WEARABLES IM ZUGRIFF DER STRAFJUSTIZ

Aljoscha Dietrich / Jochen Krüger / Karin Potel

Wissenschaftlicher Mitarbeiter

Vizepräsident des Amtsgerichts Saarbrücken a.D. und wissenschaftlicher Mitarbeiter

Studentische Mitarbeiterin
juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
66123 Saarbrücken, DE
{aljoscha.dietrich; jochen.krueger; karin.potel}@uni-saarland.de

Schlagworte: ***Wearables, Strafjustiz, Datenschutz, Datenschutzgrundverordnung, Verkehrsdaten, Berufsgeheimnisträger***

Abstract: *Wearables, wie Fitness-Bänder und Smartwatches, gehören zu den aktuellen technischen Trends. Es handelt sich um tragbare Computer, die Körperaktivitäten des Trägers überwachen. Damit werden Wearables Bestandteil moderner Gesundheitsstrategien. Vermehrt wurden bereits datenschutzrechtliche Probleme diskutiert. Dieser Beitrag befasst sich mit der spezifischen Frage, bei welchen Daten (z.B. Standortdaten) Begehrlichkeiten der Strafjustiz entstehen können. Unter diesem Aspekt werden die technischen Möglichkeiten von Wearables mit Blick auf das strafprozessuale Bezugssystem analysiert.*

1. Wearables als Trendsetter

1.1. Ausgangsüberlegungen

Wearables gehören zu den großen technischen Trends der letzten Jahre. Spätestens mit der Vorstellung der Apple Watch sind Geräteklassen wie Smartwatches oder Fitness-Bänder einem größeren Publikum bekannt. Bei Wearables handelt es sich um Computer, die am Körper getragen werden können. Mit Hilfe von Sensoren werden Körperaktivitäten des Trägers überwacht, z.B. die Anzahl der Schritte, Herzfrequenz und Verlauf der Schlafphasen. Bei diesen Kerndaten, die von Wearables erhoben werden, handelt es sich also typischerweise um Gesundheitsdaten. Damit sind Wearables Bestandteil moderner Gesundheitsstrategien. Sie sind zudem auch Element einer allgemeinen gesellschaftlichen Entwicklung, die als verstärkte Digitalisierung des Gesundheitswesens umschrieben werden kann.[1]

1.2. Entwicklungstendenzen

Wearables sind jedoch keineswegs nur Armbänder oder Uhren. In Form und Funktion zeigt sich inzwischen eine nahezu unbegrenzte Vielfalt. Die Angebotspalette reicht von Smart Glasses über intelligente Windeln bis hin zu intelligenten Schuhen. Dadurch vergrößern sich auch die potentiellen Funktionsbereiche. Sicherheit, Medizin, Wellness, Sport, Fitness, Lifestyle, Kommunikation und Mode sind nur einige der Stichworte in diesem Zusammenhang.[2] Eines der aktuellen Trendthemen in diesem Kontext lautet Quantified Self.[3] In der Sache geht es um die Selbstvermessung der Wearableträger. Zu dieser Thematik haben sich Gemeinschaften im Internet gebildet. Diese erheben und analysieren ihre eigenen Biodaten und tauschen sich mit anderen Teilnehmern darüber aus. Daneben wird bereits ein neuer Trend sichtbar: Quantified Employee. Dieser betrifft

---

1 Vgl. in diesem Zusammenhang auch das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vom 21. Dezember 2015.

2 Vgl. PwC/CIS, The Wearable Future, 2014.

3 Vgl. dazu grundsätzlich Leibenger/Möllers/Petrlic/Petrlic/Sorge, Privacy Challenges in the Quantified Self Movement – An EU Perspective, In Proceedings on Privacy Enhancing Technologies, 2016(4), S. 315–334.

im weitesten Sinne die Nutzung von Wearables im Arbeitsverhältnis. Insbesondere sind Wearables auch Teil des allgemeinen großen aktuellen Trendthemas Internet of Things (IoT, Internet der Dinge). Dabei geht es um die Verbindung der Gegenstände mit dem Internet und untereinander.

