www.jusletter-it.eu

Sandra Husi-Stämpfli

Wenn der Backofen mit dem Staubsauger kommuniziert. . .

Datenschutzrechtliche Herausforderungen intelligenter Haushaltsgeräte

The entering of intelligent utensils in our households is followed by several data protection and information security law related challenges. How far can users appraise what happens with their data when intelligent domestic appliances are used? Which risks conclude from the technical complexity of the appliances and the data processing procedures? The author picks up particular subject areas and highlights the risks for the personal rights of the users on the basis of different utensils. Subsequently possible methods of resolution are outlined by involving the newest developments in the EU data protection revision. (ah)

Category: Articles
Field of law: Data Protection
Region: Switzerland

Citation: Sandra Husi-Stämpfli, Wenn der Backofen mit dem Staubsauger kommuniziert. . . , in: Jusletter IT 11 December 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

I. Einleitung: Können Geräte «intelligent» sein?

[Rz 1] Der Inhalt des Kühlschranks kann via App ermittelt werden[1], so dass im Supermarkt die richtigen Zutaten für das Abendbrot gekauft werden können. Der Roboterstaubsauger kann so programmiert werden, dass er die Wohnung putzt, bevor die Bewohner nach einem verlängerten Wochenende nach Hause kommen[2]. Die Klimaanlage erkennt mit Sensoren, ob die Bewohner zuhause sind und ist gleichzeitig auch Alarmanlage[3].

[Rz 2] Das «intelligente» oder «smarte» Zuhause, in dem alle elektronischen Geräte miteinander vernetzt sind und kommunizieren können, ist längst keine Utopie mehr. Die Internationale Funkausstellung IFA stellte 2014 die intelligenten Häuser ins Rampenlicht und machte deutlich: Die lange gehegte Idee des vernetzten Heims ist in der Realität angekommen, sie steckt aber nicht zuletzt deshalb noch in den Kinderschuhen, weil sich die Applikationen der einzelnen Anbieter noch nicht verknüpfen lassen[4]. Dies soll sich aber bald ändern: In Anbetracht des Marktpotentials, welches die heranwachsende Generation der sog. *digital natives*, d.h. jener Generation, die

1 http://www.it-markt.ch/de-CH/News/2014/09/03/IFA-2014-LG-verleiht-dem-Zuhause-Intelligenz.aspx(alle Internetquellen zuletzt besucht am 20. November 2014).

2 http://www.lg.com/ae/vacuum-cleaners/lg-VR6270LVMB.

3 http://www.nzz.ch/wirtschaft/newsticker/google-will-nest-thermostate-zum-zentrum-im-vernetzten-heim-machen-1.18329183; http://www.20min.ch/digital/dossier/google/story/23306861.

4 Siehe dazu http://www.heise.de/tp/artikel/37/37634/1.htmlsowie http://www.energynet.de/2013/12/04/crowdfunding-fuer-schnittstelle-unterschiedlicher-smarthome-systeme-und-anwendungen/.

bereits mit Smartphones und Tablets aufgewachsen ist[5], mit sich bringt, arbeiten die Hersteller mit Hochdruck an gemeinsamen Standards und Plattformen, um die diversen Geräte einfach verknüpfen zu können[6].

[Rz 3] Die zunehmend leistungsfähigere Technik wird unweigerlich auch dazu führen, dass die «Intelligenz» der Geräte weiter wächst: Zahlreiche Geräte können bereits heute — obwohl sie nach Aussage der Entwickler noch in den Kinderschuhen stecken! — das Verhalten ihrer Umwelt (d.h. in der Regel jener Menschen, in deren Haushalt sie eingesetzt werden) wahrnehmen, analysieren, ihre eigene Funktionalität unmittelbar und auch längerfristig, im Sinne einer «Lernkurve», diesen Wahrnehmungen anpassen und mit anderen Geräten interagieren. Weitere Möglich- und Fähigkeiten sind nur noch eine Frage der Zeit, wenn man den Entwicklern Glauben schenken darf: Das Heim der Zukunft sei ein flexibel gestaltbarer Raum, in dem sich Leben und Arbeiten abwechseln. Die Wohnung der Zukunft werde «spüren, lernen und reagieren»[7].

[Rz 4] Damit wird sich die Frage stellen, ob die Menschheit ihre seit Jahrhunderten gepflegten Definitionen von «Intelligenz» sowie die damit untrennbar verknüpfte Überzeugung, die einzige intelligente Lebensform zu sein, nicht überdenken sollte: Als Intelligenz werden im Allgemeinen die geistigen Fähigkeiten verstanden, mit deren Hilfe die für das Handeln wesentlichen Eigenschaften einer Problemsituation in ihrer Zusammensetzung erkannt werden können und die Situation gemäss dieser Einsicht verändert werden kann[8]. Intelligenz in diesem Sinne war bislang dem Menschen vorbehalten. Ob Geräte künftig wirklich als «intelligent» bezeichnet werden können, wird letztendlich zu einem späteren Zeitpunkt und in anderem Rahmen zu diskutieren sein. Für die folgenden Ausführungen soll jedenfalls der Begriff der «intelligenten Geräte» unter der Prämisse verwendet werden, dass damit zwar keine menschliche Intelligenz gemeint ist, wohl aber eine hochentwickelte und durchaus — im Rahmen der jeweiligen Programmierungen — eigenständig beobachtende, analysierende und daraus agierende Interaktionsfähigkeit.

[Rz 5] Der folgende Beitrag wird die Herausforderungen, welche sich mit den Fähigkeiten «intelligenter» Haushaltsgeräte ergeben, beleuchten: Zunächst soll der aktuelle datenschutz- und informationssicherheitsrechtliche Rahmen, welchen es bei der Verwendung von «intelligenten» Geräten einzuhalten gilt, umrissen werden. Der darauffolgende Abschnitt greift sodann konkrete rechtliche Fragestellungen auf und illustriert Risiken im Bereich der Informationssicherheit anhand einzelner Geräte. Der letzte Abschnitt widmet sich schliesslich möglichen Lösungsansätzen, welche die Datenschutz- und Informationssicherheitsbedenken, die sich beim Einsatz «intelligenter» Geräte ergeben, entschärfen könnten.

---

5 http://www.oxforddictionaries.com/definition/english/digital-native.

6 Dazu und zu den geplanten Standards http://smarthomewelt.de/smart-home-zentrales-thema-ifa-2014/.

7 http://www.heise.de/newsticker/meldung/Samsung-Smart-Home-ist-erst-am-Anfang-2356446.html.

8 «Individuals differ from one another in their ability to understand complex ideas, to adapt effectively to the environment, to learn from experience, to engage in various forms of reasoning, to overcome obstacles by taking thought», Board of Scientific Affairs of the American Psychological Association, Intelligence: Knowns and Unknowns, 1996, abrufbar unter http://www.gifted.uconn.edu/siegle/research/correlation/intelligence.pdf.

II. Aktueller datenschutzrechtlicher Rahmen

1. Informationen? Personendaten? Besondere Personendaten?

[Rz 6] Die «intelligenten» Geräte sammeln eine riesige Menge an Informationen: Vom Inhalt eines Kühlschranks über den Grundriss einer Wohnung bis hin zu Körpertemperaturen. Diese Informationen werden dann zu Personendaten, wenn sie, beispielsweise aufgrund einer Produktregistrierung, der Hinterlegung von Adressen für Lieferungen oder aufgrund der Kombination mit anderen Informationen, die Identifikation einer bestimmten Person erlauben. Oder, anders formuliert: Solange niemand weiss, dass das «intelligente» Gefrierfach und die darin enthaltenen vier Sorten Eiscreme einer konkreten Person gehören, handelt es sich nicht um Personendaten.

[Rz 7] Wurde das Gefrierfach jedoch beispielsweise online beim Hersteller registriert und gleichzeitig einem grossen Detailhändler die Adresse bekannt gegeben, damit der Nachschub an Eiscreme gesichert ist, werden die Informationen rund um das fragliche Gefrierfach zu Personendaten[9]: Sie sagen etwas über die Eiscreme-Vorlieben einer konkreten Person aus und lassen damit Vermutungen bezüglich des Einkommens dieser Person zu, wenn anstelle von Billigprodukten exklusive Sorten gekauft werden. Von diesen «gewöhnlichen» Personendaten abzugrenzen sind wiederum die besonderen Personendaten[10], zu welchen unter anderem Angaben über die Religionszugehörigkeit oder zur Gesundheit gehören. Derartige Angaben bergen ein erhöhtes Stigmatisierungsrisiko und verdienen daher besonderen Schutz[11]. Um auf das Beispiel mit dem Gefrierfach zurückzukommen: Wird koscheres Eis gekauft, so könnten[12] Rückschlüsse auf religiöse Überzeugungen gezogen werden. Je nach gesellschaftlichem und politischem Umfeld kann diese Information für die betroffenen Personen weitreichende Konsequenzen mit sich bringen.

