Gerrit Hornung, Katharina Fuchs

Nutzerdaten im Smart Grid – zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung

Die Diskussion um die Auswirkungen des Einsatzes von Smart Metern auf die Persönlichkeitsrechte der Letztverbraucher hat – zu Recht – zunächst das Grundrecht auf informationelle Selbstbestimmung in den Blick genommen. Die grundrechtlichen Probleme sind damit allerdings nicht ausgeschöpft: Da die Daten der häuslichen Sphäre entstammen ist zu fragen, ob nicht auch der Schutzbereich von Art. 13 GG betroffen ist. Durch die Erhebung mittels eines IT-Systems (der Smart Meter) kann auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen. Schließlich stellt sich angesichts der Kommerzialisierung der Daten im Smart Grid die Frage, ob vermögenswerte Positionen betroffen sind.*

1 Hintergrund

Aus verfassungsrechtlicher Sicht weist die Idee eines nachhaltigen Energieinformationsnetzes[1] grundsätzliche Spannungsfelder auf. Der Staat verfolgt mit dem Ziel der effektiven Nutzung der im Netz jeweils erzeugten, gerade bei regenerativen Energiequellen stark schwankenden Energiemenge das Allgemeininteresse des Schutzes der natürlichen Lebensgrundlagen, das in Art. 20a GG als Staatsziel verankert ist. Dazu wird die Nutzung personenbezogener Daten der Letztverbraucher teils erlaubt, teils vorgeschrieben, sodass deren grundrechtlich geschützte Persönlichkeitsrechte[2] zu wahren sind; hinzu kommt das Interesse an günstigeren Preisstrukturen angesichts steigender Energiepreise.

Auch auf Seiten der Anbieter und Betreiber von Netzen und Messgeräten bestehen mit der Berufsfreiheit (Art. 12 GG) verfassungsrechtlich geschützte Interessen an neuen Geschäftsmodellen, die mit der Auswertung der Verbrauchsdaten ermöglicht werden.

Der Gesetzgeber fördert diese Entwicklung, indem er Vorgaben für die rechtliche, technische und organisatorische Gestaltung des Energieinformationsnetzes macht. Sobald jedoch wichtige Bausteine dieser Infrastruktur – wie etwa die in § 21d EnWG legaldefinierten „Messsysteme“ (Smart Meter) – dazu geeignet sind, allein oder in der Vernetzung mit elektronischen Haushaltsgegenständen in erheblichem Maße Informationen über die Privatsphäre der Letztverbraucher zu erheben und zu übermitteln, treffen den Staat grundrechtliche Schutzpflichten gegenüber den Betroffenen, deren Reichweite von den jeweils tangierten Grundrechten sowie der Intensität der in Rede stehenden Beeinträchtigung abhängt.

Prof. Dr. Gerrit Hornung, LL.M.

Lehrstuhl für Öffentliches Recht, IT-Recht und Rechtsinformatik, Direktor am Institut für IT-Sicherheit und Sicherheitsrecht (ISL), Universität Passau

E-Mail: gerrit.hornung@uni-passau.de

Dipl.-Jur. (Univ.) Katharina Fuchs

Referendarin am LG Traunstein, ehem. wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik der Universität Passau.
E-Mail: fuchs32@stud.uni-passau.de

* Eine frühere Version dieses Textes ist erschienen in: Alcatel-Lucent-Stiftung, SR Nr. 94, Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz, 2011.

1 S. aus Sicht des Gesetzgebers BT-Drs. 17/6072, 76 ff.; zu den Hintergründen der Entwicklung s. z.B. *Orlamünder*, Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsnetz, Alcatel-Lucent-Stiftung, SR Nr. 85, 2009; *Roßnagel/Jandt*, Datenschutzfragen eines Energieinformationsnetzes. Alcatel-Lucent-Stiftung, SR Nr. 88, 2010, 3 ff.; *dies.*, DuD 2010, 373 f.; *Pielow*, ZUR 2010, 115 ff.; *Raabe*, DuD 2010, 279 f.; *Wiesemann*, MMR 2011, 355; ferner *Güneysu/Vetter/Wieser*, DVBl. 2011, 870; Kritisch zum Nutzen der Erhebung von Verbrauchsdaten *Fox/Müller,* in: Alcatel-Lucent-Stiftung, SR Nr. 94, 6 ff.

2 Im wirtschaftlichen Umfeld können auch grundrechtlich geschützte Betriebs- und Geschäftsgeheimnisse betroffen sein (die dann auch juristischen Personen zustehen können). Dieser Aspekt bleibt im Folgenden außer Betracht.

