Gefahren im gläsernen Eigenheim

Die *Smart-Home*-Technologie als Herausforderung für das Datenschutzrecht

*Philipp Gispert**

Vernetzte Eigenheime bergen die Gefahr, dass höchstpersönliche Daten an den Anbieter und Dritte gelangen. Damit zwingen sie zum Umdenken vor allem in Bezug auf die datenschutzrechtliche Einwilligung und die Handhabe des sog. Koppelungsverbots, wie der Beitrag zeigt.

I. Einleitung

Über die letzten Jahre hinweg sind wir vor allem eines geworden: vernetzt. Kein Tag vergeht, an dem wir nicht per Smartphone auf soziale Netzwerke zugreifen, am Tablet E-Mails schreiben oder online Musik und Filme streamen. Die Möglichkeiten des digitalen Zeitalters sind dabei noch lange nicht ausgeschöpft, und so sollen nach dem Willen zahlreicher Hersteller immer mehr Bereiche unseres Lebens „smart" werden. Eines der ambitioniertesten Projekte des Smart Life stellt dabei das sogenannte *Smart Home* dar, das vernetzte Eigenheim, in dem Haushaltsgeräte wie Heizungen nicht nur „mitdenken", sondern auch miteinander kommunizieren und per Fernzugriff steuerbar sind. Dieser Beitrag widmet sich der Frage, ob auch das Datenschutzrecht mit der rasanten Entwicklung neuer Technologien Schritt halten kann.

II. Begriff und Funktionsweise des Smart Home

1. Begriff

Begonnen werden soll mit einer Vorstellung des Untersuchungsgegenstandes. Da es sich bei der *Smart-Home*-Technologie um einen sehr jungen Trend handelt, hat sich noch keine einheitliche Definition hervorgetan. Im Jahresbericht des Bundesdatenschutzbeauftragten aus dem Jahr 2013 wird *Smart Home* weit als „Oberbegriff für technische Verfahren und Systeme in Wohnräumen" verstanden,[1] eine intuitive Erfassung anhand von Produktbeispielen scheint daher zur Veranschaulichung geeignet.

Die Produktpalette von *Smart-Home*-Angeboten umfasst dabei gänzlich neue Geräte wie zum Beispiel Sensoren für Türen und Fenster zur Erkennung eines Einbruchs, intelligente Kühlschränke mit Vorratsanzeige und der Möglichkeit der automatischen Nachbestellung von Lebensmitteln[2] oder vernetzte Rauchmelder, die im Falle eines Brandes den Hausbewohner per Textnachricht auf seinem Smartphone vor der drohenden Gefahr warnen. Daneben werden auch Produkte angeboten, welche mit alten Geräten kombiniert werden können, um umfangreiche Neuinstallationen zu vermeiden. Dazu gehören etwa aufschraubbare Heizkörperthermostate mit Feuchtigkeitsmessung, Zwischenstecker zur Verringerung des Stromverbrauchs und Unterputz-Lichtschalter zur Fernsteuerung der Hausbeleuchtung. Die Einrichtung eines *Smart Home* beginnt meist mit dem Kauf eines sog. *Starter Kit*. Dieses enthält neben den einzelnen Geräten eine Basisstation, über welche – ähnlich wie bei einem Internet-Router – die gekauften Produkte gesteuert werden können. Einhergehend mit der zunehmenden Verbreitung von Smartphones soll das auf diese Weise vernetzte Eigenheim per Fernzugriff durch den Nutzer steuerbar sein, sodass dieser auf dem Nachhauseweg beispielsweise das Badezimmer vorheizen oder den Inhalt

* *Der Autor ist Referendar bei der Staatsanwaltschaft München I. Er dankt Wiss. Mit. Thomas Hofer (akad. Dir. am RIZ der Juristischen Fakultät der LMU München) für die Durchsicht des Beitrags und die wertvollen Hinweise und Anregungen.*

1 *Berliner Beauftragter für Datenschutz und Informationsfreiheit*, Datenschutz und Informationsfreiheit-Bericht 2013, 2013, 44.

2 Vernetzte Kühlschränke sind bislang nur geplant.

seines Kühlschranks überprüfen kann.[3] Mit einem Durchbruch auf dem Massenmarkt wird für das Jahr 2017 gerechnet.[4]

2. Funktionsweise und anfallende Daten

Ist ein *Smart Home* erst einmal eingerichtet, stellt sich die Frage nach dessen grundlegender Funktionsweise. Diese ist je nach Anbieter leicht verschieden, folgt jedoch zumeist folgendem Aufbau: Die einzelnen Geräte (Fenstersensoren, Rauchmelder usw.) kommunizieren mit der Basisstation des *Smart Home*, an welcher alle Informationen zusammenlaufen. Diese wiederum ist – sofern eine Fernsteuerung durch den Nutzer möglich sein soll – mit dem Internet-Router des Hauses verbunden und speichert die Daten der einzelnen Geräte wie z.B. die aktuelle Raumtemperatur im Schlafzimmer auf einem Server des Anbieters. Mit seinem internetfähigen Smartphone kann der Nutzer nun von unterwegs – oft mittels einer App, ansonsten über den Internet-Browser – auf diesen Server zugreifen und so die aktuellen Daten seines *Smart Home* einsehen und verändern, indem er beispielsweise schon auf dem Nachhauseweg die Heizung aufdreht.[5]