1.3. Wearables als Datenschutzproblem

Bei Wearables zeigen sich aber auch ausgeprägte potentielle Datenschutzprobleme. Mit dieser Thematik befassen sich im Sammelband «Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft» (2015)[4] gleich mehrere Beiträge.[5] Bei aller unterschiedlicher Aktzentsetzung werden dabei zwei Aspekte sichtbar: Zum einen sind Wearables ein nicht mehr wegzudenkender Bestandteil des Alltags geworden. Zum anderen haben sich im Umfeld von Wearables neue Datenbegehrlichkeiten entwickelt. Wearabledaten erlauben in ungewöhnlichem Umfang und in ungewöhnlicher Qualität Rückschlüsse auf Eigenheiten der Person. Über Wearables können Informationen gesammelt werden, die bis in die Intimsphäre reichen und daher auch Außenstehenden normalerweise nicht freiwillig zugänglich gemacht werden. So kann über die erhobenen Gesundheitsdaten die physische und psychische Verfassung des Trägers zu einem bestimmten Zeitpunkt festgestellt werden. Darüber hinaus lassen sich über Wearables Standortdaten ermitteln. Einige Geräte speichern und sammeln auch Geräusche und erfassen damit die nähere Umgebung nebst den darin befindlichen Personen. Das britische Kabinett hat aktuell entschieden, dass Minister während der Sitzungen keine Apple Watch tragen dürfen. Dies geschah offenkundig, um möglichen Spionageangriffen oder unautorisierten Aufnahmen vorzubeugen.[6]

Aber auch allgemein werden die datenschutzrechtlichen Probleme bei Wearables im Alltag schnell deutlich. So kann bei einer Nutzung von Wearables im Arbeitsumfeld der Arbeitgeber etwa Korrelationen zwischen Fitness und Arbeitseffizienz erstellen. Interessant sind Wearabledaten auch für Krankenkassen und Versicherungen, die bereits heute die Anschaffung von Wearables bezuschussen.[7] Zunächst fördert dies das Gesundheitsbewusstsein beim Kunden. Es wird sich dann aber auch verstärkt die Frage stellen, ob die Versicherungen später auf diese Daten zugreifen können. Bei negativer Auffälligkeit des Kunden könnten die Versicherungsraten erhöht oder der Versicherungsvertrag sogar ganz aufkündigt werden. Eine vergleichbare Entwicklung hat sich bereits bei KFZ-Versicherungen unter der Thematik Pay as you drive ergeben.[8]

2. Wearables im Zugriff der Strafjustiz

2.1. Zum allgemeinen rechtlichen Bezugsrahmen von Wearabledaten

Die ursprünglichen Kerndaten bei Wearables sind i.d.R. Gesundheitsdaten. Damit gehören sie zu den besonderen Arten personenbezogener Daten im Sinn des § 3 Abs. 9 BDSG. Diese werden als besonders sensibel und damit schutzbedürftig eingestuft. Dies ergibt sich z.B. aus der Wertung der §§ 4a Abs. 3 und 28 Abs. 6 BDSG. Die Verarbeitung der zuvor genannten Daten ist nur unter engen Vorgaben zulässig. Gestützt und verstärkt wird diese Einschätzung auch durch den europäischen Rechtsrahmen. In der Datenschutz-Grundverordnung (DS-GVO) und der Richtlinie für Polizei/Justiz[9] wird u.a. zwischen genetischen, biometrischen und Gesund-

---

4 Taeger (Hrsg.), Internet der Dinge, Tagungsband Herbstakademie, Oldenburger Verlag für Wirtschaft, Informatik und Recht, Edewecht 2015.

5 Wilmer, Wearables und Datenschutz – Gesetze von gestern für die Technik von morgen? In: ebenda, S. 1 ff.; Jandt/Hohmann, Life-Style-, Fitness- und Gesundheits-Apps – Laufen Datenschutz und Vertraulichkeit hinterher? In: ebenda, S. 17 ff.; Völkel, Wearables und Gesundheitsdaten: Möglichkeiten und Grenzen zur cloudbasierten Nutzung durch Ärzte und Krankenversicherungen aus datenschutzrechtlicher Sicht. In: ebenda, S. 35 ff.

6 Dominiczak, Apple Watches banned from Cabinet after ministers warned devices could be vulnerable to hacking, http://www.telegraph.co.uk/news/2016/10/09/apple-watches-banned-from-cabinet-after-ministers-warned-devices (alle Internetquellen aufgerufen am 22. Dezember 2016), 2016.

7 Klemm, Ein Fitnessband als Bonus, Frankfurter Allgemeine Sonntagszeitung, 17. Januar 2016, S. 38.

8 Vogelgesang, Datenspeicherung in modernen Fahrzeugen – wem «gehören» die im Fahrzeug gespeicherten Daten?, jM, 2016, Volume 3, Nummer 1, S. 2.

9 Richtlinie (EU) 2016/680 vom 27. April 2016.

heitsdaten[10] unterschieden. Dies führt im Verhältnis zu den bisherigen deutschen Normen zu einer weiteren Präzisierung. Solche Daten genießen allgemein ein besonders hohes Schutzniveau, und die Verarbeitung wird durch gesetzliche Hürden deutlich erschwert.[11]

2.2. Der Zugriff der Strafverfolgungsbehörden als Sonderproblem

Der vorliegende Beitrag befasst sich mit der spezifischen Frage, bei welchen Daten auch Begehrlichkeiten der Strafjustiz entstehen können.

