RECHTSRAHMEN DER DIGITALISIERUNG

KOPERNIKUS PROJEKTE
ENavi
Die Zukunft unserer Energie

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

IMPRESSUM

Herausgeber

IKEM – Institut für Klimaschutz, Energie und Mobilität e.V.

Magazinstraße 15 - 16

10179 Berlin

Tel: +49 (0) 30-4081870-10

Fax: +49 (0) 30-4081870-29

www.ikem.de

E-Mail: info@ikem.de

www.energiewende-navi.de

Autoren

Ass. jur. Fanny Knoll: fanny.knoll@ikem.de

Ass. jur. Denise Held: denise.held@ikem.de

Stand

Januar 2020

INHALT

Ein essenzieller Begleiter der Energiewende ist die Digitalisierung. Als Schnittstellenthematik ist sie omnipräsent bei der Gestaltung eines künftigen Stromsystems, das auf erneuerbaren Energien beruhen soll. In Zukunft müssen viele kleinere Erneuerbare-Energien-Anlagen (EE-Anlagen), Speicher und Lasten miteinander vernetzt und effizient gesteuert werden. Grundvoraussetzung dafür sind eine entsprechende digitale Infrastruktur, Technologien und Programmierungen. Die große Herausforderung besteht darin, bei einer stetigen, fortlaufenden Veränderung der Stromerzeugungs- und Stromverbrauchslandschaft, das Stromsystem stabil zu halten und die Versorgungssicherheit mit Strom zu gewährleisten. Die vielen kleinen und vornehmlich dezentralen EE-Anlagen, die vielfach nur volatil Strom erzeugen, stehen dabei im Gegensatz zu den vormals zentralen, fossilen Kraftwerken. Zudem nimmt die Zahl der am Stromsystem partizipierenden Akteure - ausgehend von den klassischen Akteuren wie Staat, Energieversorgungsunternehmen und Verbrauchern - mit Prosumern, Energiegemeinschaften und Aggregatoren sowie Plattformen ebenfalls zu. Viele Haushalte sind nicht mehr lediglich Verbraucher, sondern auch Stromproduzenten. Eine weitere strukturelle Veränderung zeigt sich im steigenden Stromverbrauch, d zukünftig die Zahl der Verbraucher steigen wird, indem beispielsweise künftig mehr Elektrofahrzeuge oder Wärmepumpen durch das Stromnetz mit Energie versorgt werden müssen. Der Digitalisierung kommt hier die Rolle der Ermöglichung zu, auf die das neue Stromsystem essenziell angewiesen ist und die es zu gestalten gilt.

Eine solch tiefgreifende Veränderung, wie die unseres Stromsystems in der Energiewende, geht auch mit grundsätzlichen Rechtsfragen, die insbesondere wichtige, gesellschaftspolitische Aspekte wie Daseinsvorsorge und Kritische Infrastrukturen betreffen, einher. Der folgende Beitrag beschäftigt sich daher im Wesentlichen mit dem Rechtsrahmen, der die Digitalisierung in der Energiewende flankieren soll. Der Beitrag wird auf Fragen im Bereich des Datenrechts (Datenschutz, Datensicherheit, Zugang zu Daten) als auch in der Kommunikation eingehen.

1 EINFÜHRUNG DIGITALISIERUNG

Zunächst gilt es der Frage nachzugehen, was eigentlich Digitalisierung im Zusammenhang mit der Energiewende konkret bedeutet. Dies ist nicht leicht zu beantworten. Eine Orientierung kann man anhand der Vorgehensweise des Bundesministeriums für Wirtschaft und Energie (BMWi) zur Begleitung des **Gesetzes zur Digitalisierung der Energiewende** (GDEW)[1] finden. Das GDEW ist im September 2016 in Kraft getreten, dessen Kern „die Einführung von Smart-Meter-Gateways nach BSI Standard (SMGW) als standardisierte Kommunikationsplattform für Energieerzeuger und -verbraucher“ ist. Das Ziel dabei ist, Deutschland als Vorreiter in Zukunftsfragen von Smart Grid und Smart Metering zu etablieren. Das Besondere an den gesetzlichen Vorgaben ist, dass ein „Privacy & IT-Security by Design“[2]-Ansatz verfolgt wird, welcher sich als ein Markenzeichen „Made in Germany“ entwickeln soll.[3]

---

[1] Gesetz zur Digitalisierung der Energiewende (GDEW) vom 29. August 2016, BGBl I Nr. 43, S. 2034.
[2] Datenschutz und IT-Sicherheit durch Technikgestaltung.
[3] *BMWi* (2017), Leistungsbeschreibung für den Dienstleistungsauftrag: „Digitalisierung der Energiewende: Barometer und Topthemen“, S. 1.

Die Begleitung des GDEW ist insgesamt auf fünf Jahre durch das BMWi ausgelegt, um die durch dieses Gesetz in Gang gesetzte Entwicklung mittels eines jährlich erscheinenden Barometers sowie drei Einzelgutachten mit jeweiligen Topthemen zu evaluieren.[4] Das erste **„Barometer Digitalisierung der Energiewende"**[5] für das Berichtsjahr 2018 ist im Januar 2019 erschienen und stellt der bisherigen Umsetzung des GDEWs ein eher durchwachsenes bis schlechtes Zeugnis aus. Der Smart-Meter-Rollout lässt aufgrund der hohen Sicherheitsvorgaben auf sich warten und die Verbraucher daher bspw. im Smart Home-Bereich auf alternative Produkte zurückgreifen, die nicht den hohen Sicherheitsstandards entsprechen.[6]

Neben diesem Barometer soll es **drei Einzelgutachten** mit jeweiligen Topthemen geben.[7] Die ersten beiden Einzelgutachten wurden im August 2019 veröffentlicht. Diese beschäftigen sich mit dem **Topthema 2** „Regulierung, Flexibilisierung und Sektorkopplung"[8], welches insbesondere auf die energiepolitischen Fragen der Netzregulierung (u.a. Anpassung der Netzentgeltsystematik, verstärkte netzseitige Nutzung von Smart Meter Gateways, auch Anforderungen an die Telekommunikationsinfrastruktur) eingeht, und dem **Topthema 3** „TK-Netzinfrastruktur und TK-Netzregulierung"[9], welches die Nutzung der Telekommunikationsinfrastruktur durch die Stromnetzbetreiber behandelt. Im noch ausstehenden **Topthema 1** wird die Entwicklung von digitalen Geschäftsmodellen im Energiebereich (u.a. variable Stromliefertarife, Energieablesung aus einer Hand) begutachtet.[10]

Aktuell beschäftigen sich sowohl der europäische als auch der deutsche Gesetzgeber intensiv mit den Themen Digitalisierung sowie Energiewende und bringen entsprechende Verordnungen, Richtlinien und Gesetze auf den Weg, um diese zu gestalten. In dem **Arbeitsprogramm der EU-Kommission für 2019** ist festgehalten, dass die Politik der Energieunion mit einer zukunftsorientierten Klimapolitik fortgesetzt werden soll.[11] Eine zentrale Rolle nimmt dabei das **Clean Energy Package** ein, das Ende 2018 / Ende 2019 angenommen wurde und acht Gesetzesakte enthält.[12] Auch im **Koalitionsvertrag** von CDU/CSU und SPD für die 19. Legislaturperiode findet sich ein Bekenntnis zu den national, europäisch und im Rahmen des Pariser Klimaabkommens vereinbarten Klimazielen für 2020, 2030 und 2050 für alle Sektoren.[13] Des Weiteren finden sich im Koalitionsvertrag weitreichende und vielfältige Ziele für den Fortschritt in der Digitalisierung[14] und in der Energiewende[15]. Die Digitalisierung im Energiesektor findet dabei ebenfalls eine konkrete Berücksichtigung.[16] Die für das Jahr 2020 gesetzten Klimaziele wurden zwar verfehlt, jedoch hat sich die Bundesregierung verpflichtet, ihren Beitrag zum europäischen Ziel, bis 2030 die CO_2-Emission um mind. 40 Prozent im Vergleich zum Referenzjahr 1990 zu verringern, zu leisten. Langfristiges Ziel ist die Treibhausgasneutralität bis zum Jahr 2050. Dies ist festgehalten u.a. in dem im

---

[4] Ebd.
[5] *Ernst & Young*, Barometer Digitalisierung der Energiewende – Ein neues Denken und Handeln für die Digitalisierung der Energiewende – Berichtsjahr 2018.
[6] Ebd., S. 7 f.
[7] *BMWi* (2017), Leistungsbeschreibung für den Dienstleistungsauftrag: „Digitalisierung der Energiewende: Barometer und Topthemen", S. 1.
[8] *Ernst & Young*, Gutachten – Digitalisierung der Energiewende – Topthema 2: Regulierung, Flexibilisierung und Sektorkopplung.
[9] *Ernst & Young*, Gutachten – Digitalisierung der Energiewende – Topthema 3: TK-Netzinfrastruktur und TK-Regulierung.
[10] *BMWi* (2017), Leistungsbeschreibung für den Dienstleistungsauftrag: „Digitalisierung der Energiewende: Barometer und Topthemen", S. 3 ff.
[11] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Arbeitsprogramm 2019 der Kommission – Versprechen einlösen und unsere Zukunft gestalten, COM(2018) 800 final, S. 4.
[12] https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans, zuletzt aufgerufen am 02.12.2019.
[13] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Ein neuer Aufbruch für Europa – Eine neue Dynamik für Deutschland – Ein neuer Zusammenhalt für unser Land, Zeile 6708 ff.
[14] Ebd., Zeile 1597 ff.
[15] Ebd., Zeile 3219 ff.
[16] Ebd., Zeile 3221 f., 3279 f., 3294 ff.

Oktober 2019 vorgestellten, sog. Klimapaket, das u.a. zahlreiche Maßnahmen zur Zielerreichung enthält.[17]

Gleichsam der grundlegenden Annahme, dass die Digitalisierung eine **breite Schnittstellenthematik** ist, gibt es auch eine **Vielzahl an Regularien in unterschiedlichen Gesetzen**. Je nach Anwendungsfall sind diverse Regularien zu berücksichtigen. Der folgende Beitrag soll einen Einblick in die verschiedenen Gesetzmäßigkeiten geben, wobei vereinzelt auch vertiefte Darstellungen erfolgen.