Bei der typischen *Smart-Home*-Nutzung können unterschiedliche Arten von Daten anfallen bzw. theoretisch erhoben werden. Dies beginnt bereits beim Bestellvorgang über das Internet, bei dem der Kunde seine Adressdaten für die Lieferung und die für die gewählte Zahlungsart notwendigen Informationen dem Anbieter übermitteln muss. Im *Smart Home* selbst können bei der Nutzung unterschiedliche Arten von Stamm- und Bewegungsdaten anfallen – anzumerken ist hierbei, dass die konkret anfallenden Daten je nach Anbieter und gewählten Produkten unterschiedlich sein werden und pauschalisierte Aussagen im Folgenden daher nur unter Vorbehalt getroffen werden können. Im Falle einer Heizung beispielsweise würden zu den Stammdaten, gleichsam den konstanten Grundinformationen, etwa der Raum und die Bezeichnung der Heizung gehören, während die (veränderlichen) Bewegungsdaten Aufschluss darüber gäben, welche durch die Sensoren gemessene Raumtemperatur zu welcher Zeit vorherrschte.[6] Je nach Smart-Home-Produkt würden unterschiedliche Daten anfallen, im Falle eines vernetzten Kühlschranks beispielsweise sein konkreter Inhalt, im Falle eines Smart TV die Fernsehvorlieben der Zuschauer. Ob die Daten im Einzelfall dann auch tatsächlich erhoben und verarbeitet werden, ist für den durchschnittlichen Nutzer nicht erkennbar.

III. Gefahren eines Smart Home

Derartige technische Weiterentwicklungen im eigenen Zuhause bergen neben den aufgezeigten Annehmlichkeiten auch Risiken, deren Darstellung einer datenschutzrechtlichen Bewertung vorgeschaltet sein soll. Gefahren können sich dabei sowohl durch die Einwirkung Dritter als auch im Wirkungskreis der verantwortlichen Stelle iSd § 3 Abs. 7 BDSG[7] ergeben.

1. Drohende Gefahren durch die Einwirkung Dritter

Im digitalen Zeitalter wird Cyberkriminalität zu einer stetig wachsenden Bedrohung, wie zuletzt der verheerende Hackerangriff auf die Filmproduktionsfirma Sony Pictures zeigte.[8] Mit jeder weiteren Cyberattacke wird dabei deutlich, dass unangreifbare Nerzwerke nicht existieren, sondern ein erfolgreicher Angriff meist nur eine Frage der Zeit und des kriminellem Aufwands ist. Gleiches gilt auch für das vernetzte Eigenheim, denn ist ein Hacker erst einmal in ein *Smart-Home*-Netzwerk eingedrungen, kann er die verbundenen Geräte nach Belieben steuern. Welche Schäden dabei entstehen können, richtet sich hauptsächlich nach der Art des konkret attackierten Geräts und der Absicht des Angreifers. Dabei ist nicht nur an weitgehend harmlosere Spielereien wie das plötzliche Ein- und Ausschalten der Beleuchtung zu denken, sondern vor allem an Einbruchserleichterungen durch Auswertung von z.B. Kameradaten[9] bis hin zu extremen Angriffen wie der Beschädigung von Leitungen durch drastisches Herunterregeln der Temperatur[10] sowie das Auslösen eines Brandes durch einen Angriff auf Herd und Rauchmelder.[11]

Diese Szenarien sind allerdings nur realisierbar, wenn sich ein Dritter zumindest zu einem gewissen Grad Zugang zu einem *Smart-Home*-System verschaffen kann. Eine im Jahr 2014 durchgeführte Sicherheitsstudie kommt zu dem Ergebnis, dass Sicherheitslücken bei *Smart-Home*-Angeboten längst keine Seltenheit sind und im schlimmsten Fall sogar eine Online-Manipulation ermöglichen.[12] Moderne *Smart-Home*-Lösungen, die einen Fernzugriff des Nutzers etwa über entsprechende *Smart-Home*-Apps zulassen und sich externer Speichermöglichkeiten („Cloud-Dienste") bedienen, sind angesichts ihrer Internet-Anbindung dabei besonders gefährdet. Hier sind Zugriffe auf etwaige Cloud-Da-

3 *Strese/Seidel/Knape/Botthof*, Smart Home in Deutschland – Untersuchung für das Bundeswirtschaftsministerium 2010, S. 11, abrufbar unter: http://www.iit-berlin.de/de/publikationen/smart-home-in-deutschland (Stand: 15.03.2015).

4 *Strese et al.* (Fn. 3), 12.

5 Bildlich dargestellt auf: http://www.somfy.de/home/produkte/produkte/io-homecontrol-tahoma/smart-home.html (Stand: 15.03.2015).

6 http://winfwiki.wi-fom.de/index.php/Smart_Living_und_Datenschutz#Daten_im_Smart_Home_.28Interne_Datenerfassung.2 (Stand: 15.03.2015).

7 Bundesdatenschutzgesetz vom 14. Januar 2003 (BGBl. I 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14. August 2009 (BGBl. I 2814).

8 Vgl. http://www.spiegel.de/netzwelt/web/sony-hack-james-bond-drehbuch-geleakt-weihnachtsgeschenk-angedroht-a-1008501.html (Stand: 15.03.2015).

