View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

HAUSAUTOMATIONSSYSTEME IM DATENSCHUTZRECHT

Frederik Möllers[1], Christoph Sorge[2]

[1]Wissenschaftlicher Mitarbeiter, [2]Professor
juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
Campus A5 4, 66123 Saarbrücken, DE
{frederik.moellers,christoph.sorge}@uni-saarland.de; http://www.uni-saarland.de/lehrstuhl/sorge/

Schlagworte: ***Hausautomation, Datenschutz, Telemediengesetz, Bundesdatenschutzgesetz, Cloud***

Abstract: *Hausautomationssysteme erfreuen sich immer größerer Beliebtheit. Eine mittlerweile gängige Praxis ist, die gesammelten Daten im Rahmen einer Cloud-Anwendung an den Anbieter der Hausautomationslösung zu übertragen. Neben den Komfortfunktionen wie visueller Aufbereitung und Benachrichtigungen ermöglichen diese Daten dem Anbieter aber auch Rückschlüsse über das Verhalten der Bewohner, die zu detaillierten Profilen verknüpft werden können. Unser Beitrag erörtert die Frage, welche Probleme diese Entwicklung aus rechtlicher Sicht mit sich bringt und kommt zu dem Ergebnis, dass trotz dieser Probleme ein legaler Einsatz möglich ist.*

1. Einleitung

Der kommerzielle Erfolg von Hausautomationssystemen in hat in den letzten Jahren stark zugenommen – ein Trend, der sich fortzusetzen scheint. Die Gründe hierfür sind offensichtlich: Sinkende Preise für technische Komponenten, die Integration ubiquitärer Technologien wie Smartphones und fortlaufende Verbesserungen des Wohnkomforts machen die Systeme zu attraktiven Produkten.

Anwendungsbereiche für Hausautomationssysteme sind häufig grundlegende Aufgaben, deren manuelle Bearbeitung mühsam oder fehleranfällig ist. Hierzu zählen beispielsweise das regelmäßige Lüften der Räume, das Heizen je nach Anwesenheit und Nutzung oder die Steuerung elektrischer Geräte und Lampen. Prognosen für zukünftige Geräte gehen noch weiter, ein Paradebeispiel für anstehende Entwicklungen sind etwa Kühlschränke, die bei Bedarf Lebensmittel bestellen.

Innerhalb des Gebiets der Heimautomatisierung zeichnet sich derzeit eine Zweiteilung der angebotenen Produkte ab. Einige Systeme (z.B. FS20, iComfort) sind abgeschlossen und funktionieren autonom, teilweise lassen sie sich durch entsprechende Konfiguration über die Internetanbindung des Nutzers fernsteuern. So erlauben sie auch den Zugriff von unterwegs, die Daten verlassen aber die Endgeräte des Eigentümers nicht. Die Steuerung und alle dafür nötigen Berechnungen erfolgen lokal. Andere Systeme (z.B. Loxone, Nest) hingegen verknüpfen die Steuerung des einzelnen Haushalts mit dem kollektiven „Wissen“ und der Verfügbarkeit von Cloud-Anbietern, um dem Nutzer einen Mehrwert zu bieten. Hierzu werden Daten aus den einzelnen Haushalten an den Anbieter übertragen, welcher im Gegenzug die Ergebnisse der Aggregation zurück an die Geräte sendet. Letztere lassen sich darüber hinaus über die Internetpräsenz des Anbieters bedienen.

Im Rahmen dieser Arbeit befassen wir uns mit den rechtlichen Implikationen der zweiten Kategorie von Hausautomationssystemen. Durch den Austausch der Daten zwischen dem System im Haus des Anwenders und dem Cloud-Anbieter entsteht eine neue Situation, die technisch und juristisch neue Fragen aufwirft. Die Sammlung und Verarbeitung von Daten über das Haus und die Bewohner erfolgt bisher praktisch nach Belieben des Anbieters und wird *de facto* von den Kunden geduldet, die

sich die Systeme installieren. Die rechtliche Einordnung der Datensammlung und -verarbeitung und die dadurch geltenden Rechte und Pflichten der beteiligten Parteien sind jedoch noch ungeklärt.

