ÜBERSICHT ZUR RECHTLICHEN DISKUSSION IM SPANNUNGSFELD VON DIGITALISIERUNG UND SOLIDARITÄT: DIE RECHTLICHE DEBATTE ZUM LIFELOGGING

In diesem Teilauszug einer breiteren Studie wird der Stand der rechtlichen Diskussion im Spannungsfeld von Digitalisierung und Solidarität und hier insbesondere die juristischen Herausforderungen von Lifelogging bzw. «Quantified self» betrachtet, die vom Programmierer bis zum Konsumenten für alle relevant sind. Die Analyse macht deutlich, dass viele offene Fragen bestehen, die auch das überarbeitete Datenschutzgesetz und die europäische Richtlinie, die im Mai 2018 in Kraft trat, nicht oder nur unzureichend lösen werden.

Im April 2018

Andreas Müller
andreas.mueller@politconsulting.ch

Inhaltsverzeichnis

A) Rechtliche Debatte zum Lifelogging

I) Das Thema gewinnt an Fahrt

Die Zeitschrift für Datenrecht und Informationssicherheit (digma)[1] und der Jusletter[2] behandelten Lifelogging unter Verwendung des Begriffspaars «Quantified Self» in den vergangenen zwei Jahren ausführlich. Diese Beiträge bilden so die Basis der kommenden Ausführungen, die dazu dienen sollen, die rechtswissenschaftliche Dimension von Quantified Self verständlich und bündig darzulegen und die diskussionswürdigen Aspekte hervorzuheben. Die Terminologie der juristischen Literatur aufgreifend, wird in diesem Kapitel anstelle von Lifelogging das Begriffspaar Quantified Self verwendet.

Im Bericht «Wie sieht es mit der Solidarität in einer digitalen Zukunft aus?» wurden die Chancen und Risiken von Lifelogging mit Fokus auf die Gesundheits- und die Versicherungsbranche analysiert. Es wurde gezeigt, dass diesbezüglich offene juristische Fragen bestehen, die diskutiert werden sollten.[3] In die Ideenskizze der Stiftung Sanitas hat die Frage nach einem verantwortungsvollen Umgang mit Daten Eingang gefunden. Die nachfolgenden rechtlichen Ausführungen fokussieren deshalb insbesondere das Datenschutzrecht.

Quantified Self wird auch ausserhalb der Kontexte Gesundheit und Versicherungen betrieben und die damit erhobenen Daten genutzt. Diese zwei Branchen eignen sich aber für die Darlegung der rechtlichen Fragen in Bezug auf Quantified Self sehr gut, da oft besonders schützenswerte Personendaten bearbeitet werden und bei den Krankenversicherungen das Solidaritätsprinzip rechtlich verankert ist.

---

1 BAERISWYL BRUNO, «Life Style» oder «Personalized Medecine»?, digma 2016, S. 48 ff; LANGHEINRICH MARC/SCHAUB FLORIAN/GÜNTER KARJOTH, Selbstvermessung oder Selbstüberwachung, digma 2016, S. 50 ff.; REICHERT RAMON, Das vermessene Selbst, Fitness-Tracker etablieren ein digitales Wissen der Medien und Kontrollgesellschaft, digma 2016, S. 58 ff.; ISLER MICHAEL, Lifestyle oder Medizinprodukt?, digma 2016, S. 64 ff.; GORDON CLARA-ANN, Daten aus Selbstvermessung, Eine Analyse der datenschutzrechtlichen Rahmenbedingungen von Quantified Self in der Schweiz, digma 2016, S. 70 ff.

2 PRIEUR YVONNE/HEGYI STEFAN/SPRECHER FRANZISKA, Die Messdaten der Selbstvermesser im Fokus, in: Jusletter 13. November 2017; PRIEUR YVONNE, Der Datenschutz spielt bei Quantified Self eine zentrale Rolle, in: Jusletter 13. November 2017; DIESELBE, Quantified Self birgt viel Potential für die Forschung, in: Jusletter 20. November 2017; DIESELBE, Die Kehrseite der Selbstoptimierung, in: Jusletter 27. November 2017; Dieselbe, Im Spannungsfeld zwischen Selbst- und Fremdvermessung, in: Jusletter 11. Dezember 2017; SPRECHER FRANZISKA, Quantified Self: Rechtsentwicklung – Europa gibt den Takt vor, in: Jusletter 11. Dezember 2017; WIDMER MICHAEL/HEGYI STEFAN, Ethische Normen und Werte in Zeiten von Quantified Self, in Jusletter 5. Februar 2018.

3 MÜLLER, S. 29.

II) Fragestellungen

Die rechtlichen Fragen beziehen sich sowohl auf die Quantified-Self-Produkte (QS-Produkte) selbst als auch auf die Bearbeitung der mit ihnen erhobenen Personendaten. Da mangelhafte QS-Produkte die Gesundheit gefährden können, stellt sich erstens die Frage, welchen rechtlichen Anforderungen sie genügen müssen und ob diese ausreichend sind.

Mit Quantified Self ist das Risiko verbunden, dass wir Transparenz über sensible Bereiche unserer Persönlichkeit schaffen und sich dies negativ auf uns auswirkt. Der Datenschutz bildet deshalb Kristallisationspunkte der rechtswissenschaftlichen Diskussion über Quantified Self. Zweitens wird deshalb ein Überblick über die Grundsätze der Bearbeitung von Personendaten gegeben und das Spannungsfeld von Big Data und Quantified Self thematisiert. Es rückt dabei das Recht auf informationelle Selbstbestimmung und die damit verbundenen Werte wie Privatsphäre, Autonomie und Transparenz in den Fokus.

1) Lifestyle- oder Medizinprodukt?

Die Zahl der QS-Produkte für Sport-, Fitness und Gesundheit ist gross und wenig überschaubar. Eine wichtige Rolle spielen Applikationen (Apps). Die Bewertung deren Qualität ist für Laien oft schwierig. In Studien wird immer wieder auf die mangelhafte Qualität von QS-Apps aufmerksam gemacht und bemängelt,[4] dass Qualitätsstandards fehlen.[5] Die Anbieter von QS-Apps bewegen sich aber nicht im rechtsfreien Raum. Unter Umständen sind QS-Apps als Medizinprodukte zu qualifizieren (Medical-Apps).

a) Medizinische Zweckbestimmung

Applikation zur Selbstvermessung sind gemäss Heilmittelrecht[6] Medizinprodukte, wenn sie für die medizinische Verwendung beim Menschen bestimmt sind oder angepriesen werden und deren Hauptwirkung nicht durch ein Arzneimittel[7] erreicht wird. Entscheidendes Abgrenzungskriterium der Medical-Apps zu Konsumprodukten (Gesundheits-, Fitness- und Lifestyle-Apps) ist die diagnostische, präventive oder therapeutische Zweckbestimmung.[8] Apps, die nur medizinisches Wissen vermitteln (z.B. medizinische Wörterbücher) oder administrative Prozesse

4 BECKER et al., S. 78.
5 DIESELBEN, S. 78.
6 Art. 4 Abs. 1 Bst. b HMG und Art. 1 Abs. 1 MepV.
7 GÄCHTER/RÜTSCHE, Rz. 859: «Arzneimittel sind Produkte chemischen oder biologischen Ursprungs, die zur medizinischen Einwirkung auf den menschlichen oder tierischen Organismus bestimmt sind oder angepriesen werden.».
8 FUCHS/GIOVANETTONI, Rz. 10; ISLER (2016), S. 64.

unterstützen, sind deshalb keine Medizinprodukte.[9] Apps, die die Berechnung von Medikamentendosen erlauben, sind hingegen als Medizinprodukte zu qualifizieren.[10]

b) Relevanz der Abgrenzung

Diese Unterscheidung ist relevant, weil gegenüber Medizinprodukten höhere Anforderungen bezüglich Produktesicherheit und Qualitätsmanagement gelten als bei Konsumprodukten: Die Hersteller von Medical-Apps müssen beispielsweise ein Risikobewertungsverfahren durchführen und Programmierstandards beachten.[11] Dies setzt Zeit und entsprechendes Know-how voraus.[12] Da vielen App-Entwickeln die bestehende Regulierung fremd sein dürfte,[13] ist diesbezüglich Sensibilisierungsarbeit zu leisten.

Für QS-Apps, die keine Medizinprodukte sind, gibt es keine spezifische Regulierung. Es gilt das Konsumrecht: Hinsichtlich der Produktesicherheit beim gewerblichen oder beruflichen Inverkehrbringen von Produkten das Bundesgesetz über die Produktesicherheit (PrSG) und bei Haftungsfällen das Produktehaftpflichtgesetz (PrHG) sowie das Obligationenrecht (OR).[14] Da viele Produktanbieter ihren Sitz im Ausland haben, ist die Geltendmachung und Durchsetzung insbesondere von vertraglichen Rechtsansprüchen für den Konsumenten oft schwierig und mit Risiken verbunden.[15]

c) Regulierungsbedarf?

ISLER schätzt bezüglich Medical-Apps die gesetzliche Regulierung als genügend ein, gibt aber zu bedenken, dass Überregulierungen die Innovation hemmen können.[16] STUDER sieht Verbesserungspotenzial beim Datenschutz (siehe unten) und schlägt vor, dass künftig bei der Konformitätsbewertung von Medizinprodukten ein Augenmerk auf diesen gerichtet werden sollte.[17]

BÄHLER steht der gesetzlichen Normierung von Gesundheits-, Fitness- und Lifestyle-Apps kritisch gegenüber und erachtet eine solche als verfrüht, da die Entwicklungen noch nicht hinreichend absehbar sind.[18]

---

9 FUCHS/GIOVANETTONI, Rz. 11.
10 DIESELBEN, Rz. 11.
11 ISLER (2013), S. 111.
12 Vgl. FUCHS/GIOVANETTONI, Rz. 19 ff. und KLETT, S. 107 ff.
13 ISLER (2013), S. 111.
14 PrHG und OR finden auch auf Haftungsfälle bei Medizinprodukten Anwendung.
15 BECKER et al., S. 109; PRIEUR (Datenschutz), S. 6.
16 ISLER (2016), S. 64.
17 PRIEUR (Forschung), S. 6.
18 DIESELBE (Datenschutz), S. 6.

d) Kernpunkte

Nachfolgend sind die wichtigsten Elemente der bisherigen Diskussion zusammengefasst:

- Haben QS-Produkte einen medizinischen Zweck, sind sie als Medizinprodukte speziellen gesetzlichen Anforderungen unterworfen.
- Im Bereich der Gesundheits-, Fitness- und Lifestyle-Apps gibt es keine speziellen gesetzlichen Standards. Solche wären verfrüht.
- Der Eigenverantwortung kommt ein hohes Gewicht zu. Zugleich ist es für den Konsumenten aber schwierig, bestehende Angebote auf ihre Qualität und Sicherheit zu prüfen. Anbieter von QS-Produkten im weiteren Sinne, d.h. auch Versicherer, könnten sich für einheitliche private Standards bei Gesundheits-, Fitness- und Lifestyle-Apps einsetzen. Sie könnten App-Empfehlungen machen sowie Leitfäden für deren sinnvolle Nutzung und Bewertung herausgeben.

2) Datenschutz

a) Privatsphäre und informationelle Selbstbestimmung

Die Bundesverfassung garantiert das Recht auf informationelle Selbstbestimmung.[19] Diese beinhaltet das Recht einer jeden Person, zu bestimmen, ob und zu welchem Zweck ihre Personendaten von Dritten bearbeiten werden.[20] Diese Steuerungsmöglichkeit im Dienste der Wahrung der Privatsphäre ist ein Mittel zur Gewährleistung der persönlichen Autonomie, die eine Grundlage unseres liberalen demokratischen Staatswesens bildet.[21]

Konkretisiert wird das Recht auf informationelle Selbstbestimmung durch das Datenschutzgesetz (DSG). Dieses Gesetz regelt sowohl die Bearbeitung von Personendaten durch Private als auch durch Bundesorgane. Diese Unterscheidung ist wichtig, da Bundesorgane Personendaten nur bearbeiten dürfen, wenn sie ein Gesetz dazu ermächtigt (Erlaubnisvorbehalt).[22] Private bedürfen einer solchen Ermächtigung nicht. Sofern sie die gesetzlichen Bestimmungen und den Willen der betroffenen Person beachten, dürfen sie ohne einen besonderen Rechtfertigungsgrund Personendaten bearbeiten.

Zu diesen Bestimmungen gehört namentlich, dass Personendaten nur zu den Zwecken bearbeitet werden dürfen, die bei der Beschaffung angegeben wurden (Zweckbindungsprinzip) bzw. für die betroffene Person zu diesem Zeitpunkt erkennbar waren (Erkennbarkeitsprinzip).[23] Beide Prinzipien sollen die Transparenz bewirken, die notwendig ist, damit eine Person ihr Recht auf informationelle Selbstbestimmung wahrnehmen kann. Durch die Digitalisierung und Big Data ergeben sich diesbezüglich aber diverse Herausforderungen (siehe unten).

b) Bearbeitung von Personendaten

Beim Datenschutz geht es nicht um den Schutz von Daten, sondern um den Schutz von Personen. Deshalb greift das Datenschutzrecht nur bei der *Bearbeitung* von *Personendaten* und nicht bei Sachdaten. Der juristische Begriff des Bearbeitens ist weit: Darunter fällt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten

---

19 Der Wortlaut «Schutz vor Missbrauch» des Art. 13 Abs. 2 BV ist zu eng und wird weiter ausgelegt.
20 SG-Kommentar BV-SCHWEIZER, Art. 12 Rz. 72.
21 REHBINDER, S. 10.
22 Art. 17 Abs. 1 DSG; DSG-Kommentar BAERISWYL, Art. 4 N 4.
23 Art. 4 Abs. 3 und 4 DSG.

von Daten.[24] Übermittelt ein QS-Anwender seine Personendaten auf den Server eines Dritten, auf dem sie gespeichert werden, liegt beispielsweise bereits eine Bearbeitung vor.

Personendaten sind einerseits Daten, die sich direkt einer Person zuordnen lassen (z.B. Namen, Bild), andererseits aber auch solche, die erst durch zusätzliche Informationen zuordenbar werden, sofern gemäss der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass jemand diesen Aufwand auf sich nimmt.[25]

Handelt es sich dabei um besonders schützenswerte Personendaten wie Gesundheitsdaten[26] oder werden Persönlichkeitsprofile erstellt,[27] gelten für die rechtmässige Datenbearbeitung strengere Vorschriften als bei anderen Personendaten. Insbesondere wird eine ausdrückliche Einwilligung in die Datenbearbeitung – worunter auch der Weiterverkauf von Personendaten an Dritte fällt – verlangt.[28] Des Weiteren gelten besondere Informationspflichten seitens der Bearbeiter.[29]

Mit QS-Produkten gesammelte Daten, lassen sich oft einer bestimmten Person zuordnen (z.B. mittels IP- oder MAC-Adresse). Mit Big Data nimmt die Bestimmbarkeit aufgrund der Grösse des zur Verfügung stehenden Datenpools und der hoch entwickelten Analysemöglichkeiten eher zu. Mit Quantified Self erhobenen Personendaten sind zudem nicht selten Gesundheitsdaten.[30] Werden sie so zusammengestellt, dass sie eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlauben, liegt zudem ein Persönlichkeitsprofil vor.[31] Häufig reicht deshalb für die Bearbeitung mittels Quantified Self erhobener Daten durch Dritte eine stillschweigende Einwilligung nicht aus.

c) Transparenz

Der Gebrauch des Rechts auf informationelle Selbstbestimmung setzt voraus, dass jemand erkennen kann, wer wo[32] zu welchen Zwecken seine Personendaten bearbeitet.[33] Je weniger dies

---

24 Art. 3 Bst. e DSG.

25 Art. 3 Bst. a DSG; BGE 136 II 508 E. 3.2 S. 514 (Logistep-Entscheid).

26 Art. 3 Bst. c Ziff. 2 DSG; GORDON, S. 72: «Gesundheitsdaten sind Daten, die Informationen über den physischen oder psychischen Gesundheitszustand einer Person geben, ohne dass es sich um medizinischen Ansprüchen gerecht werdende Diagnosen handeln muss.»

27 Art. 3 Bst. d DSG.

28 Art. 4 Abs. 5 Satz 2 DSG.

29 Vgl. Art. 14 DSG.

30 ISLER (2013), S. 111.

31 Art. 3 Bst. d DSG.

32 Aufgrund unterschiedlicher Datenschutzstandards in den verschiedenen Staaten, ist diese Information wichtig. Der EDÖB führt eine Staatenliste: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html>.

33 Art. 4 Abs. 4 DSG.

aus den Umständen ersichtlich wird, desto wichtiger ist die Datenschutzerklärung der Bearbeiter.[34] Dies trifft etwa zu, wenn Personendaten vom Erstbearbeiter weiterveräussert und/oder zu einem anderen Zweck bearbeitet werden, als sie erhoben wurden (Sekundärnutzung). Sowohl PÄRLI als auch BÄHLER kritisieren, dass viele Datenschutzerklärungen – falls überhaupt vorhanden - zu generell oder schwer verständlich formuliert sind, sodass viele Einwilligungen in die Bearbeitung von Personendaten zu weit gingen und deshalb zu Teilen ungültig seien.[35] Andere Autoren machen darauf aufmerksam, dass sich bei den Datenschutzerklärungen Zielkonflikte zeigen: Während QS-Nutzer über die Bearbeitung ihrer Personendaten bestmöglich informiert sein wollen und Transparenz fordern, dienen die Datenschutzerklärungen den Bearbeitern vor allem zur Compliance und weniger der Schaffung von Transparenz. Es sei jedoch zu bedenken, dass Transparenz vertrauensbildend wirken kann und deshalb für Bearbeiter auch positive Seiten hat.[36]

d) Big Data - das Ende des Datenschutzes?

Im Zeitalter der Digitalisierung und Big Data ist die Transparenz bezüglich der Bearbeitung von Personendaten, welche eine Voraussetzung für die informationelle Selbstbestimmung ist, in Frage gestellt. Es liegt eine ausgeprägte Informationsasymmetrie zwischen Bearbeitern und Betroffenen vor:[37] Personendaten werden zunehmend automatisiert und in grossen Mengen erfasst, gespeichert und ausgewertet. Es gilt das Prinzip «je mehr, desto besser».[38] Werden die Daten zudem von selbstlernenden Algorithmen bearbeitet, so sind deren Entscheidungen oft schwer voraussehbar und selten gänzlich nachvollziehbar.[39]

Indem Daten einer «unvorhersehbaren» Sekundärnutzung zugeführt werden, findet die Bearbeitung der gleichen Daten häufig in unterschiedlichen, bei der Erfassung vom Betroffenen nicht intendierten, Kontexten statt. Die kontextuelle Integrität einer Person ist dadurch gefährdet.[40] Erschliesst man den Begriff des Rechts auf Privatheit aus einer relationalen Dimension

---

34 Art. 4 Abs. 3 DSG.
35 PRIEUR (Datenschutz), S. 3; DIESELBE (Kehrseite), S. 2.
36 WIDMER/HEGYI, Rz. 32 f.
37 MÜLLER, S. 11.
38 Dies ist ein Widerspruch zum Verhältnismässigkeitsprinzip, welches besagt, dass nur gerade so viele Daten bearbeitet werden dürfen, wie für einen bestimmten Zweck erforderlich sind. Werden die Daten nicht mehr benötigt, müssen sie gelöscht werden. Da bei Big Data nicht von vornherein klar ist, wofür Daten alles gebraucht werden können, werden sie in der Regel auch nicht gelöscht.
39 HAUSER et al., S. 22.
40 DIESELBEN, S. 24.

als das Recht, sich in verschiedenen Beziehungen unterschiedlich zu präsentieren, tritt die Problematik hervor: Da man nicht in jeder Beziehung gleichwertig behandelt wird, besteht ein grosses Interesse daran, Personendaten nur gezielt preiszugeben.[41]

Unternehmen räumen sich weitgehende Nutzungsrechte an den Personendaten ein. Wer in welchem Umfang und zu welchem Zweck die Personendaten bearbeitet, ist für die Nutzer in der Regel nicht oder nur mit grossem Aufwand erkenn- und überprüfbar. Die Kontrolle über die Personendaten entgleitet und erschwert die Ausübung eigener Rechte wie dem Recht auf Berichtigung oder Vernichtung falscher Personendaten[42] und wirft wiederum die Frage nach der Reichweite von Einwilligungen in die Bearbeitung von Personendaten auf.

Zudem verschwimmen die Trennlinien zwischen Personen- und anderen Daten zunehmend, weil durch die Kombinierbarkeit von Daten aus einem grossen Fundus das Risiko der Re-Identifizierung einer Person aus nicht personenbezogen scheinenden Daten zunimmt.[43] Es muss deshalb häufiger von der Bearbeitung von Personendaten bzw. besonders schützenswerten Personendaten und den entsprechenden Rechtsfolgen ausgegangen werden als früher. Dies verdeutlicht auch die Notwendigkeit eines verantwortungsvollen Umgangs mit den eigenen Daten, auch wenn diese auf den ersten Blick nicht schützenswert erscheinen.

Wenn an dieser Stelle Big Data kritisch analysiert wird, dürfen die Chancen dieser Technologie nicht vergessen werden. Es soll aber dahingehend eine Sensibilisierung stattfinden, dass die Abwägung zwischen den Chancen und Risiken bei der Bearbeitung sehr sorgfältig vorgenommen werden muss.

e) Schwierigkeiten bei der Rechtsdurchsetzung

Die besten Gesetze bringen nichts, wenn die Rechtsdurchsetzung nicht möglich bzw. sehr schwierig ist. Prozessieren ist in der Regel aufwändig und teuer und vor allem auch dann unattraktiv, wenn sich Beweisschwierigkeiten ergeben. Insbesondere infolge Intransparenz und Informationsasymmetrien ist ein Prozess gegen (grosse) Datenbearbeiter für den Einzelnen schwierig. Erleichternde Massnahmen, z.B. eine Beweislastumkehr zugunsten betroffener Personen, werden deshalb diskutiert.[44] Schwierigkeiten beim Ausüben des Rechts auf informationelle Selbstbestimmung ergeben sich aber auch daraus, dass die Personendaten an Anbieter von

41 MATZNER, S. 75 ff.
42 Art. 15 Abs. 1 DSG.
43 THOUVENIN (Forschung), S. 33.
44 PRIEUR (Kehrseite), S. 6.

QS-Produkten übermittelt werden, die ihren Sitz und ihre Server im Ausland haben und deshalb teilweise nicht dem Schweizer Datenschutzrecht unterstehen,[45] oder aber bei einer erfolgreichen Klage die Durchsetzung des Schweizer Urteils im Ausland schwierig ist.[46]

f) Autonomie

Neben der Transparenz ist aber auch die Wahrung der persönlichen Autonomie essentiell. Werden Personendaten aufgrund äusseren Drucks Dritten zur Bearbeitung freigegeben, ist die Gültigkeit der Einwilligung in die folgende Datenbearbeitung fraglich.[47]

Im Zusammenhang mit Prämienrabatten im Versicherungssektor machte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) darauf aufmerksam, dass die Einwilligung in die Bearbeitung besonders schützenswerter Personendaten unter Umständen dann nicht mehr freiwillig erfolgt, sondern infolge finanziellen Drucks, wenn QS-basierte Versicherungsmodelle merkbar günstiger sind als alternative Modelle.[48]

g) Solidarität

Personendaten gegen günstigere Prämien? In der obligatorischen Krankenversicherung ist das bislang ein Tabu, weil das Solidaritätsprinzip, namentlich durch die Einheitsprämien, gesetzlich verankert ist. Solange das Gesetz keine Ausnahme vorsieht, dürfen Krankenversicherer die Prämien deshalb auch nicht mittels Quantified Self erhobener Personendaten «risikogerecht» ausgestalten.[49]

Auf heftige Kritik stösst gegenwärtig das Bonusprogramm Helsana+, welches mittels einer App aufgezeichnete Aktivitäten mit Barauszahlungen und Vergünstigungen in der Grundversicherung belohnt.[50] Auch wenn die Mittel dieser Auszahlungen nicht aus den Prämien der obligatorischen Krankenversicherung stammen, ist diese Entwicklung bemerkenswert.

---

45 Es gilt das Territorialitätsprinzip: Das DSG findet nur Anwendung, wenn die Daten in der Schweiz bearbeitet werden. Dafür reicht es grundsätzlich aus, wenn die Personendaten vor der Übermittlung auch nur während einer Sekunde in der Schweiz erhoben werden. Siehe dazu: GORDON, S. 72; PRIEUR (Spannungsfeld), S. 20.

46 PRIEUR (Datenschutz), S. 2.

47 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/kranken--und-unfallversicherungen/erlaeuterungen-zum-einsatz-von-fitnesstrackern-im-versicherungsb.html> (zuletzt abgerufen: 02.04.2018).

48 Fn. 55.

49 Art. 61 Abs. 1 KVG; GÄCHTER/RÜTSCHE, Rz. 1031; PRIEUR (Spannungsfeld), S. 39.

50 TISCHHAUSER PASCAL, HELSANA+-APP spioniert Nutzer aus und ergänzt mit Facebook-Daten, <https://www.blick.ch/news/politik/vertrags-bedingungen-sind-erschreckend-helsana-plus-app-spioniert-nutzer-aus-und-ergaenzt-mit-facebook-daten-id8159637.html> (zuletzt abgerufen: 25.03.2018);

Datenschutzrechtlich kritisch ist, dass die Nutzer des Programms sehr viele Personendaten freigeben, mitunter besonders schützenswerte. Bedenklich ist aber auch, dass dies gegen eine tiefe Vergütung geschieht.

h) Intensität als Problem

Die vorangehenden Ausführungen sollen zeigen, dass nicht die Bearbeitung von Personendaten per se unerwünscht und problematisch ist, sondern die zunehmende Intensität, Intransparenz und Informationsasymmetrie.[51] Je mehr Personendaten verfügbar sind und umso besser diese ausgewertet und als Selektionskriterien verwendet werden können, desto eher entgleitet dem Einzelnen die Kontrolle über sie und erhöht die Kosten der Ausübung des Rechts auf informationellen Selbstbestimmung. Diese Entwicklung trifft jene am härtesten, die sich die Kosten nicht leisten können oder wollen. Für WIDMER/HEGYI führt dies zu einer «sozialen Frage 4.0»: «Sollen Privatheit und Datenschutz Rechtsgüter sein, welche sich das Individuum leisten können muss? Oder soll das Individuum diese Rechtsgüter zumindest in gewissen Bereichen nicht «veräussern» können?»[52]

i) Rechtsentwicklungen

Die Datenschutzgesetzgebung in Europa befindet sich im Fluss. Die neue Datenschutz-Grundverordnung (DSGVO) der Europäischen Union trat am 24. Mai 2016 in Kraft und muss am 25. Mai 2018 in der gesamten EU angewendet werden. Sie führt zu einer Stärkung der Betroffenenrechte (z.B. Recht auf Vergessenwerden, Datenportabilität, strenge Einwilligungsvorschriften) und baut die Pflichten der Datenbearbeiter aus. Aufgrund ihres weiten Geltungsbereiches sind viele Schweizer Unternehmungen davon betroffen: Beispielsweise, wenn sie personenbezogene Daten von in der EU ansässigen Personen für ihre Waren- oder Dienstleistungsangebote in der EU bearbeiten.[53] Die Bestimmungen sind umfangreich und komplex. Für die Quantified Self relevanten Bestimmungen wird deshalb auf die entsprechende Literatur verwiesen.[54]

Auch das Schweizer Datenschutzgesetz befindet sich in Revision. Dabei handelt es sich um einen Balanceakt zwischen dem Schutz der Privatsphäre und dem wirtschaftlichen Bedürfnis,

---

Jacquemart Charlotte, Das Ende der Krankenversicherung?, <https://www.srf.ch/news/schweiz/umstrittene-bonus-app-das-ende-der-krankenversicherung> (zuletzt abgerufen: 23.03.2018).

51 WIDMER/HEGYI, Rz. 27.

52 DIESELBEN, Rz. 29.

53 EDÖB, S. 6 ff.

54 Näheres bei: SPRECHER, S. 4-16.

Daten ohne viele Pflichten frei bearbeiten zu können. Der Konflikt zwischen Konsumentenschutzes und Wirtschaft zeigte sich in der im letzten Jahr durchgeführten Vernehmlassung. Nach heftiger Kritik aus der Wirtschaft wurde der Entwurf abgeschwächt, was wiederum Kritik seitens des Konsumentenschutzes hervorrief.[55] In gewissen Punkten folgt der Entwurf des neuen Datenschutzgesetzes, der sich nun zur Beratung in den Räten befindet, der DSGVO, bleibt aber voraussichtlich schlanker.[56]

j) Dateneigentum?

Daten sind bekanntlich zu einem wichtigen Wirtschaftsgut geworden. Deshalb kommt immer wieder die Frage auf, ob es ein Dateneigentum braucht und wie dieses zu konzipieren wäre. THOUVENIN bietet diesbezüglich einen differenzierten Einblick:[57]

Bereits die Frage, was geschützt werden soll, ist umstritten: Soll ein Dateneigentum die syntaktische, semantische oder pragmatische Ebene von Daten umfassen?[58] Ohne einen Konsens in diesem Punkt, ist ein Dateneigentum schwer einzuführen.

Zudem ist fraglich, ob sich ein Dateneigentum rechtfertigen lässt. Während es in gewissen Konstellationen notwendig und wünschenswert ist (z.B. Daten im Konkurs), kann die Schaffung eines allgemeinen Dateneigentums zu neuen Problemen führen. Namentlich die Frage, wie sich ein allfälliges Dateneigentum zum Datenschutz verhält, ist unbeantwortet: Das Veräussern des Eigentums an Personendaten könnte zu unbefriedigenden Situationen führen, weil die Käufer (und somit neuen Eigentümer) der betroffenen Person wohl den Zugriff auf deren Personendaten verweigern dürften.[59]

k) Kernpunkte

Hier nochmals die wichtigsten Eckpunkte zur besseren Übersicht:

- Bei QS werden teilweise besonders schützenswerte Personendaten bearbeitet. Dies löst bei den Bearbeitern besondere Informationspflichten aus.

---

55 MÄDER, S. 15; RUDIN/BAERISWYL/MUND, S. 12.
56 Näheres bei: ROSENTHAL, S. 1 ff.
57 Thouvenin (Dateneigentum), S. 21 ff.; Derselbe (Datenzugangsrechte), S. 43 ff.
58 DERSELBE (Datenzugangsrechte), S. 46.
59 DERSELBE (Datenzugangsrechte), S. 56.

- Den wenigsten Nutzern dürfte vollends klar sein, was mit ihren Personendaten geschieht. Mangelndes Interesse der Nutzer, Intransparenz seitens der Bearbeiter oder infolge Big Data können Gründe dafür sein.
- Bezüglich Datenschutzerklärungen besteht Verbesserungspotenzial.
- Nicht die Bearbeitung von Personendaten per se ist ein Problem, sondern deren Zweck, Intensität sowie Art und Weise. Die Grundprinzipien des Datenschutzgesetzes konfligieren mit Big Data.
- Die Unterscheidung zwischen Personen- und Sachdaten verschwimmt aufgrund von Big Data zunehmend.
- Sind wichtige Dienstleistungen nur gegen die Lieferung von Personendaten erhältlich und weniger Personendaten-intensive Ausweichmöglichkeiten sehr unattraktiv, ist die persönliche Autonomie gefährdet.
- Die Internationalität der Sachverhalte erschwert die Rechtswahrnehmung und -durchsetzung.
- Das Verständnis des Begriffs Privatsphäre wandelt sich mit der Ubiquität der Personendaten. Welche Entwicklungen wünschenswert sind und welche nicht, muss diskutiert werden.
- Datenschutzpolitik ist ein Abwägen zwischen den Interessen der Wirtschaft und des Konsumentenschutzes.

III) Handlungsoptionen

1) Allgemein

Eine Laissez-faire-Datenpolitik wird sich nach dem «Cambridge-Analytica-Skandal» vermutlich nicht ergeben: Die Umfragen von sotomo hat zutage gebracht, dass das Thema Datenschutz viele Menschen beschäftigt. Neue Technologien wie Big Data gefährden einerseits die informationelle Selbstbestimmung, bergen aber andererseits ein hohes Innovationspotenzial. Der gesetzgeberische Balanceakt besteht deshalb darin, die Interessen von Konsumenten und Konsumentinnen durch griffige Datenschutzbestimmungen zu wahren, ohne der Wirtschaft engere Grenzen vorzugeben. Das dies keine einfache Aufgabe ist, zeigen die Diskussionen anlässlich der Revisionen der EU-Datenschutz-Grundverordnung und des Schweizer Datenschutzgesetzes. Die konkrete Weiterentwicklung der Datenschutzgesetzgebung ist folglich ein Thema, welches sich insbesondere für Expertenrunden eignet. Das gilt auch bezüglich des Themas Dateneigentum.

Namentlich unklare, schwer verständliche Datenschutzerklärungen sowie die Sekundärnutzung von Personendaten sorgen für Intransparenz, Informationsasymmetrien und erschweren die Ausübung persönlicher Rechte. Im Sinne einer «best practice» im Datenschutz sollten Unternehmen deshalb zur Behebung dieses Missstandes beitragen. Letztendlich können sie dadurch ihre Glaubwürdigkeit stärken und das Vertrauen der Kundschaft gewinnen.

Sowohl das Verständnis über Inhalt und Bedeutung von Privatheit als auch die Einstellung gegenüber verschiedenen Formen und Kontexten der Bearbeitung von Personendaten, sind dem kulturellen Wandel unterworfen. Die Bedeutungsveränderungen treten oft schleichend ein. Andreas Bernard arbeitet beispielsweise in einem Buch eindrücklich heraus, wie Technologien, die ursprünglich aus Psychiatrie und Kriminologie stammen durch Social Media, von der Gesellschaft unbemerkt, zu Alltagsanwendungen wurden, und wie sich unser Verständnis von Selbstpräsentation im Internet in den letzten zwei Jahrzehnten gewandelt hat.[60] Die Gefahr bei solch schleichenden Veränderungen ist, dass sie neue Tatsachen schaffen und unser bisheriges Normverständnis verändern, ohne das rechtzeitig eine der Sache angemessene Diskussion darüber stattgefunden hat. Was ein eigenverantwortlicher Umgang mit Personendaten im digitalen Zeitalter bedeutet und inwiefern sich Werte wie informationeller Selbstbestimmung, Transparenz, Autonomie und Solidarität verändern, soll deshalb in einem möglichst breiten Diskurs

60 BERNARD ANDREAS, Komplizen des Erkennungsdienstes, Das Selbst in der digitalen Kultur, 2. Aufl., Frankfurt am Main 2017.

anhand konkreter Beispiele besprochen werden. Bezüglich der Solidarität könnte das angesprochene Bonusprogramm der Helsana in der obligatorischen Krankenversicherung eine Manifestation eines solchen tiefgreifenden Veränderungsprozesses sein, welcher sich zur Diskussion eignet.

Ein zentrales Kriterium der (rechtswissenschaftlichen) Beurteilung solcher Sachverhalte ist das Kriterium der Verhältnismässigkeit:

- Eignen sich beispielsweise solche Quantified-Self-Bonusprogramme wirklich, um Krankenkassenkosten zu senken?
- Sind solch weitgehende Datenbearbeitungstätigkeiten zur Erreichung des Zieles notwendig?
- Oder gibt es mildere Mittel? Konsumenten sollten sich fragen, ob der Nutzen in Relation zu den gewährten persönlichen Einblicken gerechtfertigt ist und sich für sie langfristig lohnt.

2) Studie TA-Suisse

In einer dieses Frühjahr von TA-SUISSE herausgegebenen Studie,[61] werden hinsichtlich der Qualität von QS-Produkten und des Datenschutzes zahlreiche Handlungsempfehlungen gemacht. Diese Empfehlungen gliedern sich einerseits nach Stakeholdern, andererseits nach Ihrem Handlungshorizont:

«*Handlungsempfehlungen für die Jahre 2018-2021:*

1. *Die Schweizer Herstellerverbände entwickeln ein Qualitätslabel für QS-Produkte im Lifestyle-Bereich. Konsumentenorganisationen und die zuständigen staatlichen Aufsichtsstellen verstärken die Marktbeobachtung hinsichtlich den QS-Konsumprodukten.*
2. *Die Konsumentenorganisationen sowie die zuständigen Aufsichtsstellen, d.h. das Staatssekretariat für Wirtschaft sowie der Eidg. Datenschutzbeauftragte, intensivieren im Rahmen ihrer Kompetenzen die Marktbeobachtung hinsichtlich der Entwicklung von QS-Konsumprodukten und intervenieren bei Bedarf.*

[61] BECKER et al, S. 1 ff.

3. *Neue Medizinprodukte werden vor der Markteinführung durch die zuständigen Kontrollstellen, d.h. Swissmedic in Zusammenarbeit mit dem Eidg. Datenschutzbeauftragten, auf ihre Datenschutzkonformität sowie auf ihre Datensicherheit geprüft.*

4. *Der Gesetzgeber steuert den rasch wachsenden digitalen und globalen Handel mit Gesundheitsdaten in gesellschaftlich erwünschte Bahnen und stärkt die Betroffenenrechte. In den Geschäftsbeziehungen zwischen Produkteherstellern und Dienstleistern mit Selbstvermessern sind neben dem Datenschutzrecht weitere Rechtsgebiete wie das Konsumentenrecht möglichst zeitnah an diese Herausforderungen anzupassen. Konkret wird dem Gesetzgeber empfohlen, bei der Totalrevision des Bundesgesetzes über den Datenschutz die Verfahrensrechte der von Datenbearbeitungen betroffenen Personen nachhaltig zu stärken.*

5. *Konsumentenschutzorganisationen prüfen die QS-Konsumprodukte hinsichtlich Datenqualität, Datenschutz und -sicherheit, Vertragsbedingungen sowie Nutzerfreundlichkeit und veröffentlichen die Ergebnisse.*

6. *Berufsverbände und Fachorganisationen der Gesundheitsberufe empfehlen ihren Mitgliedern Medizinprodukte für ihre Fachgebiete.*

7. *Forschungsförderer (z.B. Bundesamt für Gesundheit, Innosuisse - Schweizerische Agentur für Innovationsförderung, Schweizerischer Nationalfonds, Schweizerischen Akademie der Medizinischen Wissenschaften, Stiftungen) unterstützen Projekte im Bereich Health Technology Assessment inkl. Quality Assessment zum Prüfen des Potentials von QS-Anwendungen in der Gesundheitsversorgung und -förderung. Ebenso werden Studien und Aufträge aus der angewandten Begleitforschung zu rechtlichen, ethischen, technischen und psychologischen sowie den gesellschaftlichen Auswirkungen von QS gefördert.*

8. *Bildungsinstitutionen, Konsumentenschutzorganisationen, Patientenorganisationen, das Bundesamt für Gesundheit, die Gesundheitsförderung Schweiz und eHealth Suisse regen über Veröffentlichungen, Veranstaltungen und ggf. Kampagnen eine gesellschaftliche Diskussion über die Chancen und Risiken von QS für Individuen und die Gesellschaft an.*

9. *Aus- und Weiterbildungsstätten im Gesundheitswesen (Fachschulen, Fachhochschulen und Universitäten) nehmen das Thema QS auf und machen Angebote für berufsgerechte Informationen und Kompetenzbildung.*

Handlungsempfehlungen für 2022 und darüber hinaus:

1. *Fachorganisationen der Gesundheitsförderung und Prävention empfehlen ihren Mitgliedern für die Anwendung im Lifestyle-Bereich QS-Produkte mit Qualitätslabel.*

2. *Die Schweizer Herstellerverbände publizieren ein Verzeichnis, in dem QS-Konsumprodukte mit Label aufgelistet sind.*

3. *Das Bundesamt für Gesundheit nimmt vermehrt QS-Geräte und -Apps, die sich als wirksame, zweckmässige und wirtschaftliche Medizinprodukte bewährt haben, in die Liste der von der Grundversicherung finanzierten Leistungen auf.»* [62]

3) Bemerkungen

Im ersten Teil dieses Kapitels wurde die Qualität von Gesundheits-, Fitness- und Lifestyle-Apps thematisiert und darauf hingewiesen, dass diesbezüglich Handlungsbedarf besteht. Die Handlungsoptionen der TA-Suisse werden vor diesem Hintergrund als adäquate Massnahmen gegen die oben identifizierten Lücken erachtet. In der Stossrichtung stimmen sie mit den Zielen der Stiftung Sanitas überein.

Interessanterweise werden in der achten Handlungsempfehlung zwar die Patientenorganisationen aufgeführt, nicht jedoch die Versicherer. Mit der Thematisierung des Dossiers «Solidarität in der digitalen Welt» setzt die Stiftung Sanitas ein positives Zeichen. Auch als Anwenderin / Anbieterin einer Gesundheitsapp-Lösung, könnte sie die Ausarbeitung von Standards anstossen.

Bezüglich Datenschutz gilt es die zukünftigen Entwicklungen weiterzuverfolgen. Insbesondere im Bereich der Datenzugangsrechte sind noch diverse Fragen offen, die einer genaueren Untersuchung bedürfen.[63]

62 BECKER et al, S. 137 ff.

63 Thouvenin (Datenzugangsrechte), S. 73.

LITERATURVERZEICHNIS

BAERISWYL BRUNO/PÄRLI KURT, Datenschutzgesetz, Bern 2015 (zit. DSG-Kommentar BEARBEITER, Art. … N …)

BECKER HEIDRUN et al., Quantified Self – Schnittstelle zwischen Lifestyle und Medizin, Winterthur 2017

COOPER et al., Guarding and growing personal data value, Accenture Outlook, London, 2016 (Das Dokument ist abrufbar unter: <https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf>)

EDÖB, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, Januar 2018. (Das Dokument ist abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO.html>)

EHRENZELLER BERNHARD/SCHINDLER BENJAMIN/SCHWEIZER RAINER J./VALLENDER KLAUS A. (Hrsg.), Die Schweizerische Bundesverfassung, Kommentar, 3. Aufl., Zürich/St. Gallen 2014 (zit. SG-Kommentar BV-BEARBEITER, Art. … Rz. …)

ESSELMANN F./BRINK A., Corporate Digital Responsability: Den digitalen Wandel von Unternehmen und Gesellschaft erfolgreich gestalten, in: Spectrum (12-1), S.38-41 (Das Dokument ist abrufbar unter: <https://unternehmensethik.org/wp-content/uploads/2016/09/spektrum_2016-1__SONDERDRUCK.pdf>)

FACHGRUPPE «Wirtschaftliche Potentiale und gesellschaftliche Kompetenz» des Technologieprogramms «Smart Data- Innovationen aus Daten», Corporate Digital Responsibility, Berlin, 2018 (Das Dokument ist abrufbar unter: <http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2018_02_smartdata_corporate_digital_responsibility.pdf;jsessionid=0215D020E422FF1AD1EA4BE4B4044F9F?__blob=publicationFile&v=7>)

FUCHS PHILIPP/GIOVANETTONI MARCO, Apps als Medizinprodukte – und die Folgen davon, in: Jusletter 27. Mai 2013

GÄCHTER THOMAS/RÜTSCHE BERNHARD, Gesundheitsrecht, Ein Grundriss für Studium und Praxis, 4. Aufl., Basel 2018

GORDON CLARA-ANN, Daten aus Selbstvermessung, Eine Analyse der datenschutzrechtlichen Rahmenbedingungen von Quantified Self in der Schweiz, digma 2016, S. 70 ff.

HAUSER et al., Ethische Herausforderungen für Unternehmen im Umgang mit Big Data, 2017

HORN NIKOLAI, Grundlagen der digitalen Ethik-eine normative Orientierung in der vernetzten Welt, Berlin 2017 (Das Dokument ist abrufbar unter: <https://initiatived21.de/app/uploads/2017/08/01_denkimpulse_ag-ethik_grundlagen-der-digitalen-ethik.pdf>)

ISLER MICHAEL, Lifestyle oder Medizinprodukt?, digma 2016, S. 64 ff. (zit. ISLER (2016), S. …)

DERSELBE, Mobile Medical Apps: Patient Datenschutz, digma 2013, S. 110 ff. (zit. ISLER (2013), S. …)

JÄNIG JENS-RAINER, Corporate Digital Responsability Framework, Berlin, 2017 (Das Dokument ist abrufbar unter: <http://corporate-digital-responsibility.de>)

KLETT BARBARA, Digitalisierte Gesundheit, Abgrenzungen und Regulierung, HAVE 2017, S. 104 ff.

MÄDER LUKAS, Datenschutz ohne «Swiss finish», NZZ vom 16. September 2017, 15

MANSKE JULIA/ KNOBLAUCH TOBIAS, Datenpolitik jenseits von Datenschutz, Stiftung Neue Verantwortung Berlin 2017, (Das Dokument ist abrufbar unter: <https://www.stiftung-nv.de/sites/default/files/datenpolitik.pdf >)

MATZNER TOBIAS, Der Wert informationeller Privatheit jenseits von Autonomie, in: Burk Steffen et. al. (Hrsg.), Privatheit in der digitalen Gesellschaft, Berlin 2018, S. 75 ff.

MÜLLER ANDREAS, Wie sieht es mit der Solidarität in einer digitalen Zukunft aus ?, Eine kritische Würdigung des Lifeloggings, Zürich 2017 (Das Dokument ist abrufbar unter: <https://www.sanitas.com/content/dam/sanitas-internet/main/Ueber_Sanitas/Sanitas%20Stiftung/Solidarit%C3%A4t_Lifelogging_AM_Mai_2017.pdf>)

MÜLLER LENA-SOPHIE / ANDERSEN NICOLAI, WARUM WIR UNS MIT DIGITALER ETHIK BESCHÄFTIGEN SOLLTEN, BERLIN, 2017 (DAS DOKUMENT IST ABRUFBAR UNTER: <https://initiatived21.de/app/uploads/2017/08/01-2_denkimpulse_ag-ethik_digitale-ethik-ein-denkmuster_final.pdf>)

PRIEUR YVONNE, Der Datenschutz spielt bei Quantified Self eine zentrale Rolle, in: Jusletter 13. November 2017 (zit. PRIEUR (Datenschutz), S. …)

DIESELBE, Die Kehrseite der Selbstoptimierung, in: Jusletter 27. November 2017 (zit. PRIEUR (Kehrseite), S. …)

DIESELBE, Im Spannungsfeld zwischen Selbst- und Fremdvermessung, in: Jusletter 11. Dezember 2017 (zit. PRIEUR (Spannungsfeld), S. …)

DIESELBE, Quantified Self birgt viel Potential für die Forschung, in: Jusletter 20. November 2017 (zit. PRIEUR (Forschung), S. …)

REHBINDER MANFRED, Ist Privatsphäre wichtig?, Die Sicht der Psychologie, in: Boehme-Nessler Volker/Rehbinder Manfred (Hrsg.), Big Data: Ende des Datenschutzes?, Bern 2017, S. 9 ff.

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017

RUDIN BEAT/BAERISWYL BRUNO/MUND CLAUDIA, Revision des Datenschutzgesetzes, Keine souveräne Lösung, NZZ vom 31. Oktober 2017, 12

SPRECHER FRANZISKA, Quantified Self: Rechtsentwicklung – Europa gibt den Takt vor, in: Jusletter 11. Dezember 2017

THORUN CHRISTIAN, Corporate Digital Responsability: Unternehmerische Verantwortung in der digitalen Welt, S.173-S.191 in: C.Gärtner und C.Heinrich, Fallstudien zur Digitalen Transformation, 2017

THOUVENIN FLORENT, Dateneigentum und Datenzugansrechte – Bausteine der Informationsgesellschaft?, zsr 2018, S. 43 ff. (zit. Thouvenin (Datenzugangsrechte), S. …)

DERSELBE, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Nessler Volker/Rehbinder Manfred (Hrsg.), Big Data: Ende des Datenschutzes?, Bern 2017, S. 27 ff. (zit. Thouvenin (Forschung), S. …)

DERSELBE, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, S. 21 ff. (zit. Thouvenin (Dateneigentum), S. …)

WEHOFSITS ANNA, Big Data- Ethische Fragen, Vodafone Institut für Gesellschaft und Kommunikation, Berlin 2016 (Das Dokument ist abrufbar unter: <http://www.vodafone-institut.de/wp-content/uploads/2016/10/Big-Data_Ethische-Fragen.pdf>)

WIDMER MICHAEL/HEGYI STEFAN, Ethische Normen und Werte in Zeiten von Quantified Self, in Jusletter 5. Februar 2018