[Rz 8] Sollen (besondere) Personendaten bearbeitet werden, so sind die entsprechenden datenschutzrechtlichen Vorgaben einzuhalten. Da es sich bei den Anbietern intelligenter Geräte in der Regel um juristische Personen des Privatrechts, welche auch als Privatpersonen agieren[13], handelt, gelangen in der Schweiz die Bestimmungen des Bundesgesetzes über den Datenschutz (DSG)[14] zur Anwendung. Diese Vorgaben unterscheiden sich in ihren Grundzügen nur unwesentlich von den EU-Regelungen für das Bearbeiten von Personendaten durch Privatpersonen[15], auf

---

9 Als Personendaten werden alle Informationen über eine bestimmte oder bestimmbare natürliche Person bezeichnet, wobei eine Person dann als bestimmbar angesehen wird, wenn sie direkt oder indirekt identifiziert werden kann; vgl. dazu die Definition in Art. 3 lit. a des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1) oder die Definition in Art. 2 lit. a der Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23. November 1995, S. 31 ff. (im Folgenden: Richtlinie 95/46/EG).

10 In der kantonalen Gesetzgebung ist regelmässig die Rede von «besonders schützenswerten Personendaten», vgl. dazu § 3 Abs. 4 des baselstädtischen Gesetzes vom 9. Juni 2010 über die Information und den Datenschutz, SG 153.260oder aber § 3 Abs. 4 des Zürcher Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz, LS 170.4.

11 Differenzierend dazu Beat Rudin, § 3 N 40, in: Beat Rudin/Bruno Baeriswyl, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich 2014 (im Folgenden zitiert als: PK-IDG/BS-AutorIn).

12 Müssen aber nicht zwingend, vielleicht schmeckt das Eis der fraglichen Person schlicht besser. Siehe zur Problematik der Interpretierbarkeit ausführlich http://www.heise.de/newsticker/meldung/re-publica-Big-Data-als-Ueberwachungsinstrument-2184950.html?wt_mc=sm.feed.tw.hosowie das Interview auf http://www.ted.com/talks/kenneth_cukier_big_data_is_better_data#.

13 Eine Ausnahme bieten die staatlichen Stromversorger, welche im Bereich der obligatorischen Stromversorgung eine öffentliche Aufgabe wahrnehmen und damit zum öffentlichen Organ werden — auf eine eingehende Diskussion des Smart Metering wird in diesem Beitrag aus Platzgründen verzichtet.

14 Siehe zum Nachweis Fn 9.

15 Vgl. dazu beispielsweise Art. 7 der Richtlinie 95/46/EG.

welche in den weiteren Betrachtungen immer wieder Bezug genommen werden wird.

2. Bearbeitungsvoraussetzungen

2.1. Einwilligung als Bearbeitungslegitimation

[Rz 9] Während öffentliche Organe Personendaten nur unter den strengen Voraussetzungen des Legalitätsprinzips bearbeiten dürfen[16] und sich nur in Ausnahmefällen auf die Einwilligung der betroffenen Personen berufen können[17], ist das Bearbeiten von Personendaten gestützt auf die (zumindest konkludente) Einwilligung der Betroffenen der Regelfall[18] im Kontext privatrechtlicher Datenbearbeitungsvorgänge.

[Rz 10] Damit die Einwilligung als Rechtfertigung für ein Datenbearbeiten herangezogen werden kann, muss sie von einer aufgeklärten Partei abgegeben worden sein: Die betroffene Person muss über alle im konkreten Fall erforderlichen Informationen verfügen, damit sie eine freie Entscheidung fällen kann[19]. So muss die Interessentin für einen intelligenten Kühlschrank etwa wissen, welche Daten zu welchen Zwecken erhoben werden (nur zum Bestellen von Lebensmitteln, zur Analyse des Kaufverhaltens, oder zur Optimierung der Geräte etc.?), ob die Daten weitergegeben werden, ob die Daten nur vom Hersteller des Kühlschranks bzw. der Software oder von Dritten bearbeitet werden, wo die Daten gespeichert werden (auf dem Gerät selbst, beim Hersteller, bei einer Drittperson, in einer Cloud, im Ausland?), wie lange die Daten gespeichert werden, wie die Daten gesichert werden und schliesslich, welche Rechte den von den Datenbearbeitungen betroffenen Personen zustehen und wo sie diese geltend machen können.

[Rz 11] Mit diesem Konzept des *informed consent* soll erreicht werden, dass die betroffenen Personen sich auch ein Bild von möglichen negativen Kehrseiten einer Datenbearbeitung machen und eine eigene Abwägung der Vor- und Nachteile vornehmen können.

2.2. Treu und Glaube und Transparenz

[Rz 12] Der Grundsatz von Treu und Glaube soll das Vertrauen in die Redlichkeit und die Ehrlichkeit des Gegenübers schützen[20]. Die von einer Datenbearbeitung betroffenen Personen müssen sich darauf verlassen können, dass sie im Rahmen der Aufklärung über das geplante Datenbearbeiten vollumfänglich und ehrlich informiert wurden und ihre Daten auch tatsächlich nur in der ursprünglich zugesicherten Art und Weise verwendet werden. Ein Beispiel: Der Anbieter eines intelligenten Kühlschranks darf nicht verschweigen, dass die Daten nicht nur auf dem Gerät

---

16 Art. 17 DSG und dazu ausführlich BSK-DSG-Sándor Udvary/Sarah Ballenegger, Art. 17 N 3 ff.; David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 17 N 3.

17 Vgl. dazu Art. 17 Abs. 2 lit. c DSG, welcher a maiore minus auch für die Bearbeitung von «gewöhnlichen» Personendaten gelten muss, dazu BSK-DSG-Sándor Udvary/Sarah Ballenegger, Art. 17 N 30 ff.; David Rosenthal/Yvonne Jöhri(Fn 16), Art. 17 N 80.

18 BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 13 N 3.

19 Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2101, 2127.

20 Benjamin Schindler/Tobias Tschumi, St. Galler Kommentar zur Bundesverfassung, 3. Auflage 2014, Zürich, Art. 5 N 53 ff.; BSK-ZGB I-Heinrich Honsell, Art. 2 N 4 ff.

selbst, sondern auch in einer Cloud gespeichert, oder dass die Daten nicht nur für die Bestellung von Lebensmitteln, sondern auch zur Auswertung der Essgewohnheiten analysiert werden.

[Rz 13] Eng mit dem Grundsatz von Treu und Glauben verbunden ist folglich auch das Transparenzgebot: Datenbearbeitungsvorgänge müssen transparent gemacht werden («erkennbar sein»)[21] und dürfen in der Regel[22] nicht im Geheimen von statten gehen. Dabei genügt es, dass das Bearbeiten der Daten aus den Umständen ersichtlich ist.

2.3. Verhältnismässigkeit

[Rz 14] Auch private Datenbearbeiterinnen und -bearbeiter haben den Grundsatz der Verhältnismässigkeit zu wahren. Danach sollten grundsätzlich[23] nur jene Daten bearbeitet werden, die zur Erreichung des konkreten Zwecks geeignet und erforderlich sind[24]: Der «intelligente» Kühlschrank darf etwa nur die Produkte registrieren, welche in ihm gelagert werden, nicht aber, zu welchen Tages- und Nachtzeiten die einzelnen Lebensmittel verzehrt wurden, da er diese Informationen nicht zur Bestellung von Nachschub benötigt.

2.4. Zweckbindung

[Rz 15] Die Zweckbindung soll sicherstellen, dass für die betroffene Person bereits bei der Information über das geplante Datenbearbeiten ersichtlich ist, *wofür* die sie betreffenden Personendaten bearbeitet werden und dass dieser Zweck auch so beibehalten wird[25]: Die vom «intelligenten» Kühlschrank erhobenen Daten über die konsumierten Lebensmittel dürfen nur für die Bestellung von Nachschub verwendet werden, nicht aber zur Ernährungsanalyse — es sei denn, dies wurde vorher so kommuniziert; der vom Staubsaugerroboter zur optimalen Reinigung erstellte Raumplan darf nicht an eine Marketingfirma weitergegeben werden.

[Rz 16] Eine Zweckänderung bedarf einer Rechtfertigung, d.h. entweder wiederum der Einwilligung der betroffenen Person oder aber einer Rechtsgrundlage[26].

2.5. Richtigkeit

[Rz 17] Die Wahrung der Richtigkeit der bearbeiteten Daten gehört ebenfalls zu den Grundvoraussetzungen des datenschutzkonformen Bearbeitens von Personendaten: Unvollständige oder unrichtige Daten können zu falschen Schlüssen über die betroffene Person und damit zwangsläufig zur Verletzung derer Persönlichkeit führen. Den Datenbearbeitern obliegt damit die Pflicht, sich bei der Erhebung und den weiteren Datenbearbeitungsvorgängen — ursprünglich richtige Daten können im Laufe der Zeit unrichtig werden — zu vergewissern, dass nur richtige Daten

---

21 BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 16a ff.

22 Ausnahmen können sich beispielsweise aus gesetzlichen Vorgaben oder überwiegenden Interessen an der Beschaffung der Daten ergeben, BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 16e.

23 Im Gegensatz zum Verhältnismässigkeitsgrundsatz im öffentlichen Recht ist die «Heilung» einer nicht verhältnismässigen Datenbearbeitung durch Einwilligung möglich,David Rosenthal/Yvonne Jöhri (Fn 16), Art. 4 N 19.

24 BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 9 ff.

25 Eine Zweckänderung basierend auf einer Rechtsgrundlage wird jedoch üblicherweise beim Datenbearbeiten durch öffentliche Organe der Fall sein, BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 13.

26 BSK-DSG-Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 15.

bearbeitet werden.

2.6. Gewährung von Informationszugangsrechten

[Rz 18] Die im Datenschutzrecht statuierten Schutzmechanismen würden leer laufen, wenn die von Datenbearbeitungen betroffenen Personen keine Möglichkeit hätten, Zugang zu ihren Personendaten zu erhalten und damit zu kontrollieren, ob die über sie bearbeiteten Daten richtig sind, der ursprünglich genannte Zweck tatsächlich eingehalten oder allenfalls weitaus mehr als die angekündigten Daten erhoben wurden[27].

[Rz 19] Entsprechend sieht das Datenschutzrecht vor, dass die von einer Datenbearbeitung betroffenen Personen die Möglichkeit haben müssen, Zugang zu ihren Personendaten zu erhalten, um diese allenfalls berichtigen oder löschen lassen (Ausfluss des Grundsatzes der Datenrichtigkeit), oder, im Falle von Persönlichkeitsverletzungen etwa aufgrund von nicht verhältnismässigen Bearbeitungsvorgängen, den Klageweg beschreiten zu können.

2.7. Massnahmen zur Informationssicherheit

[Rz 20] Neben der Einhaltung der rechtlichen Vorgaben sind auch organisatorische und technische Massnahmen zum Schutz der bearbeiteten Personendaten zu treffen.

[Rz 21] Während die organisatorischen Massnahmen, also beispielsweise Funktionszuordnungen, Aufgaben und Verantwortlichkeiten sowie Verhaltenskodizes, auf die Struktur und Prozesse der Datenbearbeiterin bzw. des Datenbearbeiters fokussieren, umfassen die technischen Massnahmen alle Vorkehrungen, die die Personendaten unmittelbar schützen[28].

[Rz 22] Zu den Schutzzielen, die im Allgemeinen zu wahren sind, zählen unter anderem die Vertraulichkeit, die Integrität sowie die Verfügbarkeit der Daten, aber auch die Zurechenbarkeit und die Nachvollziehbarkeit von einzelnen Datenbearbeitungen[29].

III. Herausforderungen

[Rz 23] Je ausgeklügelter und preiswerter die Technik, umso mehr Möglichkeiten können die «intelligenten» Geräte den Käuferinnen und Käufern bieten, bzw. umso mehr Möglichkeiten bieten sich den «intelligenten» Geräten zur Interaktion mit anderen Geräten: Sei dies aufgrund der fallenden Entwicklungskosten der Sensoren, welche es erlauben, «intelligente» Haushaltsgräte für eine breite Masse zu produzieren, sei es aufgrund der zunehmenden Leistungsfähigkeit der Sensoren, welche immer mehr und immer detailliertere Daten erheben und diese riesigen Datenmengen innert Sekundenbruchteilen verarbeiten können, oder sei dies durch immer stabilere und leistungsstärkere Kommunikationsnetze, welche den Austausch der Daten — zwischen den Geräten selbst, aber auch mit den Geräteherstellern — im Handumdrehen erlauben.

[Rz 24] Dieser Fortschritt und der wachsende Datenberg tangieren sämtliche der oben umrissenen Bearbeitungsgrundsätze. Im Folgenden sollen exemplarisch einzelne dieser Herausforderun-

---

27 Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz, 4. Auflage 2008, Bern, S. 168.

28 PK-IDG/BS-Baeriswyl, § 8 N 10 und 11.

29 Vgl. dazu BSK-DSG-Christa Stamm-Pfister, Art. 7 N 7 sowie PK-IDG/BS-Baeriswyl, § 8 N 21 ff.

gen beleuchtet werden:

1. Entleerung der Einwilligung?

[Rz 25] Das Konzept des *informed consent*, welches die Basis einer jeder Datenbearbeitung unter Privaten ist, geht davon aus, dass im vollen Bewusstsein der Dimension des Datenbearbeitens und aus freien Stücken eine Einwilligung erteilt wird.

[Rz 26] Damit davon ausgegangen werden kann, dass eine Käuferin oder ein Käufer eines intelligenten Geräts wirklich «informed» ist, müsste der folgende Berg an Fragen beantwortet werden können: Ganz grundsätzlich — weiss die Käuferin bzw. der Käufer überhaupt, welche Daten das Gerät erheben wird? Um den Fokus vom Gefrierfach auf ein anderes «intelligentes» Haushaltsgerät zu richten: Ist sich die Käuferin also bewusst, dass ihr Roboterstaubsauger einen Plan ihrer Wohnung erstellt? Weiss der Käufer, wozu seine Wohnungs- und An- und Abwesenheits-Daten alles genutzt werden — nicht nur für die möglichst optimale Reinigung der eigenen Wohnung, sondern unter Umständen auch für die weitere Produktverbesserung, Marktstudien oder für die kundenbezogene Werbung? Weiss die Käuferin, wo die Zeitpläne für die Reinigung (und damit verbunden vielleicht Angaben über ihre An- und Abwesenheiten zuhause) gespeichert werden und für wie lange? Ist für den Käufer transparent, ob diese Daten allenfalls auch weitergegeben und von Dritten bearbeitet werden? Und schliesslich: Erklärt der Hersteller, wie die Daten geschützt werden?

[Rz 27] Ist es faktisch überhaupt noch möglich, den Umfang der Datenbearbeitungen, welche durch den Einsatz «intelligenter» Geräte möglich werden bzw. getätigt werden, zu überblicken und zu durchschauen? Ist es dem Kunden noch möglich abzuschätzen, welche Interpretationen seiner Daten angestellt werden? Können die Kunden die Konsequenzen einer Weitergabe ihrer Daten an einen externen Datenbearbeiter oder in eine Cloud einordnen? Können wir in Anbetracht dieser Vielzahl an Fragen überhaupt noch von einem *informed* consent sprechen?

[Rz 28] In einem zweiten Schritt stellt sich die Frage der Einwilligungs*möglichkeit* — haben die Käuferinnen und Käufer überhaupt eine Option, ein Produkt zu kaufen oder nicht? Noch wird dies der Fall sein, da der Markt der intelligenten Geräte noch im Wachstum begriffen ist. Wohl aber können beispielsweise «intelligente» Kühlschränke, welche Diäten[30] oder eine besondere, allenfalls medizinisch indizierte Ernährungsweise unterstützen, von Versicherern propagiert und die Anschaffung eines solchen Geräts mit Prämienvergünstigungen oder sonstigen Vorteilen beworben werden. Ist der Entscheid, sich einen «intelligenten» Kühlschrank zuzulegen, sein Ernährungsverhalten analysieren und allenfalls sogar an die Krankenversicherung melden zu lassen, noch *frei*, wenn andernfalls Arztkosten nur noch teilweise oder gar nicht übernommen oder der Wechsel in eine andere Versicherungsklasse verweigert wird?

[Rz 29] Mit der Frage der Freiwilligkeit der Einwilligung eng verbunden ist schliesslich auch die Problematik, dass Kundinnen und Kunden viel zu schnell in eine Datenbearbeitung einwilligen, weil sie ein bestimmtes Gerät eben ohne Einschränkungen nutzen wollen. Oder, anders formuliert: Wann haben Sie das letzte Mal die AGB einer App, welche Sie heruntergeladen haben, komplett durchgelesen und allenfalls bewusst auf einzelne Funktionen verzichtet? Und wie

[30] Siehe dazu die Produktbeschreibung für den LG Smart Refrigerator unter http://www.lg.com/ae/press-release/lg-rolls-out-premium-smart-appliances-that-chat, welcher den Body Mass Index berechnet und die Diät überwacht.

gross ist die Chance, dass Sie sich durch die AGB ihres «intelligenten» Kühlschranks kämpfen, um in Erfahrung zu bringen, welche Daten das Gerät speichern kann? Kurzum: Wer von der automatischen Bestellfunktion und vom Heimlieferservice profitieren möchte, wird ohne grosses Zögern seine Einwilligung in die Übermittlung geben — ohne zu differenzieren, welche Daten übermittelt werden sollen und allenfalls wozu.