9 *Berliner Beauftragter für Datenschutz und Informationsfreiheit* (Fn. 1), 48.

10 *Schiefer, Michael; Lösche, Ulf; Morgenstern, Maik,* AV-Test-Studie – 7 Smart-Home-Starter-Kits im Sicherheits-Test, Version 1.21, S. 41, abrufbar unter http://www.av-test.org/fileadmin/pdf/av-test_2014-04_smart_home_deutsch.pdf (Stand: 15.03.2015).

11 *Berliner Beauftragter für Datenschutz und Informationsfreiheit* (Fn. 1), 47 f.

12 *Schiefer et al.* (Fn. 10), 2 ff.

ten[13] ebenso denkbar wie ein Abfangen der Login-Daten und deren Nutzung für eigene Zwecke.[14] Ausführliche Hacking-Anleitungen und Beispiele für gehackte *Smart Home*s finden sich bereits im Internet.[15]

2. Drohende Gefahren im Verantwortungsbereich der verantwortlichen Stelle

Richtet man seinen Blick auf einen denkbaren Angreifer von außen, vergisst man leicht, dass mit dem Anbieter der *Smart-Home*-Lösung bereits jemand existiert, der einfachen Zugriff auf zahlreiche Daten des Nutzers hat. Unterstellt man, dass ein Anbieter sämtliche in einem *Smart Home* anfallenden Daten seiner Kunden sammelt, so würde ihm dies weitreichende Einblicke in deren Vorlieben ermöglichen, die sich beispielsweise in Nutzerprofilen zusammenfassen ließen.[16] Smarte Kühlschränke könnten die Ernährungsgewohnheiten der Hausbewohner sammeln und an Werbepartner des Anbieters weiterleiten, während ein vernetzter Fernseher das Fernsehverhalten dokumentieren könnte – von der Auswertung der Daten von Überwachungskameras ganz zu schweigen.[17] Diese Daten könnten einerseits dem Anbieter selbst zugutekommen oder im Falle eines Verkaufs oder eines Angriffs auf die Server des Anbieters in die Hände Dritter gelangen. Darüber hinaus ist seit der NSA-Affäre bekannt, dass auch Geheimdienste großes Interesse an nahezu allen anfallenden Daten über eine Person haben, um gerade durch die Verknüpfung mehrerer Quellen möglichst detaillierte Profile erstellen zu können.

Diese Szenarien sind dabei keineswegs unrealistisch, sondern fußen auf bereits mehreren besorgniserregenden Vorfällen in der jungen Vergangenheit des Smart Life. So wurde das Beispiel der Smart TVs von LG bekannt, die bei jedem Wechsel des Fernsehsenders eine Nachricht an den Hersteller versandten, in der die ID des Gerätes und der eingeschaltete Sender enthalten waren.[18] Konkurrent Samsung warnte gar davor, keine vertraulichen Gespräche vor dem (mithörenden) Fernseher zu führen.[19]

Bedacht werden muss in diesem Zusammenhang auch, dass das vernetzte Eigenheim erst in seiner Anfangsphase steckt. Danach sind vor allem Entwicklungen im Zusammenhang mit dem Gesundheitswesen denkbar, beispielsweise mittels Internet-Sprechstunden, Transfer von im Zuhause gemessenen Bio-Daten wie Körpergewicht und Puls und deren Speicherung in einer Gesundheitsdatenbank.[20] Derartige Gesundheitsinformationen wären etwa für Versicherungen interessant und sollten aufgrund ihrer besonderen Schutzwürdigkeit, wie sie auch in ihrer Einstufung als besondere personenbezogene Daten in § 3 Abs. 9 BDSG zum Ausdruck kommt, nicht in die Hände Dritter geraten. Mit der zunehmenden Zahl an sensiblen Informationen steigt auch deren Attraktivität für die Hersteller selbst, die so noch mehr über ihre Kunden erfahren und die gewonnenen Informationen im schlimmsten Fall missbräuchlich verwenden und beispielsweise verkaufen können. Eine generelle Aussage darüber, ob eine solche Auswertung bereits tatsächlich, mit oder ohne Wissen der Kunden, stattfindet, wäre jedoch rein spekulativ.

IV. Datenschutzrechtliche Beurteilung

Die vorausgegangenen Beispiele machen deutlich, dass ein *Smart Home* nicht nur durch technische Sicherungsvorrichtungen, sondern auch durch Gesetze vor unbefugten Zugriffen und Datenmissbrauch gerade auch durch die Anbieter geschützt werden muss. Wie die derzeitige Schutzlage zu bewerten ist, soll im Folgenden untersucht werden.

