1 Intelligente Stromnetze

Die Autoren erläutern kurz, was intelligente Stromnetze sind und behaupten, dass vernetzte Stromzähler notwendig seien, um die Einspeisung erneuerbarer Energien mit der Stromnachfrage in Einklang zu bringen. Sie machen deutlich, dass sich aus dem großen Volumen an Nutzerdaten ein hohes Risikopotential ergibt, da hierdurch Rückschlüsse auf die Lebenssituation abgeleitet werden können. Laut Forschungsergebnissen soll es sogar möglich sein, aus diesen Daten zu ermitteln, welches Fernsehprogramm geschaut wurde. All diese Daten könnten neben dem eigentlichen Ziel – nämlich dem effizienten Management des Stromnetzes – auch für personalisierte Werbung missbraucht werden.
Da sich der Stromverbraucher der Einführung von „Smart Metern“ nicht entziehen könne, sehen die Autoren den Gesetzgeber in der Pflicht, weitere Regelungen zu finden, welche auf die Besonderheiten intelligenter Stromnetze besser anwendbar sind. Der Gesetzgeber habe auf diesen Bedarf mit Vorschriften in der Messzugangsverordnung (MessZV) und im Energiewirtschaftsgesetz (EnWG) reagiert. Aufgrund fehlender Normenklarheit sei jedoch nicht davon auszugehen, dass die MessZV und das EnWG die Regelungen des Bundesdatenschutzgesetzes (BDSG) verdrängen, da die Normenklarheit voraussetzt, dass die Regelungen „deckungsgleich und tatbestandskongruent“ zu den Regelungen im BDSG sein müssen.
Die Autoren untersuchen für zahlreiche Fallkonstellationen, wann Datenübermittlungen zwischen Anschlussnutzer, Messstellenbetreiber, Netzbetreiber und Energieversorger grundsätzlich zulässig seien und stellen fest, dass in vielen dieser Fälle eine wirksame Einwilligung nach §4 Abs. 1 BDSG notwendig sei. Dies gelte insbesondere für die Verarbeitung netzbetriebsrelevanter Daten, da zum Management des Stromnetzes anonymisierte Daten ausreichend seien. Die Notwendigkeit einer normalen Einwilligung ist nach Meinung der Autoren nicht für das Betreiben eines intelligenten Stromnetzes förderlich. Insbesondere die Freiwilligkeit der Einwilligung wird als Problem dargestellt, denn für den Betrieb eines solchen Stromnetzes sei es zwingend erforderlich, dass Lastprofile möglichst vieler Anschlussnutzer ermittelt werden. Hinsichtlich der zahlreichen Marktakteure und der technischen Komplexität sei es auch kaum möglich, die Betroffenen über die verschiedenen Datenverwendungen zu informieren.
Die Autoren begrüßen „uneingeschränkt“ den Ansatz, ein spezielles Datenschutzrecht für intelligente Stromnetze zu schaffen. Es wird befürwortet, dass einzelne Details in Verordnungen geregelt werden, um damit die Flexibilität zu erhöhen. Allerdings werden verfassungsrechtliche Bedenken angeführt, da dem Recht auf informationelle Selbstbestimmung Verfassungsrang zukommt und eine Verordnung diesem Anspruch nicht gerecht werden könne.

1.1 Literatur

Lüdemann V, Jürgens C, Sengstacken C (2013): Datenschutz in intelligenten Stromnetzen (Smart Grids). Zeitschrift für Neues Energierecht(06), 592-597 [https://www.wisonet.de/document/ZNER___18A5F0E423289173CBFB9DF9436BCD3E]

2 Studie zur Nutzung von Smart-Home-Anwendungen

Eine repräsentative Umfrage im Auftrag des Verbands Bitkom aus dem Jahr 2014 hat ergeben, dass 51 Prozent der Bürger in Deutschland schon einmal von Smart-Home-Anwendungen gehört haben und 14 Prozent diese auch nutzen. Für 78 Prozent der Nutzer sind Smart-Home-Anwendungen unverzichtbar. Als Hindernisse gaben die Befragten neben dem aufwendigen Einbau (37 Prozent) und zu teurer Gräte (33 Prozent) auch die Angst um die Privatsphäre (24 Prozent), Angst vor Hacker-Angriffen (19 Prozent) sowie die Sorge um den Datenschutz (17 Prozent) an.

2.1 Literatur

Bitkom (2014): 10 Millionen nutzen Smart-Home-Anwendungen. [https://www.bitkom.org/Presse/Presseinformation/10-Millionen-nutzen-Smart-Home-Anwendungen.html]

3 Beispiele für den Missbrauch von Smart-Home-Anwendungen

Der Autor nennt viele konkrete Beispiele, bei denen Smart-Home-Anwendungen durch Unbefugte gesteuert werden konnten oder die erhobenen Daten für andere Zwecke verwendet wurden: Analyse der Fernsehgewohnheiten durch TV-Hersteller, Fehlfunktionen intelligenter Steckdosen, anfällige Internetkameras, Steuerung von Heizung, Lüftung und Klimaanlage.
Er führt an, dass in einem Test von Sicherheitsberater Colby Moore nur eines von 16 vernetzten Geräten keine offensichtlichen Schwächen besaß. Nach Meinung der Marktforscher von ON World soll es bis 2018 50 Millionen vernetzte Haushalte geben. Sollten diese Systeme nicht sicher sein, muss befürchtet werden, dass sensible Informationen über Lebensgewohnheiten an Unternehmen, Kriminelle oder auch staatliche Behörden geraten könnten.

3.1 Literatur

Jakobs J (2015): Was das Smart Home über uns verrät. marconomy.de [https://www.wiso-net.de/document/MARC__43309430]

4 Smart Home als Herausforderung für das Datenschutzrecht

„Das Smart Home ist das Heim der Zukunft – hochvernetzt und hochtechnisiert. Diese Entwicklung bringt große Herausforderungen für das Recht mit sich.“

4.1 Literatur

Geminn CL (2016): Das Smart Home als Herausforderung für das Datenschutzrecht. Datenschutz und Datensicherheit - DuD, 40(9), 575–580 [https://doi.org/10.1007/s11623-016-0661-3]

5 Chancen für größere Effizienz in der Industrie und für Marktforscher

„Die Medien erfreuen sich an der Berichterstattung über schlaue Dinge im Alltag des Konsumenten. Uhren, die den Puls messen, Thermostate im Haus, die von unterwegs gesteuert werden, Handys, die automatisch senden, wenn jemand in Bedrängung gerät. Das Internet der Dinge birgt aber auch Chancen für größere Effizienz in der Industrie und für Marktforscher."

5.1 Literatur

Hedewig-Mohr S (2016): Smart home, smart car, smart …. planung & analyse(1), 56–63 [https://www.wiso-net.de/document/PUA___20160223349408]