Verbindung mit § 21g Abs. 6 S. 3 EnWG a.F. sichergestellt, dass es keinen Automatismus zwischen dem Einbau eines Smart Meters und der Nutzung der Fernauslese von Verbrauchsdaten und der damit verbundenen Preisgabe personenbezogener Daten gab.[27] Zudem wurde die Regelung des Einwilligungserfordernisses in das Fernmessen und Fernwirken in § 21g Abs. 6 S. 5 EnWG a.F. noch in der Beschlussempfehlung und im Bericht des Ausschusses für Wirtschaft und Technologie[28] eingefügt, um nochmals zu unterstreichen, dass es keinen Automatismus zwischen dem Einbau eines intelligenten Zählers und der Nutzung der Fernauslesung von Verbrauchsdaten geben sollte.[29]

Zur Sicherung des Grundrechtsschutzes wurde mit der Novelle des EnWG 2011 deshalb der zutreffend geforderte datenschutzrechtliche Maßnahmenkatalog eingeführt.[30]

b. Bewertung

Die Gesamtkonzeption des datenschutzrechtlichen Rahmens erscheint auf den ersten Blick als kohärent und durch das abgestufte Schutzkonzept

---

[26] Siehe beispielsweise: *Roßnagel/Jandt,* Datenschutzfragen eines Energieinformationsnetzes, S 88, S. 6ff.; *Müller,* DuD 2010, 359f. ; *Karg,* DuD 2010, 365f. ; Göge/Boers, ZNER 2009, S. 368f.

[27] *Lorenz/Raabe,* in: *Säcker,* Berliner Kommentar zum Energierecht, Band 1, Teil 1, § 21 g Rn. 2.

[28] BT-Drs. 17/6365, S. 12.

[29] So Brändle, VW-online, DokNr. 11001050, S. 8 mit Verweis auf die Gegenäußerung der Bundesregierung in BT-Drs. 17/6248, S. 40.

[30] BGBl. I 2011, S. 1554

auch als datenschutzrechtlich „modern“. So hat das Konzept der „Datenhoheit“ seinen Niederschlag sogar in den Grundgedanken der kommenden Datenschutzgrundverordnung gefunden[31]. Um die Defizite zu identifizieren, muss ein Blick in die Details der Regelungen genommen werden. Im Folgenden werden die einzelnen Problematiken an der Wissensbasis des Gesetzgebers herausgegriffen und einer Bewertung zugeführt. Auch wenn der Fokus der Untersuchung hier auf der Optimierung von Wissensbeständen im Verfahren liegt, können diese Defizite und die ihnen in der Folge jeweils innewohnenden Ansatzpunkte für eine zukünftige Lösung im instrumentell-institutionellen Arrangement nur verstanden werden, wenn auch der Blickwinkel materieller Normen mit einbezogen wird, da sich das hier eingeführte Vier-Säulen-Modell als geschlossenes, auch wechselwirkendes Schutzkonzept versteht.

2. Defizite innerhalb der materiellen Datenschutzvorgaben

a. Mangelnde Flexibilität für die Energieeffizienzziele

i. Fehlen einer Einwilligungsregelung

Ein erstes Beispiel für Defizite im Bereich des *normativen Wissens* im *legislativen Entscheidungsprozess* ist in dem Fehlen einer sachlichen Einwilligungsregelung zu der Verwendung von Messdaten für Effizienzmechanismen und -dienste außerhalb der bekannten marktlichen Angebote im EnWG zu sehen.

Bereichsspezifische Datenschutzregelungen sehen im Rahmen der Statuierung eines gesetzlichen Verbotes einer Datenverwendung mit Erlaubnis-

[31] Vgl. Ronellenfitsch, Hessischer Datenschutzbeauftrager als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vor der Bundespressekonferenz vom 26.08.2015: „Die Einwilligung des Einzelnen muss die Datenhoheit sichern“, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/DSK-PE-f%C3%BCr-BPK-Trilog-Deu-Final.pdf (abgerufen am 26.11.2016).

vorbehalt in der Regel neben einem Katalog von gesetzlichen Erlaubnistatbeständen auch die Einwilligung des Nutzers in eine konkrete Datenverwendung als Legitimationsgrundlage vor. Eine solche Einwilligung fand sich im novellierten EnWG nicht. Die Einwilligung des § 21g Abs. 2 EnWG bezog sich lediglich auf den personellen Anwendungsbereich des Gesetzes. Die zweite, im Rahmen der Verordnungsermächtigung des § 21g Abs. 6 S. 5 EnWG eingeführte[32] Einwilligung war lediglich Ausdruck der Hoheit des Letztverbrauchers über die Daten auf seinem Messgerät. Sie war für jeden Fall des Fernmessens, mithin in der Phase der Erhebung der Messdaten, immer kumulativ zur gesetzlichen Erlaubnis erforderlich.

Da der Verbotstatbestand des § 21g Abs. 1 EnWG spezieller und damit auch vorrangig gegenüber dem allgemeinen Verbot aus § 4 Abs. 1 BDSG angelegt war, konnte hinsichtlich der Verwendung der Messdaten nicht mehr auf die allgemeinen Erlaubnistatbestände des § 4 Abs. 1 BDSG, mithin auf die dortige Einwilligung, zurückgegriffen werden.

Dies galt, obwohl der Wortlaut des § 21g Abs. 1 EnWG den im Datenschutzrecht allgemein verankerten Grundsatz des präventiven Verbotes mit Erlaubnisvorbehalt für die Zulässigkeit einer Datenverwendung nicht explizit ausdrückte. Nach dem Wortlaut des § 21g Abs. 1 EnWG wurde einerseits durch die Formulierung *„ausschließlich durch zum Datenumgang berechtigte Stellen“* schon eine personelle Begrenzung vorgenommen und damit für jede Stelle außerhalb dieses Adressatenkreises ein Verbot ausgesprochen. Auf der anderen Seite gerierte sich der sachliche Verbotstatbestand als Zweckbestimmung. Diese ähnelte in ihrem systematischen Aufbau eher der Regelung des § 28 BDSG. Jedoch wurde durch die Formulierung, dass die Verwendung personenbezogener Messdaten „*auf Grund dieses Gesetzes nur*“ für die genannten Zwecke erfolgen durfte, das absolute Verbot jedweder anderweitigen Verwendung deutlich gemacht.

[32] Diese Einwilligung wurde erst gegen Ende des Beratungsverfahrens in das Gesetz eingefügt. Siehe hierzu auch ausführlich Brändle, VW-online, DokNr. 11001050, S. 4.

Dass diese Wertung auch der Intention des Gesetzgebers entsprach wird in der Begründung zur Gesetzesnovelle verdeutlicht, in welcher das datenschutzrechtliche Schutzkonzept anschaulich zusammengefasst wurde. „*Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind ausschließlich in den in § 21g beschriebenen Fällen zulässig und dann auch nur, wenn sie über Systeme und Vorrichtungen vorgenommen werden, die in Gesetz, Verordnung, Schutzprofilen und Technischen Richtlinien festgelegt sind*“.[33]

Damit war eine Einwilligung in die Verwendung von Messdaten zu Zwecken der Innovationsoffenheit und Energieeffizienz fördernder Dienstleitungen Dritter praktisch nicht möglich. Dies stand zwar den Regulierungszielen nicht entgegen, trug aber auch nichts zu deren aktiven Verwirklichung bei. Im Hinblick auf die aus europäischer Perspektive erwarteten Beiträge des Smart Metering zum Klimaschutz und der damit erstrebten Innovationsoffenheit für neue Effizienzdienste wird deutlich, dass der legislative Fokus hier zentral auf die Sicherung der informationellen Selbstbestimmung gelegt wurde, und nicht der Versuch einer wechselseitigen Optimierung von Klimaschutzbelangen und Datenschutz den legislativen Motiven zugrunde lag. Denn die Einwilligung kann in diesem Rahmen grundsätzlich auch als Ausdruck von Selbstbestimmung gesehen werden.

ii. Fehlende Öffnung für weitergehende Zwecke

Thematisch eng mit der fehlenden Einwilligungsregelung verbunden, war aufgrund der oben beschriebenen vom Gesetzgeber gewollten Ausschließlichkeit der in § 21 g EnWG enumerativ als zulässig normierten Zwecke, die fehlende Öffnung der klassischen bestehenden Zwecke einer Datenverwendung für neue innovative Energieeffizienzdienstleistungen. Als Erlaubnistatbestände wurden in § 21g EnWG lediglich die in Nr.1 bis 8 aufgeführten Zwecke genannt. Das damit eingebrachte datenschutzrechtli-

[33] Vgl. BR-Drucks. 343/11 S. 196.

che Grundprinzip der **Zweckbindung** von Datenverwendungen stellte ein tragendes Element für die Sicherung der Grundrechtsausübung dar. *„Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden (…), lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten*."[34] Auch Art. 6 Abs. 1 lit. b der Datenschutzrichtlinie (RL 95/46/EG) bestimmt, dass die mit der Datenverarbeitung verfolgten Zwecke festgelegt, eindeutig und rechtmäßig sein müssen. Das Prinzip dient nicht nur dazu, dem Betroffenen das notwendige Wissen zu vermitteln, zu welchen konkreten Zwecken seine Daten verwendet werden, sondern es werden auch die verantwortlichen Stellen gezwungen, die Daten zum einen nur zu den vorgesehenen Zwecken zu erheben und zum anderen diese auch lediglich zu den Zwecken weiterzuverarbeiten.[35] Die in § 21g Abs. 1 aufgezählten Zwecke hatten **abschließenden Charakter,**[36] was durch die Gesetzesbegründung hervorgehoben wurde.[37] Aufgrund der im EnWG verankerten strengen Begrenzung der Zwecke, bestand auch keine Möglichkeit, über die Verordnungsermächtigung des § 21i Abs. 1 Nr. 4 EnWG weitere Zweckfestlegungen einzuführen, welche durch erst zukünftig ersichtliche Zwecke der Datenverwendung aus Gründen der Energieeffizienz motiviert sein können.

Die Konzeption des damaligen gesetzlichen Rahmens zeigt, dass im legislativen Entscheidungsprozess eine Fokussierung auf den Schutz der informationellen Selbstbestimmung derart angelegt war, dass die Lösung des

---

34 BVerfGE 65, 1, 44.

35 Bizer, DuD 2007, 350, 352.

36 Der Katalog der gesetzlichen Erlaubnistatbestände ist abschließend in § 21g Abs. 1 Nr. 1-8 EnWG geregelt. Aufgrund des abschließenden Charakters der Regelung gibt es allerdings keine Möglichkeit, weitere sinnvolle Zulässigkeitstatbestände über die Verordnungsermächtigung des § 21i Abs. 1 Nr. 4 EnWG einzuführen. Sofern also zukünftig neue Dienstangebote für Energieeffizienzdienste entwickelt werden sollten, die nicht dem Katalog entsprechen, müssten diese im Wege einer Gesetzesänderung legitimiert werden.

37 BR-Drs. 343/11 S. 202.

Zielkonfliktes nicht mit den europäisch motivierten Zielvorgaben korrespondierte. In einer Kategorisierung wäre dieses Defizit in dem hier zuvor entwickelten Wissensmodell den ***Defiziten im Rahmen des Normwissens*** zuzuordnen. Diesbezüglich kann jedoch nicht auf Lösungsansätze der Wissensgenerierung im Verwaltungsrecht hinsichtlich des für die *normativen Wissensebene* erforderlichen Sach- und Erfahrungswissens zurückgegriffen werden. Eine Lösung muss daher in der weiteren Bearbeitung im Rahmen von fehlerhaftem Regulierungswissen und damit auch bei den regulierungstheoretischen Entscheidungen gesucht werden.

(1) Weiterentwicklung

In das MsbG - in welches eine Verlagerung der datenschutzrechtlichen Komponenten des EnWG erfolgte - wurde mit § 50 Abs. 1 MsbG nunmehr eine explizite Regelung der Einwilligung eingeführt. Des Weiteren wurde zwar die strenge Zweckbindung durch die Beibehaltung der Regelung abschließend zu verstehender Zwecke in das MsbG übernommen, allerdings werden nun in § 50 Abs. 2 Nr. 13 MsbG auch (Effizienz-)Mehrwertdienste berücksichtigt. Damit ist grundsätzlich auch von einem ***legislativen Lernprozess*** auszugehen.