2 Betroffene Grundrechte

In der bisherigen Diskussion ist ausführlich herausgearbeitet worden, dass in praktisch allen Konstellationen aufgrund der Identifizierbarkeit der Letztverbraucher einfachgesetzlich die Regeln des Datenschutzrechts und auf verfassungsrechtlicher Ebene das Grundrecht auf informationelle Selbstbestimmung einschlägig sind.[3] Dieses schützt „die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[4]

Derartige Daten fallen im Energieinformationsnetz in vielfältiger Weise an. So weisen regelmäßig alle Informationen, die zur näheren Ausgestaltung und Abwicklung der Vertragsverhältnisse zwischen den Energieerzeugern, den Energieversorgungsunternehmen, den Messstellenbetreibern, den Messstellendienstleistern und den Energieverbrauchern benötigt werden einen entsprechenden Personenbezug auf.[5]

Hierzu gehören etwa die Zahl der verbrauchten Kilowattstunden der Anschlussinhaber und der Verbrauchszeitraum (bei tageszeitvariablen Tarifen), aber auch Informationen über den Status einzelner Verbrauchsgeräte oder Angaben über die aktuellen Energieverbrauchswerte einzelner solcher Geräte.[6] Das bedeutet indes nicht, dass alle insoweit erhobenen Daten auch im selben Maße schutzbedürftig sind: So wird die Information, dass bestimmte Haushaltsgeräte zu einer bestimmten Tageszeit aktiv sind, noch relativ belanglos sein. An der Information, dass über einen längeren Zeitraum überhaupt keine Haushaltsgeräte bedient werden, könnten demgegenüber Kriminelle ein großes Interesse haben. Schließlich greifen die in § 14a EnWG normierte externe Steuerung von Verbrauchseinrichtungen sowie das Fernwirken und Fernmessen (§ 21g Abs. 6 Satz 5 und 6 EnWG)[7] direkt in die bisher abgeschottete Sphäre der Letztverbraucher ein.

Insgesamt ist deutlich, dass Smart Meter und die mit ihnen verbundenen Infrastrukturen zumindest potentiell eine besondere Eingriffstiefe hervorrufen, die durch den großen Umfang der Datenerhebung, die Vielzahl der von ihr betroffenen Lebensbereiche, die erhöhte Aussagekraft der erhobenen Daten, die steigende Anzahl der datenverarbeitenden Stellen (vor allem durch die neue Rolle des Messstellenbetreibers nach § 3 Nr. 26a EnWG) und das gesteigerte Interesse Dritter an den erhobenen Daten verursacht wird.[8]

Aus dem verfassungsrechtlichen Schutzprogramm der informationellen Selbstbestimmung lassen sich Anforderungen an eine rechtliche Regelung des Energieinformationsnetzes und an seine technische Gestaltung ableiten.[9] Der Gesetzgeber ist inzwischen aktiv geworden und hat mit dem Gesetz zur Neuregelung energiewirtschaftsrechtlicher Vorschriften (EnWRNRG)[10] mit Wirkung vom 4.8.2011 Regelungen für die Erhebung und Verwendung personenbezogener Daten im Smart Grid geschaffen.[11] Diese sehen auch Vorgaben für die Zertifizierung der Messsysteme anhand eines Schutzprofils (Protection Profile) nach Common Criteria vor (§ 21e Abs. 2 und Abs. 4 EnWG),[12] welches nicht nur datenschutzrechtliche Aspekte, sondern auch die – schon aus eichrechtlichen Gründen – überaus wichtigen Fragen der Datensicherheit berücksichtigt.[13] Auch wenn nicht alle rechtspolitischen Forderungen umgesetzt wurden,[14] hat der Gesetzgeber mit dem Instrument des Schutzprofils und mit den Vorgaben zu Verarbeitungszwecken und Erforderlichkeit der Datenverwendung (§ 21g Abs. 1 EnWG), zur Datensicherheit nach dem dynamischen Maßstab des „jeweiligen" Stands der Technik (§ 21e Abs. 3 Satz 1 EnWG), zu bereichsspezifischen Auskunftsansprüchen (§ 21h Abs. 1 EnWG), zur Anonymisierung und Pseudonymisierung (§ 21g Abs. 3 Satz 4 und Abs. 5 EnWG), zum Kopplungsverbot (§ 21g Abs. 6 Satz 3 EnWG) und zu den Informationspflichten bei „Datenpannen" (§ 21h Abs. 2 EnWG)[15] jeweils Schritte in die richtige Richtung unternommen.

Die grundrechtliche Dimension des Energieinformationsnetzes erschöpft sich jedoch nicht mit der informationellen Selbstbestimmung – die Letztverbraucher sind im Smart Grid zwar regelmäßig identifizierbar, aber nicht stets gleich zu behandeln. Soweit Smart Meter in der häuslichen Sphäre der Letztverbraucher verbaut werden und in dieser Informationen erheben, kann das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) betroffen sein. Dasselbe gilt für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung entwickelt hat. Angesichts des wirtschaftlichen Werts der im Smart Grid erhobenen und verwendeten Daten bestehen außerdem Anhaltspunkte für eine eher eigentums- oder vermögensrechtlich strukturierte Grundrechtsdimension. Diese drei Bereiche werden im Folgenden hinsichtlich der Betroffenheit der Schutzbereiche und der Frage behandelt, welche Schlussfolgerungen für das Handeln staatlicher Stellen und etwaige Schutzpflichten gegenüber den Letztverbraucher zu ziehen sind.