2 DIGITALISIERUNG UND ENEGIEWENDE

Die Digitalisierung an sich ist ein **weitreichender Begriff**, der mittlerweile die Gesellschaft, Wirtschaft sowie auch den Staat durchdringt. Entsprechend weit ist auch die hier zu betrachtende Perspektive auf den Energiesektor. Neben dem zentral diskutierten Smart-Meter-Rollout und den damit angestrebten Smart Grid werden in diesem Beitrag auch darüberhinausgehende rechtliche Rahmenbedingungen dargestellt, die bspw. ein Energieunternehmen im Allgemeinen treffen können oder bspw. für digitale Geschäftsmodelle relevant sind. Umfasst sind somit nicht nur Fragen der Digitalisierung in Bezug auf die Netzstabilität und sichere Stromversorgung, sondern auch bezüglich des Marktes im weitesten Sinne.

Im Zentrum des rechtlichen Geschehens steht – wie oben bereits angesprochen – das **Gesetz zur Digitalisierung der Energiewende** aus dem Jahr 2016, das insbesondere die Einführung eines Smart Grids regelt. Dies wurde entwickelt aus dem **Energiekonzept der Bundesregierung aus dem Jahre 2010**[18]**,** in dem die Notwendigkeit erkannt wurde, dass neben den Netzausbau auch die Netze intelligenter werden müssen – also eine Entwicklung zu einem **Smart Grid**.[19] Im Rahmen der Notwendigkeit intelligenter Netze wird ein nachfrageseitiges Lastmanagement zur stärkeren Anpassung der Energienachfrage an das Angebot durch die Bundesregierung hervorgehoben. Dies bedarf zum einem entsprechend moderner, intelligenter Netze, zum anderen ansprechende Anreize innerhalb der **Stromtarife**. Die Zukunftsvision war, dass ein Smart Grid Stromerzeuger, Speicher, Verbraucher und das Stromnetz miteinander verbindet und mit moderner Informationstechnik gesteuert werden kann. Als Grundlage dafür wurden die Einführung von intelligenten Zählern (Smart Metern) sowie die kommunikative Vernetzung und Steuerung der jeweiligen Teile des Smart Grids genannt.[20] Des Weiteren wurde ebenfalls schon mitgedacht, dass „intensive Maßnahmen“ im Bereich **Datenschutz und Datensicherheit** notwendig sind, um das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz (GG)[21]) zu gewährleisten. Diese intensiven Maßnahmen seien insbesondere gesetzlich vorzugebende Mindestanforderungen, die sich am aktuellen Stand der Technik orientieren und in Schutzprofilen und technischen Richtlinien niederzulegen seien. Damit werde insgesamt auch Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh)[22] zu ausreichender Geltung verholfen.[23]

---

[17] *BMU*, Klimaschutzprogramm 2030 der Bundesregierung zur Umsetzung des Klimaschutzplans 2050, S. 7 ff.
[18] *Bundesministerium für Wirtschaft und Technologie/Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit* (2010), Energiekonzept für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung.
[19] Ebd., S. 18 f.
[20] Ebd., S. 19.
[21] Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, BGBl. S. 1, BGBl. III/FNA 100-1, zuletzt geändert durch Art. 1 ÄndG (Art. 72, 105, 125b) vom 15.11.2019, BGBl. I S. 1546.
[22] Charta der Grundrechte der Europäischen Union vom 12. Dezember 2007, Celex-Nr. 1 2007 P/TXT.
[23] BT-Drs. 17/6072, S. 45.

Dieses Energiekonzept der Bundesregierung zusammengenommen mit der Elektrizitätsbinnenmarktrichtlinie (Richtlinie 2009/72/EG)[24] und der Gasbinnenmarktrichtlinie (Richtlinie 2009/73/EG)[25] sind die Wurzeln des GDEW.[26] Das **Messstellenbetriebsgesetz**[27], das mit dem GDEW erlassen wurde, wird als neu eingeführtes **Stammgesetz** verstanden, da es grundrechtsrelevante sowie zukunftsweisende Materien regelt und einer weiteren Zersplitterung des Energierechts vorbeugen möchte.[28]

Durch dieses Gesetz ist der **Smart-Meter-Rollout** angestoßen worden. Der grundsätzlich flächendeckende Einbau von intelligenten Messsystemen (sog. Smart Meter) soll eine Art Kommunikationsplattform im künftigen, intelligenten Stromnetz installieren, sodass Letztverbraucher, Netzbetreiber und Erzeuger Informationen zu Verbrauch und Netzzustandsdaten erhalten, sowie sichere und zuverlässige Steuerungsmaßnahmen ermöglicht werden. Mitgedacht sind dabei auch Möglichkeiten sowohl im Bereich der Steigerung der Energieeffizienz als auch bspw. variable Stromtarife. Der wesentliche Unterschied zu herkömmlichen Messystemen ist die **Plattformkompatibilität** und die Fertigung nach einem **Privacy-by-design-Standard** des Bundesamtes für Sicherheit in der Informationstechnik (BSI).[29] Ziel ist eine einheitliche Infrastruktur, die Netzbetreiber und Direktvermarktungsunternehmer eine Steuerung der Anlagen im Sinne von Systemsicherheit als auch effizienter Vermarktung ermöglicht.[30]

Das GDEW setzt einen Rechtsrahmen, um stufenweise das Energienetz zu einem intelligenten Energienetz, sog. Smart Grid, zu transformieren. Dabei soll das Smart Meter Gateway als **sichere Kommunikationsplattform, als "Herzstück",** des intelligenten Energienetzes fungieren. Die Digitalisierung als Schnittstellentechnologie ist dabei zentral für die Integration und Steuerung der dezentralen EE-Anlagen. Wesentliches Ziel der Digitalisierung ist die "Vernetzung aller Akteure der Stromversorgung im Smart Grid". Akteure sind hier Verbraucher, Erzeuger, Netzbetreiber, Aggregatoren, Direktvermarkter und Lieferanten.[31]

Dabei hat das GDEW **vier Hauptaufgaben**: (1) die Schaffung einer standardisierten, sicheren Infrastruktur, (2) die Gewährleistung von Datenschutz und Datensicherheit, (3) das Setzen von Investitionsanreizen und (4) die Gewinnung von Akzeptanz bei VerbraucherInnen.[32]

Bezüglich der **Hauptaufgabe von Datenschutz und Datensicherheit** kann man zwischen den zwei wesentlichen Interessengruppen unterscheiden – jenen, die die Daten erzeugen und jenen, die Daten benötigen. Diese Daten können zum einen essenziell für die sichere Energieversorgung und zum anderen zugleich rechtlich sensibel sein. Dies umfasst insbesondere die Energieverbrauchsdaten der VerbraucherInnen sowie die systemnotwendigen Daten über Netzzustand, Erzeugung und Verbrauch.[33] Dabei sind Datenschutz und Datensicherheit häufig die beiden Punkte, die zentral sind für die **Akzeptanz** von Digitalisierung im Allgemeinen.

Der Wunsch nach hohen Standards im Bereich des **Datenschutzes** ergibt sich aus der potenziellen, technischen Möglichkeit heraus, mittels der Auslesung von Messdaten aus den intelligenten Messsystemen Aufschluss über das Verbrauchsverhalten von Privathaushalten zu erhalten. Eine Aufschlüsselung und Auswertung des Energieverbrauchs ermöglichen Rückschlüsse auf Verhaltensweisen und Lebensgewohnheiten der jeweiligen Haushaltsbewohner. Daher müssen die intelligenten Messsystem „höchsten technischen Datenschutzanforderungen" genügen. Die Europäische Kommission hat für den Smart-Meter-Rollout ein detailliertes Datenschutzkonzept und eine sog. „data-protection-by-design"-Lösung gefordert.[34] Dies wurde vom BSI mittels Schutzprofilen und Technischen Richtlinien umgesetzt.[35] Dem

---

[24] ABl. EU 2009 L 211, 55.
[25] ABl. EU 2009 L 211, 94.
[26] BT-Drs. 18/7555, S. 62, 66.
[27] Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen vom 29. August 2016, BGBl. I S. 2034.
[28] BT-Drs. 18/7555, S. 65.
[29] BT-Drs. 18/7555, S. 1.
[30] BT-Drs. 18/7555, S. 64.
[31] *BSI/BMWi* (2019), Standardisierungstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende – Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien, S. 2.
[32] Ebd.
[33] Ebd., S. 3.
[34] Empfehlung der Europäischen Kommission, ABl. EU 2012 L 73, 9.
[35] BT-Drs. 18/7555, S. 81.

schließt sich die **Datensicherheit** an, die bezweckt, dass Daten geschützt sind vor den unbefugten Zugriff Dritter. Dabei ist auch dem Gesetzgeber bewusst, dass „auch bei sicherheitsgeprüften Anlagen nie zu 100 Prozent ein Datenleck ausgeschlossen werden kann“.[36]

3 DATEN ALS ROHSTOFF UND SENSIBLES GUT

Grundlegende Voraussetzung für die Ausschöpfung des Potenzials der Digitalisierung **sind Daten**. Auf ihnen basieren die verschiedensten Automatisierungen, Anwendungen und Dienstleistungen. Um hier einige, zum Teil sehr divers diskutierte, Möglichkeiten der Digitalisierung beispielhaft zu nennen, die den Energiesektor künftig beeinflussen können: Künstliche Intelligenz, Blockchain, Virtuelle Kraftwerke/Aggregatoren, Prosumer. Dabei sind Daten gleichzeitig „Rohstoff und ein sensibles Gut“.[37]

Eine einheitliche **Definition** von „Daten“ gibt es in der Rechtswissenschaft nicht. Zur Eingrenzung des Begriffs „Daten“ kann jedoch der abstrakten Sichtweise und Annahme gefolgt werden, dass es drei zu betrachtende Ebenen gibt. Daten betreffen als Zeichenebene die mittlere Ebene. Zu unterscheiden davon sind die zwei weiteren Bedeutungsebenen „nach oben“ und „nach unten“. Die Bedeutungsebene „nach oben“ sind Informationen; die Bedeutungsebene „nach unten“ sind Datenträger (Stoffebene).[38] Daten nehmen die Position eines grundsätzlich **schützenswerten Guts** ein. Zum einen zeichnen sich Energieverbrauchsdaten durch ihre grundrechtliche Sensibilität als datenschutzrechtlich besonders schützenswert aus. Zum anderen ergibt sich ein Schutzbedürfnis von Daten aus ihrer Systemnotwendigkeit heraus. Diese systemnotwendigen Daten sind insbesondere Daten über Netzzustand, Erzeugung und Verbrauch.[39]

Die Belange in Bezug auf Daten sind vielfältig: sie können erhoben, gesammelt, übertragen, ausgewertet und auch vermarktet werden. Was so einfach klingt, ist in der Praxis mit erheblichen Unsicherheiten in Bezug auf Zugriffs- und Verwertungsrechte sowie Fragen bezüglich Datenschutzes und Datensicherheit behaftet. Der Grundkonflikt, den auch die Gesetzgeber stets vor Augen haben, besteht zum einen aus den Interessen der Wirtschaft, die die Daten u.a. für Innovationen und diverse Geschäftsmodelle benötigen und nutzen wollen. Auf der anderen Seite stehen die Interessen der Privatpersonen und Unternehmen, die sich einen weitestgehenden Schutz ihrer Daten wünschen. Darüber hinaus ist der Schutz der Daten vor unbefugten Zugriffen Dritten essenziell für Wirtschaft als auch Privatpersonen.

Bei der Frage nach dem grundsätzlichen **rechtlichen Schutz** des schützenswerten Guts – den Daten – ist gedanklich zunächst zwischen einer rivalen und einer nicht-rivalen Nutzung des Guts zu unterschieden. Eine **rivale Nutzung** ist bekannt in Bezug zu körperlichen Gegenständen (insbes. Sacheigentum). Derjenige, der das Gut nutzen kann, schließt einen anderen von der Nutzung aus. Im Gegensatz dazu kennt die **nicht-rivale Nutzung** eine solche Beschränkung nicht. Bei solch immateriellen Gütern (bspw. geistiges Eigentum) ist grundsätzlich eine Nutzung durch mehrere Personen oder Unternehmen denkbar, ohne den jeweils anderen ausschließen zu können.[40] Die Besonderheit bei Daten ist jedoch, dass diese nicht trennscharf in ihrer Nutzung abgrenzbar sind – bei ihnen ist eine **rivale als auch eine nicht-rivale Nutzung möglich**. Daten können kopiert und vervielfältigt und anschließend parallel genutzt

---

[36] BT-Drs. 18/7555, S. 125.
[37] Vgl. Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Ein neuer Aufbruch für Europa – Eine neue Dynamik für Deutschland – Ein neuer Zusammenhalt für unser Land, Zeile 2063.
[38] *Hornung/Hofmann*, Industrie 4.0 und das Recht: drei zentrale Herausforderungen, in: Der Elektronische Rechtsverkehr Band 39 – Rechtsfragen der Industrie 4.0 – Datenhoheit – Verantwortlichkeit – rechtliche Grenzen der Vernetzung, S. 15.
[39] *BSI/BMWi* (2019), Standardisierungstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende – Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien, S. 3.
[40] *Bundeskartellamt (2017),* Big Data und Wettbewerb, Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“, S. 7 ff.

werden, was für eine nicht-rivale Nutzung spricht. Sofern die Daten bspw. auf einem Datenträger abgelegt sind, kann eine rivale Nutzung angenommen werden, da sie so gelöscht, geändert oder unzugänglich gemacht werden können.[41] Dies zeigt die rechtliche Herausforderung im praktischen, wenn es darum geht, Daten in die bisher geltende Systematik einzuordnen und rechtlich zu bewerten.

Um den Wunsch nach einer eindeutigen Regelung nachzukommen, ist viel über die Einführung eines **Dateneigentums** oder eigentumsähnlicher Rechte diskutiert worden, welches bisher de lege lata nicht existiert. Es gibt diesbezüglich eine weitreichende politische und gesellschaftliche Diskussion, ob ein solches Eigentumsrecht oder zumindest ein einheitliches Datengesetzbuch geschaffen werden sollte.[42] In der Mehrheit wird jedoch das Dateneigentum abgelehnt.[43] Insbesondere lehnt die Datenethikkommission der Bundesregierung die Einführung eines Dateneigentums sowie genereller wirtschaftlicher Verwertungsrechte an personenbezogenen Daten ab.[44]

Ganzheitlich betrachtet ergibt sich somit weder ein konsistentes Datenrecht noch ein allgemeines Recht an Daten o.ä. Vielmehr ist das Datenrecht vielschichtig aufgebaut, sodass vorliegend ein spezifischer Blick auf die relevanten Rechtsgrundlagen im Sektor Energie geworfen werden soll. Je nach Anwendungsfall ist es Aufgabe des jeweiligen Akteurs die rechtlichen Bedingungen und Voraussetzungen zu prüfen und entsprechend einzuhalten. Dies gilt für den Datenschutz, für die Datensicherheit als auch für die diversen Verwendungsmöglichkeiten von Daten.

4 DATENSCHUTZ – PERSONENBEZOGENE UND NICHT-PERSONENBEZOGENE DATEN

Ein vertiefender Blick lohnt sich zunächst in das Datenschutzrecht. Eine Definition zum Begriff Datenschutz existiert nicht. Im Allgemeinen wird darunter der Schutz des allgemeinen Persönlichkeitsrechts bzw. des Grundrechts auf informationelle Selbstbestimmung verstanden. Mit anderen Worten: Es soll Schutz vor unberechtigten Umgang Dritter mit personenbezogenen Daten gewährleistet werden.[45] Um das Bild zu komplementieren, wird die hier angestellte Betrachtung von Datenschutz weiter gefasst und auch nicht personenbezogene Daten werden in die Darstellung mit einbezogen.

Das europäische Datenschutzrecht in Bezug auf **personenbezogene Daten** hat seine Grundlage in Art. 7 und 8 Charta der Grundrechte der Europäischen Union sowie in Art. 16 Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[46] und Art. 39 EU-Vertrag (EUV)[47].[48] Im Zusammenspiel der Normen ergibt sich zum einen das Recht jeder Person auf die Achtung ihres Privat- und Familienlebens sowie ihrer Wohnung und Kommunikation, Art. 7 GRCh. Dazu kommen die grundsätzlichen Regelungen

---

[41] *Hornung/Hofmann*, Industrie 4.0 und das Recht: drei zentrale Herausforderungen, in: Der Elektronische Rechtsverkehr Band 39 – Rechtsfragen der Industrie 4.0 – Datenhoheit – Verantwortlichkeit – rechtliche Grenzen der Vernetzung, S. 16.
[42] Bspw. *BMVI* (2017), „Eigentumsordnung“ für Mobilitätsdaten? S. 129 f.
[43] U.a. *Stender-Vorwachs/Stege* (2018), Wem gehören unsere Daten? S. 1361 ff.
[44] *Datenethikkommission der Bundesregierung/Bundesministerium des Innern, für Bau und Heimat/Bundesministerium der Justiz und für Verbraucherschutz* (2019), Gutachten der Datenethikkommission der Bundesregierung, S. 18.
[45] *Mätzig/Netzband/Bruchmann*, in: Säcker, Berliner Kommentar zum Energierecht, Band 4, 4. Auflage (2017), § 19 Rn. 2.
[46] Vertrag über die Arbeitsweise der Europäischen Union idF der Bekanntmachung vom 9. Mai 2008, Celex-Nr. 1 1957 E.
[47] Vertrag über die Europäische Union idF des Vertrages von Lissabon vom 13. Dezember 2007, Celex-Nr. 1 1992 M.
[48] *Paal/Pauly*, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Einleitung, Rn. 15.

zum Schutz und Verarbeitung von personenbezogenen Daten, Art. 8 GRCh und Art. 16 AEUV. Auf nationaler Ebene spielt hier das Recht auf informationelle Selbstbestimmung, das aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), abgeleitet wird, eine Rolle.[49] Des Weiteren kommt hier für die **nicht-personenbezogenen Daten** der verfassungsrechtlich gewährte Eigentumsschutz aus Art. 14 Abs. 1 GG bezüglich von Betriebs- und Geschäftsgeheimnissen in Betracht.[50]

In der **folgenden datenschutzrechtlichen Betrachtung** wird zwischen personenbezogenen und nichtpersonenbezogenen Daten differenziert. Der Schutz von Daten gilt hier auch in Bezug auf Unternehmen mit ihren schützenswerten Betriebs- und Geschäftsgeheimnissen.[51] Im **personenbezogenen Datenschutz** spielen insbesondere die Datenschutz-Grundverordnung (DS-GVO)[52], das Bundesdatenschutzgesetz (BDSG)[53] und die Landesdatenschutzgesetze (LDSG) eine Rolle. Hinzu kommt der bereichsspezifische Datenschutz im Messstellenbetriebsgesetz (MsbG). Für den **nicht-personenbezogenen Datenschutz** sind insbesondere die Free-Flow-of-Data-Verordnung und die ePrivacy-Verordnung von Bedeutung.

4.1 Regelungssystematik von DS-GVO – BDSG – LDSG und bereichsspezifischem Datenrecht

Das Verhältnis von DS-GVO, BDSG, LDSG und dem bereichsspezifischen Datenrecht, wie bspw. aus dem MsbG, zueinander gilt es genauer zu betrachten. Grundsätzlich genießt die DS-GVO als Verordnung Anwendungsvorrang, Art. 288 Abs. 2 AEUV, vor den nationalen Gesetzen. Die DS-GVO enthält jedoch auch zahlreiche Regelungsaufträge und Öffnungsklauseln, sodass kritische Stimmen darin einen stärkeren Bezug zu einer Richtlinie anstelle einer Verordnung sehen. Soweit die DS-GVO eine solche Öffnung enthält, ist zu prüfen, ob entsprechende nationale Regelungen existieren.[54] Mit anderen Worten: das BDSG tritt zurück, sofern eine Regelung der DS-GVO unmittelbar anwendbar ist, § 1 Abs. 5 BDSG.

Auf nationaler Ebene haben Landesdatenschutzgesetze bzw. bereichsspezifisches Datenrecht, hier insbesondere das MsbG, Anwendungsvorrang vor dem BDSG, vgl. § 1 Abs. 2 S. 1 BDSG. Dabei ist insbesondere auch im bereichsspezifischen Datenrecht darauf zu achten, dass die DS-GVO grundsätzlich Anwendungsvorrang genießt.[55]

4.2 Datenschutz-Grundverordnung

Allseits bekannt ist die DS-GVO die seit dem 25. Mai 2018 gilt, siehe Art. 99 Abs. 2 DS-GVO. Die DS-GVO findet **unmittelbar Anwendung** und gilt vollumfänglich für den Energiesektor, da kein Ausschlussgrund aus Art. 2 Abs. 2 DS-GVO greift. Die DS-GVO adressiert den Schutz von natürlichen Personen bei der Verarbeitung **personenbezogener Daten** und den Verkehr solcher Daten, Art. 1 Abs. 1 DS-GVO. Augenmerk liegt hier auf der ganz oder teilweise automatisierten **Verarbeitung** personenbezogener Daten als auch auf der nichtautomatisierten Verarbeitung personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen, Art. 2 Abs. 1 DS-GVO. Nach Art. 4 Nr. 1 DS-GVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person gesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen,

---

[49] *Di Fabio*, in: Maunz/Dürig, Grundgesetzkommentar, 88. EL August 2019, GG Art. 2 Abs. 1 Rn. 173 ff.
[50] Kritisch: *Schmidt*, in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl. 2020, GG Art. 14 Rn. 6.
[51] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, S. 10.
[52] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
[53] Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. I S. 2097.
[54] *Paal/Pauly*, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Einleitung, Rn. 20 f.
[55] Ebd., Rn. 22.

wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Bei einem Verstoß gegen die DS-GVO kommen u.a. **Bußgelder** oder Schadensersatzzahlungen in Betracht, siehe Art. 77 ff. DS-GVO. Die Ahndung solcher Verstöße hat bereits zu Bußgeldern in Millionenhöhe geführt, u.a. auch in Deutschland.[56]

4.3 Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Wie bereits oben beschrieben, hat unmittelbares europäisches Recht – und somit insbes. die DS-GVO – Anwendungsvorrang, § 1 Abs. 5 BDSG. Vom Anwendungsbereich des BDSG ist die Verarbeitung personenbezogener Daten durch **öffentliche Stellen** des Bundes und der Länder sowie durch nicht-öffentliche Stellen umfasst.[57] Ein wesentlicher Unterschied von BDSG zu den Landesschutzgesetzen besteht darin, dass nur das BDSG nicht-öffentliche Stellen umfasst.[58] Der Begriff der **nicht-öffentliche Stellen** wird definiert in § 2 Abs. 4 BDSG. Demnach sind nicht-öffentliche Stellen grundsätzlich natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, § 2 Abs. 4 S. 1 Hs. 1 BDSG. Demnach unterfallen somit öffentlich-rechtliche als auch privaten Unternehmen grundsätzlich dem BDSG, insbesondere auch aus dem Energiesektor.

Landesbehörden und Gemeinden sind grundsätzlich vom BDSG umfasst, § 2 Abs. 2 BDSG, soweit nicht ein Landesdatenschutzgesetz mit spezielleren Vorschriften vorliegt oder eine Ausnahmeregelung greift, § 1 Abs. 2 BDSG. In den Anwendungsbereich der Landesdatenschutzgesetze können auch kommunale Eigenbetriebe fallen, die des Öfteren ebenfalls in der Energiewirtschaft tätig sind.[59]

4.4 Bereichsspezifischer Datenschutz - Messstellenbetriebsgesetz

Auf nationaler Ebene ergeben sich eine Vielzahl bereichsspezifischer Datenschutzregelungen, bspw. im Sozialdatenschutz, dem Datenschutz in der Steuerverwaltung, Sicherheitsrecht, etc.[60] Mit Blick auf das Datenschutzrecht im Energiesektor, ist das MsbG neben der DS-GVO das wesentliche Gesetz und enthält einen bereichsspezifischen Datenschutz für den Energiesektor. Zudem können hier noch die §§ 91 ff. Telekommunikationsgesetz (TKG)[61] genannt werden. Eingeführt wurde das MsbG durch das Artikelgesetz “Gesetz zur Digitalisierung der Energiewende”.

Das MsbG enthält Regelungen für das intelligente Stromnetz. Dort ist geregelt, wer welche Daten erheben kann und wer sie im Anschluss als berechtigte Stelle verwerten darf. In den §§ 49 bis 75 MsbG (Teil 3 – Regelungen zur Datenkommunikation in intelligenten Energienetzen) sind die **spezifischen datenschutzrechtlichen Regelungen** niedergelegt. Dass das MsbG einen abschließenden als auch datenschützenden Charakter hat, wird in § 49 Abs. 1 S. 2 MsbG klargestellt, indem eine Übermittlung, Nutzung oder Beschlagnahme der Daten nach anderen Rechtsvorschriften des Bundes oder der Länder unzulässig ist.[62] Die Datenschutzregelungen der §§ 49 ff. MsbG geht grundsätzlich anderen nationalen Datenschutzregeln vor.[63] Noch nicht abschließend geklärt ist das Verhältnis von DS-GVO und MsbG. Im Zweifel hat die DS-GVO jedoch Anwendungsvorrang.[64]

Bei einem **Verstoß gegen das MsbG** enthält § 76 Abs. 4 MsbG einen Verweis in Teil 8 des EnWG, der u.a. Bußgeldvorschriften enthält. Auf dieser Grundlage kann jedoch kein Bußgeld verhängt werden, da hier durch diesen Verweis in ein anderes Gesetz ein Verstoß gegen **Art. 103 Abs. 2 GG** (nulla poena

---

[56] Bspw. Tagesspiegel vom 5.11.2019, Deutsche Wohnen muss 14,5 Millionen Euro Strafe zahlen, https://www.tagesspiegel.de/berlin/rekordbussgeld-wegen-datenschutzverstoessen-deutsche-wohnen-muss-14-5-millionen-euro-strafe-bezahlen/25191038.html, zuletzt aufgerufen am 03.01.2020.
[57] *Gusy/Eichenhofer*, in: BeckOK Datenschutzrecht, 29. Edition 2018, BDSG § 1 Rn. 66 f.
[58] Ebd., Rn. 76.
[59] *Bartsch/Dippold*, in: vom Wege/Weise, Praxishandbuch Messstellenbetriebsgesetz, 2019, Kapitel 9 Rn. 4.
[60] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Einleitung, Rn. 303.
[61] Telekommunikationsgesetz (TKG) vom 22. Juni 2004, BGBl I Nr. 29, S. 1190.
[62] BT-Drs. 18/7555, S. 105.
[63] *Bartsch/Dippold*, in: vom Wege/Weise, Praxishandbuch Messstellenbetriebsgesetz, 2019, Kapitel 9 Rn. 29 ff.
[64] U.a. ebd., Rn. 32 ff.

sine lege-Grundsatz) vorliegt.[65] Dieser, in der Verfassung niedergelegte, Grundsatz enthält die Regel der Strafandrohungsbestimmtheit. Danach muss ein strafbares Verhalten und dessen mögliche Strafe in einem Gesetz geregelt sein.[66]

4.5 Informatorische Entflechtungsvorgaben nach § 6a EnWG[67]

Ein für den Energiesektor ebenso zu berücksichtigende und sektorspezifische Regelung ist die informatorische Entflechtung nach § 6a EnWG. Nach Abs. 1 haben vertikal integrierte Energieversorgungsunternehmen, Transportnetzeigentümer, Netzbetreiber, Speicheranlagenbetrieber sowie Betreiber von LNG-Anlagen dafür Sorge zu tragen, dass **wirtschaftlich sensible Informationen**, von denen sie innerhalb ihrer Tätigkeit Kenntnis erhalten, vertraulich behandelt werden. Umfasst sind dabei insbesondere personenbezogene Daten sowie Daten, die Betriebs- oder Geschäftsgeheimnisse enthalten.[68] In § 6a Abs. 2 S. 1 EnWG ist zudem festgehalten, dass die genannten Akteure, sofern sie Informationen veröffentlichen, die wirtschaftliche Vorteile bringen können, diese auf **nicht-diskriminierende Weise veröffentlichen**. Satz 2 der Norm statuiert, dass wirtschaftlich sensible Informationen gegenüber anderen Teilen des Unternehmens vertraulich behandelt werden müssen. Informationen aus dem Netzbereich sind daher grundsätzlich nicht an andere Unternehmensteile weiterzuleiten.[69]

Kleinere vertikal integrierte EVUs sind nach §§ 7, 7a EnWG (De-minimis-Regelung) von der rechtlichen und operationellen Entflechtung ausgenommen. Diese Ausnahmeregelung gilt jedoch nicht für die informationelle Entflechtung. Somit haben unabhängig von ihrer Größe die vertikal integrierten Energieversorgungsunternehmen die informationelle Entflechtung durch angemessene Maßnahmen sicherzustellen. Und wenn es anders nicht möglich ist, sind operationelle Maßnahmen zu ergreifen, z.B. verbindliche Verhaltensvorgaben für Mitarbeiter sowie eine aussagekräftige Dokumentation der Geschäfte.[70]

4.6 Schutz von nicht-personenbezogenen Daten auf nationaler Ebene

Zu nennende Gesetze, die den Schutz von nicht-personenbezogenen Daten im weitesten Sinne bezwecken, sind das Geschäftsgeheimnisgesetz (GeschGehG)[71] und das Unlauterer Wettbewerb-Gesetz (UWG)[72]. Des Weiteren kann hier der Schutz von geistigem Eigentum nach dem Urheber-, Marken- und Patentrecht bspw. für Datenbankwerke oder Computerprogramme von Bedeutung sein. Auch ist zivilrechtlicher Deliktsschutz nach §§ 823 ff. BGB[73] denkbar sowie ein strafrechtlicher Schutz nach §§ 202a, 303a Strafgesetzbuch (StGB)[74].[75] In einem noch weiteren Sinne sind auch wettbewerbsrechtliche Regelungen im Zusammenhang mit Daten mitzudenken. Denkbar ist hier ein unlauteres Handeln nach § 3a UWG oder Marktmissbrauch nach § 19 Gesetz gegen Wettbewerbsbeschränkungen (GWB)[76].[77]

---

[65] Danner/Theobald/Dix, 101. EL Mai 2019, MsbG § 76 Rn. 16.
[66] *Radtke/Hagemeier*, in: BeckOK Grundgesetz, 41. Edition 2019, GG Art. 103 Rn. 18, 23.
[67] Gesetz über die Elektrizitäts- und Gasversorgung vom 7. Juli 2005, BGBl. I S. 1970, ber. S. 3621.
[68] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, S. 85.
[69] Ebd., S. 86.
[70] BT-Drs. 15/3917, S. 55; *Säcker/Schönborn*, in: Berliner Kommentar, Band 1 Halbband 1 EnWG, 4. Auflage 2019, § 6a EnWG, Rn. 45 f.
[71] Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) vom 18. April 2019, BGBl. I S. 466.
[72] Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010, BGBl. I S.254, das zuletzt durch Artikel 5 des Gesetzes vom 18. April 2019, BGBl. I S. 466, geändert worden ist.
[73] Bürgerliches Gesetzbuch idF der Bekanntmachung vom 2. Januar 2002, BGBl. I S. 42, ber. S. 2909 und 2003 I S. 738.
[74] Strafgesetzbuch idF der Bekanntmachung vom 13. November 1998, BGBl. I S. 3322.
[75] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, S. 15 ff.
[76] Bekanntmachung der Neufassung des Gesetzes gegen Wettbewerbsbeschränkungen vom 26. Juni 2013, BGBl I Nr. 32, S. 1750.
[77] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, S. 19 ff.

4.7 Free flow of data-Verordnung

Ebenso gibt es einen **Schutz nicht-personenbezogener Daten auf europäischer Ebene**. Die Free flow of data-Verordnung (FFoD)[78] von November 2018 hat zum Ziel, den **freien Datenverkehr von elektronischen, nicht-personenbezogenen Daten** innerhalb der EU zu gewährleisten, vgl. Art. 1 Hs. 1 und Art. 2 Abs. 1 Hs. 1 FFoD. Da sie - im Gegensatz zur DS-GVO - nicht-personenbezogene Daten adressiert ist die FFoD eine **Ergänzung zur DS-GVO**. Die FFoD zielt auf den Abbau von Datenlokalisierungsauflagen. Datenlokalisierungsauflagen verpflichten bisher zur Verarbeitung nicht-personenbezogener Daten im Inland, was die Nutzung ausländischer Clouddienste verhindert hat.[79] Von der FFoD adressiert sind insbesondere Dienstleistungen (u.a. Datenverarbeitungsdienste) für Nutzer, die in der EU wohnhaft oder niedergelassen sind, Art. 1 lit. a) FFoD.[80]

4.8 ePrivacy-Verordnung

Des Weiteren gibt es noch auf europäischer Ebene die noch zu erlassene ePrivacy-Verordnung. Diese soll die ePrivacy-Richtlinie[81] aus dem Jahr 2002 einschließlich deren letzter Änderung durch die sog. Cookie-Richtlinie[82] aus dem Jahr 2009 ersetzen. Die neue Verordnung soll ebenfalls eine **Ergänzung zur DS-GVO** sein, indem sie Daten im Rahmen von Telekommunikationsdiensten regeln soll und neben natürlichen Personen **auch juristische Personen mithin somit Unternehmen** - und somit weiter als die DS-GVO ist - schützt.[83] Geplant war ein zeitgleiches Inkraftreten mit der DS-GVO im Mai 2018[84], jedoch konnte bisher keine Einigung erzielt werden. Im Oktober 2019 wurde unter der finnischen Ratspräsidentschaft ein aktualisierter Entwurf zur neuen ePrivacy-Verordnung[85] veröffentlicht, zu dem weiter beraten wird. Im Dezember 2019 war in den Medien zu lesen, dass eventuell eine gänzlich revidierte Fassung erstellt werden soll.[86] Weitere Entwicklungen bleiben abzuwarten.

5 DATENSICHERHEIT

Eine Begrifflichkeit, die im Rahmen der Digitalisierung stetig diskutiert wird, ist die Datensicherheit. Im Allgemeinen versteht man unter Datensicherheit die Sicherstellung von Vertraulichkeit[87], Verfügbarkeit[88]

---

[78] Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl. Nr. L 303, 59 ff.
[79] *BMWi* (2019), Schlaglichter der Wirtschaftspolitik, Monatsbericht März 2019, Aktuelle Entwicklungen in der europäischen Datenwirtschaft, S. 33 f.
[80] Erwägungsgrund Nr. 15, Art. 1 Abs. 1 Verordnung (EU) 2018/1807.
[81] Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre RL 2002/58/EG, ABl. 2002 L 201, 37.
[82] Richtlinie zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, RL 2009/136/EG, ABl. 2009 L 337, 11.
[83] *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 36 Datenschutz im Internet, Rn. 24.
[84] Ebd., Rn. 27.
[85] Entwurf zur geplanten Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der RL 2002/58/EG, Verfahren 2017/0003(COD).
[86] https://www.spiegel.de/netzwelt/netzpolitik/eprivacy-verordnung-eu-kommission-will-neuen-vorschlag-machen-a-1299506.html, zuletzt aufgerufen am 12.12.2019.
[87] Nur Befugte besitzen die Daten und können sie zur Kenntnis nehmen.
[88] Befugte können jederzeit auf die Daten zugreifen und die Funktionalität des IT-Systems wird nicht beeinträchtigt, bspw. durch Datensicherung/back-ups.

und Integrität[89] aller verarbeiteten Daten mittels aller notwendigen organisatorischen und technischen Maßnahmen (sog. TOMs).[90]

Um sich der gesellschaftlichen sowie wirtschaftlichen Bedeutung des Themas IT-Sicherheit bewusst zu werden, lohnt sich ein Blick in den „IT-Sicherheitsbericht 2019“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[91]. Zur Cybersicherheitslage 2019 wird u.a. aufgeführt, dass 114 Millionen neue Schadprogramm-Varianten im Umlauf sind und es täglich bis zu 110.000 Botinfektionen in deutschen Systemen kommt. Ein Unternehmen erlitt durch einen Ransomware-Angriff einen Schaden in Höhe von 40 mio. Euro.[92] Weiter wurden ca. 770.000 Mails mit Schadsoftware, versendet an deutsche Regierungsnetze, abgefangen. Zudem hat das BSI 11,5 Millionen Meldungen zu Schadprogramm-Infektionen an deutsche Netzbetreiber übermittelt.[93]

Ein besonderer Blick lohnt sich hier auf die Kritischen Infrastrukturen (KRITIS), zu denen auch die Energieversorgung gehört. Unter Kritischer Infrastruktur werden im Allgemeinen Strukturen oder Anlagen verstanden, deren Ausfall zu einer Versorgungskrise führen könne, die nicht ohne Weiteres behoben werden kann. Im Jahr 2019 waren 1.500 Anlagen als KRITIS-Anlagen registriert. Im Jahr 2018 wurden dem BSI 145 Meldungen bezüglich Angriffen gemacht, ein Jahr später sind es bereits 252.[94] Das BSI gibt für 2019 an, dass die Gefährdungslage für KRITIS sich weiterhin auf hohem Niveau befinde, es jedoch keine konkreten Gefährdungen, die direkt auf KRITIS abzielen würden, gebe.[95]

Dies macht deutlich, dass digitalisierte Systeme, die insbesondere wie die Energie auch essenziell die Bereiche der Daseinsvorsorge betreffen, geschützt werden müssen. Mit Bezug auf die Digitalisierung der Energiewende und den damit einhergehenden Smart-Meter-Rollout haben daher das BMWi und das BSI gemeinsam im Januar 2019 die „Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende“[96] veröffentlicht. Das Kompendium soll helfen, den wachsenden Anforderungen von Energiewende und Cybersicherheit gerecht zu werden. Es enthält einen Arbeitsplan zur Fortentwicklung des Smart Meter Gateways hin zu der angestrebten Kommunikationsplattform.[97]

Bezüglich der Frage nach den technischen Mindestanforderungen hat der Gesetzgeber in die Gesetzesbegründung zum Gesetz der Digitalisierung der Energiewende hineingeschrieben, dass zwei Ziele verfolgt werden. Zum einen sollen die intelligenten Messsysteme vielseitig einsetzbar sein, um den gesamtwirtschaftlichen Nutzen entfalten zu können und zum anderen Datenschutz und Datensicherheit zu gewährleisten.[98]

5.1 NIS-Richtlinie und IT-Sicherheitsgesetz

Bei dem in Europa existierenden Stromnetz handelt es sich um ein sogenanntes Verbundnetz. Die Stromnetze sind auf Höchst- und Hochspannungsebene verbunden. Durch den transnationalen Bezug ist der europäische Gesetzgeber gefordert, für ausreichenden Schutz dieser essenziellen Infrastruktur zu sorgen. Um den Gefahren, die mit einer zunehmenden Digitalisierung einhergehen, zu begegnen, verfolgt die EU daher eine **EU-Cybersicherheitsstrategie**[99]**,** die insbesondere auch den Energiesektor miteinschließt. Auf Grundlage dieser Strategie wurde die **Richtlinie für Netz- und**

---

[89] Die Daten liegen inhaltlich korrekt vor, stammen vom angegebenen Urheber und können nur von Befugten in zulässiger Weise modifiziert werden.
[90] *Kramer/Meints*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 49. EL Juli 2019, Teil 16.5 Datensicherheit, Rn. 3.
[91] BSI (2019), Die Lage der IT-Sicherheit in Deutschland 2019.
[92] Ebd., S. 34.
[93] Ebd., S. 35.
[94] Ebd., S. 35.
[95] Ebd., S. 46.
[96] BSI/Bundesministerium für Wirtschaft und Energie (2019), Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende – Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien.
[97] BSI (2019), Die Lage der IT-Sicherheit in Deutschland 2019, S. 54.
[98] BT-Drs. 18/7555, S. 63.
[99] *Europäische Kommission* (2013), Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN(2013) 1 final.

Informationssicherheit (NIS-Richtlinie)[100] erlassen. Ausdrückliches Ziel dieser Richtlinie ist es, ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union zu erreichen, „um so das Funktionieren des Binnenmarktes zu verbessern."[101] Dazu gehört bspw. die Pflicht aller Mitgliedstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen, Art. 1 Abs. 2 lit. a) NIS-Richtlinie. Ein weiterer Eckpfeiler der Richtlinie ist „die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen", Art. 1 Abs. 2 lit. b) NIS-Richtlinie. Insgesamt lässt sich dadurch der Wille des EU-Gesetzgebers zu mehr Sicherheit und Kooperation innerhalb der Mitgliedstaaten und untereinander erkennen. Damit kommt der EU-Gesetzgeber auch dem gestiegenen, transnationalen Sicherheitsbedürfnis nach.

Die NIS-Richtlinie wurde bereits 2017 in nationales Recht umgesetzt.[102] Zuvor war in Deutschland im Jahr 2015 das IT-Sicherheitsgesetz[103] erlassen worden, sodass es lediglich weniger Anpassungen im nationalen Recht bedurfte.[104] In Arbeit ist noch das sog. IT-Sicherheitsgesetz 2.0 beim Bundesministerium des Innern, für Bau und Heimat (BMI). Der Entwurf enthält Vorgaben zur Befugniserweiterung des BSI, eine Anhebung der allgemeinen Sicherheitsstandards sowie eine Ausweitung der Kritischen Infrastrukturen. Der Entwurf ist stark umstritten und wird derzeit überarbeitet. Es bleibt daher den konkreten Gesetzeserlass abzuwarten.

5.2 Cybersecurity-Verordnung

Ein weiterer Schritt hin zu mehr IT-Sicherheit auf Ebene der EU ist das Inkrafttreten des Rechtsakt zur Cybersicherheit (Cybersecurity-Verordnung)[105] im Juni 2019.

Die festgelegten Ziele dieser Verordnung sind (1) die Gewährleistung eines ordnungsgemäß funktionierenden Binnenmarkts und (2) ein hohes, unionweites Cybersicherheitsniveau zu erreichen, um Cyberangriffe abwehren zu können und das Vertrauen in die Cybersicherheit zu stärken, Art. 1 Hs. 1 Cybersecurity-Verordnung. Der EU-Gesetzgeber möchte dies erreichen, indem eine neue "Agentur der Europäischen Union für Cybersicherheit" (ENISA) eingerichtet und ein europäisches Schemata für eine Cybersicherheitszertifizierung erstellt wird, die für IKT-Produkte und -dienste sowie -prozesse ein angemessenes Maß an Cybersicherheit gewährleisten soll, Art. 1 Abs. 1 lit. a), b) Cybersecurity-Verordnung. Kritisch ist hier anzumerken, dass die Cybersicherheitszertifizierung bisher auf Freiwilligenbasis ausgestaltet ist, vgl. Art. 56 Abs. 2 Cybersecurity-Verordnung. Es gibt jedoch Stimmen, die zumindest für die kritischen Bereiche eine verpflichtende Zertifizierung fordern.[106] Ein Vergleich lohnt sich an dieser Stelle zum verzögerten Smart-Meter-Rollout. Gedacht ist das Smart Meter Gateway als sichere Kommunikationsplattform insbesondere auch für Smart-Home und Smart Building-Anwendungen sowie für Smart Mobility und Smart Grid. Aufgrund der Verzögerung des Rollouts werden am Markt zahlreiche Alternativtechnologien vertrieben, die nicht den hohen gesetzlichen Standards bezüglich Datenschutz und

---

[100] Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194, 1 ff.
[101] Erwägungsgrund Nr. 74 und Art. 1 Abs. 1 NIS-Richtlinie.
[102] Siehe Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017, BGBl. I S. 1885.
[103] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. I S. 1324.
[104] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/01/nis-umsetzungsgesetz.html, zuletzt aufgerufen am 20.11.2019.
[105] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013, ABl. L 151, 15 ff.
[106] *Kipker/Scholz*, MMR-Aktuell 2019, 414986, EU-Parlament verabschiedet EU Cybersecuritiy Act.

Datensicherheit entsprechen.[107] Diese Alternativtechnologien sind somit im Energiesystem etabliert und potenziell leichter angreifbar.

5.3 Sonstige Vorschriften

Des Weiteren gibt es in den einzelnen Verordnungen oder Gesetzen spezielle Vorschriften, die IT-Sicherheit gewährleisten sollen. In **Art. 32 DS-GVO** wird der Rahmen für die Sicherheit der Verarbeitung der personenbezogenen Daten gesetzt. Dadurch sollen personenbezogene Daten und deren Verarbeitungssysteme vor Angriffen, vor einem Ausfall oder einer Beeinträchtigung der Zuverlässigkeit der Systeme. Der Schwerpunkt liegt bei geeigneten technischen und organisatorischen Maßnahmen (sog. TOMs), die nach der DS-GVO Verantwortliche und der Auftragsverarbeiter vornehmen müssen.[108]

Eine weitere spezielle Regelung findet sich in **§ 22 BDSG**, der die Erhebung von sensiblen Daten ermöglicht. Beispielsweise können öffentliche Stellen unter Abwägung mit den Interessen der betroffenen Person sensible Daten erheben, wenn dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder bei zwingender Erforderlichkeit zur Wahrung des Gemeinwohls, § 22 I Nr. 2 lit. a) und b) BDSG.

Auch im MsbG finden sich in Teil 2 Kapitel 3, **§§ 19 ff. MsbG**, „Technische Vorgaben zur Gewährleistung von Datenschutz und Datensicherheit beim Einsatz von Smart Meter Gateways“. Besondere Vorschriften gelten zudem für den Bereich **Kritischer Infrastrukturen**. Für die Kritischen Infrastrukturen im Sektor Energie gilt das BSI-Gesetz mit der BSI-KritisV sowie § 11 EnWG.

6 DATENZUGANG UND WEITERVERWENDUNG VON DATEN

Bisher wurde beschrieben, welcher Schutz den Daten rechtlich angediehen und wie ihre Sicherheit gewährleistet wird. Dies schränkt die potenzielle Nutzung von Daten zwar ein, ergibt jedoch kein originäres Zugangsrecht zu Daten. Zunächst bleibt festzuhalten, dass weder auf europäischer Ebene noch auf nationaler Ebene ein eigenständiges Eigentums- oder Immaterialgüterrecht bezüglich Daten besteht.[109] Daher wird in den verschiedenen Diskussionen der Ansatz vertreten, dass vorzugsweise nicht die Zuordnung der Daten zu regeln sei, sondern der Zugang zu den Daten.[110] Mit anderen Worten: **Zugang statt Eigentum**.

Die rechtswissenschaftliche Diskussion, inwiefern ein Datenzugang gewährt werden soll und wie insbesondere nicht-personenbezogene Daten reglementiert werden sollen, ist bereits in vollem Gange. Einzelne zugleich auch vielfältige Tendenzen sind erkennbar, jedoch gibt es noch keine abschließende Bewertung oder konkrete gesetzgeberische Initiative. Somit soll und kann im Folgenden nur auf bereits bestehende Regelungen eingegangen werden und Einblicke in vorhandene sowie relevante Zugangs- und Weiterverwendungsregelungen im Energiesektor gegeben werden.

---

[107] *Ernst & Young*, Barometer Digitalisierung der Energiewende – Ein neues Denken und Handeln für die Digitalisierung der Energiewende – Berichtsjahr 2018, S. 8, 13.
[108] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, DSGVO Art. 32 – Sicherheit der Verarbeitung, Rn. 1.
[109] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, S. 18.
[110] *Czychowski/Siesmayer*, in: Kilian/Heussen, Computerrechts-Handbuch, 34. EL Mai 2018, 20.5 Rechte an Daten, Rn. 43.

Von den Zugangsregelungen sind **Weiterverwendungsregelungen** abzugrenzen. Das Informationsweiterverwendungsgesetz (IWG)[111] regelt die Weiterverwendung von bei öffentlichen Stellen vorhandenen Informationen, insbesondere zur Bereitstellung von Produkten und Dienstleistungen der digitalen Wirtschaft, § 1 Abs. 1 IWG. Zugleich wird jedoch ein Anspruch zu Zugang von Informationen ausgeschlossen, § 1 Abs. 2a IWG. Ebenso gibt es eine Regelung in § 5 UrhG, dass Gesetze, Verordnungen, etc. frei verwendet werden können; gleichwohl enthält das Gesetz ebenfalls keine originäre Zugangsregelung.

Sehr spezifische und **eng umgrenzte Zugangsregelungen** finden sich bspw. in § 33g GWB, § 60d UrhG oder § 55a UrhG. Abgesehen davon kommen noch vertragliche Abreden in Betracht gemäß dem Grundsatze der Vertragsfreiheit kann jeder mit jedem über den Zugang zu Daten grundsätzlich einen **Vertrag schließen** und dessen Inhalt – und somit die Konditionen – bestimmen.[112] Im Folgenden soll noch vereinzelt auf die für den Energiesektor relevanten, teilweise spezifischen Regelungen genauer eingegangen werden.

6.1 PSI-Richtlinie ("Open Data-Richtlinie")

In der Gesellschaft und Politik stark und kontrovers diskutiert wird die Idee von **Open Data** (offene Daten). Dieses Konzept umfasst Daten „in einem offenen Format, die von allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können."[113] Einen großen Schritt diesbezüglich hat der europäische Gesetzgeber im Juni 2019 mit der novellierten Public Sector Information-Richtlinie (PSI-Richtlinie bzw. sogenannte Open Data-Richtlinie)[114] gemacht. Die vormalige PSI-Richtlinie[115] aus dem Jahr 2013 war von dem deutschen Gesetzgeber durch das IWG in das deutsche Recht umgesetzt worden. Die Novelle soll „der Ausschöpfung des Potenzials der Informationen des öffentlichen Sektors für die europäische Wirtschaft und Gesellschaft dienen". Dazu gehört u.a. „die Bereitstellung eines Echt-Zeitzugangs zu dynamischen Daten (…), die verstärkte Bereitstellung wertvoller öffentlicher Daten für die Weiterverwendung, unter anderem von öffentlichen Unternehmen, Forschungseinrichtungen und Forschungsfördereinrichtungen."[116]

Eine wichtige Neuerung ist, dass nicht nur der Staat, sondern auch **öffentlich-rechtliche Unternehmen** von dieser Richtlinie adressiert werden.[117] Von Seiten der öffentlich-rechtlichen Unternehmen wird eine Wettbewerbsverzerrung befürchtet, da private Unternehmen die zu veröffentlichenden Daten nutzen können, sie ihrerseits jedoch noch nicht zur Herausgabe dieser Daten verpflichtet sind.[118] Die Diskussion konzentriert sich insbesondere auf die **Kategorien der hochwertigen Datensätze**. Diese sollen grundsätzlich kostenlos verfügbar, maschinenlesbar, über ein API[119] verfügbar und gegebenenfalls als Massendownload verfügbar sein, Art. 14 Abs. 1 S. 2 PSI-Richtlinie. Mittels eines sekundären Durchführungsrechtsaktes kann die EU-Kommission eine Liste bestimmter im Besitz öffentlicher Stellen oder öffentlicher Unternehmen befindlicher hochwertiger Datensätze festlegen, Art. 14 Abs. 1 S. 1 PSI-Richtlinie. Die thematischen Kategorien diesbezüglich ergeben sich aus dem Anhang I der PSI-Richtlinie und umfassen Georaum, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Unternehmen und Eigentümerschaft von Unternehmen sowie Mobilität.

---

[111] Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz – IWG) vom 13. Dezember 2006, BGBl. I Nr. 60, S. 2913.
[112] *Czychowski/Siesmayer*, in: Kilian/Heussen, Computerrechts-Handbuch, 34. EL Mai 2018, 20.5 Rechte an Daten, Rn. 44 ff.
[113] Erwägungsgrund Nr. 16 S. 1 Open-Data-Richtlinie.
[114] Richtlinie (EU) 2019/1024 des europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors.
[115] Richtlinie 2013/37/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors.
[116] Erwägungsgrund Nr. 4 PSI-Richtlinie.
[117] Art. 1 Abs. 1 b) und Art. 2 Nr. 3 PSI-Richtlinie.
[118] *Verband Kommunaler Unternehmen e.V.* (2019), Umsetzung der PSI-Richtlinie – Wettbewerbsfähigkeit öffentlicher Unternehmen sichern, S. 1 f.
[119] Ein API ist eine Anwendungsprogrammierschnittstelle, über die bspw. dynamische Daten unmittelbar nach ihrer Erhebung zur Verfügung gestellt werden können, vgl. Erwägungsgrund Nr. 31 S. 7 PSI-Richtlinie.

In der Richtlinie sind auch einige **Ausschlusskriterien** enthalten; beispielsweise sind Dokumente, die sensible Daten zum Schutz der nationalen Sicherheit, der statistischen Geheimhaltung sowie Geschäftsgeheimnisse inklusive Betriebs-, Berufs- und Unternehmensgeheimnissen enthalten, Art. 1 Abs. 2 lit. d) PSI-Richtlinie, ausgenommen. Die Bundesregierung ist bisher der Ansicht, dass die Interessen der öffentlich-rechtlichen Unternehmen ausreichend gewahrt seien.[120] Es bleibt daher abzuwarten, wie der deutsche Gesetzgeber die PSI-Richtlinie umsetzt. Ebenso bleibt abzuwarten, ob und wie die EU-Kommission Festlegungen im Bereich der hochwertigen Datensätze treffen wird.

6.2 Energieinformationsnetz

Die gesetzliche Regelung zum **Energieinformationsnetz** befindet sich insbesondere in § 12 Abs. 4 EnWG. Darin ist festgehalten, dass juristische als auch natürliche Personen den Betreibern von Elektrizitätsversorgungsnetzen unverzüglich Informationen (einschließlich Betriebs- und Geschäftsgeheimnisse) bereitstellen müssen, die notwendig sind, um die Elektrizitätsversorgungsnetze sicher und zuverlässig zu betreiben, zu warten und auszubauen. Zu den Daten gehören insbesondere Stammdaten, Planungsdaten und Echtzeitdaten. Der Informationsanspruch der Netzbetreiber richtet sich dabei gegen: Betreiber von Erzeugungsanlagen, Betreiber von Anlagen zur Speicherung elektrischer Energie, Betreiber von Elektrizitätsverteilernetzen, Betreiber von Gasversorgungsnetzen, industrielle und gewerbliche Letztverbraucher, Anbieter von Lastmanagement und Großhändler bzw. Lieferanten von Elektrizität.

Die Installation eines Energieinformationsnetzes wurde initiiert durch die Novellierung des EnWG im Jahre 2011. Informationen sind für den sicheren Betrieb der Netze wichtig, insbesondere da die Einspeisung dezentraler und volatiler wird sowie die zunehmende räumliche Entfernung von Einspeisungen und Verbrauch.[121] Die Begrifflichkeit des Energieinformationsnetzes verspricht dem geneigten Leser beim ersten Lesen einen umfassenden Zugang zu sämtlichen Informationen, die für den Betrieb eines Stromnetzes essentiell sind. Dies bedarf im Folgenden einer genaueren Betrachtung.

Die Gesetzesnovelle diente vorrangig der Umsetzung des sog. Dritten Binnenmarktpakets Energie in nationales Recht. Dieses Paket hat den EU-Strom- und Gasbinnenmarkt grundlegend verändert.[122] In Abs. 4 des § 12 EnWG sind die Rahmenbedingungen für das Energieinformationsnetz festgelegt. Mit dem Strommarkgesetz wurden diese Rahmenbedingungen noch weiter durch die Absätze 4 bis 7 konkretisiert.[123]

Die Gesetzesnovelle des EnWG 2011 enthält noch weitere, wichtige Aspekte. Grundlegend dafür ist das von der Bundesregierung im September 2010 beschlossene Energiekonzept.[124] Der anschließende Gesetzesentwurf führt in seiner Begründung aus, dass eine erste Umsetzungsmaßnahme dieses Energiekonzepts die Neuausrichtung des Zähl- und Messwesens sei. Dazu gehören die Implementierung von Datenschutz und Datensicherheit im Bereich des Smart Metering, die bessere Integration von zu- und abschaltbaren Lasten und die Einführung von Steuerungselementen für intelligente Netze („Smart Grids“).[125]

An dieser Stelle bleibt somit festzuhalten, dass das Energieinformationsnetz mit der Begrifflichkeit des Smart Grid divergiert. Ein „intelligentes Netz“ (Smart Grid) „bezeichnet ein modernisiertes Energienetz, das um einen digitalen bidirektionalen Kommunikationskanal zwischen dem Versorgungsunternehmen und dem Verbraucher sowie um intelligente Mess-, Überwachungs- und Steuerungssysteme erweitert wurde“.[126] Das Smart Grid bezeichnet daher im Grundsätzlichen die Kommunikation zwischen Verbraucher und Energieversorgungsunternehmen (EVU) sowie die digitale Infrastruktur, die dem intelligenten Netz zugrunde liegt. Ein anderes Ziel hat der Gesetzgeber mit der Einführung des

---

[120] BT-Drs. 19/7498, S. 2, 5.
[121] *Brucker/Günther*, in: Elspas/Graßmann/Rasbach (Hrsg.), 2018, EnWG, § 12 Rn. 1.
[122] BT-Drs. 17/6072, S. 45.
[123] *Brucker/Günther*, in: Elspas/Graßmann/Rasbach (Hrsg.), 2018, EnWG, § 12 Rn. 1.
[124] *Bundesministerium für Wirtschaft und Technologie, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit* (2010), Energiekonzept – für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung.
[125] BT-Drs. 17/6072, S. 45.
[126] Empfehlung der Kommission vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme, ABl. EU 2012 L 73, 9.

Energieinformationsnetzes verfolgt; nämlich die Gewährleistung einer **umfassenden Informationsbereitstellung** sämtlicher benötigten Informationen und unter Bezugnahme der wesentlichen Marktakteure.[127]

Den **Informationsanspruch** haben die Betreiber von Elektrizitätsversorgungsnetzen. Die Informationen helfen den Netzbetreibern, die Sicherheit und Zuverlässigkeit des jeweiligen Netzes umfassend und zuverlässig zu beurteilen.[128] Insbesondere sollen drei Datenkategorien zur Verfügung gestellt werden: **Stammdaten, Planungsdaten und Echtzeitdaten**. Weitere Datenkategorien sind denkbar, sofern sie dem Zweck des sicheren und zuverlässigen Netzbetriebs (§ 12 Abs. 4 S. 1 EnWG) dienen. Stammdaten sind Daten, die im Wesentlichen unverändert bleiben, wie bspw. Name des Marktakteurs, Zuordnung der Anlage zum jeweiligen Netz, Anlagengröße und -leistung, Angaben zur Fernsteuerbarkeit. Planungsdaten sind in die Zukunft gerichtete Daten und geben an, wieviel Energie ein Kraftwerk erzeugen kann oder wieviel Energie ein Großkunde beziehen wird. Echtzeitdaten geben in „Echtzeit" Auskunft über Ist-Einspeisung und Ist-Verbrauch („Real-Time-Leistungswerte").[129]

Weiter wird auch klargestellt, dass der Informationsanspruch sich nicht auf die vorzunehmende **Leistungsbilanzierung** erschöpft. Vielmehr sollen die Informationen auch die zunehmend komplexeren **Netzsteuerung** ermöglichen. Durch die Gesetzgebung soll berücksichtigt werden, dass eine solche Netzsteuerung nur möglich ist, wenn die aktuellen und erwarteten **Einspeise-, Verbrauchs- und Zustandsdaten** zur Verfügung stehen. Aus diesen Gründen richtet sich der Auskunftsanspruch gegen jene Akteure, auf deren Daten und Informationen es im Wesentlichen ankommt: (1) Verteilnetzbetreiber und Lieferanten über den Zustand und die Belastung der unteren Netzebenen, (2) gewerbliche und industrielle Letztverbraucher, die Strom in relevanten Mengen entnehmen und (3) Einspeiseanlagen mit einer gewissen installierten Einzel- oder Gesamt-Einspeiseleistung am Netzanschlusspunkt. Bei der Abfrage der Daten ist grundsätzlich die Verhältnismäßigkeit, insbes. die Kosten für die Auskunftsverpflichteten, zu berücksichtigen. Dies sei insgesamt geeignet, ein „Energieinformationsnetz zu installieren".[130]

So weit die Informationsanspruchsberechtigung von § 12 Abs. 4 EnWG gefasst zu sein scheint, so relativiert sich diese bei genauerer Betrachtung. Der Gesetzgeber hat den potenziellen Anwendungsbereich weit gefasst, um der Bundesnetzagentur die Möglichkeit zu geben, praxisnahe, konkretisierende Beschlüsse zu fassen, § 12 Abs. 6 EnWG. Über diese Beschlüsse wird potenziell der Anwendungsbereich wieder beschränkt. Durch den ersten Beschluss der Bundesnetzagentur (Stufe 1 von geplanten 5 Stufen) sind zurzeit lediglich Betreiber von Erzeugungsanlagen mit einer Nettoleistung von mindestens 10 MW, welche an die 110-kV- oder höhere Spannungsebene angeschlossen sind, informationspflichtig. Erst mit einer weiteren Beschlussfassung wird der Kreis der Informationspflichtigen erweitert.[131] Somit müssen weitere Beschlussfassungen durch die Bundesnetzagentur abgewartet werden.

6.3 Neuerscheinung: Plattformen als Intermediäre

Eine Erscheinungsform der Digitalisierung, die Datenzugangsfragen aufwirft und die auch im Energiesektor enorme marktwirtschaftliche Bedeutung entfaltet, sind Online-Plattformen. Plattformbasierte Geschäftsmodelle im Energiesektor sind zum Beispiel Vergleichs- und Vermittlungsportale, Smart-Home-Anwendungen oder die Aggregation von Speichern sowie Erzeugungsanlagen. Diese Plattformen haben durch ihren Zugang zu diversen Daten einen potenziell vorteilhaften Wettbewerbsfaktor. Insbesondere ist für viele Unternehmen die Besetzung der Kundenschnittstelle von erheblicher Bedeutung.[132]

Dies vor Augen hat die EU im Juli 2019 die Verordnung zur Förderung von Fairness und Transparenz für **gewerbliche Nutzer von Online-Vermittlungsdiensten**[133] verkündet. Das Ziel der Verordnung ist ein Beitrag zum reibungslosen Funktionieren des EU-Binnenmarktes, „indem Vorschriften festgelegt

---

[127] *Brucker/Günther*, in: Elspas/Graßmann/Rasbach (Hrsg.), 2018, EnWG, § 12 Rn. 12.
[128] BT-Drs. 18/7317, S. 81.
[129] BT-Drs. 18/7317, S. 82.
[130] BT-Drs. 17/6072, S. 67.
[131] *Brucker/Günther*, in: Elspas/Graßmann/Rasbach (Hrsg.), 2018, EnWG, § 12 Rn. 15.
[132] *Bundesnetzagentur* (2018), Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren, S. 84.
[133] Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, ABl. L 186/57.

werden, mit denen sichergestellt wird, dass für gewerbliche Nutzer von Online-Vermittlungsdiensten und Nutzer mit Unternehmenswebseite im Hinblick auf Suchmaschinen eine angemessene Transparenz, Fairness und wirksame Abhilfemöglichkeiten geschaffen werden“, Art. 1 der Verordnung. Sinn und Zweck der Verordnung ist es u.a. Handlungen von Plattformen vorzubeugen, die aufgrund der größeren Verhandlungsmacht „beispielsweise Nutzern einseitig Praktiken aufzwingen, die gröblich von der guten Geschäftspraktik abweichen oder gegen das Gebot von Treu und Glauben und des redlichen Geschäftsverkehrs verstoßen.“[134] In Art. 17 der Verordnung fordert die Kommission, dass Anbieter von Online-Vermittlungsdiensten sowie Organisationen und Verbände, zusammen mit gewerblichen Nutzern, einschließlich KMU (kleinere und mittlere Unternehmen) **Verhaltenskodizes auszuarbeiten**, die die ordnungsgemäße Anwendung der Verordnung unterstützen. Dabei soll den besonderen Merkmalen der verschiedenen Branchen sowie der KMU, worunter häufig auch EVU fallen, Rechnung tragen. Damit beruht ein wesentlicher Teil der Umsetzung der Verordnung auf **freiwilliger Zusammenarbeit** der Akteure. Es bleibt abzuwarten, inwieweit diese auf weitestgehend Freiwilligenbasis zu erstellenden Kodizes Wirkung entfalten werden. Eine Überprüfung des Erfolgs dieser Verordnung ist für Januar 2022 vorgesehen gemäß Art. 18 der Verordnung.

7 KOMMUNIKATION IM ENERGIENETZ

Ein grundlegender Umbruch vollzieht sich durch die Einführung des MsbG bei der **Struktur der Marktkommunikation** im Energienetz. Dreh- und Angelpunkt der Betrachtung sind hierbei die jeweiligen erhobenen Messdaten, die für die Abrechnung der Netznutzung und der Strommengenbilanzierung benötigt werden. Mit der Einführung des MsbG wurden verbindliche Regelungen zur Datenkommunikation im intelligenten Energienetz getroffen. Diese Regelungen finden sich in Teil 3, §§ 49 bis 75 MsbG, wieder. In diesem Teil ist festgelegt, welche Datenkommunikation von den verschiedenen Akteuren zu gewährleisten ist, um ihren gesetzlichen Aufgaben nachzukommen. Dies schließt auch die Verbrauchsvisualisierung mit ein. Ein über diesen Vorgaben hinausgehender Datenverkehr ist nur mit ausdrücklicher Zustimmung erlaubt.[135]

Die ursprüngliche Struktur, sog. **Stufen- oder Kettenmodel**, hatte den Verteilnetzbetreiber (VNB) im Zentrum als „Datendrehscheibe“. Der VNB hat die Messdaten gesammelt, aggregiert sowie kontrolliert mittels einer Plausibiliätskontrolle und ggf. Ersatzwerte gebildet. Im Anschluss hat der VNB diese Daten den ÜNB zur Verfügung gestellt. Die präzisen Vorgaben für die Kettenkommunikation wurden von der Bundesnetzagentur mit verschiedenen Festlegungen zur Abwicklung des Stromnetzzugangs gemacht.[136]

Die neue, durch das MsbG eingeführte Struktur ist die „**sternförmige Kommunikation**“ und stellt einen Paradigmenwechsel dar. „Datendrehscheibe“ sollen künftig das Smart Meter Gateway und der Messstellenbetreiber sein.[137] Die zentrale Rolle der Datenverteilung wird dabei vom Netzbetreiber auf das Smart Meter Gateway und dem Messstellenbetreiber übertragen. Die Datenaufbereitung soll im Smart Meter Gateway stattfinden und die Daten direkt aus dem Gerät an die Berechtigten übertragen werden. Zuständig für den Messstellenbetrieb ist der grundzuständige Messstellenbetreiber, § 3 Abs. 1 MsbG. Der grundzuständige Messstellenbetreiber ist der Netzbetreiber, § 2 Nr. 4 MsbG. Damit besteht Personenidentität zwischen dem Netzbetreiber und dem grundzuständigen Messstellenbetreiber. Die rechtliche Unterscheidung zwischen den beiden besteht jedoch darin, dass der Netzbetreiber Daten aus dem Smart Meter Gateway als berechtigter Empfänger erhält, jedoch nicht zur Weiterleitung wie in dem

---

[134] Erwägungsgrund Nr. 2 der Verordnung zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten.
[135] BT-Drs. 18/7555, S. 104.
[136] *Weise/vom Wege*, Auf dem Weg zur sternförmigen Datenkommunikation – Interimsszenario und Zielmodell für die Marktkommunikation 2.0, IR 2016, S. 125, 126 f.
[137] BT-Drs. 18/7555, S. 144.

früheren Kommunikationsmodell befugt ist.[138] Die Verarbeitung der erhobenen, personenbezogenen Daten ist nur den berechtigten Stellen möglich. Diese sind Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem Erneuerbare-Energien-Gesetz, Energielieferanten sowie jede Stelle, die über eine Einwilligung des Anschlussnutzers verfügt, die den Anforderungen des § 4a Bundesdatenschutzgesetz genügt, § 49 Abs. 1 und 2 MsbG. Dabei werden jedwede Daten, die erhoben wurden, geschützt. Dies schließt personenbezogene, personenbeziehbare als auch Daten ohne Personenbezug mit ein. Es verdeutlicht wiederum den **abschließenden Charakter** des MsbG.[139] Die berechtigten Stellen müssen auch eine verschlüsselte elektronische Kommunikation von **personenbezogenen Daten, von Mess-, Netzzustands- und Stammdaten** sicherstellen. Personenbezogenen Daten sind nach Möglichkeit und soweit der Verwendungszweck gewahrt wird zu verschlüsseln, zu anonymisieren oder zu pseudonymisieren. Zudem erhält der Anschlussnutzer weitgehende Informationsrechte; in § 53 MsbG und in § 54 MsbG werden strikte Vorgaben zur Transparenz von Verträgen gemacht, indem mittels eines standardisierten Formblattes eine kurze, einfache, übersichtliche und verständliche Auflistung zur Datenkommunikation gereicht werden soll.

Innerhalb der technischen Übergangsphase vom Zeitpunkt des Inkrafttretens des Gesetzes am 2.9.2016[140] bis zur Installation des Zielmodells ab dem 31.12.2019 hat die Bundesnetzagentur eine Festlegungskompetenz nach § 60 Abs. 2 S. 2 MsbG erhalten, um diese Transformation zu gestalten und anschließend - nach ihrer Einführung - weiter gestaltend zu begleiten. Diese Frist wurde so gesetzt, da „mit der direkten Datenkommunikation Effizienzgewinne und ein Mehr an Datenschutz und Datensicherheit einhergehen“ zwecks einer zeitnahen Realisierung.[141] Das Kommunikationsmodell für diese Übergangsphase wird als „**Interimsmodell**“ bezeichnet und sieht vor, dass die Aufbereitung und Übermittlung von Messwerten nicht mittels Smart Meter Gateways durchgeführt wird, sondern von einer durch die Bundesnetzagentur bestimmten, berechtigten Stelle.[142] Die Festlegungen der Bundesnetzagentur aus dem Dezember 2016 sehen vor, dass von Oktober 2017 bis Oktober 2019 die Aufgabe der Aufbereitung und Verteilung der Messdaten weiter über die Verteilnetzbetreiber fortgeführt wird.[143]

Übertragung von Messdaten mittels Elektrizitätsverteilnetz

Ein weiterer, interessanter Aspekt bezüglich der Kommunikation im Energiesektor findet sich in § 13 MsbG. In § 13 MsbG („Nutzung des Verteilnetzes zur Datenübertragung“) ist der Anspruch für Messstellenbetreiber implementiert, gegen ein angemessenes und diskriminierungsfreies Entgelt im Rahmen des technisch Möglichen Zugang zum Elektrizitätsverteilnetz des Netzbetreibers zu erhalten. Mit anderen Worten: Der Messstellenbetreiber soll die Möglichkeit haben, Messdaten mittels Elektrizitätsverteilernetz zu übertragen.[144] Daten direkt über das Elektrizitätsnetz zu übermitteln, ist technisch möglich, wird aber noch nicht praktiziert.[145]

Der Anspruch richtet sich gegen den jeweiligen Betreiber von Elektrizitätsverteilnetzen. Gemäß § 3 Nr. 3 EnWG ist ein Betreiber eines Elektrizitätsverteilnetzes eine natürliche oder juristische Person oder rechtlich unselbstständige Organisationseinheit eines Energieversorgungsunternehmen, die die Aufgabe der Verteilung von Elektrizität wahrnimmt und verantwortlich ist für den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Verteilnetzes in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitung zu anderen Netzen.

Anspruchsberechtigter ist der Messstellenbetreiber. Messstellenbetreiber wird gemäß § 2 Nr. 12 MsbG definiert als der grundzuständige Messstellenbetreiber oder Dritter, der die Aufgabe des Messstellenbetriebs durch Vertrag nach § 9 MsbG wahrnimmt. In der vorliegenden Konstellation kann der

---

[138] *Vom Wege*, in: Säcker, Berliner Kommentar zum Energierecht, Band 4, 4. Auflage 2017, § 60 Rn. 5.
[139] BT-Drs. 18/7555, S. 105.
[140] *Säcker/Zwanziger*, in: Säcker, Berliner Kommentar zum Energierecht, Band 4, 4. Auflage 2017, Einleitung Rn. 26.
[141] BT-Drs. 18/7555, S. 144.
[142] *Säcker/Zwanziger*, in: Säcker, Berliner Kommentar zum Energierecht, Band 4, 4. Auflage 2017, Einleitung Rn. 28.
[143] Genauer in: *Säcker/Zwanziger*, in: Säcker, Berliner Kommentar zum Energierecht, Band 4, 4. Auflage 2017, Einleitung Rn. 29.
[144] *Rohrer*, in: Rohrer/Karsten/Leonhardt, MsbG, Messstellenbetriebsgesetz, Kommentar, 2018, § 13 Rn. 1.
[145] Ebd., Rn. 4.

grundzuständige Messstellenbetreiber als Anspruchsberechtigter in der Regel ausgenommen werden, da ein Betreiber eines Elektrizitätsverteilnetz der „geborene“ und somit grundzuständiger Messstellenbetreiber ist[146] und daher Personenidentität besteht. Anspruchsberechtigter kann daher regelmäßig ein Unternehmen sein, das die Grundzuständigkeit für den Messstellenbetrieb mit modernen Messeinrichtungen und intelligenten Messsystemen mittels Übertragung nach §§ 41 ff. MsbG erlangt hat oder ein (wettbewerblicher) Dritter.[147]

[146] *vom Wege/Weise*, in: Rohrer/Karsten/Leonhardt, MsbG, Messstellenbetriebsgesetz, Kommentar, 2018, § 2 Rn. 26.
[147] Zur Aufzählung von Messstellenbetreibern, die nicht grundzuständiger Messstellenbetreiber sind: *Rohrer*, in: Rohrer/Karsten/Leonhardt, MsbG, Messstellenbetriebsgesetz, Kommentar, 2018, § 2 Rn. 26.