(2) Bewertung

Im Hinblick auf den im Gesetz ebenfalls als Ziel intendierten Klimaschutz und die auch nach der sogenannten „Energiewende“ notwendige Versorgungssicherheit im Energiesystem war die abschließende Beschränkung der zulässigen Zwecke auf die heute bekannten Prozesse und Datenverwendungen ohne die Möglichkeit einer Einwilligung zu kurz gegriffen. Ebenso wurde im Hinblick auf die erlaubten Zwecke der Datenverwendung das Ziel der Energieeffizienzsteigerung weitgehend außer Acht gelassen. Die Einführung einer sachlichen Einwilligungslösung und die Erweiterung der Zweckkataloge zu erlaubten Datenverwendungen auf Effizienz-Mehrwertdienste durch das MsbG zeigt nachdrücklich, dass der normative Rahmen des Energiewirtschaftsrechts grundsätzlich auf einen

Lernprozess unter der Bedingung der Anreicherung von ***Erfahrungswissen*** angelegt ist.

b. Defizitäre Steuerungswirkungen der bereichsspezifischen Datenschutzregelungen des EnWG

Wie oben ausgeführt, wird der primär inhaltlich ausgerichteten Gesetzgebung in Rechtsgebieten, welche sich durch dynamische und dezentralisierte Wissensgrundlagen auszeichnen, unter anderem eine fehlende oder defizitäre Steuerungswirkung attestiert.[38] Neben den zuvor belegten Defiziten lassen sich dem Gesamtkonzept der bereichsspezifischen Datenschutzvorgaben der §§ 21g ff. EnWG weitere Unzulänglichkeiten entnehmen, welche als Indiz für die fehlenden oder zumindest mangelnde Steuerungsfähigkeit materiellrechtlich konzipierter datenschutzrechtlicher Vorgaben angesehen werden können. Diesbezüglich wurde den bereichsspezifischen Datenschutzregelungen einerseits grundlegend die Verfassungsmäßigkeit abgesprochen, was teilweise explizit auf die divergierende Regelungstiefe gestützt wird. Andererseits bestehen weitere Bedenken hinsichtlich der Vollständigkeit materieller Vorgaben wie die Form der Einwilligung oder der Adressatenkreis der Informationspflichten. In der vorliegenden Konstellation kumuliert hinsichtlich der Wissensgenerierung, ***fehlendes Sachverhaltswissen*** über tatsächliche Marktaspekte, welches sich in der gesetzlichen Normierung abzeichnen müsste mit Norm- bzw. Erfahrungswissen.

i. Grundrechtskonformität der bereichsspezifischen Datenschutzregelungen

Einige kritische Stimmen in der Literatur hegten darüber hinaus erhebliche Zweifel an der grundsätzlichen Verfassungsmäßigkeit der bereichsspezifischen Datenschutzregelungen im EnWG.[39] Mit den Verweisen auf konkretisierende Verordnungen habe der Gesetzgeber wesentliche Entscheidun-

[38] Teil 2 B.II.1.d.

[39] *Windoffer/Groß*, VerArch 2012, 491, 506.

gen der Exekutive überlassen, was sowohl gegen den Vorbehalt des Gesetzes spreche als auch der vom Bundesverfassungsgericht entwickelten Wesentlichkeits-theorie widerspräche.[40] Zudem wurde den gesetzlichen Vorgaben teilweise jegliche datenschutzrechtliche Steuerungswirkung abgesprochen, indem die Anwendbarkeit für Sachverhalte des Smart Grids zugunsten einer Anwendung des BDSG verneint wurde.[41] Dies folge aus § 1 Abs. 3 BDSG und dem dort verankerten **Vorrang des spezielleren Gesetzes** bzw. dem Grundsatz der Subsidiarität des BDSG. Als dem BDSG vorgehend sind demnach alle Spezialregelungen anzusehen, deren Ziel und Inhalt sich mit der allgemeinen Regelung des BDSG decken.[42] Bei einer tatbestandkongruenten Regelung ist ein Rückgriff auf weitergehende Erlaubnistatbestände verwehrt, obwohl im Grundsatz auch dann auf das BDSG zurückgegriffen werden kann, wenn ausdrückliche Verweise in den Spezialgesetzen fehlen.[43] Bei § 21g Abs. 1 EnWG handele es sich um eine bereichsspezifische Grundlage im Sinne des § 4 Abs. 2 S. 2 Nr. 1 BDSG, welche den Anwendungsfall „ohne Mitwirkung des Betroffenen" regele und gerade nicht um ein eigenständiges präventives Verbot mit Erlaubnistatbestand und somit auch nicht um die nach dem Subsidiaritätsprinzip erforderliche tatbestandskongruente Regelung.[44] Nach anderer Ansicht wird dem widersprochen. § 21g EnWG sei als eigenständiges präventives Verbot mit Erlaubnistatbestand ausgestaltet.[45] Da § 21 Abs. 1 EnWG nach der Gesetzesbegründung die erlaubten Datenverwendungen abschließend regele,[46] stelle es eine tatbestandkongruente Regelung zu § 4 Abs. 1 BDSG dar. Damit sei ein Rückgriff auf die materiellen Zulässigkeitstatbe-

40 *Lüdemann/Sengstacken*, ZNER 2013, 592, 594.

41 *Franck*, Smart Grids und Datenschutz, 2016, S. 52 und 53.

42 *Dix* in: Simitis, Bundesdatenschutzgesetz, §1 Rn. 158.

43 *Dix* in: Simitis, Bundesdatenschutzgesetz, § 1 Rn. 170.

44 *Jandt/Roßnagel/Volland*, ZD 2011, 99, 103.

45 Eine Parallele findet sich in § 12 Abs. 1 TMG, der ebenfalls ein eigenständiges Verbot mit Erlaubnisvorbehalt enthält. Vgl. *Spindler/Nink* in: *Döpkens/Spindler*, Recht der elektronischen Medien, § 12 TMG Rn. 2.

46 Vgl. BR-Drs. 343/11 S. 196.

stände des BDSG für den Anwendungsbereich des §21g Abs.1 EnWG ausgeschlossen.[47] Mithin werden die bereichsspezifischen Regelungen der §§ 21g ff. EnWG für anwendbar erklärt. Gegen die Argumentation der ersten Auffassung könnte sprechen, dass die in § 21g Abs. 6 EnWG angeordnete Einwilligung in das eigentliche Fernmessen, gerade eine Mitwirkung des Betroffenen erzwingt, mithin die vermutete Konstellation in der gesetzlichen Konzeption nicht vorkommen kann. Letztendlich kann dieser Streit nach der expliziten Regelung zur Einwilligung im MsbG aber dahinstehen.

Zum Teil wurde auch darauf abgestellt, dass eine Anwendbarkeit lediglich in Verbindung mit der noch zu erlassenden Rechtsverordnung nach §21h EnWG i.V.m. § 21g Abs. 6 EnWG zu bejahen sei.[48] Zweifel bestehen diesbezüglich, ob es legitim ist die notwendigen Detailregelungen durch die Ermächtigung in § 21i Abs. 1 EnWG dem Verordnungsgeber zuzuweisen. Die Tatsache, dass der materielle Gehalt ohne diese Konkretisierungen noch unvollständig ist und das tatsächliche Marktgeschehen nicht erfasst zeigt schon, dass es sich dabei auch um wesentliche Regelungen handeln könnte. Dieser Gedanke scheint auch im Hinblick auf die jetzige Gesetzeslage schlüssig, in welcher sich der Gesetzgeber lediglich aufgrund der Gefahr einer Rechtszersplitterung entschieden hat die Materie anstatt auf Verordnungsebene auf der Gesetzesebene zu regeln. Nicht von der Hand zu weisen ist dennoch, dass er sich mit dieser Entscheidung auch der oben aufgeführten Kritik entzieht.

ii. Divergierende Regelungstiefe

Gestützt wird die Kritik teilweise auch auf die divergierende Regelungstiefe der aufgezählten Zwecke in Verbindung mit der Maßgabe, dass der

---

47 Nach a. A. Ansicht handelt es sich bei § 21 g Abs. 1 allerdings um eine bereichsspezifische Grundlage im Sinne des § 4 Abs. 2 S. 2 Nr. 1 BDSG, welche den Anwendungsfall „ohne Mitwirkung des Betroffenen“ regelt; vgl. *Jandt/ Roßnagel/Volland*, ZD 2011, 100, 103.

48 *Franck*, Smart Grids und Datenschutz, 2016, S. 51.

Gesetzgeber grundlegende Bestimmungen selbst regeln muss. Die Detaillierung der im Gesetz selbst geregelten Zulässigkeitstatbestände ist in § 21g EnWG äußerst unterschiedlich ausgestaltet. Während die komplexe Messdatenkommunikation im Rahmen der Belieferung[49] mit Energie in § 21g Abs. 1 Nr. 3 EnWG sehr wenig konkret nur den Umstand der Belieferung in seinen gesetzlichen Tatbestand aufnimmt, werden die Tatbestandsvoraussetzungen und Begleitumstände der Datenverwendung anlässlich des Aufklärens und Unterbindens einer Leistungserschleichung in § 21g Abs. 1 Nr. 8 i.V.m. Abs. 3 EnWG im Gesetz selbst nahezu abschließend definiert. Diese unterschiedliche Regulierungstiefe führt zu der Frage, ob das Gesetz selbst, im Hinblick auf die Eingriffsintensität in das Recht auf informationelle Selbstbestimmung, die bestehenden Zulässigkeitstatbestände hinreichend normklar regelt. Insbesondere im Hinblick auf den unbestimmten Adressatenkreis und die vielfältigen Kommunikationsprozesse und Datenverarbeitungsschritte, die beispielsweise mit dem

[49] Die Wahl des Tatbestandsmerkmals der „Belieferung mit Energie“ ist im Hinblick auf die Terminologie des EnWG äußerst kritisch zu betrachten. Zwar wird der Begriff „Belieferung“ selbst nicht definiert, aber zur Negativabgrenzung des Verteilungsbegriffs in § 3 Nr. 37 EnWG verwendet. Auch hier wurde die Verwendung dieses Begriffs bereits kritisiert, da dessen Inhalt im Gegensatz zum europäischen Verständnis steht. Im EnWG wird unter Belieferung der Energiebezug eines Kunden (der Vertrieb) verstanden, ohne jedoch den Transport über Leitungsnetze mit einzuschließen. Im europäischen Verständnis meint der Begriff jedoch gerade den Transport der Energie zum Kunden, vgl. Art. 2 Nr. 3 und 5 Richtlinie 2009/72/EG. Problematisch in Bezug auf die Verwendung dieses Begriffs im Bereich der Datenschutzvorschriften ist jedoch, dass Belieferung, jedenfalls im Kontext des entbündelten Systems, nur einen dieser beiden Bereiche betreffen kann. Je nach zu Grunde gelegtem Begriffsverständnis wäre eine „Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem“ entweder nur für die Abrechnung von Netznutzungsentgelten, da diese den Transport betreffen, oder nur für den Vertrieb, also den Verkauf von Energie zulässig. Folge dieser Wortlautauslegung ist, dass die Daten damit auf Grundlage von § 21g Abs. 1 Nr. 3 EnWG jedenfalls nicht sowohl vom Netzbetreiber als auch vom Lieferanten zu Abrechnungszwecken benutzt werden dürften.

unbestimmten Merkmal der *„Belieferung mit Energie“* verbunden sind,[50] könnte erwogen werden, dass hier eine detailliertere Entscheidung durch das Gesetz selbst hätte getroffen werden müssen.

Nach anderer Ansicht ist mit Blick auf das konkretisierende Postulat des Bundesverfassungsgerichts[51] einerseits zu berücksichtigen, dass mit der verpflichtenden Einführung von Messsystemen i.S.v. 21d Abs.1 EnWG erstmals die staatliche Pflicht zur Eröffnung von IKT-Schnittstellen in den betroffenen Haushalten eingeführt ist. Eine Verpflichtung, die als sehr intensive Maßnahme im Hinblick auf die Gefährdung der informationellen Selbstbestimmung zu werten sein könnte. Auf der anderen Seite soll es nach der Gesetzesbegründung *„keinen Automatismus zwischen dem Einbau eines intelligenten Zählers und der Nutzung der Fernauslesung von Verbrauchsdaten“* geben.[52] Dies senke die Eingriffsintensität derart ab, dass die Wahl der Verordnung als Mittel der Konkretisierung datenschutzrechtlicher Prinzipien grundsätzlich angemessen erscheine. Dies gilt umso mehr, als es sich beim zukünftigen Smart Grid um ein sich hochdynamisch entwickelndes System handeln wird. Im Hinblick auf die für Energieeffizienzmaßnahmen zugunsten von Klimaschutz und Versorgungssicherheit notwendige Innovationsoffenheit der Systeme und Prozesse sei es deshalb nachvollziehbar und richtig, grundsätzlich die Detaillierung von Begleitprinzipien zum Schutz der informationellen Selbstbestimmung auf das flexiblere Instrumentarium der Verordnung zu verweisen.[53]

---

50 Hierzu zählt auch die Verwendung bei der Führung des Bilanzkreises durch den VNB.

51 Vgl. BVerfGE 49,89 Kalkar I „*die nach dem Gesetzesvorbehalt tragenden Prinzipien die parlamentarische Leitentscheidung [müsse] umso konkreter sein, in je höherem Maße der Grundrechtsschutz des betroffenen Bürgers in Frage stehe, je größer die Bedeutung für die Allgemeinheit sei, je weitreichender der politische Konflikt erscheine und mit je stärkerer Intensität ein staatliches Handeln erfolge.*“

52 BT-Drucks. 17/6248, S. 24.

53 *Raabe/Lorenz/Pallas/Weis,* CR 2011, 831, 836.