3 Hiervon geht auch der Gesetzgeber aus, s. BT-Drs. 17/6072, 76 ff.; zur Diskussion s. z.B. *Göge/Boers*, ZNER 2009, 368, 370; *Karg*, DuD 2010, 365 ff.; *Raabe*, DuD 2010, 379 ff.; *Roßnagel/Jandt* (Fn. 1), 6 ff.; *dies.*, DuD 2010, 373 ff.; *Müller*, DuD 2010, 359 ff.; *Güneysu/Vetter/Wieser*, DVBl. 2011, 870, 872 f.; *Art. 29 Data Protection Working Party*, Opinion 12/2011 on smart metering, 2011; *Jandt*, in: Roßnagel (Hrsg.), Nutzerschutz – Rechtsrahmen, Technikpotentiale, Wirtschaftskonzept, 2011, i.E; zu Österreich *Renner*, DuD 2011, 524 f.; zu Einzelheiten s. v.a. die Szenarien in *Raabe/Pallas/Weis/Lorenz/Boesche*, Datenschutz in Smart Grids, 2011.

4 BVerfGE 65, 1 (42), s. zuletzt ausführlich *Albers*, Informationelle Selbstbestimmung, 2005.

5 *Roßnagel/Jandt* (Fn. 1), 22.

6 S. hierzu die Tabelle von *Roßnagel/Jandt* (Fn. 1), 21.

7 Hierzu bestehen teilweise Regelungen in den Landesdatenschutzgesetzen, s. z.B. § 36 HDSG.

8 S. näher *Roßnagel/Jandt* (Fn. 1), 6 ff.

9 S. *Roßnagel/Jandt* (Fn. 1), 26 ff., 38 ff.; *dies.*, DuD 2010, 373, 375 ff.; *Karg*, DuD 2010, 365, 366 ff.; *Raabe*, DuD 2010, 379, 381 ff.; *Art. 29 Data Protection Working Party* (Fn. 3), 16 ff.; *Raabe/Lorenz/Pallas/Weis/Malina*, DuD 2011, 519 ff.; zur technischen Umsetzung s. *Eckert*, Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz, Alcatel-Lucent-Stiftung, SR Nr. 90, 2011; *Cavoukian/Polonetsky/Wolf*, IDIS 2010, 275 ff.; zum Konzept einer anonymen Datenübertragung *Jeske*, DuD 2011, 530 ff.

10 BGBl. I 2011, Nr. 41, S. 1554.

11 S. *Roßnagel/Jandt/Volland*, ZD 2011, 99.

12 Dazu z.B. *Laupichler/Vollmer/Bast/Intemann*, DuD 2011, 542 ff.; *Müller*, DuD 2011, 547 ff.

13 S. näher *Eckert* (Fn. 9); *Eckert/Krauß*, DuD 2011, 542.

14 So die – allerdings auch weitreichende – Forderung nach einem „Energiegeheimnis" von *Roßnagel/Jandt* (Fn. 1), 38; s.a. *Jandt* (Fn. 3); kritisch auch *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Stellungnahme v. 10.6.2011, https://www.datenschutzzentrum.de/smartmeter/20110615-smartmeterregelung.pdf; s.a. die Würdigung bei *Roßnagel/Jandt/Volland*, ZD 2011, 99, 102 f.

15 S. dazu allgemein *Gabel*, BB 2009, 2045 ff.; *Eckhardt/Schmitz*, DuD 2010, 390 ff.; *Hanloser*, MMR 2010, 300 ff.; *Hornung*, NJW 2010, 1841 ff.

3 Art. 13: Unverletzlichkeit der Wohnung

Art. 13 GG verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in ihm in Ruhe gelassen zu werden.[16] Geschützt wird die „räumliche Privatsphäre";[17] historisch vor allem gegen Eingriffe bei physischer Anwesenheit von Trägern öffentlicher Gewalt. Das Bundesverfassungsgericht hat aber überzeugend dargelegt, dass „der Schutzzweck der Grundrechtsnorm vereitelt [würde], wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung […] umfasst wäre".[18] Auch solche Maßnahmen stellen also eine Beeinträchtigung des räumlich-gegenständlichen Bereichs der Privatsphäre dar, die durch eine anschließende Speicherung und Verwendung der gewonnenen Informationen oder eine Übermittlung an andere Stellen weiter fortgesetzt wird.[19]

Die durch Smart Meter gewonnenen Daten stammen vielfach aus diesem Bereich der räumlichen Privatsphäre. Ihr Einsatz ermöglicht im Falle einer entsprechend hohen zeitlichen Auflösung die Erstellung eines präzisen Lastprofils, aus dem sich detaillierte Informationen über die jeweiligen Haushaltsmitglieder und ihre Verhaltensweisen und Gewohnheiten gewinnen lassen: Da die Anzahl der zugleich betriebenen elektrischen Geräte in einem Haushalt begrenzt ist und sich die verschiedenen Apparate durch spezifische Lastprofile auszeichnen, ist es möglich, einen Großteil der Geräte – insbesondere solche mit hoher Leistung wie Kühlschrank, Spülmaschine oder Backofen – eindeutig zu identifizieren.[20] Ist es aber erst einmal gelungen, die Eckdaten und Lastprofile der leistungsintensiven Geräte zu ermitteln und in der Folge aus dem Lastgang des Haushalts herauszurechnen, steht auch der Identifikation kleinerer Verbraucher (z. B. Staubsauger oder Haartrockner) anhand von Kriterien wie Leistungsaufnahme, Funktionsweise, typische Arbeitszyklen, Nutzungszeitpunkte oder Verwendungshäufigkeit nichts mehr im Wege.