Im Folgenden erläutern wir zunächst die technischen Grundlagen von Hausautomationssystemen und skizzieren die Probleme aktueller Produkte. Nachfolgend gehen wir der Frage nach, ob es sich bei den übermittelten Informationen um personenbezogene Daten im Sinne des BDSG handelt. Anschließend widmen wir uns den datenschutzrechtlichen Folgen und ziehen ein kurzes Fazit.

2. Technische Grundlagen

Da die Technologie von Hausautomationssystemen relativ jung ist und sich für viele Komponenten noch kein Standard etabliert hat, ist die Palette an Produkten breit gestreut. Die angebotenen Systeme unterscheiden sich in vielen Aspekten – so gibt es kabelgebundene und kabellose Systeme oder solche mit bzw. ohne zentrale Steuerungseinheit. Diese Arbeit behandelt die Eigenschaften von Hausautomationslösungen mit Cloud-Anbindung, welche im Folgenden erläutert sind.

Für den Nutzer hat die Anbindung an das Internetangebot des Herstellers im Wesentlichen zwei Vorteile. Zum einen wird die Konfiguration des Fernzugriffs erleichtert; zum anderen kann der Cloud-Anbieter Informationen bereitstellen, die dem System sonst nicht zugänglich wären.

Will ein Nutzer über das Internet auf Geräte in seinem eigenen Haushalt zugreifen, steht er zunächst vor zwei Problemen. Die IP-Adresse, unter der das Heimnetz erreichbar ist, ist meist nicht statisch, sondern ändert sich je nach Internetanbieter meist nach einer gewissen Zeit (in der Regel einmal am Tag). Dieses Problem lässt sich durch die Verwendung eines *Dynamic DNS*-Anbieters umgehen. Hierbei meldet der Router (oder ein anderes Gerät) nach dem Wechsel die neue Adresse an einen Server, welcher dann den Eintrag für eine dem Nutzer zugeordnete Domain entsprechend aktualisiert. Unter der Domain (z.B. heimnetz-michael-mustermann.de) ist das Heimnetz also ständig verfügbar. Das zweite Problem stellt die *Network Address Translation* des Routers dar. Da sich hinter der IP-Adresse des Heimnetzes unter Umständen mehrere Geräte befinden, muss der Nutzer konfigurieren, wie diese erreicht werden können. Gängige Router lassen eine Konfiguration zu, so dass Verbindungen aus dem Internet auf einen Port an ein bestimmtes Gerät weitergeleitet werden. So kann beispielsweise das Webinterface der zentralen Steuereinheit aus dem Internet bedient werden.

Beide Probleme lassen sich mit einer entsprechenden Konfiguration lösen, die jedoch einen Aufwand für den Nutzer bedeutet. Aus diesem Grund bieten Hersteller inzwischen oft Internetportale[1][2], auf denen sich sowohl die Geräte im Haushalt als auch mobile Geräte anmelden können. Die gesamte Kommunikation wird somit über den Anbieter geleitet, die genannten Probleme vermieden. Darüber hinaus werden erweiterte Funktionen einfach nutzbar gemacht, wie z.B. Benachrichtigungen per E-Mail/SMS, sollte ein Rauchmelder Alarm auslösen oder ein Einbruch festgestellt werden.

Der zweite Vorteil für den Anwender liegt in den Informationen, die der Cloud-Anbieter dem System zur Verfügung stellen kann. So nutzen einige Anbieter Cloud-Services, um aufwendige Berechnungen durchzuführen, die auf einzelnen Geräten nicht möglich wären[3], während andere Wetterdaten aus dem Internet herunterladen und für Automationsregeln nutzbar machen[4]. In einigen Fällen werden Informationen aggregiert und den Nutzern wieder zur Verfügung gestellt[5].