2.2.1. Zum strafprozessualen Interesse an Wearabledaten

Dies betrifft zunächst eine andere Akzentsetzung als die zuvor angesprochene Datenschutzproblematik. Fragen der Strafverfolgung und des Datenschutzes haben jedoch eine inhaltliche und rechtstheoretische Schnittmenge. Die im Zusammenhang mit dem Datenschutz skizzierten Fragestellungen haben gezeigt, dass Wearabledaten in ungewöhnlichem Umfang, aber auch in ungewöhnlicher Tiefe Einblick in die Privat- und Intimsphäre zulassen. Dies begründet inhaltlich, warum Wearables für jeden Informationssuchenden oder -interessierten eine potentiell ertragreiche Quelle darstellen können. Damit geraten sie aber auch zwangsläufig in das Blickfeld der Strafjustiz. Geistiger Ausgangspunkt ist dabei § 152 Abs. 1 Strafprozessordnung (StPO). Dieser beinhaltet[12] das sogenannte Offizialprinzip. Danach obliegt die Strafverfolgung grundsätzlich dem Staat und nicht dem einzelnen Bürger. Verantwortlich für die Strafverfolgung ist zunächst die Staatsanwaltschaft. Diese ist an das Legalitätsprinzip gebunden (§ 152 Abs. 2 StPO). Dies bedeutet Verfolgungszwang gegenüber jedem Tatverdächtigen. § 152 Abs. 2 StPO steht in inhaltlicher Verbindung mit § 170 Abs. 1 StPO. Danach hat die Staatsanwaltschaft Anklage zu erheben, wenn die Ermittlungen dafür genügenden Anlass bieten. Innerhalb dieser skizzierten Grundlagen des Strafverfolgungssystems sind die Strafverfolgungsbehörden geradezu verpflichtet, sich auch um neue – legale – Informationsquellen zu kümmern, die bei der Aufklärung von Straftaten hilfreich sein können. Potentielle Beweismittel sind dabei auch Wearables bzw. die damit zugänglich gemachten Daten.

Mögliche Beispiele für den Kontext «Strafverfolgung und Wearabledaten» lassen sich unschwer finden. So kann bei einem Träger von Wearables von Interesse sein, ob dieser sich zu einem bestimmten Zeitpunkt an einem bestimmten Tatort befunden hat. Verbindungslinien zur Funkzellenabfrage drängen sich auf. Aber auch die Kerninformationen der Wearables, Gesundheitsdaten im engeren Sinn, können schnell ins Visier der Ermittlungsbehörden geraten. So kann es insbesondere bei Verkehrsunfällen mit tödlichem Ausgang oder jedenfalls Verletzungsfolgen um die Frage gehen, ob der Fahrer eines Fahrzeuges möglicherweise übermüdet am Steuer eingeschlafen war. Bei der Beantwortung dieser Frage kann die Analyse etwaiger Wearabledaten von entscheidender Bedeutung sein.[13]

Aber auch darüber hinaus ist der Kreis möglicher einschlägiger Fallgestaltungen, bei denen Wearables eine Rolle spielen können, an sich unbegrenzt. Dies gilt insbesondere unter dem Gesichtspunkt, dass Wearabledaten Rückschlüsse auf die physische und psychische Verfassung zu einem bestimmten Zeitpunkt zulassen. Die theoretische und praktische Relevanz dieses Aspekts ist nicht zu unterschätzen. So kann z.B. bei einem Vergewaltigungsvorwurf (§ 177 StGB) die Frage wichtig werden, ob der Beschuldigte zu einem bestimmten Zeitpunkt in einem extremen Erregungszustand war. Dies gilt insbesondere dann, wenn der Beschuldigte die Tat bestreitet. Unabhängig von spezifischen Sexualdelikten ist allgemein der Umstand zu beachten, dass strafrechtliche Verantwortlichkeit Schuld voraussetzt. Dabei kommt gerade bei schweren Delikten dem Ge-

---

10 Art. 4, Nr. 13, 14 u. 15 DS-GVO und Art. 3, Nr. 12, 13 u. 14 RL 2016/680.

11 Vgl. z. B.: Art. 9 Abs. 1 DS-GVO bzw. Art. 10 RL 2016/680.

12 Vgl. dazu und zum Folgenden Schmitt, in: Meyer-Goßner/Schmitt (Hrsg.), Strafprozessordnung, 59. Auflage, C.H. Beck, München 2016, § 152, Rn. 1 ff.