Letztlich werden auf diese Weise diverse Rückschlüsse auf die Lebensgewohnheiten der Haushaltsmitglieder möglich, die sonst nicht ohne herkömmliche Eingriffe in Art. 13 GG ermittelbar wären, etwa wann die Bewohner zu Bett gehen und morgens aufstehen, ob es nächtliche Toilettenbesuche gibt, wie häufig und mit welchen Geräten vorzugsweise gekocht wird, wie oft die Haushaltsmitglieder Besuch empfangen, wie häufig die Waschmaschine läuft etc.[21] Ferner geben etwa Dauer und Zeitraum der Nutzung eines Computers oder des Fernsehers Hinweise auf das Freizeitverhalten oder die Interessen des Nutzers. Selbst die Tatsache, dass in bestimmten Zeiträumen kein oder nur sehr wenig Strom verbraucht wird, kann zu Vervollständigung des Verbraucherprofils genutzt werden und Aufschluss über die Lebensumstände der Betroffenen geben, wie etwa über den Grund einer kürzeren oder längeren Abwesenheit (Arbeit, Krankenhausaufenthalt, Urlaubsreise).[22] Für den Eingriff kommt es nicht darauf an, ob diese Informationen definitiv einzelnen Personen zugeordnet werden können. Bei Einpersonenhaushalten ist dies allerdings ohnehin der Fall, und bei der zur Energieeffizienzberatung gegebenenfalls notwendigen geräte- und raumgenauen Auflösung der Messdaten können mit entsprechendem Zusatzwissen auch bei mehreren Bewohnern konkrete Verhaltensprofile im innerhäuslichen Bereich ermittelt werden.[23]

Dass diese Informationen dem durch Art. 13 GG geschützten räumlichen Bereich entstammen, ist weithin eindeutig. Zweifeln kann man an der Anwendbarkeit des Grundrechts höchstens deshalb, weil die Aussagekraft gegenüber einer direkten Beobachtung herabgesetzt sein kann: Die anhand eines Lastprofils gewonnene Information, dass ein Fernseh- oder Radiogerät eingeschaltet ist, gibt zunächst noch keine Auskunft darüber, welches Programm ausgewählt wurde. Vergleichbares gilt für die Nutzung anderer elektrischer Haushaltsgeräte. Deshalb ist der Hinweis zutreffend, dass in einer solchen Situation die Verbrauchsdaten von Smart Metern nicht mit einer optischen oder akustischen Überwachung des Betroffenen in seiner Wohnung gleichgesetzt werden können.[24] Dies würde sich jedoch grundlegend anders darstellen, wenn es anhand des Lastprofils eines Fernsehgeräts doch möglich sein sollte, das eingeschaltete Programm oder den abgespielten Film zu identifizieren. Genau hierfür gibt es erste Forschungsergebnisse, die anhand des Stromverbrauchs den konsumierten Inhalt bestimmen.[25]

Selbst wenn keine derartigen direkten Informationen über das Konsumverhalten in der Wohnung gewonnen werden können, kann daraus nicht der Schluss gezogen werden, Art. 13 GG sei insgesamt nicht anwendbar. Ob der Schutzbereich eines Grundrechts einschlägig ist, hängt grundsätzlich nicht davon ab, in welcher Intensität in diesen eingegriffen wird,[26] und ob der Eingriff seiner Art nach mit bisher üblichen Eingriffen vergleichbar ist. Ohnehin ist auch ohne Erkennbarkeit audiovisueller Kommunikationsinhalte zweifelhaft, ob die Eingriffsintensität wirklich geringer ist: Die Art der Erfassung von Energieverbrauchsdaten ermöglicht eine unbegrenzte Speicherung, die jederzeitige und ohne Rücksicht auf Entfernungen in Sekundenschnelle erfolgende Übermittlung sowie die Verschneidung dieser Informationen mit anderen Daten.[27] Je nach technischer Umsetzung des Energieinformationsnetzes und der im Einzelfall durch den Smart Meter erhobenen Daten erscheint es deshalb denkbar, dass ein zwar andersartiger, im Ergebnis aufgrund der gewonnenen Persönlichkeitsprofile aber doch der optischen oder akustischen Überwachung vergleichbar intensiver Grundrechtseingriff vorliegt.[28]

Gegen die Anwendbarkeit von Art. 13 GG könnte man indes vorbringen, das Bundesverfassungsgericht habe in dem vergleichbaren Fall der Online-Durchsuchung einen entsprechenden Eingriff abgelehnt. Allerdings wurde dort entscheidend damit argumentiert, der Eingriff könne unabhängig vom Standort erfolgen, der den Behörden oftmals noch nicht einmal bekannt sei, sodass die durch die Abgrenzung der Wohnung vermittelte räumliche

16 BVerfGE 32, 54 (75); 42, 212 (219); 51, 97 (110); 109, 279 (309).
17 BVerfGE 7, 230 (238); 109, 279 (309).
18 BVerfGE 109, 279 (309); s.a. BVerfGE 120, 274 (309 f.).
19 BVerfGE 109, 279 (327).
20 S. *Müller*, DuD 2010, 359, 360 f.; s. zu den betroffenen Lebensbereichen auch *Roßnagel/Jandt* (Fn. 1), 7 ff.
21 *Müller*, DuD 2010, 359, 360 f.
22 *Roßnagel/Jandt*, (Fn. 1), 2010, 8 f.
23 *Raabe*, DuD 2010, 379, 381.
24 *Göge/Boers*, ZNER 2009, 368, 369.
25 S. das Arbeitspapier des Labors für IT-Sicherheit der FH Münster, http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.
26 Die Intensität eines Eingriffs spielt vielmehr regelmäßig erst im Rahmen der Frage nach einer möglichen Rechtfertigung desselben eine Rolle, s. *Kube*, JuS 2003, 111, 112 (speziell zu Art. 2 Abs. 1 GG).
27 S. *Karg*, DuD 2010, 365, 366 f.
28 So auch *Müller*, DuD 2010, 359, 364; *Karg*, DuD 2010, 365, 366.