Auch wenn es auf die Streitentscheidung nicht ankommt, ist im Hinblick auf die oben geforderte ***Flexibilisierung von Entscheidungen*** bei begrenzten Prognosehorizonten zu soziotechnischen Entwicklungen im Rahmen von auch technischen Detailregelungen bedenkenswert, dass bei einer Bewertung nach dem Telos der Normierungen neben dem Schutz der informationellen Selbstbestimmung zudem die konkurrierenden klima- und umweltschützenden Aspekte einzubeziehen sein könnten,[54] weshalb im Hinblick auf notwendige effizienzsteigernde Innovationen wiederum der flexiblere Verordnungsweg in Teilbereichen als angemessen hätte gelten können.

iii. Weitere materiellrechtliche Kritikpunkte

An den folgenden Beispielen soll über die vorgenannten Defizite hinaus anhand von weiteren materiellen datenschutzrechtlichen Regelungen illustriert werden, dass neben den oben dargelegten Defiziten, weitere Umstände vorliegen, die - aufgrund der mangelnden Erfassung der tatsächlichen technischen Gegebenheiten und Marktprozesse - zu einer ganz oder teilweise mangelnden Steuerungsfähigkeit führen. Das Fehlen wichtiger Vorgaben, wie etwa Ansprüche an Löschung, Berichtigung und Widerspruch, ohne einen Verweis auf das BDSG bzw. lediglich der Zuweisung durch § 21i Nr. 4 EnWG auf den Verordnungsgeber, [55] unterstreichen das Argument der geringe Regelungstiefe und damit auch der ***mangelnden Steuerungsfähigkeit*** der materiellrechtlichen Normen des EnWG Einzugehen ist dabei auf das Schriftlichkeitserfordernis der Einwilligung, die an die verantwortliche Stelle gerichteten Informationspflichten und bestehende Nutzerrechte, insbesondere in Form von Löschpflichten.

[54] Wenn auch in Art. 20a GG nur als Staatsziel fundiert.

[55] *Lüdemann/Sengstacken*, ZNER 2013 (Heft 6) , S. 592 (594).

(1) Einwilligung in das Fernwirken

Die Unterrichtungspflicht der Regelung des § 21g Abs. 6 S. 5 EnWG ist nicht nur auf das Fernmessen, sondern auch auf das Fernwirken bezogen. Dies scheint in Bezug auf die Zweckbestimmung des § 21g Abs. 1 Nr. 5 EnWG, der die Zulässigkeit der Verwendung personenbezogener Daten aus dem Messsystem zum Zwecke der Steuerung von unterbrechbaren Verbrauchseinrichtungen im Sinne von § 14a EnWG legitimierte, auch naheliegend. Allerdings geht die Einwilligung in das „Fernwirken" aus § 21g Abs. 6 S. 5 EnWG nach der Wortbedeutung offensichtlich über eine die informationelle Selbstbestimmung der Betroffenen flankierende Maßnahme hinaus. Diese Datenverwendung betrifft ausschließlich eigentumsrechtlich motivierte Sachverhalte und war in den Regelungen zum Datenschutz eigentlich systemwidrig.[56] Die Integration einer systemwidrigen Regelung des Verbraucherschutzrechts unter dem Titel datenschutzrechtlicher Tatbestände deutet hier auf einem ***Mangel im legislativen Normwissen*** hin.

(2) Form der geregelten Einwilligung

Die in der Vorphase des Fernmessens erforderliche Einwilligung des Letztverbrauchers nach § 21g Abs. 6 S. 5 EnWG war nicht ausdrücklich mit einem Schriftlichkeitserfordernis versehen. Die Einwilligung bei der Bestimmung der zum Datenumgang berechtigten Stelle in § 21g Abs. 2 EnWG musste hingegen den Vorgaben des § 4a BDSG, mithin der Schriftlichkeit, entsprechen. Aus systematischer Perspektive stellte sich somit die Frage, ob im ersten Fall bewusst keine Detaillierung erfolgt ist, um dem Verordnungsgeber einen Spielraum bei der Ausgestaltung einer elektronischen Einwilligung nach dem Vorbild des TMG zu eröffnen, oder ob nach dem Gesetzeszweck ein expliziter Verweis auf das BDSG deshalb entbehrlich war, weil jedenfalls die in § 4a BDSG genannten Informati-

[56] Raabe/Lorenz/Pallas/Weis, CR 2011, 831, 837.

onspflichten schon in die Vorgaben des § 21g Abs. 6 S. 5 EnWG eingeflossen sind. Für ein Schriftformerfordernis auch bei der Einwilligung nach § 21g Abs. 6 S. 5 EnWG sprach jedenfalls, dass die Gefahren beim Wechsel der „berechtigen Stelle“ und bei der Zulassung des Fernmessens durch den Letztverbraucher sich nicht unterschieden.

Das Schriftlichkeitserfordernis nach § 4a BDSG birgt allerdings bei elektronischen Transaktionen grundsätzlich die Gefahr eines Medienbruchs. Zwar erlaubt § 126 Abs. 3 BGB auch die elektronische Form gemäß § 126a BGB, allerdings ist dann eine qualifizierte elektronische Signatur erforderlich, die wiederum keinerlei Verbreitung besitzt.[57] In Anbetracht der Tatsache, dass der liberalisierte Energiemarkt gerade darauf angelegt ist, spontan seinen Lieferanten wechseln zu können und dass eine zunehmende Nutzung dieser Option und Vereinfachung gerade über webbasierte Anwendungen geleistet werden soll, wirkte der mit der Schriftform verbundene Medienbruch antiquiert. Im Hinblick auf die Elektromobilitätszenarien der Zukunft, die sich durch hohe Transaktionsfrequenzen insbesondere bei der Nutzung von öffentlichen Ladestationen auszeichnen, ist eine damit verbundene (unter-) schriftliche Einwilligung gegenüber dem jeweiligen Ladestationsbetreiber als absolutes Ausschlusskriterium für die Entwicklung dieser Märkte zu betrachten. Aufgrund des aufgezeigten Klärungsbedarfs konnte die Vorschrift in der Praxis nicht bestehen und im Energiemarkt letztendlich auch nicht durchgreifen. Damit bestand die Forderung, in Form der angedachten Verordnung die Implementierung eines elektronischen Unterschriftensubstituts für die Einwilligung in das Fernmessen gemäß § 21g Abs. 6 S. 5 EnWG aufzunehmen.[58] Im Ergebnis zeigt der Verweis auf das antiquierte Schriftlichkeitserfordernis ein ***mangelndes legislatives Sachwissen*** zu Fragen der Informationstechnologien und adäquater technischer Substitute von Mechanismen zur

[57] Vgl. *Raabe/Lorenz*, DuD 2011, S. 279, 280.

[58] *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831, 837.

Sicherung der primären Warnfunktion durch die Anordnung von entsprechenden datenschutzrechtlichen Förmlichkeiten.

(3) Informationspflichten der verantwortlichen Stelle

Im Rahmen der Informationspflichten wurde hinsichtlich der Identität der verantwortlichen Stelle für die Erteilung der Pflichtinformationen in § 21g Abs. 6 S. 5 EnWG selbst nichts bestimmt.[59] Da im Gesetz selbst lediglich der potentielle Adressatenkreis auf die zum Datenumgang berechtigten Stellen eingegrenzt wird, ergibt sich daraus nicht, welcher Akteur die Unterrichtungspflichten wahrnehmen muss. Für den Betroffenen selbst ist die verantwortliche Stelle ebenfalls nicht normklar ersichtlich.[60] Festgehalten werden kann an dieser Stelle, dass im ***bestehenden Kommunikationsmodell*** der zur Festlegung der Prozesse berufenen BNetzA, der MSB die Stelle sein sollte, die das Fernmessen vornimmt. Allerdings sind auch Fälle denkbar, in denen der einzige dem Betroffenen bekannte Akteur der Lieferant sein dürfte.[61] Damit konnte die Regelung für die tatsächlichen Gegebenheiten auf dem Energiemarkt nicht greifen. Anderes würde gelten, wenn im Rahmen der Verordnung eine Festlegung der Verantwortlichkeit auf eine dieser Rollen vorgenommen worden wäre.

---

[59] Informationspflichten stellen unter dem Gesichtspunkt der nutzerbezogenen Transparenz einen weiteren wesentlichen Aspekt datenschutzrechtlicher Begleitprinzipien dar. Sie sichern einerseits den Aspekt der Selbstbestimmung bei Entscheidungen des Betroffenen über gewünschte und unerwünschte Datenverwendungen und sind gleichzeitig die Basis für die Ausübung nachfolgender Nutzerrechte.

[60] *ULD*, Stellungnahme zum Gesetzesentwurf der der Bundesregierung zur Neuregelung energiewirtschaftsrechtlicher Vorschriften, BT-Drs. 17/6072, S. 2.

[61] Der Lieferant ist insbesondere in den in der Praxis verbreiteten All-Inclusive-Verträgen die einzige, dem Nutzer bekannte Stelle. Auch in den künftigen Elektromobilitätsszenarien des Ladens an öffentlichen Ladestationen werden vertraglichen Bindungen in den meisten Fällen lediglich zwischen dem Betroffenen und dem Lieferanten bestehen.

(4) Nutzerrechte

Auskunftsrechte

Der einzige gesetzlich fixierte Anknüpfungspunkt für die Ausübung von Nutzerrechten findet sich in § 21h EnWG. Trotz der amtlichen Überschrift „Informationspflichten" waren darin Auskunftsrechte des Betroffenen allein gegenüber dem MSB normiert. Die Beschränkung auf den MSB ist jedoch erneut aus der Perspektive der **Sternkommunikation** motiviert, da die notwendige Ausübung von Auskunftsrechten bei den Akteuren einer Prozesskette in diesem Paradigma nicht bedacht werden musste. Im Ergebnis
bezieht sich dann – aus der Perspektive der Sicherung der „Datenhoheit" konsequent – § 21h EnWG lediglich auf die Einsicht in die im *„elektronischen Speicher- und Verarbeitungsmedium gespeicherten auslesbaren Daten"*.[62]

Da das faktische Marktgeschehen zum Zeitpunkt des Erlasses jedoch auf die Prozesse der BNetzA und damit die ***Kettenkommunikation*** ausgerichtet war, konnten die Normierungen hinsichtlich des Auskunftsrechts nicht greifen. Es hätte vielmehr der Statuierung eines Auskunftsrechts gegenüber den anderen Marktakteuren bedurft. Dies war wegen der klaren Rollen- und Verwendungszuweisungen in den Prozessfestlegungen auch mög-

[62] Die im Vergleich zu den sonstigen Regelungen unterschiedliche Wortwahl ist daraus erklärlich, dass das Messsystem im Sinne von § 21d Abs. 1 EnWG gemäß dem Schutzprofil aus grundsätzlich zwei zumindest logisch getrennten Teilen, dem Smart Meter und dem Gateway, besteht. Die Vorschrift eröffnet damit grundsätzlich einen Zugriff auf alle im Smart Meter oder im Gateway gespeicherten Daten. Problematisch ist hierbei aber, dass sich der Anspruch aus § 21h EnWG zumindest nach seinem Wortlaut nicht auf Daten des Anschlussnutzers beschränkt. Der Tatbestand ist insofern restriktiv auszulegen und in der Verordnung zu konkretisieren.

lich[63] und zudem gegenüber einem allgemeinen Verweis auf die korrespondierenden Regelungen des BDSG vorzugswürdig.[64] Daher lässt sich an dieser Stelle ein Defizit im ***legislativen Normwissen*** feststellen, da die bestehenden Marktfestlegungen der BNetzA zur Kettenkommunikation im legislativen Entscheidungsprozess zu dieser materiellen Norm hätten bekannt sein müssen.

Löschpflichten

Bezüglich gesetzlich normierter Löschpflichten findet sich, neben der speziellen gesetzlichen Löschpflicht für die Missbrauchsaufdeckung in § 21g Abs. 3 EnWG, in § 21g Abs. 6 S. 7 EnWG lediglich die unbestimmte Vorgabe, Höchstfristen für die Speicherung festzulegen. Im Hinblick auf die produktbezogene Intention des Gesetzes ist insofern offen, ob sich auch dies lediglich auf das Messsystem oder auf die gesamte Prozesskette bezieht. Mithin konnte durch die Regelung kein umfassender Schutz der informationellen Selbstbestimmung gewährt werden. Es wurde daher gefordert, in der Verordnung Löschpflichten für alle bekannten Datenverwendungen in der gesamten Prozesskette adressatenspezifisch zu statuieren.

Weitere Nutzerrechte

Auch hinsichtlich der weitergehenden Nutzerrechte wie Löschansprüche, Sperrpflichten und Berichtigungen ist ein allgemeiner Verweis auf die Regelungen des BDSG in der Verordnung nicht hinreichend,[65] da auch bei

---

63 Dass der Kreis der zum Datenumgang Berechtigten durch § 21g Abs. 2 EnWG um eine dritte, den Prozessfestlegungen unbekannte Stelle erweitert werden kann, ist unkritisch, da diese zuvor selbst eine Einwilligung beim Betroffenen eingeholt haben muss.

64 *ULD*, Stellungnahme, S. 5, das sich für einen ausdrücklichen Verweis auf das BDSG ausspricht.

65 Wohl aber hinsichtlich ihres materiellen Gehalts.

einem solchen Vorgehen jedenfalls im Falle der Kettenkommunikation[66] für den Betroffenen unklar bleibt, welcher Akteur im Markt welche Daten verwendet und mithin sein Anspruchsgegner ist. Auch hier hätte es konkreter Regelungen anhand der Prozessfestlegungen in einer Verordnung bedurft.