1. Vorgeschaltete Fragestellungen

a) Grundsätze der Datenerhebung

Unabhängig von Art und Erhebungsweise der Daten haben sich in der Vergangenheit allgemeine Grundsätze hinsichtlich des Umgangs mit Daten herausgebildet, die stets Beachtung finden müssen und deshalb in einer rechtlichen Analyse zuvorderst genannt werden müssen. Den verfassungsrechtlichen Grundstein legte das Bundesverfassungsgericht mit der Entwicklung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG, das dem Umstand Rechnung tragen soll, dass „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person technisch gesehen unbegrenzt speicherbar und jederzeit [...] abrufbar sind."[21] Der Einzelne soll damit grundsätzlich selbst darüber entscheiden können, welche Daten er von sich preisgibt.[22] Eine Ausstrahlung dieses Grundrechts auf Privatrechtsverhältnisse scheint angesichts der zunehmenden Technisierung des Alltags unumgänglich. Weitere allgemeine Grundsätze finden sich im Datenschutzrecht etwa im Grundsatz der Zweckbestimmung, wie er in § 12 Abs. 2 TMG[23] und auch §§ 28-32 BDSG zu finden ist und welcher fordert, dass erhobene Daten immer nur für einen definierten Zweck erhoben und genutzt werden dürfen. Darüber hinaus gelten für den Umgang mit Daten im Allgemeinen nach § 3a BDSG die Gebote der Datenvermeidung und der Datensparsamkeit, wonach so wenig personenbezogene Daten wie möglich zu erheben sind. Erreicht werden soll dies nach dem Gesetzeswortlaut bereits auch durch eine an diese Grundsätze angepassten Verwendung von Datenverarbeitungssystemen,

13 *Straßburg*, Connected Home 06.2014, 26 (28).

14 *Schiefer et al.* (Fn. 10), 41; *Straßburg*, Connected Home 06.2014, 26 (27).

15 Von einem konkreten Verweis auf die entsprechenden Anleitungen wurde abgesehen.

16 *Schiefer et al.* (Fn. 10), 41; *Straßburg*, Connected Home 06.2014, 26 (30).

17 Vgl. dazu EuGH, Rs. C-212/13.

18 Vgl. http://www.chip.de/news/LG-bestaetigt-Smart-TVs-spionieren-Zuschauer-aus_65512912.html (Stand: 15.03.2015).

19 http://www.sueddeutsche.de/digital/aufregung-um-spracherkennung-samsung-hoert-mit-aber-nur-manchmal-1.2341288 (Stand: 15.03.2015)

20 *Strese et al.* (Fn. 3), 38 f.

21 BVerfGE 65, 1 (42).

22 BVerfGE 65, 1 (43).

23 Telemediengesetz vom 26. Februar 2007 (BGBl. I 179), zuletzt geändert durch Art. 1 des Gesetzes vom 31. Mai 2010 (BGBl. I 692).

dem sogenannten Systemdatenschutz.[24]

b) Anwendungsfragen

Richtet man den Blick weg von den Grundsätzen auf die konkret für die *Smart-Home*-Problematik in Betracht kommenden Vorschriften, so müssen in einem nächsten Schritt die zu thematisierenden Gesetze voneinander abgegrenzt werden. Folgt man dem nach Kommunikationsebenen differenzierenden Schichtenmodell, ist das TKG[25] auf den Datentransport und den Telekommunikationsvorgang anwendbar, das TMG auf die Interaktion (bspw. auch die Kontaktaufnahme) zwischen Dienstanbieter und Nutzer, § 1 Abs. 1 TMG, und das BDSG auf die Kommunikation zwischen den beiden Letztgenannten.[26] Im Bereich des *Smart Home* werden vor allem TMG und BDSG von Belang sein, Ersteres etwa in Fällen, in denen Fernsteuerungsdienste wie Apps über das Internet in Anspruch genommen werden. Die konkret im Haus erhobenen Daten sind der Inhaltsebene und damit dem BDSG zuzuordnen und werden den Schwerpunkt der vorliegenden Untersuchung darstellen.

Viele datenschutzrechtliche Normen fordern für ihre Anwendbarkeit das Vorliegen personenbezogener Daten – im Falle des BDSG explizit in § 1 Abs. 2 BDSG –, sodass vorab zu analysieren ist, ob die in einem *Smart Home* anfallenden Daten personenbezogen sind. Dies ist nach der Definition in § 3 Abs. 1 BDSG der Fall, wenn sie Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person darstellen. Einzelangaben sind dabei solche Informationen, die sich auf eine bestimmte natürliche Person beziehen oder geeignet sind, einen Bezug zu ihr herzustellen. Hierbei handelt es sich um einen relativen Begriff des Personenbezugs, da für die Bestimmbarkeit auf die jeweils speichernde Stelle abgestellt werden muss.[27] Diese Stelle, im Falle des *Smart Home* also der Anbieter, kann eine solche Zuordnung alleine schon deshalb vornehmen, weil sie die Status-Informationen der einzelnen Geräte auf ihren Servern für den Fall des Fernzugriffs durch den Nutzer mit dessen Account verknüpfen muss. Das Vorliegen personenbezogener Daten muss bei *Smart-Home*-Anwendungen in Hinblick auf den Kunden daher grundsätzlich bejaht werden.