Privatsphäre unberührt bleibe.[29] Dies ist hier anders: Der Standort der Smart Meter liegt regelmäßig ebenso in dieser Sphäre wie die elektronischen Geräte, durch deren Verbrauchsmessung die beschriebenen Informationen über Verhaltensweisen innerhalb der Wohnung erhoben werden.

Bei einem physischen Zugriff auf Messsysteme ist Art. 13 GG ohnehin einschlägig; das hat das Bundesverfassungsgericht auch für den Fall des Zugriffs auf IT-Systeme zur Online-Durchsuchung betont.[30]

Soweit Art. 13 GG nach diesen Kriterien anwendbar ist, wird das Grundrecht auf informationelle Selbstbestimmung verdrängt.[31] Hoheitliche Eingriffe (also der Zugriff auf die Daten, solange sich diese in der häuslichen Sphäre befinden) unterliegen den allgemeinen Anforderungen von Art. 13 Abs. 2 bis Abs. 7 GG. Da Art. 13 Abs. 3 GG zur Aufklärung von Straftaten nur technische Mittel „zur akustischen Überwachung" zulässt, ist ein externer Zugriff auf die Daten zu diesem Zweck unzulässig. Denkbar wäre zum einen eine Datenerhebung im Rahmen einer Durchsuchung (Art. 13 Abs. 2 GG), zum anderen ein Zugriff auf die Daten, die an die Betreiber von Messstellen oder Netzen weitergeleitet wurden. Im präventiven Bereich lässt Art. 13 Abs. 4 GG demgegenüber (unter weiteren Voraussetzungen) allgemein „technische Mittel zur Überwachung von Wohnungen" zu. Dieser Begriff ist entwicklungsoffen und beschränkt sich nicht auf die zur Zeit der Verfassungsänderung bekannten Mittel.[32] Damit ist ein externer Zugriff zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, zumindest prinzipiell möglich.

Hinsichtlich der Rechtsverhältnisse zwischen Letztverbrauchern, Messstellen- und Netzbetreibern sowie Energieversorgungsunternehmen verstärkt Art. 13 GG die aus dem Grundrecht auf informationelle Selbstbestimmung abgeleiteten Schutzpflichten hinsichtlich der räumlichen Privatsphäre. Das betrifft insbesondere Maßnahmen der IT-Sicherheit gegen Angriffe, mit denen der Zugriff auf die Daten oder die Manipulation häuslicher Systeme (etwa deren missbräuchliche Steuerung von außen)[33] bezweckt wird.

4 IT-Grundrecht

Smart Meter und eine Vielzahl elektronischer Haushaltsgeräte, deren Verbrauch sie aufzeichnen, sind IT-Systeme. Allein deshalb fallen sie allerdings noch nicht in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses erfasst keine Systeme, die „nach ihrer technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten"; erforderlich ist nach Aussage des Bundesverfassungsgerichts vielmehr, dass sie „allein oder in ihren technischen Vernetzung personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff […] es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[34]

Ob diese Voraussetzungen erfüllt sind, hängt von der technischen Gestaltung der Smart Meter und ihrer Vernetzung mit IT-Systemen im Haushalt ab. In der reinen Information über den Stromverbrauch wird man eher eine punktuelle Aussage über einen bestimmten Lebensbereich sehen müssen. Die oben beschriebenen detaillierten Aussagen über das Verhalten der Bewohner erreichen aber bereits eine andere Qualität. Hierbei ist auch wichtig, dass das Bundesverfassungsgericht nicht verlangt, dass das IT-System tatsächlich besonders sensible Informationen enthält: Ausreichend ist vielmehr, dass das System hierzu potentiell in der Lage ist („enthalten können"). Dies wird weithin der Fall sein; auch die Gesetzesbegründung zum EnWRNRG spricht von „intelligenten Messsystemen".[35] Wenn diese schließlich mit weiteren IT-Systemen im Haushalt interagieren, so kommt der Aspekt der technischen Vernetzung ins Spiel, den das Bundesverfassungsgericht besonders hervorgehoben hat: Die steuerbaren Geräte müssen dann einheitlich betrachtet werden, und dies erhöht die Wahrscheinlichkeit, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betroffen ist.