13 Vgl. in diesem Zusammenhang auch Healey/Picard, «SmartCar: detecting driver stress.» Pattern Recognition, 2000. Proceedings. 15th International Conference on. Vol. 4. IEEE, 2000.

sichtspunkt der Schuldunfähigkeit gemäß § 20 StGB oder der verminderten Schuldfähigkeit gemäß § 21 StGB eine ins Gewicht fallende Bedeutung zu. Dies gilt insbesondere bei Gewalt- und Aggressionsdelikten.[14]

In diesem Zusammenhang können über Wearabledaten, die Auskunft über die psychische Verfassung des Beschuldigten zum Tatzeitpunkt geben, auch Entlastungsgesichtspunkte deutlich gemacht werden. So spielt im Rahmen des § 20 StGB das Tatbestandsmerkmal «tiefgreifende Bewusstseinsstörung» eine wesentliche Rolle. Ein praktischer Anwendungsfall dafür ist z.B. ein Zustand hochgradigen Affekts, aber auch Schlaf oder Schlaftrunkenheit.[15] Jedenfalls kann bei Feststellung der Schuldunfähigkeit der Beschuldigte nicht bestraft werden, bei verminderter Schuldfähigkeit gemäß § 21 StGB kann die Strafe gemildert werden. Allgemein eröffnen Wearabledaten potentielle Einblicke in die Psyche eines Betroffenen, die es in dieser objektivierbaren Form zuvor nicht gegeben hat. Dies begründet das spezifische strafrechtliche Interesse an einem Zugriff auf Wearables und die damit verbundenen Daten. Damit kann im Ergebnis dem Schuldprinzip, das für das Strafrecht prägend ist, verstärkt Rechnung getragen werden.

2.2.2. Zum strafprozessualen Bezugsystem

Ermittlungstechnische Zweckmäßigkeit oder Wünschbarkeit ist allein kein ausreichendes rechtliches Kriterium. Dies macht im deutschen Recht vor allem § 136a StPO deutlich. Danach dürfen bestimmte Ermittlungstechniken wie Quälerei oder Hypnose nicht eingesetzt werden. Aussagen, die unter Verletzung dieses Verbots zustande gekommen sind, dürfen nicht verwertet werden (§ 136a Abs. 3 S. 2 StPO). Allgemein ergeben sich die Voraussetzungen für einen – rechtmäßigen – strafprozessualen Zugriff aus dem strafprozessualen Bezugssystem. Unter diesem Aspekt sollen auch die technischen Möglichkeiten bei Wearables erörtert und strukturiert werden. Dabei rücken zwei zentrale Differenzierungsmöglichkeiten der StPO in den Vordergrund.

Zum einen differenziert das strafprozessuale Normenprogramm danach, ob der Zugriff beim Beschuldigten selbst oder bei einem unbeteiligten Dritten erfolgt. Befinden sich Daten noch auf dem Wearable des Beschuldigten selbst, kann die zentrale Durchsuchungsnorm des § 102 StPO in Betracht kommen. Anders wäre es, wenn die Wearabledaten nur noch in einer Cloud bei einem Dritten gespeichert sind. Auf diese kann gemäß § 103 StPO nur unter erschwerten Voraussetzungen zugegriffen werden. Sonderprobleme entstehen, wenn die Daten bei einem Geheimnisträger im Sinn des § 203 StGB, z.B. einem Arzt, ausgelagert sind. Dann ist das in § 97 StPO geregelte grundsätzliche Beschlagnahmeverbot bei Berufsgeheimnisträgern zu beachten. Berücksichtigt werden muss bei dieser Personengruppe daneben auch das grundsätzliche Verbot der Erhebung von Verkehrsdaten gemäß § 100g Abs. 4 StPO.

Zum anderen kennt die StPO spezielle Eingriffsnormen für spezielle Arten von Daten. Beispiel dafür ist die zuvor erwähnte Erhebung von Verkehrsdaten gemäß § 100g StPO. Bei § 100g StPO muss die – auch – technikgeprägte Frage beantwortet werden, ob im Zusammenhang mit Wearables Verkehrsdaten im Sinn der StPO erfasst und gespeichert werden. Dazu gehören auch Standortdaten bei mobilen Anschlüssen gemäß § 96 Abs. 1 Nr. 1 Telekommunikationsgesetz (TKG). Zudem enthält § 100g Abs. 3 StPO[16] eine spezielle Ermächtigungsgrundlage für die Funkzellenabfrage.

3. Technischer Aufbau von Wearables im Lichte des strafprozessualen Normenprogramms

Für die Beantwortung rechtlicher Fragestellungen im Zusammenhang mit Wearables ist es wesentlich, den Aufbau und die Funktionsweise der Geräte und die erhobenen Daten näher zu analysieren.