2. Datenerhebung durch die verantwortliche Stelle

a) Kein Vorliegen der gesetzlichen Erlaubnistatbestände des § 28 Abs. 1 BDSG

Hinsichtlich der im Rahmen einer typischen *Smart-Home*-Nutzung anfallenden Daten, insbesondere der unter II.2. angesprochenen Bewegungsdaten, stellt sich die Frage, ob eine Erhebung und Verwertung durch den Anbieter von § 28 Abs. 1 S. 1 Nr. 1, 2 BDSG erfasst ist. Hintergrund dieser Prüfung ist, dass § 28 BDSG mehrere gesetzliche Erlaubnistatbestände für den Umgang mit Daten durch die verantwortliche Stelle normiert und das Bestehen einer gesetzlichen Erlaubnis gegenüber der Einholung einer expliziten Einwilligung schon alleine deshalb vorzugswürdig ist, weil diese widerrufen werden kann.[28]

Zunächst ist ein Subsumtionsversuch unter die von § 28 Abs. 1 S. 1 Nr. 1 BDSG erfasste Situation anzustellen, wonach u.a. eine Erhebung und Übermittlung personenbezogener Daten zulässig ist, wenn sie zur Durchführung des zwischen Kunde und Anbieter bestehenden Schuldverhältnisses erforderlich ist. Ein *Smart Home* begründet sich nicht nur durch den einmaligen Kauf von intelligenten Produkten, da es gerade von der jederzeitigen Zugriffs- und Steuermöglichkeit des Nutzers leben soll. Das Schuldverhältnis erschöpft sich daher nicht nur in einem Kaufvertrag nach § 433 BGB, sondern umfasst zusätzlich noch die Bereitstellung des Servers, über den der Nutzer die Vorgänge in seinem Zuhause beeinflussen kann. In fast schon bedenklichem Ausmaß wird dabei von den Herstellern verschwiegen, dass die Nutzung der *Smart-Home*-Apps meist nur für einen Zeitraum von zwei Jahren kostenfrei ist, bevor zusätzliche Gebühren fällig werden.[29] Somit besteht zwar ein über den Kauf hinausgehendes Rechtsverhältnis zwischen Kunde und Anbieter, allerdings ist nicht ersichtlich, inwiefern die dauerhafte Speicherung von Bewegungsdaten hierfür erforderlich wäre, da die Bereitstellung der Server – anders als etwa bei einem volumengebundenen Internet-Tarif – unabhängig von der tatsächlichen Nutzung des Fernzugriffs erfolgt. Eine Speicherung der Daten auf den Servern hat daher nur so lange zu erfolgen, wie der Nutzer darauf zugreifen möchte. Im Falle der Fernregulierung der Heizung ist die aktuelle Temperatur in einem Zimmer mithin nur bis zu ihrer Änderung relevant, die entsprechenden Daten sind anschließend zu überschreiben. Die Information, wann die Temperatur wie viel Grad betrug, würde die Erstellung von Bewegungsprofilen ermöglichen und über den Zweckbindungsgrundsatz hinausgehen.

Die dauerhafte Erfassung der über die aktuellen Bestandsdaten hinausgehenden Informationen über den Nutzer findet daher keine gesetzliche Grundlage in § 28 Abs. 1 S. 1 Nr. 1 BDSG.

Im Rahmen von *Smart Cars*, die teils ähnliche juristische Problemstellungen aufweisen wie das *Smart Home*, wird darüber hinaus diskutiert, ob eine Datenerhebung durch § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt sein könnte.[30] Nach dieser Vorschrift ist eine Datenerhebung zulässig, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung

24 *Gola/Schomerus*, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 3a Rn. 4.

25 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 22 des Gesetzes vom 25. Juli 2014 (BGBl. I 1266).

26 *Schaar*, MMR 2001, 644 (645).

27 *Gola/Schomerus*, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 3 Rn. 10.

28 *Gola/Schomerus*, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 4a Rn. 37ff.

29 Bei T-Online etwa http://tarife-und-produkte.t-online.de/smart-home-app-haussteuerung-ueber-das-smartphone/id_68259258/index (Stand: 15.03.2015).

30 *Roßnagel*, SVR 2014, 281 (285).

oder Nutzung nicht überwiegt. Der Bejahung einer hierin liegenden Erlaubnis für die Datenerhebung im *Smart Home* scheitert bereits daran, dass die möglichen Interessen des Anbieters nicht berechtigt sind. Zwar wird oft angeführt, dass die Erhebung von Daten der Verbesserung des Angebots und damit letztendlich der Steigerung des Benutzerkomforts dient, allerdings kann sich durch diese Ausdrucksweise höchstens die Datenspeicherung bei Abstürzen und anderen Fehlfunktionen rechtfertigen. Inwiefern das Anlegen eines vollständigen Nutzerprofils einen signifikanten Beitrag zur Verbesserung der Produktqualität und damit zur Wahrung berechtigter Anbieterinteressen dient, ist nicht ersichtlich, zumal das Gebot der Datensparsamkeit des § 3a BDSG hierdurch eine bedenkliche Aufweichung erführe. Hinzu kommt, dass die Berufung auf berechtigte Interessen niemals die Erstellung und Nutzung eines umfassenden Persönlichkeitsprofils rechtfertigt,[31] sodass selbst im Falle der Annahme eines berechtigten Interesses die Schutzbedürftigkeit des Nutzers nicht zuletzt im Hinblick auf sein Grundrecht auf informationelle Selbstbestimmung überwiegt. Eine gesetzliche Erlaubnis für eine umfassende Datenerhebung und -speicherung kann somit weder in § 28 Abs. 1 S. 1 Nr. 1 noch Nr. 2 BDSG gefunden werden.

b) Möglichkeit einer Einwilligung

Besteht keine gesetzliche Erlaubnis für die Erhebung von Daten, verbleibt nur die Möglichkeit, die Einwilligung des Nutzers einzuholen, § 4 Abs. 1 BDSG, für Telemedien gilt § 12 Abs. 1 TMG. Dabei hat sich der Grundsatz der informierten Einwilligung herausgebildet, weshalb in inhaltlicher Hinsicht festzustellen ist, dass weder zu pauschal gehaltene noch mutmaßliche, stillschweigende, konkludente oder fingierte Einwilligungen dieser Anforderung genügen.[32] Der Umfang der Informationen ist dabei grundsätzlich auf ein vernünftiges Maß zu beschränken,[33] damit der Betroffene auch tatsächlich informiert wird und nicht von einer vielleicht sehr detaillierten, aber unüberschaubaren Menge an Hinweisen in für den Laien unverständlicher juristischer Terminologie abgeschreckt wird. Eine Platzierung der Einwilligung in den AGB ist bei entsprechender Hervorhebung möglich,[34] elektronische Einwilligungen müssen nach § 13 Abs. 2 TMG protokolliert und jederzeit abrufbar sein.