Um die Vorteile nutzen zu können, müssen die Daten von den Geräten der Anwender zum Anbieter übertragen und dort vorgehalten werden. Dies setzt Vertrauen in den Anbieter voraus, da dieser uneingeschränkten Zugriff auf Messdaten und sogar Steuerungen hat.

---

[1] https://www.meine-homematic.de/, abgerufen am 10.1.2014.
[2] https://ninjablocks.com/#mobile/, abgerufen am 10.1.2014.
[3] https://nest.com/support/article/What-is-Auto-Tune, abgerufen am 10.1.2014.
[4] http://www.loxone.com/dede/produkte/miniserver/miniserver.html, abgerufen am 10.1.2014.
[5] https://www.netatmo.com/de-DE/weathermap sowie http://worldcup.netatmo.com/de/, abgerufen am 10.1.2014.

3. Gefahren und Probleme aktueller Systeme

Bei der Sicherheit aktueller Hausautomationssysteme kommt es immer wieder zu Problemen. Die Hersteller konzentrieren sich meist auf die oben genannten Probleme der Erreichbarkeit und andere grundlegende Funktionalitäten, bei nicht essentiellen Merkmalen wie Verschlüsselung oder Zugriffskontrolle treten häufig Implementierungsfehler auf. Diese können mitunter sogar dazu führen, dass Unbefugte Zutritt zum Haus oder zur Wohnung erhalten[6]. Für die Sicherheit der Fernzugriffsschnittstellen und für die Authentifizierung sicherheitskritischer Geräte (z.B. Türschlösser) existieren jedoch Protokolle, welche in der Regel umgesetzt werden und adäquaten Schutz bieten.

Eine weitere Gefahr besteht darin, dass bestimmte Angriffe bei der Entwicklung der Systeme unberücksichtigt bleiben und somit erst gar keine entsprechenden Schutzmechanismen umgesetzt werden. Die Kommunikation innerhalb eines Hausautomationsnetzwerks wird i.d.R. nicht verschlüsselt. Ein Angreifer kann so Datenverkehr von außen abfangen und Verhaltensprofile über die Bewohner erstellen. Dass dies praktisch möglich ist und dass auch Verschlüsselung nicht vollständig gegen diese Art von Angriffen schützen kann, wurde in der jüngeren Vergangenheit gezeigt[7].

Die Gefährdung geht aber nicht nur von Angreifern aus, die den Funkverkehr vor Ort mitschneiden. Bietet ein System eine Cloud-Anbindung an, so kann der Betreiber alle übermittelten Daten protokollieren und ebenso genaue Profile über die Nutzer erstellen. Hier besteht also erhebliches Missbrauchspotential. Auch für einen aufrichtigen Betreiber könnte dies ein Problem darstellen, falls deshalb die Verarbeitung rechtlich eingeschränkt wird – eine Fragestellung, die wir in den nächsten Abschnitten untersuchen. Die Tatsache, dass die Daten vieler Nutzer im System des Betreibers vorhanden sind, macht letzteres außerdem zu einem attraktiven Ziel für Angriffe aus dem Netz.

4. Personenbezug erhobener Daten

Aus rechtlicher Sicht stellt sich zunächst die Frage nach dem Personenbezug erhobener Daten (und somit nach der Anwendbarkeit des Datenschutzrechts). Personenbezogene Daten sind nach §3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.