(5) Bewertung

Sowohl die angezweifelte Verfassungsmäßigkeit des materiellrechtlichen Datenschutzkonzepts des EnWG, als auch dessen geringe Regelungstiefe und die damit verbundenen fehlenden materiellen Vorgaben für die datenschutzgerechte Kommunikation, führt vor Augen, dass die gesetzlichen Regelungen die im Smart Grid bestehenden Realweltphänomene des Energiemarktes tatsächlich nicht erfassen konnten, sofern man der Auffassung der kritischen Stimmen folgt. So zeigt die rechtswissenschaftliche Diskussion um Verfassungsmäßigkeit und Anwendbarkeit des EnWG für datenschutzrechtliche Konstellationen doch sehr deutlich, dass dem Gesetzgeber im legislativen Entscheidungsprozess das für die Schaffung von den gegebenen Realbereich abdeckenden Normen erforderliche ***Normwissen fehlte***. Damit können die materiellen Normen hinsichtlich der tatsächlichen Gegebenheiten des Energiemarktes nicht greifen, was sich in mangelnder Durchsetzungskraft und ***Steuerungsfähigkeit des Gesetzes*** wiederspiegelt. Dies lässt sich zumindest teilweise der Unkenntnis marktlicher Gestaltungen und damit dem ***fehlenden Sachwissen*** und der Unübersichtlichkeit des Realweltphänomens Smart Grid zuordnen, dessen vollständige Erfassung den Staat an seine Grenzen bringt. Damit wird bestätigt, dass sich die gesetzliche Ex-Ante-Steuerung der Datenverarbeitung angesichts der dynamischen Entwicklung von Technik und Anwendungen grundsätzlich als zunehmend schwierig darstellt.[67]

---

66 In Fällen der Sternkommunikation ergibt sich der jeweilige Anspruchsgegner aus den zuvor erteilten Einwilligungen.

67 *Ladeur*, DuD 2000, S. 16, 16.

Letztlich ist der im Datenschutzkonzept der §§ 21g ff. EnWG eingeschlagene Weg der ***Flexibilisierung*** in Form von Verlagerung von Normsetzung auf den Verordnungsgeber zu begrüßen. Dadurch wird eine ***Kompensation von mangelndem Sach- und Erfahrungswissen*** durch die sich schnell entwickelnde Technik möglich, indem besser und schneller auf tatsächliche Veränderungen der Marktgegebenheiten reagiert werden kann. Zudem kann dadurch zumindest teilweise dem Problem des eingeschränkten Prognosehorizonts begegnet werden. Allerdings fehlte es auch hier am Normwissen, indem nicht gesehen wurde, dass eine fast vollständige Verlagerung der Vorgaben auf den Verordnungsgeber und damit eine Verweigerung normativer Grundsatzentscheidungen aus verfassungsrechtlicher Sicht angreifbar, wenn nicht unzulässig sein musste. Zudem wurde nicht gesehen, dass eine Flexibilisierung durch die Möglichkeit der Durchführung eines modifizierten Feststellungsverfahrens sichergestellt werden kann, wie es Gegenstand der vorliegenden Untersuchung ist.

Zwar werden durch die Verlagerung sowie die detaillierteren neuen Ausgestaltungen im MsbG einige der oben genannten Kritikpunkte obsolet, jedoch bestätigen dies gerade das oben gefundene Ergebnis, dass Wissensdefizite beim Gesetzgeber bestanden und diese in der Praxis auch erhebliche Auswirkungen zeigten. Damit kann das legislative Umsteuern weniger auf Verordnungsebene zu regeln und mit dem MsbG ein zentrales Gesetz zu schaffen als Indiz für die im Legislativprozess angelegte ***Lernfähigkeit*** gesehen werden. Im Fokus steht somit nach wie vor die Frage nach Mechanismen der Flexibilisierung und Revisibilität sowie der Verbesserung von Lernfähigkeit, die wie oben beschrieben durch eine Optimierung von Verfahren eingesetzt werden können.

c. Defizite innerhalb der technischen Datenschutzvorgaben

i. Produkt- statt prozessbezogener Datenschutz – Schutzprofile für Smart Meter

Als weiteres Beispiel für Defizite im Bereich des ***Erfahrungswissens*** im legislativen Entscheidungsprozess kann zudem die rein produktbezogene Sicht des Gesetzgebers auf das Smart Meter und die damit verbundene Beauftragung des BSI zur Entwicklung eines produktbezogenen Datenschutzkonzeptes aus Schutzprofilen und Technischen Richtlinien für das Smart Metering angeführt werden.

(1) Entwicklung

Wie bereits in einem Überblick eingeführt,[68] wurden im Jahr 2006 von der *Bundesnetzagentur* Festlegungen bezüglich einheitlicher *Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität* (GPKE) getroffen. Enthalten war damals auch die erste Fassung des Prozesses „Zählerstand-/Zählwertübermittlung“,[69] welcher die Übermittlung der Messdaten vom Netzbetreiber an den Netznutzer regelte.[70] Die neueste Fassung dieses Prozesses datiert nach der EnWG-Novelle des Jahres 2011 und hat das den Prozessen zugrundeliegende Kommunikationsmodell unverändert gelassen.[71]

Bei den Festlegungen handelt es sich um Verwaltungsakte in Form von Allgemeinverfügungen, die dementsprechend für die betroffenen Marktakteure verbindlich sind. Diese Rechtsnatur ergibt sich schon aus § 60a Abs.

---

68 Teil 1 C.II.2

69 Die Ermächtigung zum Erlass dieser Regelungen ergibt sich beispielsweise für den hier relevanten Prozess aus § 27 Abs. 1 Nr. 11 StromNZV und § 29 Abs. 1 EnWG in Verbindung mit § 54 Abs. 1 EnWG.

70 BNetzA, Anlage zum Beschluss BK6-06-009 vom 11.07.2006, S. 78ff

71 BNetzA, Anlage 1 zum Beschluss BK6-11-150 vom 28.10.2011, S. 30ff

2 EnWG.[72] Diese Allgemeinverfügungen werden grundsätzlich mit einem Widerrufsvorbehalt versehen und können auch atypisch auf Grundlage des § 29 Abs. 2 EnWG nachträglich geändert werden. Unter dem Gesichtspunkt eines gesteigerten Vertrauensschutzes hatte die Energiewirtschaft mittlerweile jedoch erhebliche Investitionen in ihre Systeme getätigt. Deswegen war unter dem Gesichtspunkt der notwendigen Willkürfreiheit eine abändernden Entscheidung hinsichtlich einer nicht unbedingt notwendigen grundsätzlichen Änderung nicht zulässig. Denn dies hätte dem Sinn der durch die Festlegungen angestrebten Vereinheitlichung, die gerade auch kleineren Akteuren den Marktzugang erleichtern soll, widersprochen. Infolgedessen muss als „Status Quo" festgehalten werden, dass das Paradigma der Kettenkommunikation jedenfalls derzeit geltendes Marktrecht ist.

Im Kern folgen die dort festgelegten Prozesse zur Marktkommunikation mit Messdaten nach wie vor dem Prinzip der „*Kettenkommunikation*". Die Messdaten werden demnach vom jeweils zuständigen MSB erhoben und an die berechtigten Marktteilnehmer weitergeleitet. Die Weiterleitung wiederum wird durch die damalige MessZV sowie durch Festlegungen der BNetzA konkretisiert. So ist der VNB nach § 4 Abs. 4 MessZV zur Übermittlung abrechnungsrelevanter – und somit netzentgelt- oder bilanzierungsrelevanter – Messdaten an den Netznutzer, und damit den Lieferanten, verpflichtet. § 4 Abs. 3 MessZV wiederum verpflichtet den Messstellenbetreiber, dem Verteilnetzbetreiber die hierzu benötigten Daten zu übermitteln. Darüber hinaus ist der Verteilnetzbetreiber im Rahmen des oben erwähnten Bilanzkreissystems verpflichtet, bilanzierungsrelevante Messdaten an den jeweiligen Bilanzkreiskoordinator (üblicherweise der Übertragungsnetzbetreiber) zu übermitteln.

Das BSI trat, noch ohne bereichsspezifisch explizit normiertes Mandat, als weiterer Akteur im September 2010 in den Prozess der Entwicklung des

[72] Zudem wurde diese Ansicht auch durch die Entscheidung des BGH bestätigt, BGH ZNER 2008, 228.

Smart Grid ein. Das BMWi hielt - vor dem Hintergrund eines europarechtlich vorgegebenen strengen Rollout Planes[73] - die Sicherstellung von Datenschutz und Datensicherheit durch Anforderungen an die Sicherheitsarchitektur von intelligenten Netzen in Form eines Schutzprofils für erforderlich. Im September 2010 wurde das BSI zu Erarbeitung dementsprechender Schutzprofile und sowie daran anschließend einer Technischen Richtlinie vom BMWi beauftragt.[74] Das BSI begann daraufhin Anfang 2011 mit der Erstellung eines *produktbezogenen* ersten Entwurfes zum *Schutzprofil für die Kommunikationseinheit eines Intelligenten Messsystems für Stoff und Energiemengen*[75] und dem dazugehörigen *Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen*[76].[77]

Das primär *produktbezogene Schutzprofil* für die Kommunikationseinheit eines Intelligenten Messsystems hat die Aufgabe strukturiert Bedrohungen darzulegen und die Mindestanforderungen für entsprechende Sicherheitsmaßnahmen zu definieren. Der Aufbau eines Schutzprofils ist in den Common Criteria geregelt. Es beansprucht dabei technikneutral und offen für neue technische Möglichkeiten zu sein. Zudem stellt es die Grundlage für eine mögliche Evaluierung von *Produkten* dar, welche nach positiv erfolgter Prüfung ein Zertifikat über die Erfüllung der Schutzziele erhalten.

Das Schutzprofil fokussiert bislang lediglich auf die zu erfüllende Sicherheitsleitung des Gateways als Kommunikationseinheit eines intelligenten

---

73 EU-Richtlinie 2006/32/EG.

74 *BSI,* Smart Meter Gateway, S. 9.

75 *BSI,* Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (Smart Meter Gateway Protection Profile), BSI-CC-PP-0073.

76 *BSI,* Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit einer intelligenten Messsystems für Stoff- und Energiemengen, (Security Module PP), BSI-CC-PP-0077.

77 *Laupichler/Vollmer/Baast/Intemann,* DuD 2011, 542, 543.

Messsystems, dessen zentrale Aufgabe die Verbindung des elektronischen Zählers im lokalen metrologischen Netz (LMN/MAN) mit den verschiedenen Marktteilnehmern im Weiterverkehrsnetz (WAN) und dem Endverbraucher im lokalen Heimnetz (HAN).[78] Hierfür definiert das Schutzprofil logische Schnittstellen flankiert von einer Display Schnittstelle für die lokale Visualisierung der Verbrauchsdaten und einer Schnittstelle zu einem physikalisch integrierten Sicherheitsmodul des Gateways.

Die Perspektive des Schutzprofiles ging nun von einer ***sternförmigen Kommunikationsstruktur*** aus, in welcher durch das Gateway die Kommunikationswege zu jedem einzelnen Marktteilnehmer ermöglicht werden. Die Kommunikationswege werden im Sinne einer Gewährleistung von Authentizität, Integrität und Vertraulichkeit separiert und kryptographisch gesichert, um die Messwerte dann signiert und verschlüsselt an autorisierte Marktakteure weiterzugeben. Eine Weitergabe von Daten von den Marktteilnehmern an Dritte ist somit nicht vorgesehen. Grund hierfür ist die Annahme, datenschutzrechtliche Vorkehrungen seien durch die Implementierung von Sicherungsmechanismen für die Datenhoheit des Kunden zu verwirklichen. Damit ist Ziel der *sternförmigen Kommunikation* des Gateways, „*dass der Kunde in die Lage versetzt wird, eine detaillierte Übersicht über seinen Verbrauch zu erhalten, ohne dass hoch aufgelöste Verbrauchsdaten an Dritte weitergeleitet werden müssen*“.[79] Im Schutzprofil wird zur Sicherung der Ausübung der materiellen Datenhoheit zudem eine Einsatzumgebung des Gateways festgelegt, welche es dem Kunden erlaubt, sich jederzeit von der physischen Unversehrtheit des Gateways zu überzeugen. Im Sinne der Datensparsamkeit und Datenvermeidung sollen ausschließlich abrechnungsrelevante Werte oder Betriebsdaten in pseudonymisierter Form das Gateway verlassen.

[78] *BSI*, Das Smart-Meter-Gateway – Sicherheit für intelligente Netze, S. 12.

[79] *Laupichler/Vollmer/Bast/Intemann*, DuD 2011, 542, 544.