Um diesen Grundprinzipien im Falle des vernetzten Eigenheims Rechnung zu tragen, empfiehlt sich dabei zumindest eine Untergliederung nach den einzelnen Geräten und eine besondere Hervorhebung der nach § 4 Abs. 3 S. 3 Nr. 2 BDSG geforderten Zweckbestimmung, damit dem Nutzer angezeigt wird, welche Geräte welche Informationen sammeln und ob seine Daten an Werbepartner weitergegeben werden sollen. Richtet man den Blick auf soziale Netzwerke wie Facebook, so zeigt sich, dass die Schwelle zur Erteilung datenschutzrechtlicher Einwilligungen bei den Nutzern bedauernswerterweise sehr gering angesetzt ist. Nachdem die vernetzte Technologie immer stärker in höchstpersönliche Lebensbereiche vordringt, erscheint es daher generell zunehmend fragwürdig, den Anbietern mittels einer einzigen Einwilligung gleichsam das Tor zu sämtlichen personenbezogenen Daten des Nutzers zu öffnen. Als Lösung bietet es sich neben der verbesserten Aufklärung der Verbraucher auch hinsichtlich der Kombinationsmöglichkeit von Daten aus verschiedenen Quellen an, die formalen Anforderungen an eine Einwilligung stärker vorzugeben, sodass der Betroffene nicht durch engzeilige Textmassen vom Lesen abgeschreckt wird. Ebenfalls angedacht werden kann eine Verpflichtung der Anbieter, dem Nutzer in bestimmten Zeiträumen mitzuteilen, welche Daten bislang über ihn erhoben wurden. Eine derartige Mitteilung könnte darüber hinaus mit einem deutlichen Hinweis auf die Widerrufsmöglichkeit der Einwilligung erfolgen.

Nicht unerwähnt bleiben darf in diesem Zusammenhang auch das Koppelungsverbot des § 28 Abs. 3b BDSG, das verbietet, den Abschluss eines Vertrages an die Erteilung einer Einwilligung zur Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung zu knüpfen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen nicht in zumutbarer Weise möglich ist. Die Rechtsprechung macht vom Koppelungsverbot bislang jedoch nur sehr zurückhaltend Gebrauch.[35] Zudem erscheint es wegen der vielen Smart-Home-Anbieter mit unterschiedlichen Angebotsstrukturen wenig wahrscheinlich, dass § 28 Abs. 3b BDSG vor der Einführung derartiger Geschäftsmodelle durch die Hersteller abschrecken wird. Verträge, in denen die Nutzer mit ihren Daten bezahlen, sind in sozialen Netzwerken schon selbstverständlich – wer z.B. Facebook nutzt, erklärt sich laut der Datenverwendungsrichtlinie damit einverstanden, dass das Netzwerk sämtliche erhaltene Informationen verwendet, um Werbeanzeigen zu schalten.[36] Trotz der bestehenden Unterschiede in den Bezahlmodalitäten (in kostenlosen sozialen Netzwerken wird mit Bereitstellung der eigenen Daten „bezahlt", während *Smart Home* Produkte kostenpflichtig sind) lässt sich ein solches Modell auf *Smart Home* übertragen. So könnte der Kunde beim Kauf eines Starter Kits zur Einwilligung darüber aufgefordert werden, dass seine privaten Gewohnheiten und Vorlieben in den eigenen vier Wänden ausgewertet und für Werbezwecke verwendet werden. Dieses Beispiel macht vor dem Hintergrund der zunehmenden Technisierung unseres Alltags deutlich, dass eine deutlich strengere Handhabe des Koppelungsverbots durch die Rechtsprechung wünschenswert ist, um derartige Praktiken einzuschränken und für datenschutzrechtlich unbedenkliche Alternativangebote zu sorgen. Daraus ergäbe sich der positive Nebeneffekt, dass hohe Datensi-

31 *Roßnagel*, SVR 2014, 281 (285).

32 *Gola/Schomerus*, in: Gola/Schomerus (Hrsg.), BDSG, 11. Aufl. 2012, § 4a BDSG, Rn. 11, 19; *Spindler*, GRUR-Beil. 2014, 101 (103); BGHZ 95, 365 (367ff.).

33 *Zscherpe*, MMR 2004, 723 (725).

34 *Plath/Frey*, BB 2009, 1762 (1766); a.A. *Weichert*, SVR 2014, 241 (243).

35 Etwa OLG Brandenburg, MMR 2006, 405 (407), das genug Alternativen zum Online-Auktionshaus eBay sah und eine Anwendung des Koppelungsverbots daher ablehnte.