Einzelangaben sind solche Angaben, die sich auf eine einzelne Person – im Gegensatz zu einer Personengruppe – beziehen[8]. Daten wie die Temperatur in einer Wohnung oder Zeitpunkte, zu denen die Wohnung betreten wird, beziehen sich zunächst auf alle Personen, die dort wohnen oder sich aufhalten. In Deutschland rechnet das Statistische Bundesamt jedoch damit, dass 40% aller Haushalte Einpersonenhaushalte sind[9]. Auch, wenn in einem Haushalt mehrere Personen leben, können die Angaben über den Haushalt als Ganzes auf die Einzelperson (namentlich die Person, die beim Anbieter des Hausautomationssystems registriert ist) „durchschlagen“[10]: Ergibt sich aus den Daten beispielsweise, dass sich gerade niemand in der Wohnung aufhält, betrifft diese Angabe jeden Bewohner. Die gelegentliche Anwesenheit von Besuchern kann ebenfalls nichts daran ändern, dass erhobene Daten dem Vertragspartner des Hausautomations-Anbieters zugeordnet werden – sie führt lediglich zu einer gewisse Fehlerwahrscheinlichkeit dieser Zuordnung. Eine ähnliche Konstellation findet sich bei der Frage, ob eine IP-Adresse, die ein Internetanbieter einem Privatkunden zuweist,

---

[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8868, abgerufen am 10.1.2014.

[7] *Möllers/Seitz/Hellmann/Sorge*, Short paper: Extrapolation and Prediction of User Behaviour from Wireless Home Automation Communication, Proc. of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’14), Association for Computing Machinery (ACM), S. 195–200 (2014).

[8] *Gola/Schomerus*, BDSG, 11. Auflage (2012), §3 Rn. 3.

[9] *Statistisches Bundesamt*: Wirtschaftsrechnungen, Fachserie 15, Sonderheft 1, Wiesbaden (2013), Stand: 1.1.13, S.19.

[10] So die Formulierung bei *Gola/Schomerus*, §3 Rn. 3.

ein personenbezogenes Datum ist: Die Einordnung als Einzelangabe wird in der Literatur – unabhängig davon, ob der Personenbezug letztlich angenommen oder abgelehnt wird – nicht als problematisch angesehen, obwohl ein PC ebenfalls von mehreren Personen genutzt werden kann.

Die Einzelangaben betreffen auch „persönliche oder sachliche Verhältnisse“ von Personen. Dieser Begriff ist umfassend zu verstehen[11]; insbesondere umfassen „sachliche Verhältnisse“ Angaben über Sachverhalte, die mit der betreffenden Person in Beziehung gebracht werden können[12]. Angaben, die ein Hausautomationssystem erhebt, wie die Temperatur in der Wohnung des Betroffenen, fallen unproblematisch unter diesen Begriff.

Schließlich ist die Person in aller Regel auch bestimmt, da beim Anbieter des Hausautomationssystems namentlich registriert. Selbst, wenn nur eine E-Mail-Adresse vorliegt, ermöglicht aber auch diese in vielen Fällen die Identifikation des Betroffenen. Als Zwischenfazit lässt sich also festhalten, dass der Personenbezug der erhobenen Daten im Regelfall zu bejahen ist.

Im nächsten Schritt soll geprüft werden, ob die Daten auch zu den „besonderen Arten personenbezogener Daten“ gehören – in §3 Abs. 9 BDSG definiert als „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“ Auf den ersten Blick scheint der Bezug zu Hausautomationssystemen fernliegend, und in der Tat sind wohl nur in Einzelfällen Rückschlüsse möglich: Verlässt ein Nutzer die Wohnung immer 20 Minuten vor der katholischen Sonntagsmesse und kehrt 20 Minuten nach deren Ende zurück, ist er mit hoher Wahrscheinlichkeit ein gläubiger Katholik; verlässt er die Wohnung eine Woche lang nicht, deutet dies auf eine Erkrankung hin. Würde andererseits jedes Datum, das potentiell – und sei es nur mit kleiner Wahrscheinlichkeit – auf Gesundheit und Religion zurückschließen lässt, zu den „besonderen Arten personenbezogener Daten“ gezählt, würde dies zu erheblichen praktischen Problemen führen; so wird in der Literatur[13] zum Beispiel auf islamische Vornamen hingewiesen, die ebenfalls Rückschlüsse auf die Religion erlauben. Eine Lösung besteht darin, Daten, die solche Rückschlüsse ermöglichen, nur dann als personenbezogen einzuordnen, wenn eine entsprechende Auswertungsabsicht besteht[14]. Dies ist zwar unbefriedigend, da der rechtliche Charakter von Daten sich somit ohne Verknüpfung mit Zusatzinformationen im Nachhinein ändern kann; eine rein an den theoretisch möglichen Rückschlüssen orientierte Auslegung würde aber in so vielen Bereichen zum Entstehen „besonderer Arten personenbezogener Daten“ führen, dass dies durch den Gesetzgeber kaum gewollt sein kann. Zusammenfassend lässt sich also festhalten, dass die von Hausautomationssystemen erhobenen Daten in der Regel nicht als besondere Arten personenbezogener Daten zu betrachten sind.