[Rz 30] Die Vorstellung, dass die Benutzerin und der Benutzer eines «intelligenten» Haushaltsgeräts tatsächlich als aufgeklärte Partei den Entscheid zum Einsatz des Geräts fällen, oder gar als dem Hersteller ebenbürtiges Gegenüber Einschränkungen einzelner Bearbeitungsvorgänge ausbedingen kann, erscheint in Anbetracht der zunehmenden Komplexität der technischen Lösungen idealistisch und überholt. Gleichwohl wird auch künftig im Kontext privater Datenbearbeitungen nicht auf das Erfordernis der Einwilligung verzichtet werden können, da andere Rechtfertigungsgründe für Datenbearbeitungen unter Privaten konzeptionsfremd wären und allzu sehr in die Privatautonomie der Parteien eingreifen würden[31].

2. Wahrnehmung der eigenen Rechte?

[Rz 31] «Wo kein Kläger, da kein Richter»: Wer nicht weiss, wer was unter welchen Voraussetzungen mit seinen Daten anstellt (siehe die Fragestellungen unter Ziff. III.1.), kann auch seine Rechte nicht wahrnehmen. Im Kontext der intelligenten Haushaltsgeräte wird diese Problematik besonders deutlich:

[Rz 32] «Intelligente» Haushaltsgeräte können zwar in der Regel einem Produzenten zugeordnet werden. Ob die erhobenen Daten aber auf dem Gerät verbleiben und dort ohne Zugriffsmöglichkeit des Herstellers genutzt werden, ob die Daten direkt vom Hersteller des Geräts bearbeitet werden, oder ob ein anderes Unternehmen die Datenbewirtschaftung übernimmt, lässt sich in der Regel nur schwer eruieren. Gänzlich unübersichtlich wird die Situation spätestens dann, wenn Daten auch noch an Versicherungen, Ärzte oder andere Interessierte übermittelt und auch von diesen bearbeitet werden: Ist die Zweckbindung noch gewahrt? Sind die Daten im neuen Kontext noch richtig[32]? Werden die Sicherheitsstandards eingehalten? Werden die Daten auch wieder gelöscht?

[Rz 33] Um wieder auf das Beispiel des «intelligenten» Gefrierfachs zurückzukommen: Ich kenne wohl den Gerätehersteller und gehe allenfalls davon aus, dass die Daten, die das Gefrierfach generiert, von ihm bearbeitet werden. Sobald die Daten aber von einer Drittperson bearbeitet werden, weil der Gerätehersteller nicht über das fachliche Know-How verfügt, um den Inhalt meines Gefrierfachs zu analysieren und meinem Diätplan anzupassen, verwischen die Spuren. Kann ich allenfalls sogar via App mein Ess-Verhalten mit meinem Fitnessprogramm verknüpfen, so kommen die Daten unweigerlich auch beim Betreiber des Fitness-Apps zu liegen. Falls ich dieses App noch mit einem Gesundheits-App verknüpft habe, welche es meinem Arzt erlaubt, meine Bemühungen zur Senkung meines Cholesterinspiegels zu verfolgen und meiner Krankenkasse Auskunft darüber gibt, ob ich das Fitnessabonnement, welches mitfinanziert wurde, tatsächlich genutzt wird, so werden die Daten weiter und weiter gestreut.

---

31 Mögliche Lösungsansätze für diese Problematik folgen unter Ziff. IV.1.1 «Stärkung der Einwilligung und der Möglichkeiten zur Wahrnehmung der eigenen Rechte».

32 http://www.woz.ch/1349/big-data/wir-schwimmen-im-datenmeer.

[Rz 34] Die betroffenen Personen dürften heillos überfordert sein, den Lauf ihrer Daten in diesem Dschungel nachzuverfolgen und ihre Rechte wahrzunehmen. Der Schutz der eigenen Daten droht leer zu laufen: Wie soll die Eigentümerin eines intelligenten Kühlschranks nachvollziehen können, ob die gespeicherten Angaben zu ihrem Ernährungsverhalten richtig sind und ob die daraus gezogenen Schlüsse stimmen? Wie soll der Eigentümer eines intelligenten Staubsaugers kontrollieren, ob, wie in der Gebrauchsanweisung geschrieben, der Grundriss der Wohnung tatsächlich auf dem Gerät gespeichert wird, und nicht wie die programmierten An- und Abwesenheitszeiten (während derer geputzt oder eben nicht geputzt werden soll) ebenfalls in der Cloud?

[Rz 35] Viele Konsumentinnen und Konsumenten flüchten sich in die Annahme, es werde seitens der Hersteller schon alles richtig gemacht, ausserdem habe man ja nichts zu verbergen und wer wolle und könne schon bei Samsung, LG oder Miele seine Rechte geltend machen? Diese Entwicklung ist gefährlich: Wenn durch die schiere Komplexität der Ausgangslage und der Verfahren die Wahrnehmung der eigenen Rechte (faktisch oder aus der Perspektive der Betroffenen) verunmöglicht wird, wenn die Betroffenen resignieren, wie soll dann der Schutz der Persönlichkeitsrechte gewährleistet werden?

3. Spannungsfeld Technik

[Rz 36] Im Folgenden sollen einzelne Herausforderungen, welche sich aufgrund der technischen Komplexität der intelligenten Haushaltsgeräte ergeben, erläutert werden. Dabei kann es keineswegs darum gehen, die einzelnen Bereiche abschliessend zu behandeln, vielmehr sollen möglichst plastisch Risiken und Kompliziertheit der Thematik illustriert und so zur Basis für die Diskussion möglicher Lösungsansätze (Ziff. IV), gemacht werden.

3.1. Mangelnde «Privacy-Einstellungen»

[Rz 37] Wenn «intelligente» Haushaltsgeräte in Betrieb genommen werden, so sollten sie entweder als Grundeinstellung möglichst wenig Personendaten verwenden, oder aber die Benutzerin oder den Benutzer darauf hinweisen, dass gewisse «Privacy-Einstellungen» möglich sind[33]. Verfügt ein Gerät über keine «Privacy-Einstellungen» oder werden die Einschränkungsmöglichkeiten nicht transparent gemacht, so führt dies dazu, dass sich die Benutzerinnen und Benutzer notgedrungen den Datenkraken ausliefern. Insbesondere der Grundsatz der Zweckbindung kann so ganz bewusst durch die Anbieter umgangen werden. Ein Beispiel:

[Rz 38] Das Unternehmen Amazon wird mit ECHO einen Lautsprecher auf den Markt bringen[34], welcher nicht nur Musik abspielen, sondern auch als persönlicher Assistent fungieren kann. ECHO hört auf Sprachkommandos und kann etwa auch den Wecker stellen, die Einkaufsliste ergänzen und verschiedene Fragen mit Hilfe von Internet-Quellen beantworten. Um ECHO zu aktivieren, muss der Nutzer den Namen «Alexa» aussprechen, erläuterte Amazon am Donnerstag. Das setzt voraus, dass die sieben Mikrofone des Geräts ständig angeschaltet sein müssen, um das Code-Wort nicht zu verpassen. ECHO könne einen Nutzer auch verstehen, während der Lautsprecher gerade Musik abspielt. Die Sprach-Befehle werden auf Amazons Servern in der

33 Zur Thematik von privacy by default and design siehe Ziff. IV.2. «Verantwortung der Hersteller».

34 http://www.amazon.com/oc/echo.

Internet-Cloud verarbeitet[35].

[Rz 39] Was sich auf den ersten Blick als praktischer Alltagshelfer anpreist, hinterlässt den Eindruck eines Spions in den eigenen vier Wänden: Oder wie würde man es wohl interpretieren, wenn eine staatliche Stelle sieben Mikrofone in einer Wohnung installieren und diese ständig auf Empfang geschaltet lassen würde? Noch ist unklar, ob die Mikrofone die Gespräche, die sie zwangsläufig «mithören», um das Codewort nicht zu verpassen, an die Cloud schicken, um dort das Herausfiltern von für Amazon sicherlich höchst interessanten Informationen über Musik- oder Literaturvorlieben zu ermöglichen. Ebenso unklar ist derzeit auch, ob die Fragen, die via ECHO bzw. Internet beantwortet werden sollen, gespeichert und ausgewertet werden können. Amazon hat es versäumt, bei der Präsentation von ECHO auf mögliche «Privacy-Einstellungen» hinzuweisen; das Risiko, dass die Sensoren in ECHO von Amazon für Analysen der Kundschaft verwendet werden, kann damit nicht von der Hand gewiesen werden[36]. Der Grundsatz der Zweckbindung und insbesondere auch der Transparenz erscheint hier doch latent gefährdet, wie kurz nach der Präsentation von ECHO in diversen Foren festgehalten wurde[37].

3.2. Speicherort und Kontrolle über die eigenen Daten

[Rz 40] Weitere Fragestellungen können sich je nach Speicherort der Daten ergeben. Werden Daten in einer Cloud gespeichert, so verliert der Benutzer des Haushaltsgeräts faktisch jegliche Kontrolle über die Daten: Wo die Daten virtuell gelagert werden, ist in der Regel sehr schwer nachvollziehbar. Ob die Daten angemessen gesichert sind, muss schlicht angenommen werden, und ob das Datenschutzniveau desjenigen Landes, in dem die diversen Server der Cloud physisch stehen, den hiesigen Vorstellungen von einem angemessenen Datenschutzniveau entspricht, ist entsprechend schwer (oder gar nicht) überprüfbar. Darüber hinaus ist es für die betroffene Person faktisch unmöglich, ihre Zugangsrechte geltend zu machen und beispielsweise die Löschung der Daten zu verlangen bzw. zu überprüfen, ob die Daten auch tatsächlich gelöscht wurden.

[Rz 41] Davon auszugehen, dass mit einer Speicherung der Daten auf dem Gerät selbst alle Risiken ausgeräumt sind, ist jedoch verfehlt — die Risiken verlagern sich lediglich: Angenommen, der intelligente Kühlschrank wird in einer Mietwohnung eingebaut. Was geschieht mit den Daten bei einem Mieterwechsel? Kann der neue Mieter die Daten der vorgängigen Mietpartei am Kühlschrank auslesen? Muss der Vermieter die Daten löschen, oder kann der ehemalige Mieter vor seinem Auszug die Daten löschen — oder, ganz grundsätzlich: Ist das definitive Löschen der Daten überhaupt möglich? Oder aber der Roboterstaubsauger: Können die darauf gespeicherten Daten und die Zugriffsmöglichkeiten gelöscht werden, falls das Gerät weiterverkauft werden soll? Kann also ein Reset vorgenommen werden, der auch die Daten (und nicht nur die Einstellungen) komplett und unwiederbringlich löscht?

[Rz 42] Diese Fragestellungen deuten an, dass sowohl die Speicherung von Daten auf «intelligenten» Haushaltsgeräten selbst wie auch in den entsprechenden Clouds unweigerlich Auswirkungen auf die informationelle Selbst*bestimmung* der betroffenen Personen haben: Die Grundsätze der Transparenz (*wo* werden die Daten gespeichert?), der Verhältnismässigkeit (werden die Daten

35 http://www.tagesspiegel.de/wirtschaft/sprachgesteuerter-lautsprecher-amazon-hoert-mit/10947822.html.

36 http://www.slashgear.com/tags/amazon-echo/.

37 Siehe exemplarisch http://www.consumerreports.org/cro/news/2014/11/amazon-echo-is-either-the-coolest-wireless-speaker-ever-or-the-creepiest/index.htm.

wirklich gelöscht, wenn sie nicht mehr erforderlich sind?) und der Richtigkeit (*wie* wird sichergestellt, dass bei einem Gerätenutzerwechsel keine Vermischung der Profile stattfindet und Daten nicht plötzlich falsch zu geordnet werden?) werden massiv strapaziert und teilweise sogar ausgehöhlt. Dass die Wahrnehmung der Persönlichkeitsrechte zudem aufgrund der Globalisierung der Datenbearbeitungen erheblich erschwert wird, rundet das Bild des Kontrollverlusts schliesslich ab.

3.3. Sicherheitsfragen

[Rz 43] Solange ein Haushaltsgerät nicht an das Internet angeschlossen wird, muss der Informationssicherheit keine besondere Beachtung geschenkt werden. Da es aber *gerade* der Sinn und Zweck «intelligenter» Haushaltsgeräte ist, via Web mit anderen Geräten und Dienstleistern zu kommunizieren, eröffnet sich ein weiteres Feld an Fragestellungen und Risiken:

[Rz 44] Von Benutzerinnen und Benutzern oftmals vergessen oder schlicht nicht ernst genug genommen wird die eigene Verantwortung zum Schutz des Heimnetzwerks: Der mangelnde Schutz des privaten W-LAN führt dazu, dass die interne Kommunikation der heimischen Geräte ohne grosse Schwierigkeiten angezapft und Lebensgewohnheiten sowie An- und Abwesenheiten ausgelesen werden können. Hier sind die Userinnen und User in der Pflicht — es ist an ihnen, ihre Heimnetzwerke eigenverantwortlich mittels Verschlüsselungen zu sichern[38].

[Rz 45] Neben dem Heimnetzwerk können natürlich auch die Geräte selbst Ziel von Angriffen werden, wie eindrücklich eine Aktion anlässlich der Black Hat Convention Europe 2014 zeigte: Spanische Smart Meter wurden innert kürzester Zeit gehackt und die Programmierungen so verändert, dass sich der Strom in einzelnen Haushalten abdrehen sowie die Stromrechnung manipulieren liess. Auch ein Wurm wäre einfach einzuspeisen gewesen, so dass die Stromzufuhr in mehreren (!) Haushalten gleichzeitig unterbrochen und so ein Blackout herbeigeführt hätte werden können[39].

[Rz 46] Wer glaubt, dass es für eine solche Aktion eines besonderen Know-Hows bedarf, und «intelligente» Haushaltsgeräte nur von Profis manipuliert werden können, liegt jedoch falsch, wie das folgende Beispiel der Roboterstaubsauger illustriert: Intelligente Roboterstaubsauger vermessen mit ihren Sensoren die Wohnungen, welche sie putzen sollen. Einzelne Modelle tun dies mittels Lasern, andere jedoch mit Videokameras[40]. Auch wenn der Zweck der Kameras nicht die Übermittlung der vom Staubsauger gewählten Route auf das Smartphone des Besitzers ist, sondern vielmehr die Kartographierung des Raums und allfälliger Hindernisse, so sind die Kameras zwangsläufig zusammen mit dem Staubsauger mit dem Internet verbunden. Derartige Kameras können wie Webcams ohne grossen Aufwand gehackt werden: Sogenannte Remote Access Trojans, die ähnlich arbeiten wie die herkömmlichen Remote Access Tools, geben dem jeweiligen Besitzer die komplette Kontrolle über das Gerät und können im Internet als fix-fertige Software bezogen werden[41]. Das Einschleusen des Trojaners auf das Zielgerät erfolgt in der Regel durch

---

[38] Werden die Informationen schliesslich an den Hersteller oder gar an externe Programme zur weiteren Analyse gesandt, so stellt sich die Frage, wie die entsprechenden Schnittstellen und die Daten auf ihrem Weg geschützt werden — noch immer fehlen einheitliche Standards zur Verschlüsselung der Daten während ihres Transports.

[39] http://futurezone.at/science/spanische-smart-meter-koennen-einfach-gehackt-werden/91.479.373; http://eandt.theiet.org/news/2014/oct/smart-meters-hacking-spain.cfm.

[40] http://futurezone.at/produkte/dyson-360-eye-staubsaug-roboter-per-app-steuern/83.837.741.

[41] http://www.pcwelt.de/ratgeber/So_belauschen_Hacker_Sie_ueber_Ihre_Webcam-IT-Sicherheit-7915977.html. Die

vermeintliche *patches* oder Foren, die infizierte Hilfelinks anbieten. Die Kamera kann dann nach Belieben in Betrieb genommen werden und das Leben der Bewohner aufzeichnen — der durch diese Zweckentfremdung der Kamera mögliche Eingriff in die Privatsphäre ist immens.

[Rz 47] Damit derartige Angriffe analysiert und entsprechende *patches* entwickelt werden können, bedarf es der Protokollierung der Vorfälle, welche sich beim Einsatz eines Geräts ereignet haben — was aber nicht dazu führen darf, dass eine personenbezogene Auswertung der Nutzung des Geräts stattfindet. Es genügt, dass Angriffe oder Fehlfunktionen in anonymisierter Form von einem Gerät an die Entwickler gemeldet werden.

[Rz 48] In diesem Kontext stellt sich sodann auch schon die nächste Frage: Wer ist für die Durchführung der Updates der Software verantwortlich? Kann der Entscheid, ob ein Sicherheitsupdate übernommen werden soll, den Nutzerinnen und Nutzern überlassen werden, wenn andernfalls gravierende Sicherheitslücken und Angriffsmöglichkeiten bestehen blieben, wenn unter Umständen sogar unmittelbare Gefahren für die Nutzerinnen und Nutzer oder Dritte bestehen? Ausgehend vom Grundgedanken der Einwilligung und der informationellen Selbstbestimmung muss die Antwort dann klar «ja» heissen, wenn die Gefahr nur die einzelne Nutzerin und den einzelnen Nutzer betrifft[42]. Die Anbieter dürfen sich nicht länger hinter dem Argument verstecken, für die Nutzerinnen und Nutzer sei es gar nicht nachvollziehbar, welche Aktualisierungen weshalb vorgenommen werden müssen, und eine Einwilligung in das Update erübrige sich daher; vielmehr sind die Softwareentwickler gehalten, die Besitzerinnen und Besitzer der Geräte in für sie verständlicher und insbesondere sachlicher Weise über die geplante Aktualisierung zu informieren.

IV. Lösungsansätze

[Rz 49] In Anbetracht der vorangehend aufgezeigten Herausforderungen, welche «intelligente» Haushaltsgeräte mit sich bringen, könnte sich der Schluss aufdrängen, dass der Einsatz solcher Geräte kategorisch zu vermeiden sei, da sich die Risiken, welche sich durch den Einsatz «intelligenter» Haushaltsgeräte für die Persönlichkeitsrechte der Benutzerinnen und Benutzer ergeben, nicht mehr beherrschbar sind. Eine derartige Haltung wäre jedoch weltfremd und würde den zweifelsohne nützlichen Seiten dieser Geräte, welche nicht nur den Alltag der normalen Hausfrau bzw. des normalen Hausmannes erleichtern, sondern durchaus auch bei medizinischen Leiden unterstützend wirken oder gar den Verbleib einer behinderten[43] oder betagten[44] Person in der eigenen Wohnung ermöglichen können, nicht gerecht. Vielmehr sind nach der hier vertretenen Ansicht auf drei Ebenen Massnahmen zu treffen: Die Konsumenten müssten in ihrer Position gestärkt, die Hersteller in die Verantwortung genommen und die Kontroll- und Sanktionsmechanismen den aktuellen Gegebenheiten angepasst werden.

Autorin hat den Test gemacht: Auf www.malwarebytes.orgfinden sich tatsächlich zahlreiche Anleitungen zum Hacken von anderen Geräten.

42 Kann aufgrund einer Sicherheitslücke jedoch in das Gesamtsystem eingedrungen werden, wie dies bei den Spanischen Smart Metern der Fall war, darf der Entscheid nicht einzelnen Nutzerinnen und Nutzern überlassen werden. Gleichwohl ist auch in diesen Fällen offen und verständlich über das Update zu informieren.

43 http://www.digitalstrom.com/Pressemitteilungen/Neue-Moeglichkeiten-fuer-Rollstuhlfahrer-im-Smart-Home.html?listtype=date.

44 http://www.connected-home.de/ratgeber/smarte-hilfe-intelligente-technik-fuer-senioren-1467511.html.

1. Stärkung der Konsumentinnen und Konsumenten

1.1. Stärkung der Einwilligung und der Möglichkeiten zur Wahrnehmung der eigenen Rechte

[Rz 50] Die Ausführungen zu den rechtlichen Herausforderungen, welche der Einsatz intelligenter Haushaltsgeräte mit sich bringt, haben unzweifelhaft gezeigt, dass die Konzeption der Einwilligung und die Wahrnehmung der eigenen Rechte reflektiert werden muss.

[Rz 51] Die Komplexität der Bearbeitungsvorgänge droht die Einwilligung und den ihr zugrunde liegenden Gedanken der informationellen Selbstbestimmung zu entleeren. Deshalb jedoch die informationelle Selbstbestimmung als wesentliches Element der Privatautonomie komplett in Frage zu stellen, wäre aus grundrechtlicher Sicht höchst bedenklich und verfehlt. Vielmehr muss nach der hier vertretenen Auffassung den Konsumentinnen und Konsumenten wieder die Möglichkeit gegeben werden, ihre Selbstbestimmungsrechte *faktisch* wahrzunehmen. Konkret würde dies bedeuten, dass den Konsumentinnen und Konsumenten alle Informationen zur Verfügung gestellt werden müssen, die sie für den Entscheid, ob sie ein Gerät nutzen wollen, benötigen — und zwar in übersichtlicher Form und in einer leicht verständlichen Sprache, und nicht wie bisher in seitenlangen hochtechnischen AGB, welche irgendwo nach langem Suchen aufzufinden sind.

[Rz 52] Dass eine Rückbesinnung auf den Kern der Einwilligung und die verstärkte Fokussierung auf die Aufklärung über die Datenbearbeitung als vielversprechende Lösung und gangbarer Ansatz gewertet werden kann, zeigen auch die Reformbemühungen der EU: Die Richtlinie 95/46/EG, welche von der Schweiz im Rahmen der Schengen Assoziierung[45] übernommen wurde und derzeit noch das Datenbearbeiten zwischen Privatpersonen regelt, enthält nur rudimentäre Bestimmungen zur Einwilligung. Dies rührt natürlich nicht zuletzt daher, dass zum Zeitpunkt der Ausarbeitung der Richtlinie 95/46/EG eine dermassen rasante technische Entwicklung nicht absehbar war und dass ganz im Sinne der marktwirtschaftlichen Orientierung der damaligen EG die Privatautonomie im Vordergrund stand: Die Mitgliedstaaten der EU bzw. der damaligen EG sollten den Parteien möglichst wenig Vorgaben machen, wie sie ihren Willen zu bilden hatten. Die aktuelle Version der Datenschutzgrundverordnung[46] trägt der schleichenden Aushöhlung der Einwilligungsmöglichkeiten der Konsumentinnen und Konsumenten Rechnung und sieht nun eine explizite Pflicht der Datenbearbeiter vor, die Betroffenen über die Verarbeitung und Weitergabe ihrer Daten zu informieren, Nutzungsbedingungen leicht verständlich zu formulie-

[45] Art. 2 Abs. 2 i.V.m. Anhang B des Abkommens vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SAA, SR 0.362.31.

[46] Die Datenschutzgrundverordnung soll die Richtlinie 95/46/EGablösen. Der ursprüngliche Vorschlag für die EU-Datenschutzgrundverordnung, auf welchen im Folgenden, sofern nicht anders angegeben, verwiesen wird, ist abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF. In Anbetracht dessen, dass der Revisionsprozess ausgesprochen komplex ist und die EU nahezu keine konsolidierten Dokumente veröffentlicht, lassen sich die Änderungen und Diskussionen nur sehr schwer nachvollziehen. Einen guten Überblick über den aktuellen Stand, sowie diverse inoffizielle Dokumente gibt die Homepage von Jan Philipp Albrecht, dem Verhandlungsführer des Europäischen Parlaments in der Datenschutzrevision: http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html. Derzeit ist noch unklar, ob die EU-Datenschutzgrundverordnung schengenrelevant sein soll und damit ebenfalls von der Schweiz übernommen werden muss. Es ist anzunehmen, dass die Schweizer Rechtsetzung die Grundzüge der EU-Datenschutzrevision im Rahmen des sogenannt autonomen Nachvollzugs übernehmen wird. Der Einfachheit halber soll für die folgenden Ausführungen davon ausgegangen werden, dass die Schweiz die Revisionsbemühungen der EU ebenfalls berücksichtigen und zur Stärkung der Persönlichkeitsrechte der Konsumentinnen und Konsumenten nutzen wird.

ren[47], auf seitenlange AGB zu verzichten und Persönlichkeitsprofile nur dann zu erstellen, wenn die Betroffenen dies aufgrund ihrer Geräteeinstellungen erlauben — technische Standards sollen auf EU-Ebene festgelegt werden[48].

[Rz 53] Von Datenbearbeitungen betroffene Personen dürfen nicht länger zu unmündigen und unaufgeklärten Daten«objekten» gemacht, sondern müssen in ihren Kompetenzen als Daten«subjekte» gestärkt werden. Sie müssen die Möglichkeit haben, die Datenbearbeitungsvorgänge zu hinterfragen und zu durchschauen. Ein Verstecken der Datenbearbeiter hinter der technischen Komplexität der Anwendungen darf nicht mehr möglich sein, und das Pauschal-Argument, dass die Vorteile eines Bearbeitungsvorgangs die Eingriffe in die Persönlichkeitsrechte längst überwiegen würden und daher vorbehaltslos in Kauf genommen werden sollen, darf nicht mehr gelten.

[Rz 54] Diese Stärkung der Position der Konsumentinnen und Konsumenten wird auch in einem weiteren Punkt deutlich: Während bislang davon ausgegangen wurde, dass die von einer Datenbearbeitung betroffenen Personen in Eigenregie die für den konkreten Fall zuständigen Aufsichtsbehörden ermitteln und dort ihre Anliegen anbringen könnten[49] — auch hier wird die Zurückhaltung bei der Regelung privater (Datenbearbeitungs-)Verhältnisse deutlich — wird neu der sogenannte «one stop shop» vorgesehen[50]: Danach soll «die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, die einzige Anlaufstelle für den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter (sein)». Damit wird dem Umstand Rechnung getragen, dass es für Laien bzw. für von Datenbearbeitungen betroffene Personen wesentlich einfacher ist, den Hauptsitz eines Unternehmens in Erfahrung zu bringen, als zu eruieren, welche Zweigniederlassung nun für das Datenbearbeiten verantwortlich war.

[Rz 55] Diese Änderungen rechtlicher Natur sind zwar nicht fundamental oder müssten als Paradigmenwechsel bezeichnet werden — sie dürften aber, so sie denn in dieser Form die Revisionsdiskussion überstehen — durchaus effektiv, erfolgversprechend und damit eine echte Stärkung der Position der Nutzerinnen und Nutzer «intelligenter» Haushaltsgeräte sein.

1.2. Verstärkte Wahrnehmung der Eigenverantwortung

[Rz 56] Rechtliche Bestimmungen sind unbestrittener Massen ein wesentliches Element des Systems zum Schutz der Persönlichkeitsrechte. Findet jedoch kein Umdenken sowohl seitens der Userinnen und User, und damit zwangsläufig auch seitens der Hersteller statt, so dürften auch die neuen Regelungen nur im absoluten Minimum befolgt und der Schutz der Persönlichkeitsrechte weiterhin mit fadenscheinigen Argumenten möglichst rudimentär gehalten werden.

---

47 Siehe dazu auch die Änderungen, welche der Vorschlag für Erwägung 31 der Datenschutzgrundverordnung im Laufe der Debatte erfahren hat, Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), S. 18, abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fDE, sowie die vorgeschlagene Ikonographie im Anhang 1 der EU-Datenschutzgrundverordnung.

48 Art. 20 EU-Datenschutzgrundverordnung, siehe dazu auch die Begründung für den Änderungsvorschlag in Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, (Fn 46), S. 113.

49 Art. 22 Richtlinie 95/46/EG.

50 Die Bestimmung fand sich im ersten Entwurf der EU-Datenschutzgrundverordnung noch nicht, ist jedoch einsehbar in den Änderungsvorschlägen des Europäischen Parlaments, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres(Fn 46), S. 179.

[Rz 57] Wie bereits im Abschnitt zur Einwilligung unter Ziff. III.1. dargelegt, sind Userinnen und User sehr schnell bereit, die AGB eines Anbieters anzunehmen, wenn sie sich dadurch (finanzielle, oder schlicht Bedienungs-)Vorteile erhoffen. Datenschutz als entscheidendes Kriterium beim Kauf eines Gerätes wird nach wie vor nur selten in die Waagschale geworfen und auch Konsumentenschützerinnen und -schützern zeigen in dieser Sache nur sehr wenig Initiative. Hier muss zweifelsohne ein Umdenken der Konsumentinnen und Konsumenten geschehen. Dieses Umdenken kann aber nur dann stattfinden, wenn Konsumentenorganisationen, Datenschutzaufsichtsstellen und andere Einrichtungen das Bewusstsein für die Eigenverantwortung bei der Nutzung «intelligenter» Geräte stärken.

2. Verantwortung der Hersteller

[Rz 58] Weshalb sollte ernsthaft betriebener Datenschutz und Informationssicherheit nicht als Verkaufsargument und als Vorteil bzw. Qualifikation gegenüber anderen Anbietern genutzt werden? Die Zauberworte dürften hier wohl privacy by design und privacy by default sein: Unternehmer könnten beispielsweise von sich aus möglichst datensparsame Anwendungen anbieten und ihre Geräte mit datenschutz-freundlichen Voreinstellungen auf den Markt bringen. Auch eine starke Zweckbindung bzw. das (gelebte!) Versprechen, die erhobenen Daten ausschliesslich für die in den AGB klar umschriebenen und für die fraglichen Dienstleistungen erforderlichen Zwecke zu verwenden, könnte als Verkaufsargument genutzt werden. Und schliesslich wäre es auch denkbar, dass Anbieter intelligenter Haushaltsgeräte die Möglichkeit bieten, die Geräte auch ohne die Bekanntgabe von Personendaten zu nutzen[51].

[Rz 59] Dieser Ansatz wird auch von der EU unterstützt: So soll die EU-Datenschutzgrundverordnung die Anbieter nun verpflichten, ihre Geräte entweder mit datenschutzfreundlichen Voreinstellungen auszuliefern oder aber bei der ersten Inbetriebnahme datenschutzfreundliche Einstellungen anzubieten[52]. Derzeit ist noch unklar, ob und wenn ja welche EU-Behörde ermächtigt werden soll, branchenweite Standards verbindlich festzulegen[53] — immerhin sind aber Bestrebungen zu erkennen, gewisse Minimalstandards überhaupt zu regeln.

[Rz 60] Wer nun annimmt, dass mit dieser top-down Regelung das Verantwortungsbewusstsein quasi aufoktroyiert werden kann, und ein eigenständiges Umdenken damit gar nicht erforderlich ist, liegt jedoch falsch: Zum einen werden derartige Ansätze von der riesigen Masse von Lobbyisten in Brüssel vehement bekämpft und sind noch keineswegs definitiv. Und zum anderen muss man kein Verhaltenspsychologe sein, um zu erkennen, dass Überzeugungen anderer, deren Sinnhaftigkeit nicht verstanden, sondern lediglich unter rechtlichem Zwang umgesetzt werden, über kurz oder lang durch findige Winkelzüge ausgehöhlt und damit leer laufen werden.

[Rz 61] Würden privacy by design und privacy by default endlich von einzelnen marktstarken Unternehmen zum Verkaufsargument gemacht, so wäre es durchaus denkbar, dass andere Her-

---

51 Oliver Raabe/Eva Weis, Datenschutz im «Smart Home», RDV 2014, S. 237; siehe beispielsweise auch im Kontext des Smart Metering Oliver Raabe/Mieke Lorenz/Frank Pallas/Eva Weis/Alfred Malina, 14 Thesen zum Datenschutz im Smart Grid, DuD 2011, S. 521 — die Argumentation, dass für eine Vielzahl der Anwendungen ein Personenbezug nicht notwendig ist, lässt sich auch für «intelligente» Haushaltsgeräte übernehmen.

52 Erwägung 61 sowie Art. 23 Abs. 1 und 2 der EU-Datenschutzgrundverordnung.

53 Art. 23 Abs. 3 und 4 der EU-Datenschutzgrundverordnung in ihrer Ur-Fassung sahen diese Kompetenz für die Kommission vor. Im Änderungsvorschlag des Europäischen Parlaments, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres(Fn 46), wurde anstelle der Kommission das Europäische Parlament vorgesehen.

steller nachziehen und ihren Umgang mit den Daten ihrer Kundinnen und Kunden überdenken. Letztendlich könnte dieses Umdenken dazu führen, dass sich die Hersteller intelligenter Haushaltsgeräte ebenfalls ihrer Verantwortung bewusst werden und branchenweite Standards und Verhaltensregeln definieren. Ohne diese Initiative der Marktteilnehmer dürfte auch die Verankerung von privacy by design und privacy by default im EU-Recht ihre Signalwirkung schnell verlieren.

3. Stärkung der Kontroll- und Sanktionsmöglichkeiten

[Rz 62] Rechtliche Regelungen und die Stärkung des Verantwortungsbewusstseins im Umgang mit Personendaten bleiben zahnlose Tiger, wenn keine Kontrollmechanismen und Sanktionen, die als solche ernst zu nehmen sind, etabliert werden.

[Rz 63] Es ist nicht von der Hand zu weisen, dass staatlichen Kontrollorganen derzeit oftmals die Ressourcen fehlen, um die hochtechnisierten Datenbearbeitungsvorgänge, welche sich mit intelligenten Geräten ergeben, nicht nur auf ihre Rechtmässigkeit hin zu kontrollieren, sondern eben auch die Einhaltung der informationssicherheitsrechtlichen Vorgaben zu überprüfen. Wenn schon aufgrund des begrenzten Headcounts keine oder nur zu wenig Informatiker beschäftigt werden können, so müssten doch zumindest die finanziellen Ressourcen bestehen, um das technische Know-How einzukaufen[54]. Auf eine (in der Regel politisch gefärbte) Diskussion um die Frage, was eine «ausreichende» Kontrolle im Sinne des EU-Rechts ist, soll hier verzichtet werden. Klar ist, dass die Kontrollorgane nicht hinter dem technischen Fortschritt her hinken dürfen, wenn der Schutz der Persönlichkeit der Nutzerinnen und Nutzer «intelligenter» (Haushalts-)Geräte auch von staatlicher Seite ernsthaft gewährleistet werden soll.

[Rz 64] Die EU trägt auch diesem Umstand in ihrer Datenschutzrevision Rechnung, und zwar in zweierlei Hinsicht: Zum einen soll die EU-Datenschutzgrundverordnung die Position der staatlichen Aufsichtsbehörden stärken und umschreibt dazu deren Zuständigkeiten, ihre Aufgaben, ihre Unabhängigkeit und insbesondere auch die Zusammenarbeit mit anderen Aufsichtsbehörden weitaus ausführlicher, als dies bislang die Richtlinie 95/46/EG getan hatte. Zum anderen sollen Datenbearbeiter (und deren Auftragnehmer im Falle einer Auslagerung der Bearbeitungsvorgänge) unter bestimmten Voraussetzungen interne Datenschutzbeauftragte ernennen müssen. Diese(r) Datenschutzbeauftragte muss ihre bzw. seine Aufgaben unabhängig wahrnehmen können — so sieht Art. 35 Abs. 7 der EU-Datenschutzgrundverordnung beispielsweise vor, dass eine Kündigung der bzw. des Datenschutzbeauftragten nur dann zulässig sein soll, wenn sie bzw. er die Voraussetzungen für die Erfüllung ihrer bzw. seiner Pflichten nicht mehr erfüllt, und Art. 36 Abs. 2 EU-Datenschutzgrundverordnung betont noch einmal die Weisungsunabhängigkeit des bzw. der Beauftragten.

[Rz 65] Dass sowohl externe wie auch interne Kontrollinstanzen innerhalb des EU-Raumes gestärkt werden sollen, ist ausgesprochen erfreulich und zeigt, dass Persönlichkeitsrechte nicht bloss auf dem Papier festgehalten, sondern auch faktisch geschützt werden müssen. Entsprechend sollen auch Verletzungen von Persönlichkeitsrechten nicht mehr als Kavaliersdelikte verstanden werden — auch wenn keine *materiellen* Schäden entstehen, so können den betroffenen Personen

54 Ausführlich dazu Beat Rudin, Die datenschutzrechtliche Umsetzung von Schengen in den Kantonen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis, Zürich 2009, S. 237 ff.

erhebliche immaterielle Nachteile aus der Missachtung von Datenschutzgrundsätzen oder informationssicherheitsrechtlichen Vorgaben erwachsen. Grosskonzerne zeigten sich bislang von den Sanktionen, welche gegen sie ausgesprochen wurden, reichlich unbeeindruckt. Kein Wunder: Die bisher relevante Richtlinie 95/46/EG überliess — ihrer Natur als Richtlinie entsprechend — die Festlegung von Sanktionen den Mitgliedstaaten, und trug damit nur in beschränktem Masse zu einem stringenten, wirksamen und vor allem EU-weit verbindlichen Sanktionskatalog bei.

[Rz 66] Die EU will dieses Defizit nun ändern: Unternehmen sollen mit Bussen in der Höhe von bis zu fünf Prozent ihres *Jahresumsatzes* belegt werden, wenn sie gegen die Vorgaben der EU-Datenschutzgrundverordnung verstossen. In Anbetracht dessen, dass beispielsweise Amazon im Jahr 2013 allein in der Bundesrepublik Deutschland einen Jahresumsatz von 10,535 Milliarden Dollar verzeichnete[55], kann davon ausgegangen werden, dass diese Bussen durchaus ihre Wirkung haben können — wenn sie denn tatsächlich in der EU-Datenschutzgrundverordnung verbleiben sollten und nicht den Lobbyisten in Brüssel zum Opfer fallen.

V. Fazit

[Rz 67] Wenn der Backofen mit dem Staubsauger kommuniziert… was bis vor wenigen Jahren noch Utopie war, hat heute bereits Einzug in unsere Haushalte genommen. «Intelligente» Geräte als Spielereien von Technikfreaks und Nerds abzutun, wäre kurzsichtig: «Intelligente» Geräte können unseren Alltag durchaus vereinfachen und dürften insbesondere im Bereich medizinischer Betreuung oder Unterstützung wertvolle Dienste leisten. Ebenso kurzsichtig wäre es aber, diese Geräte ohne jegliche Reflexion einzusetzen und die eigenen Persönlichkeitsrechte mit der Argumentation, es werde schon nichts passieren und ausserdem habe man ja nichts zu verbergen, zugunsten von vermeintlichen Erleichterungen ihres Sinnes zu entleeren. Der rasende technische Fortschritt und die zunehmende Globalisierung der Datenbearbeitungsvorgänge stellen nicht nur die aktuellen datenschutzrechtlichen Grundsätze vor Herausforderungen, sondern bringen auch erhebliche informationssicherheitsrechtliche Risiken mit sich, welche sich in gravierender Art und Weise auf die Nutzerinnen und Nutzer auswirken können.

[Rz 68] Noch stecken die «intelligenten» Haushaltsgeräte in ihren Kinderschuhen, noch haben wir uns nicht daran gewöhnt, via App den Inhalt unseres Kühlschranks abzufragen und von unterwegs die fehlenden Zutaten für unser Abendbrot zu bestellen. Aber, erinnern wir uns noch zurück an die Zeit ohne Smartphones — wie oft stellen wir uns heute die Frage, wie wir «damals» überhaupt unseren Alltag organisieren konnten? Unsere Gesellschaft hat sich innert kürzester Zeit an die Vorteile des permanenten Online-seins gewöhnt, dabei jedoch zunehmend ihre informationelle Selbstbestimmung aus den Augen verloren. In diesen Belangen einen Wandel herbeizuführen, erscheint nun ausgesprochen schwierig. Entsprechend sollte es nicht verpasst werden, bei der weiteren Entwicklung «intelligenter» Haushaltsgeräte datenschutzrechtliche Vorgaben und informationssicherheitsrechtliche Anliegen verstärkt zu berücksichtigen: Die Position der Konsumentinnen und Konsumenten muss gestärkt, die Hersteller müssen vermehrt zur Verantwortung gezogen und Kontroll- und Sanktionsmechanismen wirklich wirksam ausgestaltet werden.

55 http://www.buchreport.ch/nachrichten/handel/handel_nachricht/datum/2014/01/31/keine-spur-von-schwaeche.htm.

[Rz 69] Die Bestrebungen der EU, der Einwilligung der von Datenbearbeitungen betroffenen Personen wieder ihr ursprünglich zugedachtes Gewicht zu verleihen und gleichzeitig die Wahrnehmung der Rechte der Betroffenen zu stärken, sind ein wichtiges Signal in diese Richtung und sollten auch in der Schweiz ernstgenommen werden — im Interesse der Sache und unabhängig davon, ob die EU-Regelungen künftig für die Schweiz verbindlich sein werden oder nicht. Ebenso grosse Bedeutung sollte dem Ansatz der EU-Datenschutzrevision, privacy by design und privacy by default in der EU-Datenschutzgrundverordnung zu verankern, zugemessen werden. Und mit der geplanten Verschärfung des Sanktionenkatalogs sollte auch dem letzten Datenschutz-Muffel bewusst werden: «Datenschutz ist kein lästiges Anhängsel, er ist keine überflüssige Bürokratie, er ist Voraussetzung dafür, dass auch in der Informationsgesellschaft das Recht auf informationelle Selbstbestimmung durchgesetzt werden kann.»[56]

[Rz 70] All dies sind Signale, welche auch den Konsumentinnen und Konsumenten bewusst machen sollten, dass sie gegenüber den Herstellern «intelligenter» Geräte im Vorteil sind: Es ist an den Konsumentinnen und Konsumenten, ihre Rechte wahrzunehmen und sich auf ihre Selbstbestimmung zu besinnen — im Zeitalter von Facebook, Internetforen, Tweets und shitstorms kann schliesslich ohne grossen Aufwand Druck auf Hersteller ausgeübt werden, und letztendlich bestimmen die Konsumentinnen und Konsumenten, ob sich datenschutzfreundliche Geräte besser verkaufen lassen als Datenkraken.

[Rz 71] Noch beanspruchen wir für unsere Gesellschaft, intelligenter als unsere Haushaltsgeräte zu sein. Diesen Vorteil sollten wir so schnell nicht aus der Hand geben.

Dr. iur. Sandra Husi-Stämpfli, LL.M. ist stellvertretende Datenschutzbeauftragte des Kantons Basel-Stadt.
Die Autorin dankt Lorenz Overhage, MLaw für die akribischen Recherchearbeiten, sowie Martin Husi und Walter Stämpfli für die kritische Durchsicht des Dokuments.

[56] Jörg Tauss, SPD, Rede vor dem Deutschen Bundestag, 29. März 2007, abrufbar unter http://dipbt.bundestag.de/dip21/btp/16/16091.pdf(zuletzt besucht am 17. November 2014), S. 9244.