36 https://de-de.facebook.com/about/privacy/advertising (Stand: 15.03.2015).

cherheit zu einem Wettbewerbsfaktor würde, mit dem man ebenso um die Gunst der Kunden werben könnte wie mit technisch überzeugenden Produkten.

c) Heimliche Datenerhebung durch die verantwortliche Stelle

Selbst wenn eine datenschutzrechtliche Einwilligung ausbleibt, hat der durchschnittliche *Smart-Home*-Käufer kaum Möglichkeiten herauszufinden, ob nicht doch gegen seinen Willen Daten über ihn erhoben und an Werbepartner des Anbieters verkauft oder gar an Geheimdienste übermittelt werden. Umso wichtiger sind aus diesem Grund noch strengere Bußgeld- und Strafvorschriften zur Abschreckung, als sie sich bisher etwa in den §§ 43 f. BDSG finden. § 43 Abs. 1 Nr. 1 BDSG sanktioniert dabei die unbefugte Erhebung und Verarbeitung nicht allgemein zugänglicher Daten, für die Annahme einer Straftat nach § 44 Abs. 1 BDSG muss hierbei noch Bereicherungs- oder Schädigungsabsicht bestehen, wie sie im Falle des Weiterverkaufs von Nutzerprofilen der *Smart-Home*-Bewohner gegeben sein dürfte. Aus dem praktischen Unvermögen der Kunden, derartige Verstöße selbst zu enttarnen und eine Sanktionierung in die Wege zu leiten, resultiert die Notwendigkeit einer Verbesserung des Verbraucherschutzes. Diese kann durch eine gesetzgeberische Verpflichtung zum Erwerb von Datenschutz-Prüfsiegeln gelingen und durch umfassendere Verbraucherinformationen im Rahmen von Aufklärungskampagnen unterstützt werden.[37] Ebenfalls sinnvoll erscheint es, für technische Überprüfungen, ob heimlich Nutzerdaten gesammelt und erhoben werden, nicht mehr auf Tests privater Unternehmen oder Hacker-Tagungen zu warten, sondern derartige Untersuchungen in ein staatliches Kontrollsystem einzubinden und so mehr Transparenz für die Verbraucher zu schaffen.

Darüber hinaus besteht für den Anbieter die Pflicht, den Hausbewohner nach § 33 BDSG zu informieren, wenn ohne seine Kenntnis Daten über ihn gespeichert werden, während im Falle ungewollten Datenabflusses an Dritte § 42a BDSG die Informierung der Betroffenen gebietet. Dass Unternehmen aus Furcht vor einer mit der Meldung einhergehenden Rufschädigung durch Vertrauensverlust nur in Notfällen hiervon Gebrauch machen, ist häufig zu lesen, weshalb derartige Regelungen nur geringen Erfolg versprechen.[38] Umso dringlicher ist daher der Aufruf an den Gesetzgeber zu richten, durch das Einführen entsprechender Sanktionen die Einhaltung der Normen zu sichern.

d) Dritte im Smart Home

Ein eigener Problemkreis offenbart sich zunehmend bei neuen Technologien mit ihren Auswirkungen auf Dritte. Während die Frage, ob ein Beifahrer in einem vernetzten Auto angeschnallt war, vor allem in Haftungsfällen relevant werden kann, stellt sich beim *Smart Home* zunächst die Frage, ob Dritte wie etwa Besucher vom Schutzbereich des BDSG erfasst sind. Auch hier ist auf das Kriterium der Bestimmbarkeit der natürlichen Personen nach § 3 Abs. 1 BDSG abzustellen, dessen Vorliegen bei einem Besucher nach dem heutigen Stand der *Smart-Home*-Technologien wohl abgelehnt werden muss, da seine Identität für den Anbieter unbekannt bleiben wird. Deutlich häufiger und daher auch schützenswerter sind Mitbewohner in einem *Smart Home*, deren Bestimmbarkeit für den Anbieter jedenfalls dann gegeben sein wird, wenn er ein eigenständiges Benutzerprofil und damit einen eigenen Zugang zu den Steuerungsfunktionen des *Smart Home* erhält. Bislang sind getrennte Benutzerprofile innerhalb eines Haushalts selten möglich, erscheinen jedoch ohne weiteres denkbar. In diesem Falle ist der Mitbewohner als Inhaber eines eigenen Accounts datenschutzrechtlich als eigenständiger Benutzer zu werten, sodass die obigen Ausführungen entsprechend gelten und – je nach Umfang der Datenerhebung – seine Einwilligung notwendig sein kann. Teilen sich mehrere Bewohner einen *Smart-Home*-Account, ist die Identität des nicht beim Anbieter registrierten Mitbenutzers für diesen – nach heutigem Stand – zumindest ohne Zusatzinformationen nicht ersichtlich, weshalb eine Anwendbarkeit der datenschutzrechtlichen Regelungen gemäß § 3 Abs. 1 BDSG nicht einschlägig ist.

Insgesamt zeigen sich bei diesem Problemkreis zahlreiche Parallelen zu Beifahrern in sogenannten *Smart Cars* – beiden Technologien ist gemein, dass die Erfassung von Beifahrer- bzw. Mitbewohnerdaten noch eine untergeordnete Rolle spielt.[39] Es ist jedoch daran zu denken, dass auch den Dritten das Grundrecht des Einzelnen auf informationelle Selbstbestimmung zusteht, was die Hersteller bei der Planung neuer Technologien stärker berücksichtigen müssen. Aufseiten des Gesetzgebers ist vor allem daran zu denken, dass auch Dritte darüber informiert werden müssen, wenn Daten über sie erhoben werden. Ist dies aus Gründen der Praktikabilität nicht möglich und scheitert darüber hinaus eine Anonymisierung und Pseudonymisierung nach § 3a S. 2 BDSG, müssen Dritte zumindest in Zivil- und Strafprozessen durch Beweisverwertungsverbote hinsichtlich der so erlangten Daten geschützt werden. Zugleich müssen Anbieter nach den bei heimlichen Datenerhebungen anwendbaren Rechtsvorschriften sanktioniert werden, wenn sie Daten über Dritte systematisch speichern.

3. Datenschutzrechtliche Reaktionsmöglichkeiten auf die Einwirkung Dritter

Schließlich sind die eingangs unter III.1. dargestellten Zu- und Eingriffe Dritter in ein *Smart Home* einer kurzen rechtlichen Würdigung zu unterziehen. Hierbei ist zunächst an die Vorschriften der §§ 202a-202c StGB zu denken. Benutzt ein Angreifer ein heruntergeladenes oder selbstgeschriebenes Programm, um sich in die *Smart-Home*-Technologie eines Haushalts zu hacken, ist in der Regel der sog. Ha-

37 Beispiele für verlässliche Prüfsiegel unter https://www.datenschutzzentrum.de/guetesiegel/ (Stand: 15.03.2015).

38 http://www.manager-magazin.de/unternehmen/it/a-195014-2.html (Stand: 15.03.2015).

39 So für *Smart Cars Weichert*, SVR 2014, 201 (204).

cker-Paragraph § 202c Abs. 1 Nr. 2 StGB erfüllt, der u.a. die Herstellung eines Computerprogramms zum Zwecke des Ausspähens (§ 202a StGB) oder Abfangens (§ 202b StGB) von Daten sanktioniert. Für das eigentliche Ausspähen und Auslesen der Daten ist speziell beim *Smart Home* auch an § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) zu denken, wenn in dem Haus Überwachungskameras eingesetzt werden. Beschränkt sich der Angriff nicht nur auf ein „passives" Mit- und Auslesen der Daten, muss neben der nach § 303a StGB strafbaren Datenveränderung auch eine Strafbarkeit nach § 303b StGB (Computersabotage) gedacht werden. Der Tatbestand der Computersabotage fordert u.a., dass durch eine Tat nach § 303a StGB eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich gestört wird. Ob die Manipulation des „Geöffnet"- bzw. „Geschlossen"-Status eines einzelnen Fenstersensors ausreicht, um die Merkmale der wesentlichen Bedeutung und der erheblichen Störung zu bejahen, wird wohl erst durch die Rechtsprechung beantwortet werden. Eindeutig erfüllt sind die Merkmale hingegen, wenn viele zentrale Bestandteile des Eigenheims vernetzt sind und angegriffen werden, beispielsweise bei einem Angriff auf die Basisstation, der zahlreiche Haushaltsgeräte auf einmal kompromittiert und etwa die Fingerabdruckerkennung der Haustüröffnung außer Kraft setzt.

Die bestehenden strafrechtlichen Regelungen sind daher grundsätzlich als ausreichend anzusehen, um im Zusammenhang mit einem *Smart Home* begangene Straftaten hinreichend zu sanktionieren. Defizite bestehen allerdings in der Strafverfolgungspraxis, da die Ermittlung der Täter wie bei allen Internetstraftaten häufig schwierig ist.

V. Fazit und Ausblick

Wie viele moderne Technologien bietet auch das *Smart Home* Vorteile in Hinblick auf Komfort und Sicherheit, birgt darüber hinaus aber vor allem Risiken bezüglich der unberechtigten Weiterverwertung der Daten und kann in bisher nie da gewesener Weise in den höchstpersönlichen Lebensbereich der Nutzer eindringen. Die Schwächen des Datenschutzrechts treten in Ansehung neuer technischer Entwicklungen besonders offensichtlich zum Vorschein und zwingen mittelfristig zu gesetzgeberischen Reformen, um das Szenario des „gläsernen Bürgers" zu verhindern. Vor allem sollten Verbraucher vor der Erteilung ihrer datenschutzrechtlichen Einwilligung besser, aber nicht zwangsläufig ausführlicher über die Tragweite ihres Handelns informiert werden und das zunehmend zur Makulatur verkommende Koppelungsverbot effektiv genutzt werden, um einen Markt zu schaffen, in dem auch beim Thema Datenschutz um ein hohes Niveau gewetteifert wird. Zusätzlich entwickelt sich der Schutz der Daten Dritter zu einer Herausforderung, welcher der Gesetzgeber dadurch begegnen sollte, dass er die Hersteller zur stärkeren Anonymisierung der erhobenen Daten zwingt und Verstöße gegen datenschutzrechtliche Vorschriften generell stärker sanktioniert. Bis derartige Lösungen gefunden sind, liegt es im Verantwortungsbereich der Kunden, genau abzuwägen, welchen Preis sie für das vernetzte Eigenheim zu zahlen bereit sind – nicht nur finanziell.