Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg

ALGORITHMEN

#seiunberechenbar ... in Sachen Gesundheit

PantherMedia / Wavebreakmedia ltd

Erkrankungen, Allergien, Fitnessdaten und Co. sind die persönlichsten Informationen eines Menschen. Doch auch sie fließen in algorithmische Bewertungen ein – wenn man es nicht verbietet.

Eine tolle Sache: Jogging-Shirt und -Hose überstreifen, Turnschuhe anziehen, ran mit der „Fitness-Uhr" ans Handgelenk: Und schon kann der Hobbysportler über Stock und Stein flitzen und die Aufzeichnungen seiner Gesundheitsdaten seinem „Wearable" überlassen. Kein lästiges Pulsfühlen mehr, kein umständliches Blutdruckmessen nach dem Lauf: Alles perfekt aufgezeichnet durch den digitalen Helfer am Handgelenk. Und der weiß auch noch viel mehr: Wieviel Schritte wir geschafft haben, ob wir dabei ins Keuchen gekommen sind oder am Hügel schlapp gemacht haben. Kurzum: Er gibt uns alle nur erdenklichen Daten über unsere körperliche Fitness.

Intime Daten im Netz

Doch diese Daten sieht nicht nur der Nutzer. Eine Untersuchung des Marktwächters Digitale Welt der Verbraucherzentralen ergab: Keine der geprüften Fitness-Apps, die per Handgelenk-Gerät eine Verbindung zum Internet aufbaut, ließ sich ohne Netzanbindung nutzen. Privatsphäre? Fehlanzeige. Die digitalen Geräte am Arm sammeln neben dem Pulsschlag auch Daten wie etwa den Kalorienverbrauch ihrer Nutzer oder wie lange und wie gut diese schlafen.

Bei den meisten von dem Marktwächter untersuchten Apps werden zahlreiche Nutzerdaten, darunter auch Gesundheitsdaten, an die Anbieter gesendet. Die Ergebnisse einer technischen Prüfung des Marktwächters zeigen zudem, dass eine Kontrolle über die eigenen Daten bei der Wearable- und Fitness-App-Nutzung für Nutzer kaum möglich ist: Die gesammelten Daten wurden vom Smartphone direkt an die Anbieter weitergeleitet.

Maik Morgenstern ist Technischer Leiter von AV-Test, einem unabhängigen Forschungsinstitut für IT-Sicherheit. Er sieht die Nutzung insbesondere von Fitnesstrackern durchaus kritisch: „Einerseits lassen sich bei manchen Geräten Daten durch Angreifer auslesen und manipulieren. Andererseits erheben einige Hersteller unnötig viele Daten." Diese würden dann an eigene Server übermittelt und es bleibe unklar wie diese Daten genutzt, verarbeitet und an wen sie weitergegeben werden.

Deswegen rät Morgenstern Käufern dazu, sich zu überlegen, ob es immer die vernetzte Variante sein muss – oder ob nicht auch ein klassisches Gerät ausreiche. Denn natürlich gebe es auch Vorteile bei der Nutzung, etwa Komfort bei der Speicherung der Daten und potentiell bessere Auswertemöglichkeiten von persönlichen Gesundheitsparametern. „Aber immer unter der Prämisse, dass die IT-Sicherheit und der Datenschutz gewährleistet sind."

Warum die Weitergabe von Gesundheits-Daten für Verbraucher prekär sein kann, zeigt ein Blick auf die zahlreichen potentiellen Interessenten für solch sensible Daten. Datenschützer rechnen mit großer Wahrscheinlichkeit damit, dass diese in Zukunft verkauft werden könnten, sobald eine genügend hohe Anzahl von ihnen über Verbraucher gesammelt sein wird.

Banken, Versicherungen, Arbeitgeber als potentielle Interessenten

Schauen wir uns an, was sich mit Gesundheitsdaten so alles herausfinden lässt: Da ist nicht nur die Fitness, die sich anhand der mit solchen Geräten erhobenen Daten feststellen lässt – sondern auch das sonstige Lebensverhalten. Algorithmen errechnen aus einem individuellen Datensatz aufgrund ihrer Fähigkeit, große Mengen an Vergleichsdaten auszuwerten und einzuordnen, ganze Gesundheitsprofile von Menschen. Und die sind interessant für:

Pharma-Anbieter: Wenn ich weiß, welches Wehwehchen der eine oder andere Nutzer hat, kann ich ihm gleich punktgenau die Werbung für weitere vermeintliche durch Algorithmen festgestellte Leiden zukommen lassen.

Arbeitgeber: Wie gut in Schuss ist denn der neue Bewerber wirklich? Lebt er wirklich so fit und gesund, wie er im Bewerbungsgespräch vorgibt?

Versicherungen: Kann ich dem Kunden einer privaten Zusatzversicherung wirklich einen Rabatt geben, weil er sagt, dass er sich gesund ernähre und viel bewege? Die Daten aus der Gesundheits-App legen schonungslos klar, ob er sich wirklich so fit hält, wie er sagt.

Geldinstitute: Ein Baudarlehen mit 25 Jahren Laufzeit? Tut uns sehr leid, lieber Herr Müller: Ihre Gesundheitsdaten – kombiniert mit den Daten über Ihren Konsum von Genussmitteln, generiert aus Kunden- und Rabattkarten – sehen leider ganz und gar nicht gut aus. Entweder Sie bekommen den gewünschten Kredit erst gar nicht. Oder nur mit horrenden Sicherheitsaufschlägen wie einer Restschuldversicherung.

Krankenversicherungstarife, die finanzielle Anreize mit der fortlaufenden, dauerhaften Offenlegungsverpflichtung von Daten verknüpfen, lehnt der Bundesverband der Verbraucherzentralen ab. „Nach aktuellem Prinzip finanzieren die Jungen und Gesunden die Alten und Kranken. Doch sobald eine Kasse genügend Daten besitzt, um jeweils das individuelle Risiko zu berechnen, wird dieses Grundprinzip aufgelöst. Wer krank oder schwach ist, darf dafür nicht bestraft werden", sagt Kai Vogel, Leiter Team Gesundheit und Pflege beim Verbraucherzentrale Bundesverband e. V. Zumindest bei Privaten Krankenkassen, bei denen das Solidaritätsprinzip nicht gesetzlich verankert ist, ist das eine reale Gefahr.

Diese Szenarien sind technisch gesehen schon längst möglich. Denn eine weitere Entwicklung lässt Datenschützer, Ärzte und Verbraucher aufhorchen: der Trend zur digitalen Gesundheitsakte.

Alle Gesundheitsdaten der Deutschen auf einem Server?

Tatsache ist: Der beste Datenschutz, den Versicherte genießen können, ist der abschließbare Stahlschrank mit Papier-Karteikarte bei seinem Hausarzt. Doch die Technik schreitet voran. Eine Idee, die ab 2021 Wirklichkeit werden soll: die Daten aller gesetzlich Krankenversicherten in Form von digitalen Patientenakten zu speichern, um Ergebnisse zu bündeln und unnötige Untersuchungen zu vermeiden. Diesbezüglich gibt es allerdings datenschutzrechtliche Bedenken.

Befürworter einer digitalen Datensammlung hingegen betonen die hilfreiche Dimension der Digitalisierung: Mit Hilfe von Algorithmen erkennen und diagnostizieren Mediziner heute Krankheiten wie Krebs genauer als menschliche Ärzte. Ein gutes Beispiel dafür sind die Untersuchungen von Zellbefunden oder Hautveränderungen. Lernende Algorithmen erkennen mittlerweile auf diesen Gebieten schon Muster, wo das menschliche Denken allein aufgrund der Datenfülle versagen muss. Auf diese Weise können Algorithmen heute bereits Wahrscheinlichkeiten errechnen, ob ein Patient in Zukunft an einer bestimmten Krankheit leiden wird – und können so Leben retten.

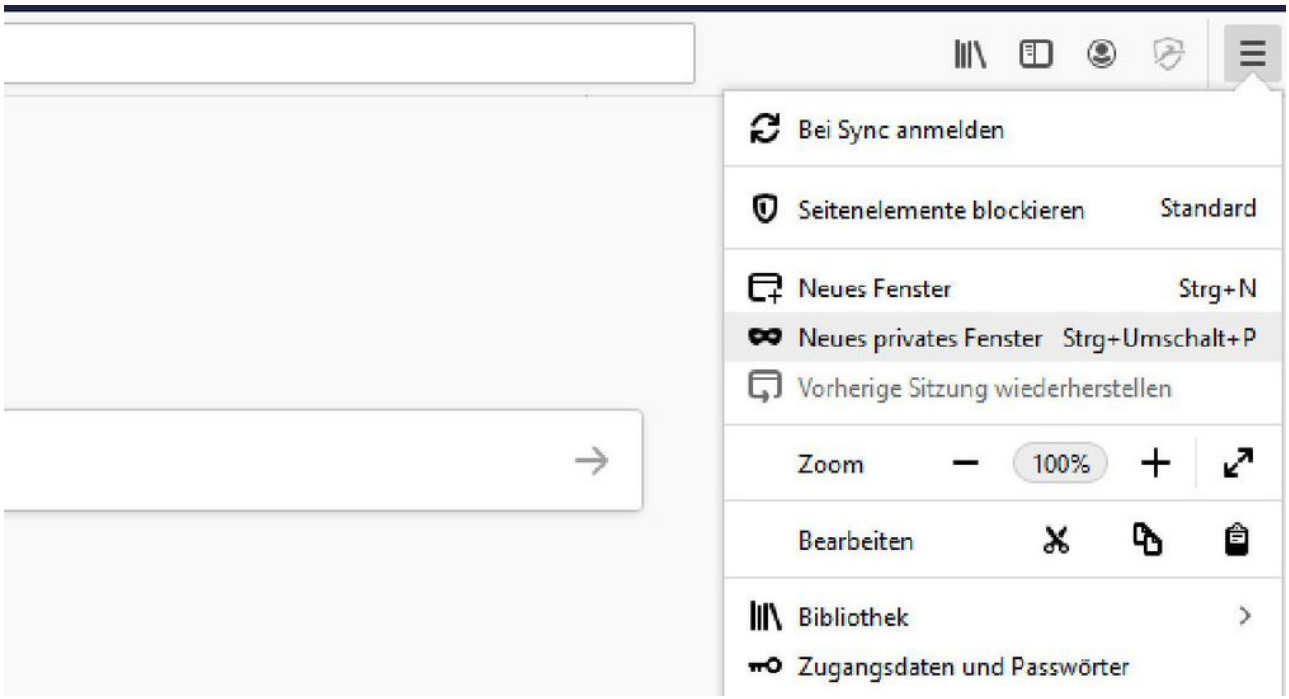
Doch auch dieser Vorteil der digitalen Technik ist mit einem ethischen Dilemma verbunden, stellt Professor Stefan Funke vom Institut für formale Methoden der Informatik an der Universität Stuttgart fest: „Mittlerweile sagen uns Algorithmen vieles anhand unserer medizinischen Befunde voraus. Aber da ist natürlich die große Frage: Wollen wir das eigentlich wissen?" Funke betont das Recht auf Nichtwissen. Dies sei gerade bei medizinischen Fragen ganz wichtig – auch aus ethischen Perspektiven.

So mache ich mich unberechenbar in Sachen Gesundheit

Wie kann nun ein Verbraucher agieren, der seine sensiblen Gesundheitsdaten schützen will? Die Tipps von Ärzten, Verbraucher- und Datenschützern lauten:

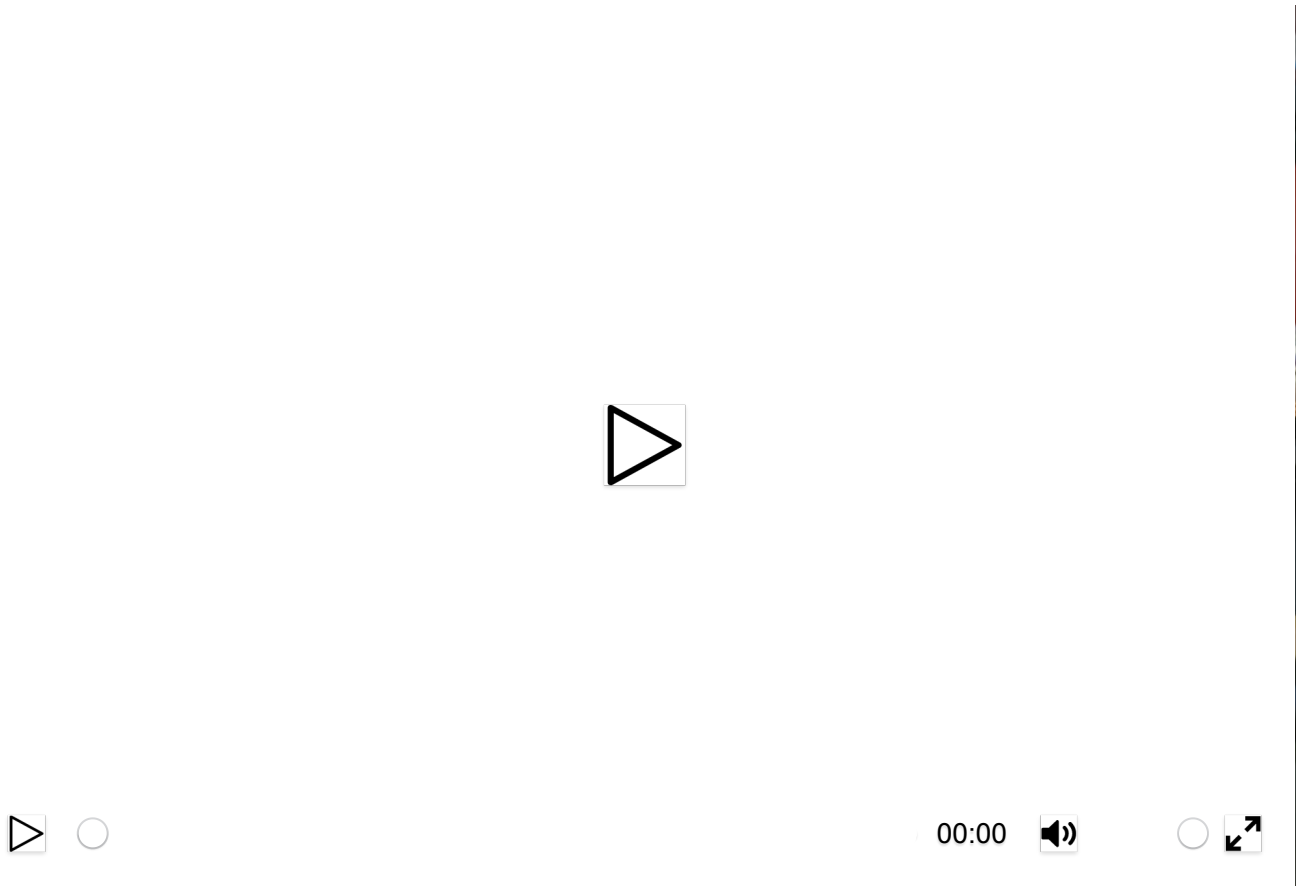
1. Prüfen Sie, ob Sie wirklich ein **Fitness-Wearable brauchen**: Die schlichte Pulsmessung am Handgelenk tut es auch. Wenn Sie ein solches Gerät benutzen wollen: Achten Sie darauf, dass Sie die Einstellungen ändern können, die den Zugriff auf die Daten erlauben. Tragen Sie solche Geräte, die mit dem Netz verbunden sind, nicht ständig, sondern nur bei sportlichen Aktivitäten – so fallen weniger Daten an.
2. Seien Sie sich stets bewusst, dass bei der **Nutzung von Wearables und Fitness-Apps** zahlreiche sensible Daten gesammelt und verarbeitet werden, wenn die Daten im Netz gespeichert und abrufbar sind. Prüfen Sie die Grundeinstellungen des Geräts: Lassen sich Ortungsdienste ausschalten? Können Sie über die Speicherung und Übertragung von persönlichen Gesundheitsdaten bestimmen?
3. Aus den Bedienungsanleitungen solcher Geräte sollten **Datenschutzhinweise** hervorgehen, die verständlich und in deutscher Sprache verfügbar sein sollten. Falls dies nicht der Fall ist, sollte das für Sie ein Ausschlusskriterium zur Nutzung eines solchen Gerätes sein.
4. Die **Zugriffsrechte der Apps für Wearables** sollten überprüft werden. Fitness-Programme wie „Google Fit“ oder „Fitbit“ benötigen Zugriff auf die Aktivitäts- oder Wearable-Sensorendaten, um dem Benutzer Ergebnisse und Auswertungen zu präsentieren. Andere unberechtigte Zugriffe sollten deaktiviert werden, ansonsten könnten auch private Dateien eingesehen, verändert oder gelöscht werden. Das gleiche gilt für Termine und Kontaktdaten. Besonders kritisch sind auch Zugriffe anderer installierter Apps auf Wearable-Sensorendaten und Aktivitätsdaten mit denen Rückschlüsse auf den Gesundheitszustand möglich sind. Dieser Zugriff sollte auf keinen Fall gewährt werden, denn sie könnten die körperliche Verfassung ausspionieren.
5. Beim **Suchen und Surfen im Web soweit wie möglich keine Spuren** hinterlassen. Das gilt besonders beim Besuch von Websites mit Gesundheitsseiten (Ratgeberseiten mit medizinischer Diagnose, Beratung und Therapie, Seiten von Selbsthilfegruppen, Seiten mit Versicherungsangeboten, Online-Apotheken im Netz, u.a.). Dazu lässt sich einerseits der private Modus nutzen, andererseits können diverse Tools dabei helfen.

"PRIVATES FENSTER" IM FIREFOX ÖFFNEN



Das sagen die Experten

PD Dr. Jessica Heesen zum Thema Gesundheit



Weitere Informationen

Marktwächter-Untersuchung der Verbraucherzentralen hinsichtlich Fitness-Trackern

Test von Fitness-Trackern in Bezug auf Datenschutz-Sicherheit

Informationen der Krankenkassen zum Thema digitale Patientenakte

Link dieser Seite:

https://mlr.baden-wuerttemberg.de/de/unsere-themen/verbraucherschutz/algorithmen/gesundheit