(2) Defizit

Die Beauftragung des BSI ohne einen verfahrensrechtlich fixierten Rahmen zur Kooperation könnte sich als defizitär hinsichtlich des ***legislativen Erfahrungswissens*** erweisen. Die gesetzliche Konzeption weist unter dem Aspekt des technisch gestützten Datenschutzes bzw. der Datensicherheit primär auf die Umsetzung der Schutzmechanismen der am Anfang der Informationskette – und damit auf dem Messsystem – hin, was sich explizit in den Motiven des Gesetzgebungsverfahrens wiederspiegelt.[80] Der technische Datenschutz sichert nach diesem Konzept jedoch lediglich die sog. „Datenhoheit“[81] des Nutzers über die Verwendung der Messdaten – sowohl im als auch aus dem Messsystem – in der Phase der Erhebung durch die berechtigte Stelle. In den Spezifikationen und Erläuterungen zum Schutzprofil[82] und zur Technischen Richtlinie[83] wird dabei im Gegensatz zu der oben erläuterten Verbindlichkeit der Vorgaben für die Marktkommunikation davon ausgegangen, dass das Gateway grundsätzlich mit einer Mehrzahl unterschiedlicher Akteure kommuniziert, für die jeweils ein gesondertes Kommunikationsprofil auf dem Gateway hinterlegt wird.[84] Nach Darstellung des BSI soll durch diese Kommunikationsprofile sichergestellt werden, dass „nur berechtigte Kommunikationspartner Zugriff auf die erfassten Werte haben“[85] und dass solche Messdaten, die zu anderen als zu Abrechnungszwecken an externe Kommunikationspartner übermittelt werden, keinen expliziten Personenbezug

80 Vgl. BR-Drs. 343/11, S. 196.

81 Vgl. BR-Drs. 343/11, S. 202; BT-Drs. 17/6248, S. 24.

82 Siehe *BSI*, Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, (Smart Meter Gateway Protection Profile), BSI-CC-PP-0073.

83 Siehe *BSI*, Technische Richtlinie, BSI TR - 03109, Version0.20.

84 Vgl. z.B. BSI-PP, Z. 332f sowie die Kardinalitäten in der Abbildung auf S. 13 des Schutzprofils.

85 Vgl. *Laupichler/Vollmer/Bast/Intemann*, DuD 2011, 542, 544. Zur Annahme der Mehrzahl externer Kommunikationspartner siehe auch die dortige Abbildung 1.

aufweisen.[86] Dies lässt darauf schließen, dass bei der Ausgestaltung des Schutzprofils im Grundsatz von einem ***sternartigen Kommunikationsmodell*** ausgegangen wurde, bei der die Kommunikation jeweils direkt zwischen dem Gateway und den unterschiedlichen Marktakteuren stattfindet. Ähnliche Grundannahmen sind auch im ersten Entwurf zur Technischen Richtlinie zu Grunde gelegt, in welcher ebenfalls eine – jedenfalls dem Grundsatz nach – direkte Kommunikation zwischen Gateway und den unterschiedlichen Marktteilnehmern angenommen wird, auch wenn diese hier über den MSB geleitet wird.[87] Daraus ergibt sich eine nicht auflösbare ***Inkongruenz*** zwischen den technischen Schutzmechanismen und der tatsächlichen Abwicklung der Marktkommunikation mit der Konsequenz, dass der Schutz bislang ins Leere laufen musste.

Auch wenn zum damaligen Zeitpunkt Schutzprofil und Technische Richtlinie a priori lediglich Vorgaben für von zukünftigen intelligenten Messsystemen zu unterstützende Funktionalitäten machten, mitnichten aber die tatsächliche Ausgestaltung der Messdatenkommunikation definierten, so zeichnete sich dennoch ein grundsätzlicher Konflikt zwischen den beschriebenen Kommunikationsmodellen ab.

---

86 Vgl. BSI-CC-PP-0073, Z. 1031: *„When the TOE submits information about the consumption or production of a certain commodity that is not relevant for the billing process, there is no need that this information is sent with a direct link to the identity of the consumer. In those cases the TOE shall replace the identity of the consumer by a pseudonymous identifier“*

87 Vgl. BSI-TR - 03109, Z. 411 ff: *„Bei der Übertragung von nicht abrechnungsrelevanten Messwerten vom Smart Meter Gateway an einen Marktteilnehmer [...] wird die im Datensatz enthaltene Identifikation des Zählers durch ein Pseudonym ersetzt. Damit auch die Identität des sendenden Gateways unerkannt bleibt, müssen die Daten zusätzlich über einen Dritten (z.B: den Messstellenbetreiber) an den Endempfänger vermittelt werden.“* Fraglich ist derzeit noch, inwiefern hier das energiewirtschaftsrechtliche – und insbesondere netzentgelt- und bilanzierungsrelevante Daten einschließende – Verständnis von Abrechnungsrelevanz zu Grunde gelegt wird.

Gesetzestext und Materialien untermauern die offensichtliche Wertung des Gesetzgebers, den technisch unterstützenden Datenschutz lediglich auf dem Endgerät zu realisieren. Aus diesen ergibt sich das Motiv des Gesetzgebers den technischen Datenschutz primär beim Messsystem und damit in der Herrschaftssphäre des Nutzers zu implementieren und die technischen Obliegenheiten den unmittelbar „fernmessenden" Akteuren aufzuerlegen. Hierzu wird ausgeführt, § 21e EnWG lege *„eine ausnahmslose Geltung von noch in und aufgrund einer Rechtsverordnung im Einzelnen zu benennenden Datenschutz- Datensicherheits- und Interoperabilitätsanforderungen für Messsysteme fest".*[88] In systematischer Hinsicht ergibt sich dies zudem aus der gesetzlichen Überschrift, welche sich explizit auf die *„Allgemeine Anforderungen an Messsysteme zur Erfassung elektrischer Energie"* und somit auf das Endgerät bezieht. Die systematische Stellung der Regelung lässt auch nicht zwingend darauf schließen, dass neben den produktbezogenen Regeln zusätzliche technische Maßnahmen entlang der Prozesskette angedacht waren. Mithin ordnet der Normappel des §21e Abs. 2 EnWG lediglich den Einsatz technischer Systeme an, welche einem Schutzprofil nach § 21i EnWG in Bezug auf das Messsystem entsprechen.

Das eigentliche ***Defizit im Erfahrungswissen*** könnte letztlich darin begründet sein, dass im Ergebnis aus technischer Sicht nur ein Ende-zu-Ende Datenschutz sachgerecht für die Herausforderungen an die Informationelle Selbstbestimmung im Rahmen des Smart Grid ist.

(3) Einfluss des MsbG

Durch die Einführung des MsbG hat sich die Konfliktlage noch verstärkt. Gesetzlich normiert wurde mit § 60 MsbG nun die ***Sternkommunikation***. Des Weiteren wurden die Schutzprofile und Technischen Richtlinien, welche ausschließlich auf dieser Sichtweise beruhen, mit Einführung des §

[88] BT-Drs. 17/6072, S. 80.

20 Abs. 2 MsbG verbindlich gemacht. Die Prozesse, nach welchen die gegenwärtige Marktkommunikation abläuft, sind jedoch weiterhin die durch die Beschlüsse der BNetzA festgelegten. Damit passen die Sicherungen für die technischen Komponenten und teilweise auch die technischen Komponenten selbst nicht zur Marktkommunikation. Die BNetzA wird nach eigenen Aussagen eine Zeitspanne von drei Jahre benötigen bis die Prozesse an die neuen gesetzlichen Gegebenheiten angepasst sind.[89]

(4) Bewertung

Letztlich hatte der Gesetzgeber offensichtlich kein vollständiges bzw. lediglich ein einseitiges Entscheidungswissen. Mängel sind hier schon bei der Generierung des erforderlichen ***Sachwissens*** über das tatsächliche Funktionieren der Marktprozesse ersichtlich. Mit der Fokussierung auf das Produkt des Smart Meters in der Gestaltung der technischen Säule der datenschutzrechtlichen Konzeption, hat er sich mangels erforderlichem ***Erfahrungswissen*** für eine begrenzte Sichtweise entschieden. Ausschlaggebend war diesbezüglich die Beauftragung des BSI für die Anreicherung des legislativen Entscheidungswissens als sehr technikzentrierte Sichtweise im Rahmen einer Expertifizierungsbestrebung. Letztlich fehlte mangels vorliegendem Erfahrungswissen auch die normativ verfahrensrechtliche ***Integration von Behördenwissen*** der BNetzA. Wie oben dargestellt,[90] muss der Gesetzgeber den informativen Wissensvorsprung von Behörden nutzen, was wie aufgezeigt, hinsichtlich der festgelegten Prozesse der BNetzA nicht geschehen ist.

89 *V.Wege/Wagner*, N&R, 2016, 2, 10.

90 Teil 2 B.II.1.c.ii.

ii. Auseinanderfallen legislativer und behördlicher Perspektive – Kommunikationsparadigmen

(1) Defizit

Weiterer Anknüpfungspunkt für die Offenlegung einer Perspektive des Gesetzgebers, welche sich nicht mit den durch die Festlegungen der BNetzA verfestigten marktlichen Gegebenheiten deckt, ist der Wortlaut des § 21g Abs. 1 EnWG „aus dem Messsystem". Die Formulierung „aus dem Messsystem" ist aus der Gesetzeshistorie gewachsen, da der Auftrag für ein Schutzprofil für Smart Meter Gateways[91] schon vor Erlass des Gesetzes vergeben wurde.[92] Die dort entwickelte Sichtweise ging vor dem Hintergrund eines „*Internet der Energie*" von einer Sternkommunikation[93] aus. Während es sich bei den ursprünglichen von der BNetzA festgelegten Kommunikationsprozessen um solche einer Kettenkommunikation handelte,[94] ging man bei Erstellung des Schutzprofils für Smart Meter Gateways von der Sichtweise einer Sternkommunikation aus.[95]

Charakteristisch für das Kommunikationsparadigma der **Sternkommunikation** ist,[96] dass sämtliche zum Datenumgang berechtigte Stellen selbst

---

91 *BSI*, Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, (Smart Meter Gateway Protection Profile), BSI-CC-PP-0073.

92 Der Auftrag zur Erarbeitung dieses Schutzprofils wurde bereits deutlich vor der Novelle des EnWG im September 2010 erteilt. Siehe auch *Kowalski*, Entwicklung von Schutzprofilen, in: Bub/Wolfenstetter, IT-Sicherheit zwischen Regulierung und Innovation, S. 137.

93 Siehe hierzu ausführlich *Raabe/Lorenz/Pallas/Weis*, CR 2011, 832.

94 Siehe hierzu ausführlich *Raabe/Lorenz/Pallas/Weis*, CR 2011, 832.

95 *BSI*, Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, (Smart Meter Gateway Protection Profile), BSI-CC-PP-0073.

96 Siehe hierzu ausführlich *Raabe/Lorenz/Pallas/Weis*, CR 2011, 832.

mit dem Messsystem kommunizieren können und dürfen.[97] Auf Basis dieses Paradigmas würde es bei den jeweiligen Marktakteuren nur unmittelbar aus dem Messsystem stammende Messdaten geben. In der Gesamtschau des datenschutzrechtlichen Schutzkonzeptes des EnWG ist davon auszugehen, dass sich der Gesetzgeber diese Sicht bei der systematischen Gestaltung der Vorschriften zu eigen gemacht hat. Orientiert man sich hingegen an den derzeit geltenden Festlegungen der BNetzA zur Marktkommunikation,[98] so muss von einer **Kettenkommunikation** ausgegangen werden. [99] Nach dem Sinn und Zweck des Gesetzes kann die Auslegung der Formulierung „aus dem Messsystem" also nur in dem Sinne erfolgen, dass auch die lediglich mittelbar aus dem Messsystem stammenden Daten bei den jeweils zum Datenumgang berechtigten Stellen entlang der Prozesskette erfasst sind.[100] Tatsächlich musste damit für die bestehende Gesetzeslage eine Auslegung gefunden werden, welche mit beiden Paradigmen kompatibel ist.

(2) Weiterentwicklung

Nimmt man die durch die Einführung des MsbG eingeführten **Neuerungen** in den Blick, so hat sich der Gesetzgeber auch nach Übernahme von Teilen des § 21g EnWG in den neuen § 50 des MsbG durch Beibehaltung

---

97 BSI-CC-PP-0073, Z. 332f; für jeden auf das Messsystem zugreifenden Akteur würde dabei ein gesondertes Berechtigungsprofil auf dem Gateway hinterlegt. So auch die BSI-Mitarbeiter Laupichler/Vollmer/Bast/Intemann, DuD 2011, 544, die auch dort von einer Mehrzahl externer Kommunikationspartner sprechen und dies in Abbildung 1 auch so aufzeigen.

98 Siehe hierzu insbesondere den Prozess Zählerstand-/Zählwertübermittlung in BNetzA, Anlage 2 zum Beschluss BK6-09-034 vom 09.09.2010, S. 11ff. Eine Änderung dieses Prozesses erfolgte dann nach der Novelle 2011 in BNetzA, Anlage 1 zum Beschluss BK6-11-150 vom 28.10.2011, S. 30ff. Diese Änderung ließ das Kommunikationsparadigma jedoch unberührt.

99 Siehe hierzu auch ausführlich *Raabe/Lorenz/Pallas/Weis*, CR 2011, 831.

100 Im Ergebnis auch *Weis/Pallas/Lorenz/Raabe*, Handbuch zur Elektromobilität, im Erscheinen, Rn. 69.

der Formulierung *„aus dem Messsystem […]“* und die Einführung der Überschrift des § 60 MsbG *„sternförmige Verteilung am Gateway“* zwar explizit für eine sternförmige Kommunikation zwischen Gateway und den jeweils sachlich berechtigten Marktakteuren entschieden, allerdings bleiben in der Praxis schier unüberwindbare Probleme, da bis zum Ablauf der vorgegebenen Übergangsfrist von Seiten der Marktakteure mit den Festlegungen der BNetzA, welche von einer Kettenkommunikation ausgehen, gearbeitet werden muss.