5. Datenschutzrechtliche Betrachtung

Das Telemediengesetz (TMG) gilt nach § 1 Abs. 1 „für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien)“. Der Begriff der elektronischen Informations- und Kommunikationsdienste wird weit ausgelegt und beinhaltet „praktisch also jeden Online-Auftritt“[15]. Die reine Signalübertragung über TK-Netze ist von der Definition ausgenommen; Cloud-Dienste für die Hausautomation erfordern zwar Telekommunikation, stellen diese jedoch nicht selbst bereit.

---

[11] *Gola/Schomerus*, §3 Rn. 5.
[12] *Gola/Schomerus*, §3 Rn. 7.
[13] *Gola/Schomerus*, §3 Rn. 56a.
[14] *Gola/Schomerus*, a.a.O.
[15] *Müller-Broich*, Telemediengesetz, 1. Auflage, Nomos, Baden-Baden 2012, §1 Rn. 6.

Genauer betrachtet werden muss aber, welche Aspekte genau unter die Regelungen des TMG fallen. Zunächst findet eine Datenübertragung vom Haushalt des Nutzers zum Anbieter statt. Das bedeutet aber nicht, dass der Nutzer einen Informationsdienst bereitstellt und somit zum Diensteanbieter im Sinne des TMG wird; es fehlt hier schon an der Erbringung eines Dienstes[16].

Der Cloud-Dienst hingegen ist ein elektronische Informationsdienst, da Informationen aufbereitet und dem Nutzer angezeigt sowie darauf aufbauende Dienste angeboten werden; dass die zugrundeliegenden Daten ursprünglich (teilweise) aus dem Haushalt des Nutzers selbst stammen, spielt dafür keine Rolle. Für den Cloud-Dienst ist das TMG also unproblematisch anwendbar; das gilt auch für die Regelungen zum Datenschutz (§§ 11 bis 15a), da keiner der Ausschlussgründe des §11 Abs. 1 vorliegt. Zu beachten ist indes, *was* das TMG regelt: Für die Nutzung des Informationsdienstes selbst (also beispielsweise den Aufruf einer Website, auf der Daten über Zimmertemperaturen und Heizungseinstellungen dargestellt sind) und die *dafür* notwendige Datenverarbeitung gilt das TMG. Für die eigentlichen Inhalte ist dies aber nicht der Fall. In der Literatur wird mitunter der Begriff des „Schichtenmodells" verwendet[17]. Vereinfacht dargestellt[18], betrifft die unterste Schicht, Telekommunikation, den Transport von Daten und ist im Telekommunikationsgesetz (TKG) geregelt. Regelungen zu elektronischen Kommunikations- und Informationsdiensten (mittlere Schicht) finden sich im TMG, während der Umgang mit Inhaltsdaten (obere Schicht) im BDSG geregelt ist. Dieses Schichtenmodell ist zwar inspiriert durch Schichtenmodelle der Kommunikation aus der Informatik, insbesondere das ISO/OSI-Schichtenmodell, sollte aber nicht damit gleichgesetzt werden.