Damit eine „grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung" besteht, verlangt das Bundesverfassungsgericht des Weiteren, dass „der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das System selbstbestimmt verfügt".[36] Hierfür ist unerheblich, dass Messeinrichtungen und Messsysteme nach § 21b Abs. 4 Satz 1 EnWG regelmäßig nicht im Eigentum des Letztverbrauchers stehen werden: Entscheidend ist nicht die sachenrechtliche Zuordnung, sondern die selbstbestimmte Nutzung „als" eigenes System. Die Literatur geht überwiegend davon aus, dass dies zumindest auch schuldrechtliche Zuordnungen, etwa im Arbeitsverhältnis, erfasst.[37] Soweit allerdings IT-Systeme nach ihrer Konzeption gerade darauf angelegt sind, Dritten Daten zu übermitteln – dies dürfte bei isolierter Betrachtung auf Smart Meter zutreffen –, so entfällt die Nutzung „als eigenes" System.[38]

Jedenfalls nutzt der Letztverbraucher aber die in der Wohnung befindlichen IT-Systeme als eigene. Soweit es also nach den oben genannten Kriterien auf die (gesamte) vernetzte Haustechnik ankommt, liegt in jedem Fall die grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung vor. Das gilt beispielsweise in dem in § 14a EnWG ausdrücklich vorgesehen Fall, dass Betreibern von Elektrizitätsverteilernetzen „die Steuerung

29 BVerfGE 120, 274 (310 f.); a.A. z.B. *Buermeyer*, HRRS 2007, 392, 395 ff.; *Hornung*, DuD 2007, 575, 577 f.; *Kudlich*, HFR 19-2007, 4 ff.; *Rux*, JZ 2007, 285, 292 ff.; *Schaar/Landwehr*, K&R 2007, 202, 204; *Schantz*, KritV 2007, 310 ff.; wie das BVerfG *Gercke*, CR 2007, 245, 250; *Schlegel*, GA 2007, 648 ff.

30 BVerfGE 120, 274 (310).

31 BVerfGE 51, 97 (105); s.a. *Di Fabio*, in: Maunz/Dürig, GG, 61. Ergänzungslieferung 2011, Art. 2 Rn. 21 ff.

32 *Gornig*, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 6. Auflage 2010, Art. 13 Rn. 129.

33 Zu den externen Gefahren, die beim Einsatz von Smart Metern und Smart Grids drohen und den zu deren Abwehr unerlässlichen Schutzmaßnahmen s. *Eckert* (Fn. 9); *Eckert/Krauß*, DuD 2011, 535 ff.

34 BVerfGE 120, 274 (313 f.).

35 BT-Drs. 17/6072, 76, 78 f. in Anlehnung an die Formulierung in den Richtlinien 2009/72/EG (ABl. EU 2009 Nr. L 211 S. 91) und 2009/73/EG (ABl. EU 2009 Nr. L 211 S. 134).

36 BVerfGE 120, 274 (315).

37 Zu den Auswirkungen des Grundrechts auf das Arbeitsrecht s. z.B. *Stögmüller*, CR 2008, 435 ff.; *Wedde*, AuR 2009, 373 ff.; erste Gerichtsentscheidungen erkennen dies zumindest am Rande an, s. Hessischer VGH, NJW 2009, 2470; LAG Niedersachsen, MMR 2010, 639.

38 S.a. *Luch*, MMR 2011, 75, 76.

von vollständig unterbrechbaren Verbrauchseinrichtungen“ der Letztverbraucher gestattet wird.

Soweit der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme reicht, müssen hoheitliche Eingriffe im präventiven Bereich den Anforderungen genügen, die das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung aufgestellt hat: vor allem Gefahr für ein überragend wichtiges Rechtsgut, Richtervorbehalt, zweistufiger Kernbereichsschutz.[39]

Für den Bereich der Strafverfolgung fehlen dagegen bislang Leitlinien des Gerichts. Ebenso wie beim Grundrecht auf informationelle Selbstbestimmung und bei Art. 13 GG bestehen aber Auswirkungen auf das Privatrecht,[40] die sich insbesondere in staatlichen Schutzpflichten niederschlagen.[41] Der Gesetzgeber ist deshalb gehalten, sich „schützend und fördernd“[42] vor die Vertraulichkeit und Integrität informationstechnischer Systeme zu stellen.

Insbesondere der Schutz der Integrität der Smart Meter und der mit ihnen vernetzten IT-Systeme der Letztverbraucher gewinnt hiermit eine besondere Bedeutung. Dem ist präventiv auf technischer Ebene im Rahmen des gesetzlich geforderten „jeweiligen Stands der Technik“ (§ 21e Abs. 3 Satz 1 EnWG) durch erhöhte Anforderungen Rechnung zu tragen. Überdies schlägt sich die Schutzpflicht in einem Auftrag an den Gesetzgeber nieder, durch gesetzliche Regelungen insbesondere dort Vorgaben zu machen, wo es im Verhältnis zwischen Bürgern und großen Wirtschaftsunternehmen zu einem Machtungleichgewicht kommt. Man kann aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme insoweit nicht nur zivilrechtliche Ansprüche auf Unterlassung nicht autorisierter Systemzugriffe ableiten, sondern auch einen positiven Anspruch auf Schutz der durch einen Dienstanbieter zur Nutzung bereitgestellten Systeme vor unbefugten Zugriffen Dritter.[43] Wenn der Gesetzgeber Schutzvorgaben an den Verordnungsgeber delegiert (§ 21i EnWG), so sind diese Anforderungen auf der Verordnungsebene ebenfalls umzusetzen.