---

14 Vgl. dazu Fischer, Strafgesetzbuch, 64. Auflage, C.H. Beck, München 2017, § 20, Rn. 1.

15 Vgl. Fischer, ebenda, § 20, Rn. 28.

16 In der seit 10. Dezember 2015 geltenden Fassung – vgl. dazu Schmitt (Fn. 12), § 100g, Rn. 2 ff.

3.1. Zur Dynamik des technischen Fortschritts

Es gibt bei Wearables eine vielfältige Angebotspalette mit unterschiedlichen Funktionsweisen. Insbesondere handelt es sich bei Wearables um eine sehr dynamische Produktgruppe. Neue Gerätegenerationen bedeuten i.d.R. auch erhöhte Leistungsfähigkeit mit neuen Funktionen und Möglichkeiten. Zunächst dienten Smartwatches meist nur als Ergänzung für Smartphones. Zwischenzeitlich entwickeln sie sich in Richtung autonom arbeitender Geräte. Insbesondere sind Wearablemodelle inzwischen oftmals mit eigener Mobilfunkkommunikation ausgestattet.

3.2. Sensorik

Wearables sind bereits mit einer Vielzahl von Sensoren erhältlich. Der Markt ist relativ unübersichtlich. Um einen Eindruck der aktuellen Möglichkeiten zu erhalten, sollen die Sensoren des aktuellen Marktführers Apple Watch (Series 2) vorgestellt werden. Da es vom Hersteller offiziell keine exakte Beschreibung gibt, muss auf Hardwareanalysen von Dritten – sogenannte Teardowns – zurückgegriffen werden. Laut Chipworks[17] und den eher spärlichen Informationen von Apple[18] beinhaltet die Apple Watch Series 2 aktuell folgende Sensoren: Beschleunigungssensor, Herzfrequenzsensor, Gyroskop, Bewegungssensor, Barometrischer Luftdrucksensor. Zudem enthält die Smartwatch Mikrofon und Lautsprecher, sowie zur Funkkommunikation NFC, WLAN und Bluetooth. Standortdaten können u.a. mit Hilfe von GPS bestimmt werden.

3.3. Analysemöglichkeiten auf der Grundlage der erhobenen Daten

Mit den beschriebenen Sensoren lassen sich unterschiedliche Informationen gewinnen. Über die GPS-Sensoren kann die genaue Position ermittelt werden. Zudem ist über die Bestimmung der exakten Höhe auch eine Indoornavigation möglich. Aus den Bewegungen des Trägers kann die Anzahl der Schritte berechnet werden. In Kombination mit der Analyse der Herzfrequenz lassen sich zudem Aussagen über die Fitness bzw. Aktivitäts- und Ruhezustände treffen.[19] Zugleich dürfte es auch möglich sein, aus den Bewegungsmustern Anzeichen auf Krankheiten und Behinderungen abzuleiten. Nahe liegt auch, dass sich alkohol- oder drogenbedingte Ausfälle identifizieren lassen.

Die Entwicklungstendenz von Wearables ist dadurch geprägt, dass jede Generation mit mehr Sensorik ausgestattet ist. Dadurch werden die so erhobenen Daten in ihrem Analysepotential immer mächtiger und erlauben damit auch eine immer präzisere Aussage über den Träger selbst. Als Qualitätssprung ist die Erfassung der elektrodermalen Aktivität durch sogenannte Galvanic-Skin-Response-(GSR)-Sensoren zu bewerten. Mit Hilfe dieser Sensorik wird die elektrische Leitfähigkeit der Haut untersucht. Diese Technologie gibt sehr genaue Auskünfte über die physiologische Erregung, die beispielsweise durch Stress oder Emotionen ausgelöst wird. Daher findet sie unter anderem auch in Lügendetektoren Anwendung. GSR-Sensoren gehören zwar noch nicht zum selbstverständlichen Bestandteil von marktgängigen Wearables. In einzelnen Gerätetypen, wie dem Microsoft Band, sind sie jedoch bereits jetzt enthalten.[20]

3.4. Verarbeitung der Daten

Die Wearbaledaten müssen zunächst (zwischen-)gespeichert werden. Da die Rechenkapazität der Wearables normalerweise äußerst gering ist, werden die Daten zwecks Verarbeitung in der Regel ausgelagert. Die meis-

---

17 Gingerich/Morrison, Apple Watch Series 2 Teardown, http://www.chipworks.com/about-chipworks/overview/blog/apple-watch-series-2-teardown, 2016.

18 Apple Introduces Apple Watch Series 2, The Ultimate Device For A Healthy Life, http://www.apple.com/pr/library/2016/09/07Apple-Introduces-Apple-Watch-Series-2-The-Ultimate-Device-For-A-Healthy-Life.html, 2016.

19 Vgl. hierzu und zum Folgenden: Sung/Marci/Pentland, Wearable feedback systems for rehabilitation, Journal of neuroengineering and rehabilitation 2.1 (2005): 1.