Innerhalb des BDSG ergeben sich auf den ersten Blick keine besonderen Probleme: Der Anbieter geht mit den Daten „als Mittel für die Erfüllung eigener Geschäftszwecke" um, indem er einen kommerziellen Cloud-Dienst anbietet. Nach §28 Abs. 1 Satz 1 Nr. 1 ist das „Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung" somit zulässig, soweit es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Da die Diensterbringung aufgrund eines Vertrags mit dem Nutzer erfolgt, ist sie unproblematisch möglich. Der Vertragszweck kann dabei auch weitgehende Auswertungen beinhalten, beispielsweise die Generierung von Empfehlungen für das Heiz- und Lüftverhalten anhand von Innentemperaturen und Wetterverhältnissen, so dass das BDSG nicht etwa als Innovationshemmnis wirkt. Für anderweitigen bzw. über das zur Diensterbringung notwendige Maß hinausgehenden Umgang mit den Daten ergeben sich für die Hausautomation keine Besonderheiten. Aufgrund des Zweckbindungsgrundsatzes ist die anderweitige Verarbeitung und Nutzung aber nur eingeschränkt möglich. Erlaubt ist z.B. die Übermittlung für Forschungszwecke nach §28 Abs. 2 Nr. 3.

Tatsächlich problematisch ist allerdings ein anderer Aspekt: Vertragspartner des Cloud-Dienstleisters wird in der Regel lediglich ein Mitglied des betreffenden Haushalts sein, wohingegen die erhobenen Daten sich auch auf andere Personen beziehen können. Der Cloud-Dienstleister hat dann kein „rechtsgeschäftliches Schuldverhältnis mit dem Betroffenen", womit die Datenverarbeitung unzulässig werden könnte. Bräuchle[19] weist in einem verwandten Kontext auf das Problem der „innerfamiliären Überwachung" hin: Bei Smart-Meter-Systemen, die die aktuelle Nutzung elektrischer Energie durch einen Haushalt in kurzen Zeitabständen an einen Messstellenbetreiber übermitteln, besteht ebenfalls die Möglichkeit, dass Vertragspartner auf diese Daten zugreifen, sie sich aber

---

[16] Auch die in der Gesetzesbegründung aufgeführten Regelbeispiele für Telemedien sind ausschließlich solche, bei denen übermittelte Informationen einen Mehrwert für den Nutzer darstellen, vgl. Deutscher Bundestag, Drucksache 16/3078 vom 23.10.2006, Seite 13.

[17] So bei *Ernst,* Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, S. 1917, 1918; zur früheren Rechtslage *Schaar*: Datenschutzrechtliche Einwilligung im Internet, MMR 2001, S. 644, 645.

[18] Beispielsweise gilt das BDSG subsidiär auch für Telemedien.

[19] *Bräuchle*: Die datenschutzrechtliche Einwilligung in Smart Metering Systemen – Kollisionslagen zwischen Datenschutz- und Energiewirtschaftsrecht, in: Plödereder/Grunske/Schmeider/Ull (Hrsg.): Informatik 2014, Proceedings, Lecture Notes in Informatics Band P-232,: http://subs.emis.de/LNI/Proceedings/Proceedings232.html, S. 515, 521f.

(auch) auf andere Personen beziehen. Der abwesende Vertragspartner kann somit das genaue Stromnutzungsprofil – oder im Fall von Hausautomationssystemen beispielsweise das Lüftungsverhalten – seines Mitbewohners auch überwachen, während er selbst verreist ist.