Das Verständnis der Entwicklung des Paradigmas der Sternkommunikation aus dem Kettenparadigma ist aus gegebenem Anlass gerade heute wieder aktuell, weil es bis zu einer vollständigen Umstellung eine **Übergangsphase** geben wird, in welcher weiterhin Prozessvorgaben zur Marktkommunikation, welche von einer Kettenkommunikation ausgehen, für die Marktteilnehmer bestehen, diese aber mit den Systemen an den Endpunkten, die von einer Sternkommunikation ausgehen, ausführbar bleiben müssen. Daher erhält die BNetzA mit § 75 S. 1 Nr. 1 MsbG die Möglichkeit, die bis zum 31. Dezember 2019 bestehende Übergangsphase technisch zu gestalten.[101] Hierzu kann die BNetzA insbesondere Festlegungen und Sonderregelungen vorsehen.[102]

Für diese Übergangsphase behält die Auslegung zum früheren § 21g EnWG Gültigkeit, indem diese im Hinblick auf die besonderen Gefahren der digitalen Fernkommunikation weiterhin so auszulegen bleibt, dass darunter alle Daten fallen, welche aus dem Zähler stammen und über die Schnittstelle kommuniziert werden können. Die Formulierung „aus“ ist dabei nicht im Sinne von unmittelbar dem System entspringend auszulegen. Es sind auch Daten erfasst, die ursprünglich aus dem Messsystem stammen, aber an andere Marktakteure übermittelt werden. Dabei handelt es sich nicht nur um reine Messwerte, sondern um jegliche messrelevanten Informationen, was auch signierte Werte und Datenpakete aus reinen

[101] BT-Drs. 18/7555, Begründung S. 108.

[102] BT-Drs. 18/7555, Begründung S. 108.

Messwerten mit Verknüpfungen zur Zählpunktbezeichnung darstellen können. Nach dem Sinn und Zweck des Gesetzes sind damit ebenfalls die lediglich mittelbar aus dem Messsystem stammenden Daten bei den jeweils zum Datenumgang berechtigten Stellen entlang der Prozesskette erfasst.[103]

Mit § 60 MsbG hat sich der Gesetzgeber nun grundsätzlich und ausdrücklich für eine sternförmige Marktkommunikation der relevanten Daten entschieden, indem er den Begriff schon in die Überschrift aufgenommen hat.[104]

(3) Bewertung

Letztlich handelt es sich bei der Annahme eines „Internet der Energie“ um eine Problematik im Rahmen des ***behördlichen Erfahrungswissens***. Mangels bestehender Erfahrung hinsichtlich eines Smart Grid wurden Anleihen im Kontext des offenen Internet gesucht, obwohl eine Vergleichbarkeit nicht gegeben ist. Auch diesbezüglich kann eine einseitige Expertifizierung, wie es durch die Beauftragung des BSI vor der gesetzlichen Legitimationsgrundlage geschehen ist, nicht ausreichen. Auch hier hätte es ***Kooperationen*** bedurft, welche die Einbeziehung bestehenden Behördenwissens zumindest in Erwägung ziehen. Mit der Grundannahme eines „Internet der Energie“ lag schon nicht das notwendige Erfahrungswissen für die technischen, datenschutzrechtlichen Konzepte vor. Im Er-

---

103 Im Ergebnis auch *Weis/Pallas/Lorenz/Raabe*, in: *Boesche/Franz/Fest/Gaul*, Berliner Handbuch zur Elektromobilität, S. 298 ff.

104 Auf Basis dieses Paradigmas wurde angenommen, dass es bei den jeweiligen Marktakteuren nur unmittelbar aus dem Messsystem stammende Messdaten geben würde. In Gesamtschau des datenschutzrechtlichen Schutzkonzeptes des EnWG war jedoch, wie sich hier bestätigt, davon auszugehen, dass sich der Gesetzgeber diese Sicht bei der systematischen Gestaltung der Vorschriften zu eigen gemacht hat. Bei einer Orientierung an den derzeit noch geltenden Festlegungen der BNetzA zur Marktkommunikation, musste hingegen von einer Kettenkommunikation ausgegangen werden.

gebnis lag durch die Nichtbeachtung der bestehenden Prozessfestlegungen der BNetzA beim Gesetzgeber mangelndes marktliches Wissen über tatsächliche Gegebenheiten vor.

d. Überleitung

Anhand der 2011 geschaffenen gesetzlichen Regelungen zum Datenschutz im Smart Grid schien ein Rollout aufgrund der unzureichenden gesetzlichen Rahmenbedingungen nicht realisierbar. Dies war überwiegend der mangelnden Kenntnis der tatsächlichen Gegebenheiten des Energiemarktes zuzuschreiben und der daraus resultierenden Perspektive, welche sich defizitär auf die legislative Umsetzung der bereichsspezifischen Regelungen auswirkte. Zudem wurden Prioritäten bestimmter Regulierungsziele nicht richtig eingeschätzt und fanden damit nur unzureichend Eingang in die Gesetzesmaterie. Diese blieb für die Praxis nicht folgenlos. Für die Marktteilnehmer bestanden dadurch erhebliche Unsicherheiten, einerseits zur technische Entwicklung der Smart Meter und weiterer Komponenten, andererseits hinsichtlich der Umsetzung von notwendigen neuen Marktprozessen. Dies war einerseits Folge der unzulänglichen gesetzlichen Vorgaben, andererseits bedingt durch ein Auseinanderfallen der bestehenden Prozessvorgaben der BNetzA und der gesetzlichen Regelungen, welche nicht ineinandergriffen und somit die Durchführung der Marktprozesse für die Marktteilnehmer wesentlich erschwerte und erschwert.

Weitere Konsequenzen hatten die unzureichenden materiellen Regelungen und die hierzu eingenommenen Perspektiven jedoch auch in wesentlichem Umfang für die Arbeit der Regulierungsbehörde. Hierauf soll im Folgenden eingegangen werden.

Teil 3:
Instrumentelle Ableitungen für ein lernfähiges Verfahren

A. Instrumente zur Gestaltung von Lernfähigkeit im Verfahren

I. Speicher und grundlegende symbolische Strukturen für lernfähige Verfahren

Im Hinblick auf die ***Lernfähigkeit*** und notwendige ***Reversibilität*** im Verfahren ist hinsichtlich der erarbeiteten Herausforderungen an das Sach- und Normwissen aus behördlichen und privaten Wissensbeständen, ein im abstrakten Wissensmodell deutlich sichtbares Element bislang noch nicht berücksichtigt. Denn „*aus Information wird Wissen durch Einbindung in einem zweiten Kontext von Relevanzen. Dieser zweite Kontext besteht nicht, wie der erste, aus Relevanzkriterien, sondern aus bedeutsamen Mustern, die das System in einem speziell dafür* ***erforderlichen Gedächtnis speichert und verfügbar*** *hält*."[1] Der Aspekt der Persistierung von gewonnenem dezentralen Sach- und Normwissen wird im bestehenden Festlegungsverfahren nicht förmlich adressiert, obwohl gerade die ***Methodik der Wissensgenerierung und Wissenspeicherung*** im Verfahren einen entscheidenden Moment im Rahmen von reversiblen Lernprozessen darstellt.

[1] *Willke*, Systemisches Wissensmanagement, S. 11; *Albers*, Komplexität verfassungsrechtlicher Vorgaben, in: Spiecker/Collin, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, S. 55.

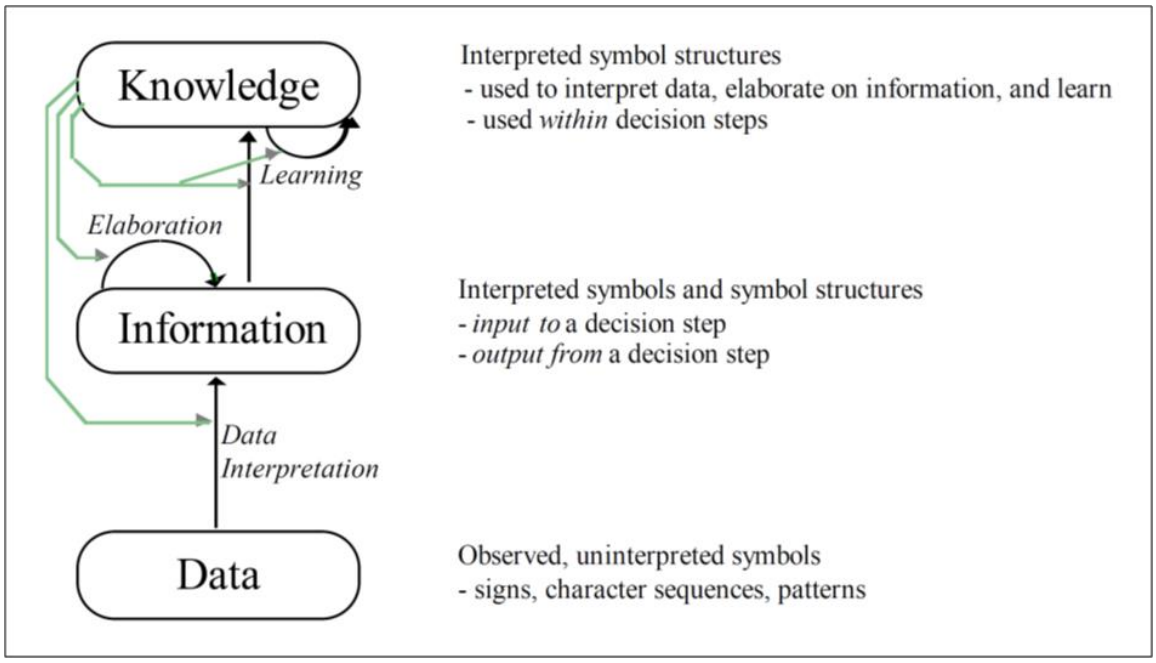

Abbildung 1: Allgemeines Modell von Wissen und Entscheidung[2]

In abstrakter Betrachtung des Entscheidungsmodells von Aamodt/Nygård ist neben der Feststellung, dass das gewonnene Sach- und Normwissen, wie auch die Ergebnisse von Abwägungsentscheidungen in dem mehrdimensionalen Optionenraum grundsätzlich gespeichert und verfügbar gehalten werden muss, noch eine weitere Dimension ersichtlich: Die Frage nach der effektiven ***Form der zu gestaltenden Wissensbasis***.

Grundsätzlich sind nach diesem Modell die notwendigen Informationen zur Generierung von Entscheidungswissen in Daten verkörpert, die wiederum durch eine geeignete, ***interpretationsfähige Symbolik*** repräsentiert werden. Die Entscheidung, als Ergebnis eines zweckgerichteten Lernprozesses, kann sich nun erneut in diesen Symboliken zeigen.

[2] Abbildung von Aamodt/Nygård, Different roles and mutual dependencies of data, information,and knowledge - an AI perspective on their integration, Data and Knowledge Engineering 16 (1995) 191, 200.

Im Recht sind diese Symboliken in der Regel ***textuelle Repräsentationen*** in Gesetzestexten, historischen Materialien und behördlichen Entscheidungen. Die Interpretation geschieht in der Regel in Form des klassischen juristischen ***Gedankenexperimentes*** durch die zur Entscheidung berufenen Akteure. Es stellt sich im Hinblick auf die Komplexität der entscheidungsrelevanten Dimensionen des notwendigen verteilten Sach- wie Normwissens und auf die beschriebenen Defizite die Frage, ob die rein textuelle Repräsentation sowie das klassische Gedankenexperiment in derartigen Verfahren, welche auf Erkenntnisse zu komplexen informationstechnischen Sachverhalten und den technischen Ausgleich von z.T. grundrechtlichen Wertungen zu funktionalen und nichtfunktonalen Aspekten von vielfältigen Messdatenverwendungen in diesen infrastrukturellen Architekturen gerichtet sind, die ***geeigneten symbolischen Strukturen*** für einen effektiven und reversiblen Lernprozess darstellen. Naheliegender erscheint auf den ersten Blick, jedenfalls für Teilaspekte der sachlichen und normativen Wissensgenerierung die Wahl einer ***bildhaften Symbolik*** zur Schaffung und Persistierung des Entscheidungswissens zu sein.

In der Literatur ist anerkannt, dass die Rechtsordnung häufig Spielräume im Umgang mit dem Steuerungsfaktor Recht belässt. Sie eröffnet zwar einen rechtlich definierten Korridor rechtmäßigen Verhaltens, belässt aber regelhaft Möglichkeiten für die Wahl von Optionen in diesem Korridor. Das Recht kann in diesem Optionenraum die Zielerreichung durch Vorgabe von Zielen oder Konzepten stimulieren und den Vorgang der Optionenwahl durch Verfahrensregeln disziplinieren. Die Beachtung von Recht und Gesetz ist insofern eine notwendige, aber keineswegs stets hinreichende Bedingung zur Bewältigung des rechtsnormativ zur Lösung aufgegebenen Problems. Soweit im Recht Spielräume verbleiben, ist es den Rechtsanwendern aufgegeben, im Interesse der Problembewältigung zusätzliche Faktoren zu aktivieren, darunter auch Wissen.[3] Der Begriff der

[3] *Hoffmann-Riem*, Regulierungswissen in der Regulierung, in: Bora/Henkel/Reinhard, Wissensregulierung und Regulierungswissen, S. 137.