5 Kommerzialisierung der Verbrauchsdaten?

Eine letzte grundrechtliche Frage wird durch den besonderen Charakter der durch Smart Meter erhobenen Daten aufgeworfen, die nicht nur den neuen Funktionalitäten des Energieinformationsnetzes dienen, sondern auch Grundlage für neue Abrechnungsmodelle und andere wirtschaftlich relevante Tätigkeiten sind. Dies kommt besonders deutlich in der Wertung des Gesetzgebers zum Ausdruck, die § 14a Satz 1 EnWG zugrunde liegt: Im Gegenzug für das Überlassen der externen Steuerung wird die Berechnung eines reduzierten Netzentgelts explizit vorgeschrieben. Der Sache nach steht dies auch insgesamt hinter der Idee der Smart Meter: Die Effizienzsteigerung und Verbesserung der Auslastung wird durch die Erhebung der Verbrauchsdaten und (noch effektiver) durch die anbieterseitige Steuerung von Verbrauchseinrichtungen verbessert. Beide Mittel stammen aus der Sphäre der Letztverbraucher oder greifen in sie ein – deshalb sollen die Letztverbraucher hiervon auch profitieren.

Hierin liegt eine interessante Perspektive sowohl auf die raumbezogen geschützte Privatsphäre (Art. 13 GG und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme), als auch auf das Grundrecht auf informationelle Selbstbestimmung, das losgelöst von solchen Räumen die Persönlichkeitsrechte schützt: „Gehören“ die durch elektronische Haushaltsgeräte erzeugten Verbrauchsdaten den Bewohnern der Häuser und Wohnungen? Können sie im Grundsatz frei entscheiden, ob sie diese an Betreiber von Netzen und Messstellen „verkaufen“, und im Gegenzug Rabatte erhalten? Und muss der Staat, wenn er im übergeordneten Interesse den Einbau – und perspektivisch die Nutzung? – von Smart Metern vorgibt, neben Vorschriften zum Schutz der Persönlichkeitsrechte auch solche zu reduzierten Entgelten wie in § 14a Satz 1 EnWG machen?

Trotz des Bezugs zur räumlichen Wohnungssphäre, der Nutzung der im Eigentum der Letztverbraucher stehenden Elektrogeräte und der individuellen Lebensführung, die die Basis für die erhobenen Verbrauchsdaten bildet, kann man nicht so weit gehen, diese Position der grundrechtlichen Eigentumsgarantie zuzuordnen. Zwar schützt Art. 14 GG auch die rechtliche Zuordnung privater vermögenswerter Güter zu einem Rechtsträger, und dies geht weit über das hinaus, was umgangssprachlich und nach bürgerlichem Recht (§ 903 BGB) unter „Eigentum“ verstanden wird.[44] Bei der Nutzung feingranularer Verbrauchsdaten ist aber – jenseits der Frage, ob diese sich überhaupt zu einer einigermaßen abgrenzbaren vermögenswerten Position verdichten – die Funktion der Eigentumsgarantie nicht betroffen, dem Einzelnen „die privat verfügbare ökonomische Grundlage individueller Freiheit“ zu gewährleisten.[45] Das gilt insbesondere im Verhältnis zu Netz- und Messstellenbetreibern, weil diese die Energie bereitstellen, die Grundlage für die Verbrauchsdaten ist.

Dennoch ist der wirtschaftliche Wert dieser Daten grundrechtlich nicht belanglos. Er wirft nämlich die grundsätzliche Frage auf, ob die oben erörterten Persönlichkeitsrechte (auch) eigentumsähnlich strukturiert sind. In Deutschland wird das für das Grundrecht auf informationelle Selbstbestimmung überwiegend abgelehnt,[46] während man in anderen Ländern offen für diese Perspektive ist.[47] Allerdings wird auch das deutsche allgemeine Persönlichkeitsrecht – das verfassungsrechtlich die Basis der

39 BVerfGE 120, 274 (327 ff.).

40 Zum Einfluss des Grundrechts auf das Privatrecht s. *Roßnagel/Schnabel*, NJW 2008, 3534 ff.; zu § 823 Abs. 1 BGB *Bartsch*, CR 2008, 613 ff.

41 S. ausführlich *Heckmann*, in: Rüssmann (Hrsg.), Festschrift für Gerhard Käfer, 2009, 129 ff. sowie *Roßnagel/Schnabel*, NJW 2008, 3534, 3535; *Holznagel/Schumacher*, MMR 2009, 3, 6 f.; *Luch*, MMR 2011, 75, 78 f.; tendenziell zurückhaltend gegenüber der Ableitung spezifischer Schutzpflichten *Sick*, VBIBW 2009, 85 ff.

42 So die Formulierung des Bundesverfassungsgerichts zu Art. 2 Abs. 2 GG, s. BVerfGE 39, 1 (42); 46, 160 (164); 53, 30 (57); 88, 203 (251); 90, 145 (195); 115, 118 (152), 121, 317 (356); ebenso zu Art. 5 Abs. 3 GG: BVerfGE 35, 79 (113); 85, 360 (384).