Ausgehend von einem relativen Personenbezugsbegriff[20] kann im vorliegenden Fall unterschieden werden: Für den Anbieter gibt es i.d.R. keine Anknüpfungspunkte, Daten anderen Personen als seinem Vertragspartner zuzuordnen; da er also keine (für ihn) personenbezogenen Daten Dritter hat, schränkt das BDSG die Datenverarbeitung insofern auch nicht ein. Kennt der Anbieter aber andere Bewohner – etwa, wenn Familienmitglieder eigene, personalisierte Zugänge zu dem System erhalten–, ist eine Einwilligung gemäß §4a Abs. 1 BDSG erforderlich. Gleiches gilt, wenn man – entgegen unserer Auffassung – einen absoluten Personenbezugsbegriff zugrunde legt[21]. Für den Vertragspartner, der die Identität der im Haus Anwesenden kennt, fällt die Datenverarbeitung aber unter die Ausnahme des §1 Abs. 2 Nr. 3 BDSG, wonach die Datenverarbeitung „ausschließlich für persönliche oder familiäre Tätigkeiten“ vom BDSG nicht erfasst wird[22]. Eine legale Nutzung von Cloud-Diensten für die Hausautomation ist also auch in Mehrpersonenhaushalten möglich.

6. Fazit

Hausautomationssysteme können den Wohnkomfort erheblich steigern und zu einer effizienteren Energienutzung beitragen, beinhalten aber auch ein neues Risiko für den Datenschutz. So können Angreifer vor Ort können bei unzureichender Absicherung genaue Profile der Nutzer anlegen; die Nutzung von Cloud-Diensten der Anbieter führt ebenfalls zu einer Preisgabe personenbezogener Daten. Nach gegenwärtigem Recht ist unseres Erachtens eine datenschutzkonforme Nutzung solcher Dienste dennoch möglich; die Gefahr innerfamiliärer Überwachung ist damit aber nicht gebannt und wird in der Zukunft vermutlich an Bedeutung gewinnen.

7. Literatur

Bräuchle, Thomas, Die datenschutzrechtliche Einwilligung in Smart Metering Systemen – Kollisionslagen zwischen Datenschutz- und Energiewirtschaftsrecht, in: Plödereder/Grunske/Schmeider/Ull (Hrsg.): Informatik 2014, Proceedings, Lecture Notes in Informatics Band P-232, http://subs.emis.de/LNI/Proceedings/Proceedings232.html, S. 515ff. (2014).

Ernst, Stefan, Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem, Neue Juristische Online Zeitschrift, S. 1917ff. (2010).

Gola, Peter/Schomerus, Rudolf, BDSG, 11. Auflage (2012).

Kühling, Jürgen/Klar, Manuel: Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, Neue Juristische Wochenschrift, S. 3611 (2013).

Möllers, Frederik/Seitz, Sebastian/Hellmann, Andreas/Sorge, Christoph, Extrapolation and Prediction of User Behaviour from Wireless Home Automation Communication, Proc. of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’14), Association for Computing Machinery (ACM), S. 195–200 (2014).

Müller-Broich, Jan, Telemediengesetz, 1. Auflage, Nomos, Baden-Baden (2012).

Pahlen-Brandt: Zur Personenbezogenheit von IP-Adressen, Kommunikation und Recht, S. 288 (2008).

Schaar, Peter: Datenschutzrechtliche Einwilligung im Internet, MultiMedia und Recht, S. 644ff. (2001).

Statistisches Bundesamt, Wirtschaftsrechnungen, Fachserie 15, Sonderheft 1, Wiesbaden (2013), Stand: 1.1.2013.

[20] Nach diesem Verständnis sind Daten nur personenbezogen, wenn die verantwortliche Stelle den Personenbezug herstellen kann (und nicht etwa auch, wenn beliebige Dritte das können). In der Literatur ist dies herrschende Meinung (vgl. *Kühling/Klar*, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, S. 3611, 3615, mit weiteren Nachweisen).

[21] So z.B. *Pahlen-Brandt*: Zur Personenbezogenheit von IP-Adressen, KuR 2008, S. 288. Der BGH hat die Frage mittlerweile dem EuGH vorgelegt (Beschluss vom 28.10.2014, Az. VI ZR 135/13).

[22] Anderer Auffassung: *Bräuchle*, S. 522 (mit weiteren Nachweisen), der auf die im Vergleich zu den üblicherweise von §1 Abs. 2 Nr. 3 BDSG erfassten Fällen höhere Bedrohung der informationellen Selbstbestimmung hinweist.