Regulierung soll es grundsätzlich ermöglichen, Muster staatlicher Intervention und gesellschaftlicher Wirkungen herauszuarbeiten und das staatliche Handeln durch eine Analyse einem strategischen Gebrauch zugänglich zu machen.[4] Er kennzeichnet somit die theoretisch reflektierte ***Typisierung von Instrumenten*** und diese ***bündelnde Regimes*** und will deren absichtsvollen Einsatz unter Berücksichtigung der Entwicklungspfade und funktionalen Erfordernissen befördern. Er ist in dieser Perspektive ***interdisziplinär und symbolischen Mustern zugänglich*.**

Recht als soziale Erscheinung lässt sich gleichsam auch als Kommunikationssystem beschreiben - ein System, in welchem Informationen produziert, gespeichert, verarbeitet und ausgetauscht werden.[5] Die Übermittlung der Informationen geschieht durch ein physikalisches Medium, welches sich erheblich auf die in der Gesellschaft eingenommene Perspektive auswirkt. Sei es Papier oder Bildschirm, das Medium verursacht den Wandel und zwar dann nicht nur im Medium, sondern in der Art der Informationen des so beschriebenen Kommunikationssystems Recht.[6] Folgender Satz umschreibt die Folgen historische Entwicklung in zutreffender Form: „*Während Stein oder Tontafeln räumliche Bindung und Dauerhaftigkeit zulassen und somit Tradition und Hierarchie begünstigten, ermöglichte das leicht transportable Papier die Ausdehnung der Herrschaft in den Raum, während Breitenwirkung dann der (Buch)Druck durch preiswerte Vervielfältigung erzielte und die Elektrizität letztendlich durch ihre Geschwindigkeit den sozialen Wandel brachte*."[7] Es werden somit Bilder vom Recht und Bilder im Recht also innerhalb des Rechtssystems unterschieden.[8] Bilder im Recht sind selten. Zwar besteht der forensische Gebrauch visueller Kommunikationsmittel, allerdings hat der Kernbereich

---

4 *Eifert, Regulierungsstrategien,* in: Wolfgang Hoffmann-Riem/Schmidt-Aßmann/ Vosskuhle Grundlagen des Verwaltungsrechts Bd. I, § 19 Rn. 8.

5 *Röhl/Röhl,* Allgemeine Rechtslehre, S. 19.

6 *Röhl/Röhl,* Allgemeine Rechtslehre, S. 19.

7 *Röhl/Röhl,* Allgemeine Rechtslehre, S. 19.

8 *Röhl/Röhl,* Allgemeine Rechtslehre, S. 20.

der juristischen Fachkommunikation Bilder bisher gemieden. Zwar ist die herkömmliche Rechtstheorie noch auf den sprachwissenschaftlichen Ansatz fixiert, das Recht wird sich jedoch in Zukunft der Bilder nicht erwehren können, denn zwischenzeitlich kommuniziert alle Welt mit Bildern. Insbesondere ***logische Bilder*** können als Unterstützung schwieriger Fragestellungen oder, schwierige Prozesse und Entscheidungen erleichtern. Wissensbestände lassen sich verbal vergleichsweise zuverlässiger und mit weniger Streuung übertragen (als Textkommunikation).[9] Bilder helfen dem Gedächtnis, denn für diese ist die Gedächtnisleistung erheblich höher als für abstrakte oder konkrete Begriffe.[10] Bilder prägen und mobilisieren zudem ***Schemawissen***, indem sie typische Abläufe zeigen.[11]

Daher stellt sich die Frage, ob ein Festlegungsverfahren, das auf Kommunikation in dezentralen hochverteilten Wissensstrukturen angewiesen ist und die technische Konzeption kritischer, komplexer IKT Systeminfrastrukturen im Grenzbereich staatlicher Daseinsfürsorge sowohl hinsichtlich des Sachwissens, als auch für die normative Entscheidung zum Interessenausgleich, nicht eher Strukturmerkmale klassischer ***raumbedeutsamer Infrastrukturvorhaben*** aufweisen und die dort verwendeten ***symbolischen Strukturen des bildhaften Plans***, als Repräsentation in der Vorbereitung und Gegenstand von behördlichen Entscheidungen, zumindest aus wissenstheoretischer Sicht angemessen wäre.

9 *Röhl/Röhl*, Allgemeine Rechtslehre, S. 22.

10 *Röhl/Röhl*, Allgemeine Rechtslehre, S. 22.

11 *Röhl/Röhl*, Allgemeine Rechtslehre, S. 22.

B. Lernfähigkeit und Stabilisierung von Wissen in nicht förmlichen Verfahren

Eine weitere Dimension im Hinblick auf die ***Lernfähigkeit*** eines entsprechend angereicherten Festlegungsverfahrens eröffnet der Befund, dass die ***Methodik der Wissensgenerierung und Wissenspersistierung*** im bestehenden Festlegungsverfahren, weniger den modernen Formen entspricht, wie sie im Bereich der vergleichbaren Standardisierung von komplexen IKT-Infrastrukturen des privaten Sektors etabliert sind. Mit Blick auf die diesbezüglichen Bestrebungen bei der Konsensfindung privater Verbände wie DKE/VDE zur Positionierung im Rahmen der Konsultationen der BNetzA zu Protokollen und Marktstandards des Smart Grid, weisen die dortigen Verfahrensgestaltungen auf die Wahl ***moderner Verfahrensstufungen*** und selbstregulativer Instrumente, wie sie im Bereich der privaten Standardisierung komplexer IKT Usus sind. Auch wenn aus Gründen der Ressourcenknappheit eine Verlagerung der dort bestehenden Mechanismen zu Konsensbildung und Persistierung von Wissen in den privaten Bereich bislang nachvollziehbar war,[1] ist vor dem Hintergrund der Anreicherung des Verfahrens zur Sicherung der informationellen Selbstbestimmung und der oben erarbeiteten Verortung des Smart Grid als doppelte kritische Infrastruktur eine derartige Privatisierung zukünftig nicht angemessen, da es sich bei dem Verfahren um eine Kompensation originärer staatlicher materieller Schutzmechanismen im Rahmen der Gewährleistungsverantwortung handelt.[2] Anhand zweier Beispiele aus dem Bereich der bislang nicht förmlichen Kooperationsverfahren zur IT-Sicherheit und zum Datenschutz im Smart Grid sollen moderne Verfahrenselemente ge-

1 Bislang ist insofern von einer eher moderierenden Funktion der BNetzA auszugehen.

2 Teil 3 C.I.2.c.

zeigt werden, die den Aspekt der Nutzung des „Plans“ für die Darstellung und Abwägung von funktionalen und nichtfunktionalen IKT-Artefakten, seiner symbolischen Grundlagen und den modernen Verfahrensstufungen in nicht förmlichen Aktivitäten außerhalb der bestehenden Festlegungsverfahren illustrieren.

I. Beispiel: IT-Sicherheit im Smart Grid

Im März 2011 erteilte die Europäische Kommission und die Europäische Freihandelsassoziation (EFTA) das Smart Grid Mandat M/490, welches im Juni 2011 von den drei europäischen Standardisierungsorganisationen (ESOs), CEN, CENELEC und ETSI angenommen wurde. Der damit verbundene Auftrag an CEN, CENELEC und ETSI bestand darin, ein Rahmenwerk zu entwickeln, um die kontinuierliche Weiterentwicklung der relevanten Normen und Standards im Umfeld des Smart Grid zu ermöglichen. Hauptaspekte des Mandats sind unter anderem die ***Informationssicherheit im Smart Grid***. Um diese Aufgabe zu bearbeiten, haben die ESOs ihre strategischen Ansätze kombiniert und im Juli 2011 zusammen mit den relevanten Akteuren der Privatwirtschaft die CEN-CENELEC-ETSI ***Smart Grid Coordination Group*** (SG-CG) ins Leben gerufen. Ende 2012 wurde das Mandat M/490 bis zum Jahre 2014 mit dem Ziel einer Feinabstimmung und weiterer Detaillierung der Ergebnisse verlängert. Die Resultate wurden im Dezember 2014 den Technical Boards von CEN, CENELEC und ETSI übergeben. Die Informationssicherheit spielte innerhalb des M/490 eine zentrale Rolle. Die „Smart Grid Information Security (SGIS)“ Gruppe beschreibt in ihrem Abschlussbericht, wie Security Standards dazu beitragen, ein dezidiertes Sicherheitsniveau auf technischer, organisatorischer und prozesstechnischer Ebene im Smart Grid zu erreichen. Ziel des Mandates war es ***nichtförmliche Leitlinien*** für System-Designer, Betreiber sowie Entwickler von Smart Grid Infrastrukturen zu entwickeln. Für den Untersuchungsgegenstand ist die ***Verfahrensstufung*** in diesem rein selbstregulativen Verfahren der IT-Sicherheit, wie sie in Abbildung 2 gezeigt wird, interessant, da die Gruppe eine eigene Metho-

dologie in einem „*User Manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM)*“ [3] entwickelt hat, die als State-Of-The-Art im Bereich nichtstaatlicher Regulierung des Smart Grid angesehen werden kann. Diese Methodologie ermöglicht anhand verschiedener ***Use Cases***[4]**,** welche aus den verschiedenen Sichten der relevanten Akteure zum Sach- und Normwissen entwickelt und in einem Use-Case-Repository gespeichert werden, eine systematische Ableitung des Schutzbedarfs aus den verschiedenen Blickwinkeln. Dies geschieht systematisch auf Basis des ***Smart Grid Architecture Model*** (SGAM) als Referenzmodell, welches durch die bildhafte Darstellung der verschiedenen Domänen, Zonen und Schichten des Energiesystems eine erhöhte Interoperabilität zwischen den relevanten Sichten generieren soll.

[3] ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_Overview.pdf, (abgerufen am 16.11 2016).

[4] UseCases werden in der Informatik verwendet um Anforderungen an ein IT-System oder Teile davon als Szenario in natürlicher Sprache zu formulieren. Allerdings werden hierfür Entwurfsmuster („Pattern“) verwendet, weshalb dieser Entwurf schon seminformal vorliegt. *Vgl. Georgiades/Andreou* in: Favaro/Morisio, Safe and Secure Software Reuse, S. 267.

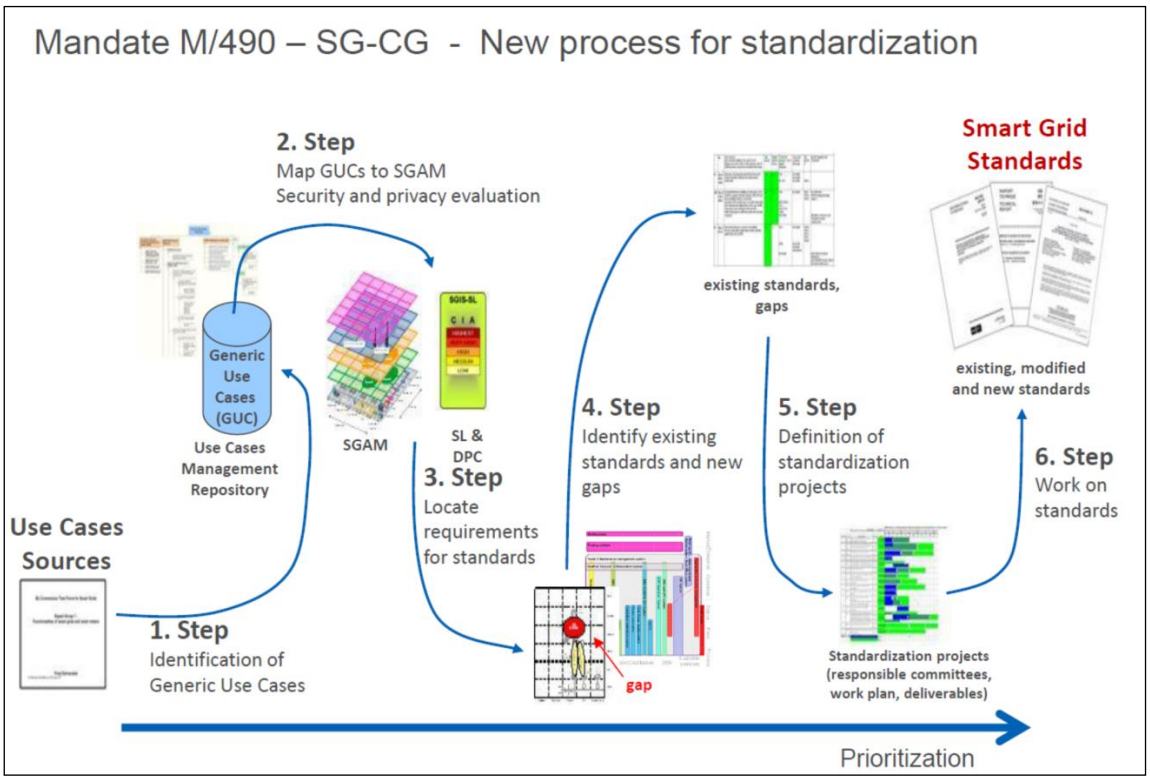

Abbildung 2: Standardisierungsprozess im Mandat 490 [5]

Aus diesen Befunden werden anschließend die ***SGIS Security Levels*** (SGIS-SL) abgeleitet, welche verschiedene technisch wirksame Maßnahmen auf Basis der Klassifikation von Teilprozessen der Datenverwendung darlegen. Abschließend findet eine nichtförmliche ***Empfehlung auf Basis des SGAM*** statt, welche die Teilprozesse einem Sicherheitslevel zuordnet. Das "European Set of Recommendation" stellt damit eine Menge an nichtförmlichen Empfehlungen für Sicherheitsmaßnahmen für Smart Grid Akteure dar.