43 Treffend *Luch*, MMR 2011, 75, 78 f.

44 S. z.B. *Wieland*, in: Dreier, Grundgesetz Kommentar, Band I, 2. Auflage 2004, Art. 14 Rn. 38 ff. m.w.N.

45 BVerfG, NJW 1998, 1934, 1936; s.a. *Depenheuer*, in: v. Mangoldt/Klein/Starck (Fn. 31). Art. 14 Rn. 11 ff.

46 *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, 141 ff.; *Pitschas*, DuD 1998, 139, 148; *Simitis*, in: ders. (Hrsg.), BDSG, 7. Auflage 2011, Einl. Rn. 26; *ders.*, NJW 1998, 2473, 2476 f.; *Trute*, JZ 1998, 822, 825 ff.; *ders.*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2.5 Rn. 19, 21; *Weichert*, NJW 2001, 1463 ff.; *ders.*, in: Taeger (Hrsg.), Informatik – Wirtschaft – Recht: Regulierung in der Wissensgesellschaft, FS für Wolfgang Kilian, 2004, 281 ff.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 207 f., 230; s. aber anders *Ladeur*, NJW 2000, 1977, 1980: quasi-eigentumsrechtlich geschütztes Interesse am eigenen Bild (allgemeiner *ders.*, DuD 2000, 12, 18 f.); darauf aufbauend für Daten in sozialen Netzwerken *Hoeren*, ZRP 2010, 251, 252.

47 Insbesondere in den USA, s. die Nachweise bei *Ladeur*, DuD 2000, 12, 18 f.; Simitis (Fn. 46), Einl. Rn. 26.

informationellen Selbstbestimmung ist im Zivilrecht durchaus „kommerzialisiert".[48] Auf verfassungsrechtlicher Ebene scheint einer eigentums- oder vermögensorientierten Konzeption die gesellschaftlich-demokratische Dimension informationeller Selbstbestimmung entgegenzustehen: Nicht nur der Einzelne, auch die Gesellschaft insgesamt hat ein Interesse an selbstbestimmter Persönlichkeitsentfaltung, ohne die eine freiheitliche Gesellschaft nicht möglich ist, und die unbeobachtete Bereiche des Ausprobierens und der geschützten Kommunikation erfordert.[49] Soweit Daten Ergebnis von Kommunikation (oder als Informationen Ergebnis kognitiver Prozesse der verantwortlichen Stelle) sind, ist die eigentumsorientierte Sichtweise auch deswegen unzureichend, weil erhobene Daten dann immer schon auch dem Kommunikationspartner „gehören".

Allerdings besteht im Energieinformationsnetz die Besonderheit, dass die personenbezogenen Daten, die erhoben und verwendet werden sollen, einer (oder, wenn sowohl Art. 13 GG als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen, zwei) räumlich geschützten Sphäre entstammen, die dem Letztverbraucher grundrechtlich zugeordnet ist, und in der sie „produziert" werden. Außerdem sind die Daten nach der gesetzlichen und wirtschaftlichen Konzeption des Smart Grid jenseits der Letztverbrauchersphäre ohnehin kommerzialisiert und werden (wenn auch möglicherweise in aggregierter, also nicht mehr einzelnen Verbrauchern zuordenbarer Form) zum Wirtschaftsgut, das auch den Wirtschaftsgrundrechten unterfällt. Wieso diese Dimension im Rahmen des Grundrechtsschutzes des Letztverbrauchers nicht ebenfalls eingreifen soll, leuchtet nicht ein. Dazu muss man informationelle Selbstbestimmung nicht als solche eigentums- oder vermögensähnlich konzipieren. Es spricht aber dafür, diese Dimension als Verstärkung des Schutzes der Letztverbraucher zu begreifen, deren Besonderheiten im Rahmen grundrechtlich begründeter Schutzprogramme zur berücksichtigen sind.

6 Fazit: Gestaltungsziele für Sicherheit und Nutzerschutz

Im Ergebnis haben alle drei untersuchten Bereiche verfassungsrechtliche Auswirkungen für Sicherheit und Nutzerschutz im Energieinformationsnetz. Am deutlichsten sind diese für das Handeln staatlicher Stellen, weil Art. 13 GG und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme andere (und höhere) Anforderungen an die Rechtfertigung von Eingriffen beinhalten. Der besondere Charakter der Daten ist, soweit der Schutzbereich der beiden Grundrechte betroffen ist, zumindest auf der Verhältnismäßigkeitsebene auch dann zu berücksichtigen, wenn die Daten nicht beim Letztverbraucher, sondern bei Netz- und Messstellenbetreibern durch staatliche Stellen erhoben werden.[50]

Für den Bereich der Umsetzung zwischen privaten Betreibern und Letztverbrauchern ergeben sich ebenfalls höhere Anforderungen, als dies bei isolierter Betrachtung des Grundrechts auf informationelle Selbstbestimmung der Fall wäre. Dementsprechend sind bei der Verabschiedung der Rechtsverordnung nach § 21i EnWG und bei der Erarbeitung der Vorgaben für die technische Umsetzung durch Schutzprofile hohe Anforderungen an den Persönlichkeitsschutz der Letztverbraucher vorzusehen, die überdies den besonderen Strukturen der zusätzlich einschlägigen Grundrechte Rechnung tragen müssen.

48 Seit BGHZ 26, 348 (Herrenreiter-Entscheidung).

49 S. BVerfGE 65, 1 (43): „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

50 Daraus lässt sich ein zusätzliches Argument für den Vorschlag eines Energiegeheimnisses ableiten, s. dazu *Roßnagel/Jandt* (Fn. 1), 38.