THERESA RATH / FELIX EKARDT / ALEXANDER SCHIELA

Cybersicherheit in der Energiewende und das deutsche Recht

Unter besonderer Beachtung der erhöhten Vulnerabilität von Energieanlagen und Kritischer Infrastruktur

IT-Versorgungssicherheit

Die Energie- und Klimawende geht mit einer zunehmenden Digitalisierung insbesondere des Stromnetzes einher. Dies birgt die Gefahr von Cyberattacken, die schlimmstenfalls die Versorgungssicherheit gefährden können. Dieser Beitrag beleuchtet mögliche Arten und Folgen von Cyberattacken auf dem Energiemarkt sowie den nationalen Rechtsrahmen de lege lata.

Lesedauer: ●● Minuten

I. Problemstellung

Gem. Art. 2 Abs. 1 Paris-Abkommen (PA) muss die globale Erwärmung auf deutlich unter 2 Grad Celsius begrenzt werden und dabei eine Obergrenze von 1,5 Grad angestrebt werden.[1] Um einem 1,5-Grad-Pfad gerecht zu werden, sind weitreichende Änderungen auf dem Energiemarkt notwendig, insbesondere ein baldiger völliger Ausstieg aus den fossilen Brennstoffen (bei Strom, Wärme, Mobilität, Landwirtschaft, Zement und Kunststoffen), neben einer tiefgreifenden Umstellung im Agrar- und Tierhaltungssektor.[2] Im Zuge des Ausbaus der erneuerbaren Energien ist eine zunehmende Digitalisierung insbesondere des Stromnetzes erforderlich. Dies ist vor allem auf die Dezentralität und Volatilität der erneuerbaren Energien zurückzuführen, welche die Netzbetreiber vor neue Herausforderungen stellen. Die voranschreitende Digitalisierung – deren ambivalente ökologische Effekte andernorts mehrfach untersucht wurden –[3] bringt jedoch auch das Risiko von Angriffen auf digitale Bestandteile des Stromnetzes mit sich.

Bisher lag der Fokus bei Cybersicherheit in Stromnetzen insbesondere auf den Mittel- und Hochspannungsnetzen, da vor allem Großkraftwerke in das Stromnetz einspeisten.[4] Der Ausbau der erneuerbaren Energien führt zu neuen Akteurskategorien am Energiemarkt – sog. Prosumer oder Flexumer –, zu bidirektionalen Leistungsflüssen im Stromnetz und, auf Grund der Volatilität der erneuerbaren Energien, zu einer komplexeren Netzsteuerung und -überwachung. Das Stromnetz entwickelt sich zu einem Smart Grid; Maßnahmen zum Last- und Einspeisemanagement im Stromnetz verändern sich dadurch.[5] Dies gilt insbesondere auch vor dem Hintergrund der Sektorkopplung, da nach und nach auch Bedarfe aus den Sektoren Verkehr und Wärme über elektrifizierte Anwendungen gedeckt werden, etwa durch den Einsatz von Wärmepumpen oder den Rückgriff auf Elektromobilität.[6] Die Notwendigkeit von Anwendungen zur Cybersicherheit verlagert sich somit von einigen großen Anlagen hin zu zahlreichen kleinen Einzelanlagen und von der Mittel- und Hochspannungsebene auf die Verteilernetze. Während ein Angriff auf eine einzelne dieser verhältnismäßig kleinen Anlagen kaum eine Auswirkung auf die Stabilität des Netzes haben mag, spielen die Verflechtung und mögliche Wechselwirkungen zwischen mehreren dieser Einzelanlagen eine Rolle bei der Gefährdung der Systemsicherheit.[7] Dies gilt umso mehr, als vor dem Hintergrund des Kriegs in Osteuropa Energieversorgungsaspekte Teil der Auseinandersetzung werden. Die Art der Kriegsführung hat sich in den letzten Jahren wesentlich verändert. Cyberangriffe spielen eine zunehmende Rolle, wie sich etwa an einem Angriff von russischer Seite auf das ukrainische Stromnetz eindrucksvoll zeigte, in dessen Folge mehrere tausend Haushalte in der Ukraine von der Stromversorgung getrennt wurden.[8] Gleiches gilt für die Angriffe auf das Stromnetz des AKW Saporischschja. Auch in Deutschland vermerkte das Bundesamt für Sicherheit in der Informationstechnik (BSI) steigende Zahlen von Cyberattacken auf Kritische Infrastruktureinrichtungen.[9] Doch nicht nur die Möglichkeit von Cyberangriffen, sondern auch die insgesamt gesteigerte Komplexität des Stromnetzes und die dadurch erhöhte Anfälligkeit für Störungen durch Extremwetterereignisse oder menschliches Versagen erhöhen das Bedürfnis nach technologischen Lösungen für ein reibungsloses Funktionieren der Anlagen und des Netzes, um die Aufrechterhaltung der Versorgungssicherheit gewährleisten zu können.[10] Aus alledem ergeben sich mögliche Anforderungen an eine energiewendetauglich begriffene Cybersicherheit. Aktuelle und bereits bestehende gesetzliche Regelungen auf nationaler Ebene,[11] die darauf zu reagieren versuchen, werden im vorliegenden Beitrag näher beleuchtet.

II. Rechtsrahmen de lege lata und Optimierungsoptionen

Auf der nationalen Ebene existieren verschiedene Rechtsquellen, die Auswirkungen auf die Cybersicherheit auf dem Energiemarkt haben. Davon betreffen manche konkret Bereiche, die sich ausschließlich auf die Energieversorgung beziehen – wie etwa Vorschriften aus dem Energiewirtschaftsgesetz (EnWG) und

---

1 Näher zu Inhalt, Rechtsverbindlichkeit und (drastischer) Reichweite Ekardt/Bärenwaldt/Heyl Environments 2022, 112; Wieding/Stubenrauch/Ekardt Sustainability 2020, 8858; Ekardt/Wieding/Zorn Sustainability 2018, 2812; aufgegriffen in BVerfGE 157, 30 ff.; dazu teils krit. (weil in einigen Punkten zu defensiv) Ekardt/Heyl Nature Climate Change 2022, 697 ff.; Ekardt/Heß NVwZ 2021, 1421 ff.

2 Näher dazu Weishaupt/Ekardt/Garske/Stubenrauch/Wieding Sustainability 2020, 2053; Ekardt/Bärenwaldt/Heyl Environments 2022, 112; Ekardt, Sustainability: Transformation, Governance, Ethics, Law, 2019.

3 Garske/Bau/Ekardt Sustainability 2021, 4652; Ekardt/Rath ZNER 2022, 211 ff.

4 Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 2.

5 Etezadzadeh, Smart City – Made in Germany/Volk/Konermann, 2020, S. 292 f.; TU Berlin, Digitalisierung in der Energiewirtschaft/Ritschel/Sprengel/Walther, 2021, S. 52 f.

6 Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 2.

7 Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 3; Krebs/Hagenweiler, Energieresilienz und Klimaschutz, 2021, S. 14 f.

8 Hierzu Barda Wirtschaftsinformatik & Management 2022, 32 (34); Smith Journal of Energy & Natural Resources Law, 36:4, 373 (377).

9 Krebs/Hagenweiler, Energieresilienz und Klimaschutz, 2021, S. 18; vgl. hierzu außerdem mit Blick auf den Russland-Ukraine-Konflikt Bundesamt für Verfassungsschutz, Sicherheitshinweis für die Wirtschaft – Betreff: Krieg in der Ukraine, 2022.

10 Mit einem Überblick zu möglichen Störursachen Krebs/Hagenweiler, Energieresilienz und Klimaschutz, 2021, S. 13 ff.

11 Zu Regelungen auf EU-Ebene s. Rath/Eckardt/Schiela MMR 2023, 83.

dem Messstellenbetriebsgesetz (MsbG). Andere Vorschriften betreffen auch andere Sektoren, etwa solche aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), und Gesetzesänderungen, die durch das IT-Sicherheitsgesetz 2.0 in bereits bestehende Gesetze integriert wurden.[12] Teils wird bei diesen Gesetzen durch aktuell auf EU-Ebene im Gesetzgebungsprozess befindliche Novellierungen ein Überarbeitungsbedarf ausgelöst, der ebenfalls im Folgenden kurz angesprochen werden soll.

1. BSIG und KritisV

Das BSIG ist im Jahr 2009 in Kraft getreten. Nach § 3 Abs. 1 BSIG ist die vorrangige Aufgabe des BSI die Förderung der Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Die Informationstechnik umfasst gem. § 2 Abs. 1 BSIG alle technischen Mittel zur Verarbeitung und Übertragung von Informationen. Die Aufgaben des BSI im Einzelnen umfassen einen langen Katalog, der in § 3 Abs. 1 S. 2 BSIG aufgeschlüsselt ist. Für den Energiemarkt relevant nimmt das BSI nach § 3 Abs. 1 S. 2 Nr. 17 BSIG Aufgaben wahr als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse (vgl. §§ 8a bis 8c BSIG sowie § 8f BSIG). Gem. § 2 Abs. 10 BSIG sind Kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die
1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Welche Einrichtungen, Anlagen oder Teile davon konkret als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten, wird gem. § 10 Abs. 1 BSIG durch das BMI per Rechtsverordnung bestimmt, unter Festlegung der in den jeweiligen Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads.

Betreiber Kritischer Infrastrukturen sind nach § 8a Abs. 1 BSIG verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Diese Verpflichtung umfasst nach § 8a Abs. 1a BSIG ab dem 1.5.2023 auch den Einsatz von Systemen zur Angriffserkennung. Nach § 8a Abs. 3 BSIG haben Betreiber Kritischer Infrastrukturen die Erfüllung dieser Anforderungen regelmäßig dem BSI nachzuweisen; das BSI kann die Einhaltung dieser Anforderungen nach § 8a Abs. 4 BSIG überprüfen.[13] § 8b BSIG enthält weitreichende Meldepflichten für Betreiber Kritischer Infrastrukturen.[14] Das Vorliegen einer Kritischen Infrastruktur richtet sich nach der auf § 10 BSIG beruhenden Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (KritisV). In § 2 Abs. 1 KritisV sind kritische Dienstleistungen im Sektor Energie definiert als solche, die die Versorgung der Allgemeinheit mit Elektrizität (Stromversorgung), die Versorgung der Allgemeinheit mit Gas (Gasversorgung), die Versorgung der Allgemeinheit mit Kraftstoff und Heizöl (Kraftstoff- und Heizölversorgung) oder die Versorgung der Allgemeinheit mit Fernwärme (Fernwärmeversorgung) betreffen. Als Kritische Infrastruktur gelten sie dann, wenn es sich um Anlagen oder Teile davon handelt, die nach § 2 Abs. 6 Nr. 1 KritisV einer bestimmten Kategorie aus dem Anhang zuzuordnen sind und einen bestimmten Schwellenwert, der im Anhang zur KritisV definiert ist, erreichen oder überschreiten.[15] Die Schwellenwerte sind dabei so festgelegt, dass ein Ausfall der Anlage oder des Anlagenteils hypothetisch 500.000 Menschen von der Versorgung abschneiden müsste, um diese als Kritische Infrastruktur zu qualifizieren.[16] Für diejenigen Einrichtungen, die nicht unter diese Definition fallen, bedeutet das grundsätzlich, dass für sie keine besonderen Verpflichtungen im Hinblick auf ihre Cybersicherheit bestehen, vorbehaltlich speziellerer gesetzlicher Vorschriften. Dadurch erhöht sich für sie das Risiko von Störungen und Ausfällen, etwa durch gezielte Cyberangriffe. Für die durch diese Einrichtungen versorgten Bürger bedeutet dies eine potenzielle Unterbrechung der Versorgungssicherheit, was für die Betroffenen verheerende Folgen haben kann.[17] Es zeigt sich also, dass durch die aktuelle Gesetzeslage Akteure im Bereich der Daseinsvorsorge vom Begriff der Kritischen Infrastruktur – und dem damit einhergehenden Pflichtenkatalog – ausgeschlossen sind, obwohl ihre tatsächliche Bedeutung für die Bürger klar auf der Hand liegt.

Die aktuell auf EU-Ebene im Gesetzgebungsprozess befindliche Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) würde in Bezug auf das BSIG einigen Änderungsbedarf auslösen. Zunächst wären der § 2 Abs. 10 BSIG und die in Bezug genommene KritisV so anzupassen, dass sie sich mit dem durch die Richtlinie vorgeschriebenen Anwendungsbereich (Art. 2 NIS-2-RL-E) decken. Durch die NIS-2-RL wird der Anwendungsbereich der Richtlinie im Vergleich zur bisher gültigen NIS-RL stark erweitert und vor allem an der Unternehmensgröße ausgerichtet.[18] Die in der KritisV genannten Schwellenwerte wären hinfällig, es wären fortan die Kriterien des Umsatzes und der Mitarbeiterzahl entscheidend. Zudem müsste der eher allgemein gehaltene § 8a BSIG eine Erweiterung und Konkretisierung erfahren, um den Maßnahmen-Anforderungen des Art. 18 NIS-2-RL-E gerecht zu werden. Auch die in §§ 8b, 8c BSIG vorgeschriebenen Meldepflichten hinsichtlich Cybersicherheitsvorfällen müssten weiter verschärft werden mit Blick auf Art. 20 NIS-2-RL-E. Neu wäre vor allem die Pflicht zum Bericht auch der „near misses". Schließlich ist auch das Bußgeldniveau anzuheben (vgl. § 14 Abs. 5 BSIG, Art. 31 Abs. 4, 4a NIS-2-RL-E).

2. EnWG

§ 11 Abs. 1a und 1b EnWG verpflichtet Marktteilnehmer dazu, angemessene Vorkehrungen zum Schutz vor Störungen ihrer IT-Sicherheit zu etablieren. Zudem haben sie nach § 11 Abs. 1c EnWG die Pflicht, Störungen unverzüglich dem BSI zu melden.[19] Das EnWG ist dabei lex specialis zum BSIG in Bezug auf den Schutz von Energieversorgungsnetzen und sonstigen Energieanlagen in den Bereichen Strom und Gas.[20] Die Schwellenwerte aus der KritisV spielen demnach für die Begründung der Pflich-

---

12 Einen Überblick über die geltenden Regelungen gibt auch Dittrich MMR 2022, 1039.

13 Vgl. Atug DuD 2020, 668 (669).

14 Hierzu im Einzelnen Atug DuD 2020, 668 f.; TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 89.

15 von Bremen EWerk 2020, 29 (30); TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 90 ff.

16 BBK, Klärung und Erweiterung des KRITIS-Vokabulars, 2021, S. 8; von Bremen EWerk 2020, 29 (30).

17 Hierzu Fekete, Kritische Infrastruktur und Versorgung der Bevölkerung/Begerow/Fekete/Lechleuthner, 2022, S. 16 f.

18 Hierzu und zur Kritik an der NIS-2-RL s. Rath/Eckardt/Schiela MMR 2023, 83.

19 Ausf. zu den Sicherheitskatalogen der Bundesnetzagentur TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 97 ff.

20 von Bremen EWerk 2020, 29 (30); TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 92 ff.

ten aus § 11 Abs. 1a, 1b und 1c EnWG keine Rolle.[21] Betreiber anderer Energieanlagen – zB von Fernwärmenetzen – müssen also im Umkehrschluss gleichzeitig Betreiber iSv § 2 KritisV iVm Anhang 1 Teil 3 KritisV sein.[22] Insgesamt fallen nach diesen Regelungen nur knapp 30% der deutschen Netto-Nennleistung unter das Kriterium der Kritischen Infrastruktur, was im Umkehrschluss bedeutet, dass es für die übrigen rund 70% nach derzeitiger Gesetzeslage keine einheitlichen Anforderungen zur IT-Sicherheit gibt.[23]

Auch diese Anforderungen an Marktteilnehmer müssten bei Verabschiedung des NIS-2-RL-E erheblich verschärft werden. Ähnlich wie § 8a BISG lassen auch § 11 Abs. 1a und 1b EnWG mit offenen Formulierungen („angemessenen Schutz") viel Raum für Interpretationen. Diese müssten durch den konkreten Maßnahmenkatalog des Art. 20 NIS-2-RL-E ersetzt werden. Auch die Meldepflichten in § 11 Abs. 1c EnWG ebenso wie die Bußgeldhöhe in § 95 Abs. 2 EnWG bedürften der Anpassung.

3. MsbG

Im deutschen Recht wird der Umgang mit personenbezogenen Daten iRd Messstellenbetriebs durch das Messstellenbetriebsgesetz (MsbG) geregelt, welches grundsätzlich vorrangig vor Datenschutzgrundverordnung (DS-GVO)[24] und Bundesdatenschutzgesetz (BDSG) gilt. In Teilen ist das Verhältnis von DS-GVO und MsbG noch ungeklärt. Dort, wo das MsbG hinter den Anforderungen der DS-GVO zurückbleibt, dürfte der Schutzmaßstab der DS-GVO anzulegen sein (dazu sogleich). Für nicht im MsbG geregelte Datenverarbeitungen gilt ebenfalls weiterhin die DS-GVO. Im Übrigen gilt das MsbG.

Das MsbG, das im Jahr 2016 durch das Gesetz zur Digitalisierung der Energiewende eingeführt wurde, enthält zahlreiche Vorgaben zum Einsatz von intelligenten Messsystemen. Grundsätzlich gilt, dass Messstellenbetreiber Messstellen, soweit dies technisch möglich und wirtschaftlich vertretbar ist (vgl. §§ 30, 31 MsbG), dann mit intelligenten Messsystemen auszustatten haben, wenn beim jeweiligen Letztverbraucher ein Jahresverbrauch von über 6.000 kW/h oder bei Anlagenbetreibung eine installierte Leistung von über 7 kW vorliegt (vgl. § 29 Abs. 1 MsbG). Nach der geänderten Heizkostenverordnung, die auf das MsbG verweist und auf Basis des § 6 Abs. 1 Nr. 1 Gebäudeenergiegesetz (GEG) erlassen wurde, gilt die Anforderung der Fernablesbarkeit für neuinstallierte Zähler ab Inkrafttreten der geänderten Verordnung, mithin ab dem 1.12.2021. Bereits installierte Zähler müssen bis Ende 2026 nachgerüstet oder ersetzt werden. Da über diese intelligenten Messsysteme personenbezogene Daten an verschiedene Adressaten übermittelt werden,[25] trifft das MsbG zahlreiche Bestimmungen zur Verarbeitung dieser Daten, die in den §§ 49 ff. MsbG ausformuliert sind[26] und die grundsätzlich vorrangig vor den Bestimmungen der DS-GVO anzuwenden sind.[27] In den §§ 19 ff. definiert das MsbG zahlreiche technische Vorgaben zur Gewährleistung von Datenschutz und Datensicherheit beim Einsatz von Smart-Meter-Gateways, deren Darstellung im Einzelnen den Rahmen dieses Beitrags sprengen würde. Es sei jedoch erwähnt, dass das BSI mit der Zertifizierung der Smart-Meter-Gateways betraut ist (vgl. § 24 MsbG) und ihm weitere Kompetenzen, wie etwa der Erlass technischer Richtlinien, zukommen.

4. IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz 1.0 aus dem Jahr 2015 ergänzte bzw. änderte als Artikelgesetz einige bestehende Gesetze mit dem Fokus auf Gewährleistung von IT-Sicherheit.[28] Kernziele des Gesetzes waren die Verbesserung der Sicherheit und des Schutzes der IT-Systeme und Dienste insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS) – wie etwa der Strom- und Wasserversorgung.[29] Im Bereich der Energiewirtschaft wurden wichtige Änderungen im BSIG und im EnWG durch das IT-Sicherheitsgesetz realisiert. Betreiber Kritischer Infrastrukturen wurden über das IT-Sicherheitsgesetz verpflichtet, bestimmte Standards hinsichtlich ihrer Vorkehrungen zur Cybersicherheit einzuhalten. Im Jahr 2021 wurde das IT-Sicherheitsgesetz 2.0 verabschiedet. Durch dieses Gesetz wurden die Befugnisse des BSI deutlich erweitert. Auch der Anwendungsbereich hinsichtlich der Definition von Betreibern Kritischer Infrastrukturen wurde ausgedehnt. Das BSI erhält durch das Gesetz u.a. die Befugnis, Sicherheitslücken in IT-Sicherheitssystemen zu detektieren.[30] Für diejenigen Komponenten, die explizit für den Betrieb einer Kritischen Infrastrukturanlage ausschlaggebend sind, werden über ein sog. „BSI-Sicherheitskennzeichen" Mindeststandards definiert.[31] Durch das IT-Sicherheitsgesetz 2.0 wurden außerdem umfassendere Pflichten für die Betreiber Kritischer Infrastrukturen eingeführt sowie Unternehmen im besonderen öffentlichen Interesse in den Anwendungsbereich des BSIG aufgenommen (dazu bereits oben).[32] Die Verabschiedung der NIS-2-RL hätte in Bezug auf die Definition der Betreiber Kritischer Infrastrukturen sowie die Pflichten dieser ebenfalls Änderungsbedarf im oben beschriebenen Sinne zur Folge.

5. DS-GVO und ePrivacy-Verordnung

Ergänzend zu einer früheren Untersuchung der EU-Rechtslage und ausführend zu den oben bereits getätigten Erörterungen zum MsbG wird nachstehend noch ein Blick geworfen auf einen unmittelbar in Deutschland geltenden, aber EU-rechtlich geregelten Bereich: Wie anhand des MsbG bereits für intelligente Messsysteme ausgeführt, bringt auch der Datenschutz gewisse Anforderungen an die Cybersicherheit mit sich. Dies gilt insbesondere für die Verpflichtung, bestimmte Sicherheitsvorkehrungen zum Schutz personenbezogener Daten zu treffen. Immer dann, wenn personenbezogene Daten von Verarbeitungsprozessen betroffen sind, finden die Vorschriften der DS-GVO Anwendung, die seit 2018 in Kraft ist und als Verordnung unmittelbar in den Mitgliedstaaten gilt. Bei den von intelligenten Messsystemen in Smart Grids aufgezeichneten Daten handelt es sich

---

21 OLG Düsseldorf Beschl. v. 19.7.2017 – VI-3 Kart 109/16 (V), ausdrücklich zwar nur für § 11 Abs. 1a EnWG; dies gilt durch die Umsetzung der NIS-RL jedoch nun auch für § 11 Abs. 1c, vgl. BT-Drs. 18/11242, 55.

22 Ausführlicher zu den jeweiligen Anwendungsbereichen von Bremen EWerk 2020, 29 (30 f.); TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 93 f.

23 TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 95.

24 VO (EU) 2016/679 des europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (DS-GVO), ABl. 2016 L 119, 1.

25 Lüdemann/Jürgens/Sengstacken ZNER 2013, 592; Göge/Boers ZNER 2009, 368; Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things/vom Wege/Reichwein, 2. Aufl. 2020, § 17 Rn. 54; Wimmer EnWZ 2020, 387 (389); Bretthauer EnWZ 2017, 56 (57); außerdem handelt es sich auch um personenbezogene Daten iSd BDSG.

26 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz/Wiesemann, 3. Aufl. 2019, Kap. 6 Rn. 14.

27 Vgl. zum Verhältnis von DS-GVO und MsbG auch Ekardt/Rath ZNER 2022, 211 ff.; sollen über das MsbG hinaus Daten iRd Nutzung intelligenter Messsysteme verarbeitet werden, ist die Erfüllung eines Erlaubnistatbestands nach Art. 6 DS-GVO notwendig.

28 TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 89.

29 BSI, Das IT-Sicherheitsgesetz – Kritische Infrastrukturen schützen, 2016, S. 5.

30 Vgl. § 7b BSIG, der auch als „Hackerparagraf" bezeichnet wird; hierzu Kipker/Scholz DuD 2021, 40 (42); Krebs/Hagenweiler, Energieresilienz und Klimaschutz, 2021, S. 84 f.; von Bremen EWerk 2020, 29 (33).

31 TU Berlin, Digitalisierung in der Energiewirtschaft/Brühl/Stocker/Kaufmann, 2021, S. 105 f.; Kipker/Scholz DuD 2021, 40.

32 Kipker/Scholz DuD 2021, 40 (42 f.); von Bremen EWerk 2020, 29 (33 f.); krit. evaluierend zum IT-Sicherheitsgesetz 2.0 Atug Int. Cybersecur. Law Rev. 2021 (2), 7 ff.

um solche personenbezogenen Daten,[33] also Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. Art. 4 Nr. 1 DS-GVO). Denn im Wege des Smart Metering werden durch die intelligenten Messsysteme zahlreiche Verbraucherdaten aufgezeichnet, die Rückschlüsse auf den Lebenswandel zulassen. Die Aufzeichnung von Verbrauchsdaten erfolgt zwar auch beim Einsatz herkömmlicher Messsysteme (zB des bislang verbreiteten elektromechanischen Ferraris-Zählers). Allerdings erhöhen sich beim Einsatz eines Smart Meters sowohl die Quantität als auch die Qualität der erfassten Daten erheblich.[34] Denn insbesondere die kurzen Erhebungsintervalle (alle 15 Minuten) lassen verstärkt Rückschlüsse auf die Lebensgewohnheiten der jeweiligen Verbraucher in ihrem Wohnraum zu.[35] Zudem kann aus Kenntnissen über Zustand und Energieeffizienzklasse der Haushaltsgegenstände gefolgert werden, in welchen finanziellen Verhältnissen die Verbraucher leben. Insbesondere können mit Hilfe der Zähler sogar einzelne Haushaltsgeräte identifiziert werden, was wiederum noch detailliertere Rückschlüsse auf das Nutzerverhalten zulässt.[36] Auch die Daten über die Erzeugungswerte können einzelnen Prosumern (selbst Strom produzierenden Verbrauchern) zugeordnet werden, wenn im jeweiligen Stromnetz auch Erzeuger mit EE-Anlagen einbezogen sind.[37] Dabei gilt dies sowohl für die Daten, die auf der Entnahmeseite erhoben werden, als auch für diejenigen, die auf der Einspeiseseite anfallen; allerdings sind letztere in ihrer Entstehung tendenziell eher nicht verhaltensabhängig.[38]

Gem. Art. 4 Nr. 2 DS-GVO meint Verarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Den für die Datenverarbeitung Verantwortlichen trifft nach Art. 25 Abs. 1 DS-GVO die Pflicht, unter Berücksichtigung verschiedener dort genannter Faktoren, u.a. Zweck der Verarbeitung und Risiken für Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen – wie zB Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die Rechte der betroffenen Personen zu schützen. Außerdem hat der Verantwortliche nach Art. 25 Abs. 2 DS-GVO geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Eine Konkretisierung dieser Vorschrift enthält Art. 32 DS-GVO, der beispielhaft konkrete Maßnahmen nennt, durch die die Verantwortlichen und die Auftragsdatenverarbeiter ein dem Risiko angemessenes Schutzniveau gewährleisten sollen.[39] Dazu zählen etwa die Verschlüsselung personenbezogener Daten oder die Implementierung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Art. 42 DS-GVO enthält Aussagen zu datenschutzspezifischen Zertifizierungsverfahren sowie zu Datenschutzsiegeln und -prüfzeichen, deren Einhaltung nahelegt, dass den Vorschriften aus Art. 25 und 32 DS-GVO Genüge getan ist.

Ergänzend sei hier angemerkt: Durch die sich im EU-Gesetzgebungsverfahren befindliche ePrivacy-Verordnung soll die elektronische Kommunikation zukünftig dem Maßstab der DS-GVO angenähert werden, ohne über deren Regelungen hinauszugehen.[40] Zudem soll das Setzen und Verwenden von Cookies auf Webseiten und das Tracking von Nutzern genauer geregelt werden. In Art. 17 ePrivacy-Verordnungsentwurf ist festgelegt, dass der Betreiber eines elektronischen Kommunikationsdienstes die Endnutzer zu informieren hat, wenn ein besonderes Risiko besteht, dass die Sicherheit von Netzen und elektronischen Kommunikationsdiensten beeinträchtigt werden könnte. Bisher ist das Gesetzgebungsverfahren hinsichtlich der Verordnung noch zu keinem Abschluss gelangt.

III. Fazit und Ausblick

Anforderungen an die Cybersicherheit von Energieerzeugungsanlagen bzw. energierelevanten Unternehmen sind auf nationaler Ebene in zahlreichen Gesetzen geregelt, die teilweise durch neue EU-Richtlinien in naher Zukunft erhebliche Änderungen erfahren werden. Dennoch ist unklar, ob diese Änderungen ausreichend sind, um der stetig zunehmenden Zahl von Cyberangriffen erfolgreich zu begegnen. Das Recht der Cybersicherheit wird umso wichtiger, je mehr Strom- und ggf. auch Wärmenetze digitalisiert werden, wobei dies mit der fortschreitenden Energiewende einhergeht. Der Gesetzgeber ist daher dazu aufgerufen, das Thema Cybersicherheit mit in den Fokus seiner gesetzlichen Bemühungen und Ausbauvorhaben zu stellen und regelmäßig den Rechtsrahmen auf seine Wirksamkeit hin zu überprüfen.

Schnell gelesen ...

- Für eine erfolgreiche Energiewende wird eine zunehmende Digitalisierung insbesondere der Stromnetze notwendig sein, welche die Energieversorgung einem größeren Risiko durch Cyberattacken aussetzt.
- Einige der Gesetze, die auf nationaler Ebene Regelungen zur Cybersicherheit treffen, werden durch die Umsetzung der (noch zu verabschiedenden) NIS-2-Richtlinie in wesentlichen Bereichen geändert werden. Dies betrifft insbesondere die Definition des Begriffs „Kritische Infrastruktur" im BSIG.
- Je weiter die Energiewende fortschreitet, desto wichtiger wird es werden, das Recht der Cybersicherheit breiter aufzustellen und in Bezug auf einzelne Energieanlagen womöglich Feinjustierungen vorzunehmen.

33 Lüdemann/Jürgens/Sengstacken ZNER 2013, 592; Göge/Boers ZNER 2009, 368; Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things/vom Wege/Reichwein, 2. Aufl. 2020, § 17 Rn. 54; Wimmer EnWZ 2020, 387 (389); Bretthauer EnWZ 2017, 56 (57); außerdem handelt es sich auch um personenbezogene Daten iSd BDSG.

34 Es fallen grds. drei wesentliche Arten von Daten an: Messwerte, Netzzustandsdaten und Stammdaten, vgl. Lüdemann/Ortmann/Pokrant RDV 2016, 125 (127).

35 Greveler/Justus/Löhr, Hintergrund und experimentelle Ergenisse zum Thema „Smart Meter und Datenschutz", 2011, S. 1; Karg DuD 2010, 365 (366); Müller DuD 2010, 359 (361); Cavoukian/Polonetsky/Wolf, SmartPrivacy for the Smart Grid, 2009, S. 11; Bretthauer EnWZ 2017, 56 (57); Bretthauer EnWZ 2020, 387 (389).

36 Greveler/Justus/Löhr, Identifikation von Videoinhalten über granulare Stromverbrauchsdaten, 2012, Kap. 4.1; Müller DuD 2010, 359 (361).

37 Haubrich, Energieoptimierendes Verbraucherverhalten, 2017, S. 80.

38 Haubrich, Energieoptimierendes Verbraucherverhalten, 2017, S. 80.

39 Vgl. ausf. zu diesen Vorschriften Nwankwo/Stauch/Radoglou-Grammatikis u.a. Electronics 2022,
11, 965 (969 ff.).

40 KOM(2017) 10 final v. 10.1.2017 – Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der RL 2002/58/EG (VO über Privatsphäre und elektronische Kommunikation).

Ass. iur. Theresa Rath,
ist Doktorandin an der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin, in Verbindung mit der Universität Rostock, Juristische Fakultät.

Professor Dr. Dr. Felix Ekardt, LL.M., M.A.,
ist Leiter der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin, in Verbindung mit der Universität Rostock, Juristische Fakultät.

RA Alexander Schiela
ist bei Flick Gocke Schaumburg in Berlin tätig und Doktorand an der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin.

Dieser Beitrag referiert einige Ergebnisse des dreijährigen Konsortial-Forschungsprojekts „Wärmewende in der kommunalen Energieversorgung (KoWa)“.