[5] Vgl. *Stein, Johannes*, "Smart Grid – Stand der europäischen und internationalen Normung", Vortrag vom 30.09.2014 in Stuttgart, online unter http://www.smartgrids-bw.net/fileadmin/documents/Vernetzte_Intelligenz__Johannes_Stein.pdf (abgerufen am 26.11.2016).

Auch wenn sich die Methodologie dieses Vorgehens einer förmlichen Struktur von materiellen Abwägungsbelangen und konkreten Gewichtungen, wie sie z.B. im Konditionalprogramm des Bauplanungsrechts vorliegen[6], enthält und mit der Beschränkung auf die Zielvorgabe „Informationssicherheit“ nur einen geringen Ausschnitt der möglichen (widerstreitenden) Interessen spiegelt, so ist die Kombination aus der textuellen Beschreibung von Use Cases, die Persistierung in einem zentralen Repository und die grundlegende Integration der bildhaften Darstellung der Schichtensystematik des Smart Grid auf Basis des SGAM-Referenzmodells eine sinnvolle systematische Stufung der notwendigen Lernschritte zu technikwirksamen Normierungsschritten. Allerdings ist festzuhalten, dass die normative Entscheidung zu den konkreten Sicherheitsleveln (SGIS) einem metrischen Modell der klassischen IT-Sicherheit entspringt um eine Quantifizierung von Risiken zu ermöglichen. Ob dieses Entscheidungsmodell der Quantifizierung auch für Aspekte des Schutzes der informationellen Selbstbestimmung angemessen ist, muss an dieser Stelle dahinstehen.

II. Beispiel: Orientierungshilfe datenschutzgerechtes Smart Metering

Die formale Basierung von spezifischen datenschutzrechtlichen Sichten auf IT-Prozesse im Energiemarkt ist schon heute eine geübte Praxis bei den Datenschutzaufsichtsbehörden. Wie in Tabelle 1: *Beispiel Use Case „Beendigung der Energieversorgung“*“ gezeigt, bezieht sich die Bewertung des Datenschutzbedarfes auf konkrete Maßnahmen der Datensicherheit, die im Prozess der Beendigung der Energieversorgung zu berücksichtigen wären.

[6] Siehe das Beispiel in **Fehler! Verweisquelle konnte nicht gefunden werden.** .

Tabelle 1: Beispiel Use Case „Beendigung der Energieversorgung“

Use Case	**Beendigung des Energielieferungsvertrages**	
Ziel	Übermittlung der Abrechnungsdaten für die Endabrechnung, Löschen aller Daten des Energielieferanten als Kommunikationspartner des Gateways	
Akteure	Letztverbraucher, Energielieferant, Gateway-Administrator	
Prozessbeschreibung	Die Abrechnungsdaten für die Endabrechnung werden ein letztes Mal versendet, der Gateway-Administrator unterbricht zum Kündigungsdatum die Kommunikation mit dem Energielieferanten, löscht die Tarif- und Berechtigungsprofile und alle weiteren Daten des Energielieferanten (Zertifikate).	
Daten	Abrechnungsdaten (Verbrauch), Zertifikate, Schlüssel, Berechtigungsprofildaten	
Datenfluss	Letztverbraucher → Energielieferant Gateway-Administrator →Letztverbraucher	
Anmerkungen	Es wird davon ausgegangen, dass die im Schutzprofil vorgesehene sternförmige Kommunikation, die über Tarif- und Berechtigungsprofile ermöglicht wird, in Anspruch genommen wird und dadurch ein direkter Datenfluss von Letztverbraucher (Smart Meter) zu Energielieferant stattfindet. Datenflüsse zwischen Gateway-Administrator und Energielieferanten, die zur Umsetzung der Beendigung des Energielieferungsvertrages notwendig sind, werden bewusst nicht betrachtet, da diese Daten nicht mit Smart Meter, sondern konventionell erhoben wurden (beispielsweise über Verträge).	
	Datenschutzbedarf	**Begründung**
Datenschutzbedarf gesamt	Hoch	Ergibt sich nach dem Maximumprinzip aus den aufgeführten Schutzzielen
Verfügbarkeit	Normal	
Integrität	Hoch	Änderungen im Bereich des Zertifikatsmanagements, Berechtigungsprofile etc.
Vertraulichkeit	Hoch	Zugriff des Gateway-Administrators, dieser nimmt eine zentrale Rolle mit umfangreichen Rechten ein, so dass die Vertraulichkeit sichergestellt werden muss
Transparenz	Hoch	Nachvollziehbarkeit der Kündigung und deren Umsetzung (insb. Löschung des Berechtigungsprofils)
Intervenierbarkeit	Normal	
Nichtverkettbarkeit	Normal	
Maßnahmen	Der Letztverbraucher muss über die vollzogene Kündigung informiert werden. Ein Nachweis über ein gesichertes Änderungsmanagement nach Stand der Organisationslehre (ITIL, ISO 27001, ISO 29100/1001, BSI-Grundschutz) zur Sicherung der Transparenz und Integrität muss beim Energielieferanten und Gateway-Administrator vorhanden sein. Der Letztverbraucher braucht eine zentrale Anlaufstelle, um im Zweifelsfall schnell intervenieren zu können und seine Rechte einzufordern.	

Mit Blick auf das korrespondierende Prozessmodell der BNetzA zum Prozess Lieferende zeigt sich die Lücke zwischen diesen Modellen. Das Prozessmodell der BNetzA ist ausschließlich auf funktionale Aspekte des Rollenmodells aus der Perspektive der Marktbedürfnisse des Energiemarktes angelegt und implementiert mithin weder datenschutzrechtliche Maßnahmen zur Vefügbarkeit, Vertraulichkeit, Integrität, Transparenz Intervenierbarkeit und Nichtabstreitbarkeit und deren Methoden, noch eventuelle Neben-läufigkeiten im Informationsfluss.

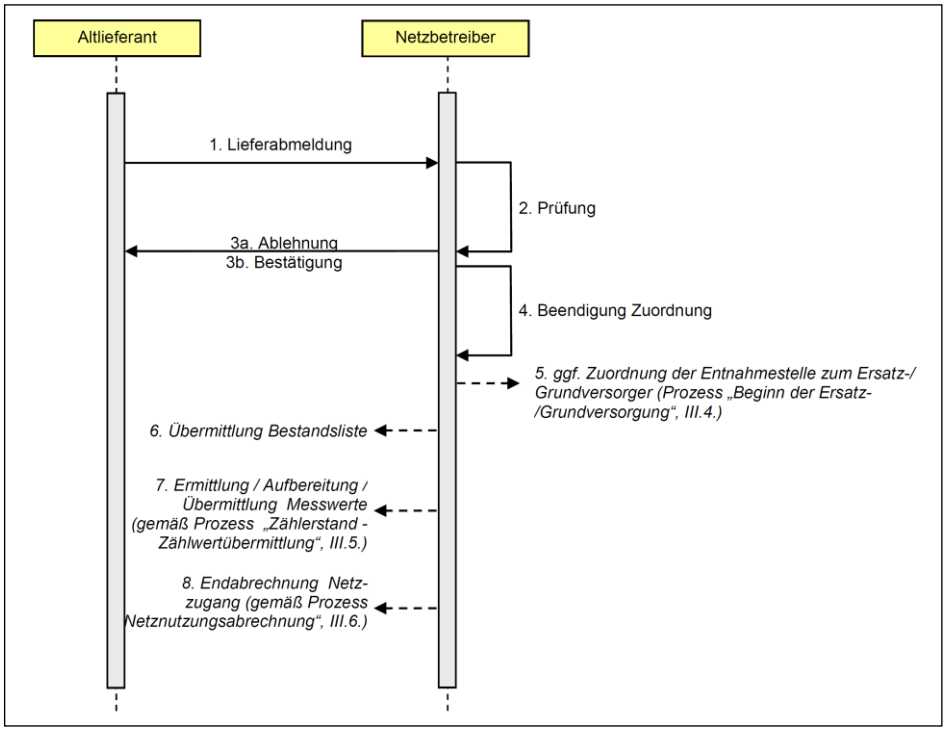

Abbildung 3: Bildliche Darstellung des Prozesses“ Lieferende“[7]

Damit zeigt sich, dass diese Aktivitäten der beiden Behördenstrukturen nicht aufeinander bezogen sind und die Berücksichtigung der datenschutzrechtlichen Obliegenheiten trotz des Vorhandenseins von grundlegenden Modellierungslogiken kein förmlicher Aspekt der Konsensbildung im Festlegungsverfahren ist.

7 BNetzA, Anlage zum Beschluss BK6-06-009 vom 11.07.2006 (GPKE), S. 21.

Literaturverzeichnis

Aamodt, Agnar/Nygård, Mads, Different roles and mutual dependencies of data, information, and knowledge - an AI perspective on their integration, Data and Knowledge Engineering 16, 1995, S. 191ff.

Aichele, Christian (Hrsg.) Smart Energy - Von der reaktiven Kundenverwaltung zum proaktiven Kundenmanagement, Wiesbaden, 2012.

Albers, Marion, Komplexität verfassungsrechtlicher Vorgaben, in: Spiecker gen. Döhmann, Indra/Collin, Peter (Hrsg.) Generierung und Transfer staatlichen Wissens in System des Verwaltungsrecht, Tübingen, 2008, S. 55 ff.

Appel, Ivo, Klassisches Verwaltungsrecht und Steuerungswissenschaft, VVDStRL 67 (2008), S. 226 ff.

Attendorn, Thorsten, Die Regulierungsbehörde als freier Marktgestalter und Normsetzer? Die Zugangsanordnung nach § 21 TKG im Vergleich zur Festlegungsentscheidung nach § 29 EnWG, Möhnesee, 2008.

Atzeni, Paolo/Cheung, David/Ram, Sudha (Hrsg.): Conceptual Modeling. 31st International Conference ER 2012, Florence, Italy, October 15-18, 2012. Proceedings, Berlin, Heidelberg 2012, 487 ff.

Augsberg, Ino,(Hrsg.) Ungewissheit als Chance - Perspektiven eines produktiven Umgangs mit Unsicherheit im Rechtssystem, Tübingen, 2009.

Augsberg, Ino, Informationsverwaltungsrecht - Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen, Tübingen, 2014.

Baur, Jürgen F./Salje, Peter/Schmidt-Preuß, Matthias (Hrsg.), Regulierung in der Energiewirtschaft – Ein Praxishandbuch, Köln 2011.

Beenken, Petra/ Appelrath, Hans-Jürgen/Eckert, Claudia, Datenschutz und Datensicherheit in intelligenten Energienetzen, in: Schartner, Peter, Weippl, Edgar (Hrsg.): Proceedings of D-A-CH Security 2010, Wien, Österreich.

Benz, Arthur/Lütz, Susanne/ Schimank, Uwe/Simonis, Georg (Hrsg.), Handbuch Governance. Theoretische Grundlagen und empirische Anwendungsfelder, Wiesbaden, 2007.

Bielenberg,Walter/Runkel, Peter/Spannowsky, Willy (Hrsg.): Raumordnungs- und Landesplanungsrecht des Bundes und der Länder, Stand 2016.

Bizer, Johann/Lutterbeck, Bernd/Rieß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft – Freundesgabe für Alfred Büllesbach, Stuttgart, 2002.

Bizer, Johann, Mut zur Selbstregulierung, DuD 2003, S. 394 ff.

Bizer, Johann, Datenschutzrechtliche Informationspflichten, DuD 2005, S. 451 ff.

Bizer, Johann, Sieben Goldene Regeln des Datenschutzes, DuD 2007, S. 350 ff.

Büllesbach Alfred, Selbstregulierung im Datenschutzrecht, RDV 2005, S. 13 ff.

Bundesbeauftragter für Datenschutz und Informationssicherheit, 23. Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010, online über http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23TB_09_10.pdf?__blob=publicationFile&v=6

Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie 2009), online über http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile

Bundesministerium für Wirtschaft und Energie, Strategie Intelligente Vernetzung, online über http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/strategie-intelligente-vernetzung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Bundesministerium für Wirtschaft und Energie, Baustein für die Energiewende: 7 Eckpunkte für das „Verordnungspaket Intelligente Netze“, online über https://www.bmwi.de/BMWi/Redaktion/PDF/E/eckpunkte-fuer-das-verordnungspaket-intelligente-netze,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf