Verbraucherschutz und rechtliche Aspekte: **Hintergrundinformationen für junge Menschen und Lehrende**

Worum geht es?

Mit Selbstvermessungstechnologien lassen sich körperbezogene Daten erfassen und messen. Mit den auf diese Weise erfassten Daten erhalte man nicht nur mehr Kontrolle über seinen Körper und seine Gesundheit. Man könnte anschließend selbstständig darüber entscheiden, ob und inwiefern man seine Verfassung oder sein Verhalten, gesünder zu leben, verändern möchte. Der Vorteil für die Verbraucherin und den Verbraucher bestünde darin, dass sie oder er ständig über den eigenen Körper- und Gesundheitszustand informiert wird. Demgegenüber stehen mit diesen Technologien verbundene Unsicherheiten, die es aufzudecken und zu begrenzen gilt. Die Nutzung von Wearables – am Körper getragene Messgeräte – bringt eine Masse von Daten hervor, an denen externe Akteure interessiert sind. In der Medizin können solche Technologien Ärzt*innen und Patient*innen bei Diagnosen und Therapien unterstützen, die Forschung erfährt mehr über das Gesundheitsverhalten der Nutzer*innen und kann aus mehreren Perspektiven wichtige wissenschaftliche Schlussfolgerungen ziehen. Die Werbeindustrie oder Krankenkassen sind ebenso an solchen Informationen interessiert, denn damit ließen sich beispielsweise kommerzielle Ziele besser verfolgen bzw. längerfristig Kosten einsparen.

Während die mittels Wearables erhobenen Daten in der Regel benutzt werden, um sich ein Bild über die eigene körperliche oder gesundheitliche Verfassung zu verschaffen, ist bislang nicht nachgewiesen, inwiefern diese Geräte und Apps Nutzer*innen dazu bewegen, ihr Verhalten mit Blick auf ihre Gesundheit zu verändern.

Ausblick

Zurzeit nutzen 14 Prozent der deutschen Internetnutzer*innen ein Wearable; das Marktpotenzial scheint aber wesentlich größer. Laut dem Digitalverband Bitkom (2015) gaben 40 Prozent der Befragten einer Telefonbefragung an, sich zumindest für die Nutzung einer Smartwatch zu interessieren, obwohl zum Zeitpunkt der Befragung solche Technologien noch nicht genutzt wurden. Man rechnete bis zum Jahr 2018 mit einem Marktwachstum von jährlich 21 Prozent.

Der allgemeine Trend, Apps und Wearables zu nutzen, wird durch eine im Rahmen des LogMySelf-Projekts durchgeführte Befragung bestätigt. Zwischen 40 bis 80 Prozent der etwa 1000 befragten jungen Personen zwischen 14 und 25 Jahren können sich demnach je nach Anwendungsbereich vorstellen, Selbstvermessungstechniken zu nutzen.

Beide Beobachtungen weisen auf einen Prozess hin, in dem neue und marktgetriebene Formen des Monitorings und Managements der Gesundheit, des Lebensstils und Verhaltens entstehen oder bereits entstanden sind. Mit dem Eintritt kommerzieller Akteure in Bereiche der Medizin und des Gesundheitswesens rücken auch ethische und rechtliche Probleme in den Vordergrund und es steigt die Aufmerksamkeit für neue technologische Risiken für die Gesundheit, die Sicherheit und die Privatsphäre.

Vor dem Hintergrund der zu erwartenden, zunehmenden Nutzung von Selbstvermessungsgeräten, auch durch junge Menschen, nimmt die Bedeutung eines sicheren Umgangs mit Daten zu.

Perspektive des Verbraucherschutzes

Aus Sicht des Verbraucherschutzes werfen Selbstvermessungstechniken Fragen über die Technologie, über deren Nutzung und über mögliche Risiken der Erfassung und Weiterleitung der Daten sowie die

Wirkung der Selbstvermessungstechnologien für Individuen und Gesellschaft auf. Dazu zählen Fragen nach der technischen Qualität der Wearables und Apps, nach der Notwendigkeit, der Sicherheit und der Zuverlässigkeit der Vermessung und Datenauswertung. Aber auch die Bedeutung von Verbesserungspotenzialen –persönlich oder für die Gesellschaft – oder der Beitrag der Quantifizierung und der Überwachung unserer Körperfunktionen für die Verbesserung der Lebensqualität verlangen eine ernsthafte Aufmerksamkeit und eine entsprechende öffentliche Debatte, weil eine Vielzahl individueller und gesellschaftlicher Interessen zunehmend davon betroffen sein werden.

Aus der Perspektive des Verbraucherschutzes stellen deshalb der Datenschutz und die Datensicherheit zentrale Themen der Diskussion dar.

Datenschutz

Die Anwendung von Gesundheits-Apps enthält Risiken hinsichtlich des Datenschutzes, denn die mit Geräten und Apps gesammelten Daten ermöglichen (genaue) Einblicke in die persönliche Lebensführung und werden als hochsensibel gehalten. Es handelt sich dabei um personenbezogene Daten, also Daten, die „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ beinhalten.[1] Personenbezogene Daten geben nicht nur Aufschluss über eine Person, sondern sie ermöglichen es auch, Personen direkt oder indirekt zu identifizieren. Deswegen ist die Erhebung, die Speicherung und die Nutzung solcher Daten nur dann erlaubt, wenn eine gesetzliche Gestattung oder eine Einwilligung des Betroffenen hierzu vorliegt.

Die Datensouveränität (der selbstbestimmte Umgang mit Daten) des Einzelnen ist hiermit allerdings nicht erreicht. Sie setzt voraus, dass sich der Einzelne der Risiken und Potenziale des Dateneigentums bewusst ist und diese angemessen und unter Wahrung der informationellen Selbstbestimmung in unserer vernetzten Welt einsetzen kann.[2] Da diese Voraussetzung nicht von jedem Einzelnen erfüllt wird, ist der Konflikt zwischen der freien Datennutzung und der souveränen Datenverwaltung des Einzelnen damit nicht aus der Welt. Eine weitere Einschränkung der Datensouveränität des Einzelnen hängt mit der mangelnden Transparenz der Verwendungen vieler Datenanalysetechniken zusammen, die keinen Einblick in den Umgang mit den erhobenen Daten gewähren. Auch das Nutzen von Datenspuren durch Dritte ist schwierig zu kontrollieren: Erstens können Daten über verschiedene Geräte eines Individuums unbemerkt gesammelt werden und zweitens wird ein Großteil dieser Daten in Drittländer exportiert, wo deren Nutzung nicht mehr dem deutschen oder europäischen Rechtsrahmen unterliegt.

Aber aus Sicht des Verbraucherschutzes ist zunächst entscheidend, dass der / die einzelne Nutzer*in das Grundrecht auf informationelle Selbstbestimmung auch im Kontext der Wearable- und Fitness-App-Nutzung für sich beanspruchen kann und dass dies gesetzlich legitimiert wird.[3] Das beinhaltet, dass jede*r selbst darüber bestimmen soll, welche Daten er / sie von sich preisgibt, wie diese weiterverarbeitet werden und wer Zugriff darauf hat. Dies entspricht auch dem Wunsch der Verbraucher*innen, was den Umgang mit ihren Gesundheits- und Fitnessdaten betrifft.

[1] im Sinne des BDSG §3 Abs. 1 (deutsches Bundesdatenschutzgesetz).
[2] Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Deutscher Ethikrat. Stellungnahme (2017).
[3] Bundesverfassungsgericht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG hergeleitet (Grundgesetz für die Bundesrepublik Deutschland).

Wie bereits angedeutet, drängt sich vor diesem Hintergrund allerdings die Frage auf, wie informiert der / die Konsument*in sein soll oder sein kann, bevor man seine Informationen mittels Selbstvermessungstechnologien preisgibt. Unter diesen Bedingungen ist weiter relevant, wie datenschutzgerechte Anwendungen für Nutzer*innen deutlich erkennbar gemacht werden können.

Datensicherheit

Die Datensicherheit sollte sich in Form von technischen und organisatorischen Maßnahmen niederschlagen.[4] Sie sollten die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen durch Sicherheitsvorkehrungen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen gewährleisten. Diejenigen, die für die Datenverarbeitung verantwortlich sind, haben die Verpflichtung, diese Daten vor dem Zugriff durch unbefugte Dritte zu schützen. Ein Beispiel wäre der Fall, in dem Unbefugte ohne viel Mühe auf sensible Nutzerdaten zugreifen könnten, wenn die Datenübertragung zwischen Fitness-App und Anbieterserver nicht nach dem Stand der neuesten Technik gesichert wäre. D.h., dass bei unzureichender Sicherung der Geräteverbindung das Tragen eines Wearables auf die Identität des Nutzers schließen lässt.

Wenn für eine Dienstleistung über erforderliche Daten hinaus personenbezogene Daten erhoben werden, müssen diese nicht nur hinreichend gesichert sein. Es muss vor allem eine informierte Einwilligung des / der Nutzer*in eingeholt werden. Aus Perspektive des Verbraucherschutzes muss daher geklärt werden, inwieweit Wearable-Anbieter ihren Nutzer*innen Möglichkeiten zur Einflussnahme und Kontrolle ihrer Daten einräumen.

Diskussionsfragen für Modul 3

Mögliche Leitfragen

Welche Vorkehrungen könnte man treffen, um seine mit dem Wearable erhobenen Daten sicher zu speichern?

Auf gespeicherte Daten können Anbieter von Wearables und Apps zugreifen. Sie bräuchten dafür aber die informierte Einwilligung der Nutzer*innen. Sind junge Menschen z.B. über die AGB ausreichend über die Bedingungen, die dem Anbieter den Zugang zu den gespeicherten Daten erlauben, informiert?

Wenn dies nicht der Fall ist, erkundigt man sich über den Daten- und Verbraucherschutz im Zusammenhang mit der digitalen Selbstvermessung?

Welche Folgen könnte die Verletzung der Verpflichtung, gespeicherte Daten vor dem Zugriff unbefugter Dritter zu schützen, nach sich ziehen?

Was könnte gesellschaftlich getan werden, um den Datenschutz und die Datensicherheit besser zu gewährleisten?

Welche Vorkehrungen haben die Teilnehmer*innen bereits für ihren persönlichen Datenschutz und ihre Datensicherheit getroffen?

[4] gemäß § 9 BDSG.

Hinweise auf Materialien für Modul 3

Das Modul 3 „Verbraucherschutz u. rechtliche Aspekte“ umfasst neben einer Einführung mit Diskussionsfragen das „Miniszenario 3 Familienplanung im Blick“. Beide Texte dienen einer vertieften Auseinandersetzung mit ethischen, sozialen und rechtlichen Aspekten der digitalen Selbstvermessung. Entsprechende Diskussionsfragen ergänzen das Miniszenario.

Die Datei „Graphic Recording“ enthält die Grafik „Problemaufriss Self-Tracking“, in der die mit der Datenerhebung und -sammlung einhergehende Problematik, wie vom Experten Jochen Meyer betrachtet, dargestellt wird. Dort befindet sich auch eine graphische Wiedergabe hierzu aus Sicht der freien Wissenschaftlerin Julia Krüger.

Die Materialien enthalten des Weiteren auch die bereits für Modul 2 aufbereiteten kurzen Videosequenzen zum Thema Daten und ein Video in Langfassung.