20 Microsoft Band features and functions, https://support.microsoft.com/en-ph/help/4000319/band-hardware-features-and-functions, 2016.

ten Wearables verfügen aktuell über kein eigenes Mobilfunkmodul. Daher werden die Daten zunächst per Bluetooth an das Smartphone des Nutzers übertragen. Viele Smartphones verfügen zwar heutzutage über eine große Rechenleistung. Der Großteil der Anbieter setzt dennoch typischerweise auf eine Datenverarbeitung in der Cloud. Grund dafür dürften ökonomische Interessen beim Anbieter sein. Allgemein gilt: personenbezogene Daten haben einen hohen wirtschaftlichen Wert.[21] Zudem können die Daten in der Cloud mit weiteren Daten des Anwenders zusammengeführt werden. Dies entspricht der Angebotsphilosophie z.B. von Apple Health oder Google Fit. Der Benutzer erhält zumeist lediglich Zugriff auf die Auswertung seiner Daten. Nur wenige Anbieter gewähren den Nutzern auch Zugriff auf die erfassten Rohdaten. So bietet der Marktführer von Fitnessarmbändern, Fitbit, zwar einen Datenexport an. Hierbei handelt es sich jedoch nur um stark aggregierte Daten. Beispielsweise wird die Summe der Kalorien oder Schritte pro Tag mitgeteilt.

Der Wearableträger muss also auf die Analysequalität sowie die Sicherheit und den Datenschutz beim jeweiligen Anbieter und seiner Cloud vertrauen. Insbesondere besteht auch die Gefahr, dass der Anbieter viel intimere und tiefere Einblicke in das Privatleben des Nutzers erhält und speichert, als er diesem offiziell mitteilt. Die Vernetzung der einzeln erhobenen Daten sowie die Verknüpfung mit den Aktivitäten und Erlebnissen des jeweiligen Nutzers bieten dabei besondere Möglichkeiten. So konnte ein Wearablenutzer anhand der Kurve seiner Herzfrequenz nachträglich den exakten Zeitpunkt feststellen, an dem sein damaliger Partner ihm das Ende der Beziehung mitgeteilt hatte.[22] Bei Wearables wird damit eine datenschutzrechtliche Grundgefahr sichtbar, die auch in Tabelle 1 verdeutlicht wird. Soweit es um die Analyse von nur eindimensionalen Daten geht, ist das Gefährdungspotential typischerweise überschaubar. Bei einer Kombination von diversen Einzeldaten (mehrdimensionale Daten) wird das Gefährdungspotential jedoch signifikant erhöht. Werden die verknüpften Daten beim Wearableträger auch noch in Relation zu weiteren Nutzern gesetzt, ermöglicht dies ein umfassendes Bild über den Wearablenutzer im Verhältnis zu anderen. Dies erlaubt einerseits die Zuordnung zu bestimmten definierten Gruppen. Anderseits können Individuen dadurch anhand definierter Kriterien identifiziert werden. Damit kann in der Sache auch ein soziales Ranking – mit im Einzelfall negativen Folgen für den Betroffenen – vorgenommen werden.[23] Gleichzeitig stellt sich dabei aber auch die allgemein bedeutsame Frage nach der Zuverlässigkeit der Messmethoden und damit der Richtigkeit der Daten bei Wearables.[24]

Durch die Korrelation mehrerer Daten kann zudem ein schärferes Profilbild bei einer bestimmten Person geschaffen werden. Dies erleichtert gerade auch die hier interessierenden Strafverfolgungsmaßnahmen, etwa im Rahmen einer Rasterfahndung gemäß § 98a StPO.

	EINZELNE NUTZER	MEHRERE NUTZER
EINDIMENSIONALE DATEN	Berichte / Reports (z.B. Anzahl der Schritte in einem Zeitraum)	Wettbewerb / Benchmarking (Wer läuft am meisten an einem Tag)
MEHRDIMENSIONALE DATEN	Korrelationen (z.B.: gibt es einen Zusammenhang zwischen durchschnittlicher Schlafdauer und Arbeitsleistung?)	Clustering / Einteilung in Gruppen (z.B.: «Hohe oder niedrige Arbeitsleistung»)

Tabelle 1: Kategorisierung von Daten, dazu Leibenger/Möllers/Petrlic/Petrlic/Sorge **(Fn. 3), S. 316.**

3.5. Speicherorte

Aus strafprozessualer Perspektive interessiert vor allem die Frage, wo die einzelnen Daten gespeichert werden, wo also Zugriffsmöglichkeiten für die Behörden bestehen. Die Rohdaten werden zunächst auf dem Wearable

21 Vgl. Wilmer (Fn. 5), S. 3.

22 Soto, Tweet, https://twitter.com/iamkoby/status/689521611611971588, 2016.

23 Etwa bei Kündigungsentscheidungen durch den Arbeitgeber.

24 Vgl. zu dieser Problematik International Working Group on Data Protection in Telecommunications, Arbeitspapier zum Datenschutz bei tragbaren Endgeräten («Wearables»), Seoul 2015, S. 7.

selbst gespeichert und typischerweise über das Smartphone des Nutzers an die Cloud des Anbieters übermittelt.[25] Es kann davon ausgegangen werden, dass die Daten auf dem Wearable und dem Smartphone nach der Übertragung in die Cloud gelöscht werden.

Handelt es sich um medizinische Wearables und werden die Daten in der Cloud des behandelnden Arztes gespeichert, sind die Beschlagnahmemöglichkeiten deutlich eingeschränkt.[26] Allgemeine tatsächliche Probleme entstehen, wenn sich eine Cloud mit Wearabledaten im Ausland befindet und deutsche Behörden darauf nicht ohne weiteres zugreifen können.[27] Auf die damit verbundenen Probleme hat in jüngster Zeit auch die Bundesbeauftrage für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, aufmerksam gemacht.[28] Ein faktisches Zugriffsproblem ergibt sich auch, wenn an sich zugriffsfähige Daten zwischenzeitlich gelöscht wurden. Dann können möglicherweise IT-forensische Methoden zur Datenwiederherstellung[29] weiterhelfen.

3.6. Zur Frage der Erfassung von Standortdaten

Die in § 100g Abs. 1 S. 3 StPO genannten Standortdaten spielen allgemein eine nicht unwesentliche Rolle im Rahmen von strafprozessualen Ermittlungen. Standortdaten sind Teil der sogenannten Verkehrsdaten im Sinne des § 96 i. V. m. § 3 Nr. 30 TKG. Sie dürfen nach § 96 Abs. 1 Nr. 1 TKG vom Diensteanbieter bei mobilen Anschlüssen erhoben werden. Definiert wird der Begriff in § 3 Nr. 19 TKG. Danach werden Standortdaten als Daten beschrieben, «[...] die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben [...]». Standortdaten im Sinne des TKG sind damit aufs engste mit einem Telekommunikationsvorgang verbunden.

Dies muss betont werden. Denn üblicherweise werden Standortdaten von Wearables zunächst mit Hilfe des GPS-Sensors und damit ohne Telekommunikationsvorgang erfasst. Ein Telekommunikationsvorgang im Sinne des § 3 Nr. 22 TKG liegt jedoch dann vor, wenn ein Datenaustausch mit dem Internet über ein Mobilfunkgerät erfolgt. Dies bedeutet in der Sache: Bei der Übertragung von Daten z.B. in die Cloud oder bei Abfragen von Informationen aus dem Internet (etwa Wetterdaten) entstehen Standortdaten im Sinne des TKG.

Diese Differenzierung der Standortdaten – mit oder ohne Bezug zu einem Kommunikationsvorgang – ist auch unter dem Gesichtspunkt der sogenannten Vorratsdatenspeicherung von Bedeutung. Durch das «Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten» vom 10. Dezember 2015 wurde der Bereich Vorratsdatenspeicherung (VDS) neu geregelt. Dieses Gesetz bewirkt u.a. eine Änderung des § 113b TKG. Standortdaten müssen gemäß Abs. 1 Nr. 2 vom Diensteanbieter für vier Wochen gespeichert werden. Der neue § 113b Abs. 4 TKG enthält zudem ausdrückliche Speicherpflichten für Funkzellenabfragen i.S.d. § 100g Abs. 3 StPO.[30] Diese Ermittlungstechnik ermöglicht bei Mobilfunknutzern die Feststellung, wer sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort[31] aufgehalten hat.

Dies zeigt auch das Beispiel des Grünenpolitikers Malte Spitz. Dieser hatte die ihn betreffenden Vorratsdaten eingeklagt und sie «ZEIT ONLINE» zu Analysezwecken zur Verfügung gestellt. Die Daten wurden visualisiert und mit frei verfügbaren Informationen über den Abgeordneten verknüpft.[32] Daraus ergab sich ein extrem genaues Bild über die Lebensführung des Abgeordneten.

---

25 Vergleiche zum Datenfluss bei Wearables näher Abschnitt 3.4.

26 Vgl. § 97 Abs. 1 i.V.m. § 97 Abs. 2 S. 3 StPO.

27 Bei großen Wearableanbietern wie Apple und Fitbit handelt es sich um US-amerikanische Unternehmen.

28 Vgl. ZD-Aktuell, BfDI: Datenschutz bei Gesundheitsdaten mangelhaft, ZD-Aktuell 2016, 05420.

29 Carrier, File System Forensic Analysis, Addison-Wesley, Upper Saddle River, NJ 2005; Dewald/Freiling, Forensische Informatik, Norderstedt 2011.

30 Vgl. dazu und zum folgenden Schmitt (Fn. 12), § 100g, Rn. 27 bzw. Rn. 36 ff.

31 Dieser Ort definiert sich durch die Reichweite der Funkzelle.

32 Biermann, Was Vorratsdaten über uns verraten, http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz, 2015.

4. Bewertung und Zusammenfassung

Angesichts der skizzierten Vielfalt an denkbaren Fallgestaltungen ist eine strafprozessuale Einzelanalyse der Wearabledaten im vorliegenden Rahmen nicht möglich. Ein allgemeiner Aspekt hat sich jedoch herauskristallisiert – neue technische Entwicklungen bedeuten typischerweise auch neue Ermittlungsmöglichkeiten mit neuen strafprozessualen Fragestellungen. Dies soll abschließend an einigen Punkten aufgezeigt werden.

1. Die zentrale Beschlagnahmenorm des § 94 StPO orientiert sich an körperlichen Gegenständen und muss daher durch methodische Weiterentwicklung in die Welt der digital gespeicherten Informationen übertragen werden.[33]
2. Neue Normen wie § 100g StPO haben zwar mit dem Tatbestandsmerkmal «Verkehrsdaten» eine ausgeprägte digitale Dimension. Dies bedingt aber auch neue Konkurrenzprobleme mit den allgemeinen Durchsuchungsnormen wie z.B. § 103 StPO.[34]
3. Darüber hinaus verdeutlicht gerade die Analyse der Wearabledaten mögliche verallgemeinerungsfähige Gesichtspunkte bei digitalen Beweismitteln.[35]
    a. Die Digitalisierung der Gesellschaft führt zu einem erheblichen Bedeutungszuwachs der digitalen Beweismittel. Neue Ermittlungsmethoden wie die Funkzellenabfrage belegen dabei eine häufig anzutreffende Schwäche von digitalen Beweismitteln – sie erfassen oftmals eine Vielzahl von Unschuldigen und haben damit eine rechtsstaatlich unerwünschte Streubreite.
    b. Digitale Beweismittel sind charakterisiert durch effektive Möglichkeiten der Verknüpfung von Einzeldaten. Daraus resultiert eine ungewöhnliche Eingriffstiefe des strafprozessualen Zugriffs.
    c. Wearabledaten erlauben Einblick bis in die Intimsphäre. Daher stellen sich neuartige Fragen mit Blick auf die Begrenzungsfunktion des Artikels 1 Grundgesetz (GG, Menschenwürde). Diese wurde bisher z.B. bei der Beschlagnahme und Verwertung von Tagebüchern erörtert.[36] Wearabledaten sind nicht allgemein der Verwertung entzogen. Art. 1 GG schützt aber einen absolut unantastbaren Kernbereich privater Lebensgestaltung.[37] Unzulässig ist unter anderem eine nahezu lückenlose Registrierung aller Bewegungen und Lebensäußerungen eines Betroffenen. Dies veranschaulicht das spezifisch rechtsstaatliche Gefährdungspotential bei der Verwertung von Wearabledaten.
    d. Das aktuelle Urteil des EuGH vom 21. Dezember 2016[38] zu Fragen der Vorratsdatenspeicherung macht zudem die europäische Dimension der angesprochenen Probleme deutlich. Das nationale Normenprogramm kann nicht ohne Blick auf den europäischen Rechtsrahmen umgesetzt werden.

Jedenfalls bestätigt die strafprozessuale Diskussion von Wearabledaten die allgemeine Einschätzung von Singelnstein:[39] Technischer Fortschritt macht gerade auch das strafprozessuale Ermittlungsverfahren zu einem ausgeprägt dynamischen Rechtsgebiet.

---

33 BVerfG E 124, 43 = NJW 2009, 2431 ff.

34 Vgl. dazu LG Saarbrücken, Beschluss vom 23. April 2009 = MMR 2010, 205 mit Anmerkung von Bär.

35 Vgl. allgemein zu digitalen Beweismitteln Momsen/Hercher, Digitale Beweismittel im Strafprozess – Eignung, Gewinnung, Verwertung, Revisibilität, http://www.strafverteidigervereinigungen.org/Material/Themen/Technik%20&%20Ueberwachung/37_momsen.html, 2013.

36 Vgl. Schmitt (Fn. 12), Einleitung, Rn. 56a.

37 Vgl. dazu BVerfG, NStZ 2012, 497 Rn. 99 und 106.

38 ECLI:EU:C:2016:970.

39 Vgl. Singelnstein, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593.