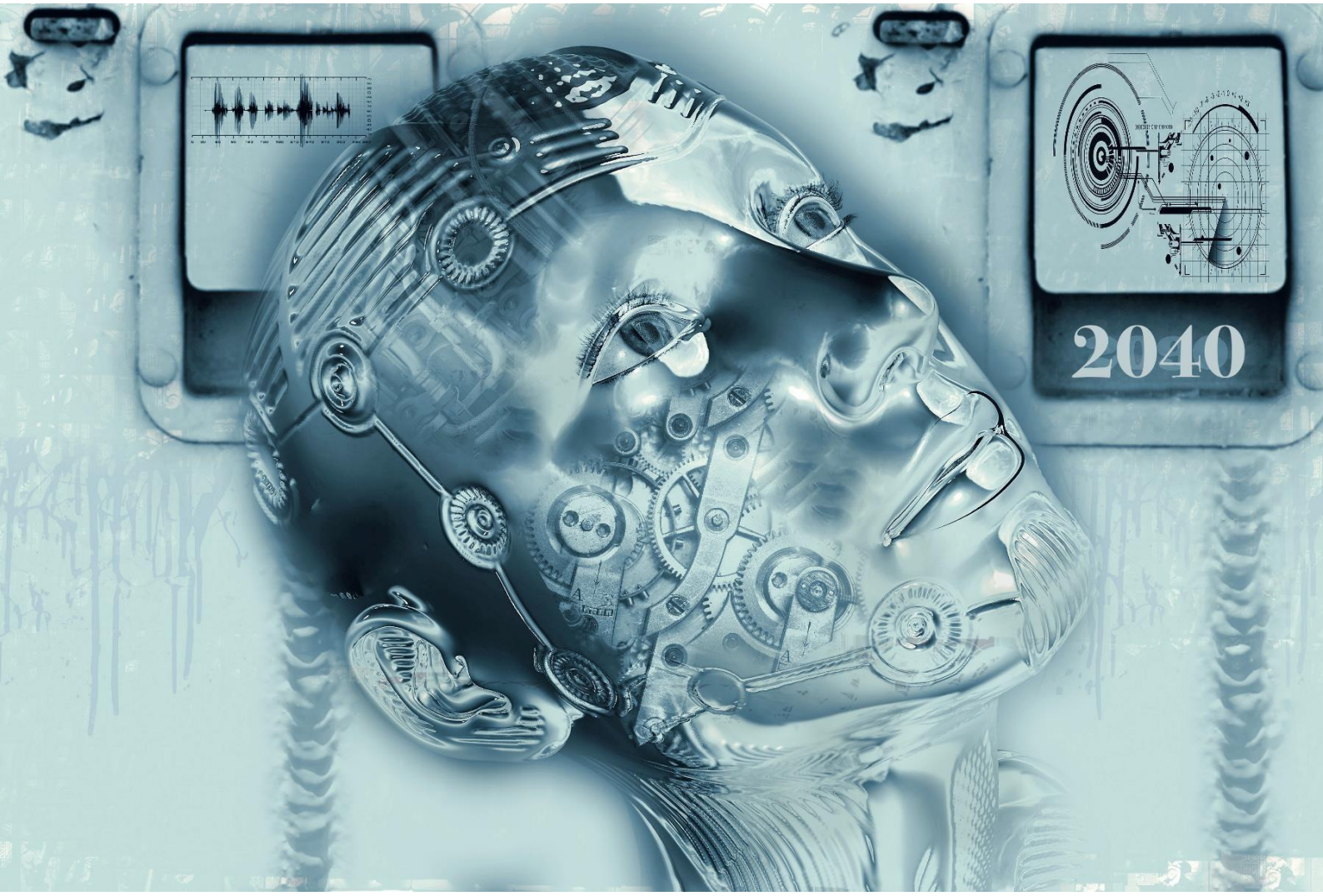
DHBW
Duale Hochschule
Baden-Württemberg
Karlsruhe



Unser Leben mit KI

Der gläserne Bürger: Persönliche Daten als Gold der Zukunft

Einleitung

Schon heute ist die Nutzung persönlicher Daten ein relevanter Wirtschaftsfaktor. Die Branche für Personal-Advertising hat im Jahr 2018 ein Volumen von 1,6 Mrd. €, mit steigender Tendenz (vgl. Bründl 2016). Durch die Verwendung von Trainingsdaten, entstanden in den letzten Jahren etliche KI Systeme wie Apples Siri, Amazons Alexa oder IBMs Watson, welche sich zu marktreifen Produkten entwickelt haben. Wie die Entwicklung in 20 Jahren aussieht lässt sich auch für Experten nur schwer einschätzen, mit hoher Sicherheit werden aber alle Lebensbereiche der Gesellschaft betroffen sein.

Doch wie genau könnte die Nutzung unserer persönlichen Daten durch KI im Jahr 2040 aussehen? Welche Lebensbereiche werden davon beeinflusst? Wie gehen wir mit unseren Daten um und wo liegen vielleicht die Grenzen der Datennutzung?

Mit unserem Essay betrachten wir die Lebensbereiche Gesundheit & Sicherheit der Bürger in Europa im Jahr 2040. Doch warum werden genau diese Lebensbereiche beleuchtet? Zum einen sind Gesundheit und Sicherheit typische Themen des Alltags, zum anderen sehen wir in diesen Bereichen ein großes Wachstumspotential.

Mit unserem Szenario stützen wir uns auf aktuelle Literatur und Forschungsergebnisse und extrapolieren diese um eine Prognose zu wagen. Danach befassen wir uns mit den ethischen Aspekten dieser Entwicklungen und decken die damit einhergehenden Gefahren auf. Zuletzt definieren wir Empfehlungen, welche die ethischen Risiken berücksichtigen um auch in Zukunft eine **faire und demokratische Gesellschaft** zu erhalten. Dabei legen wir einen besonderen Fokus auf die Schaffung einer **digitalen Souveränität**.

KI im Jahr 2040 – Sicherheit oder totale Überwachung?

Durch Deep-Learning, welches auf großen Datenmengen basiert (vgl. Buduma/Locascio 2017), ist es bereits heute möglich (teil)-autonome Drohnensysteme im Sicherheitssektor einzusetzen (vgl. Welchering 2019). Im Zeitraum von 2009 bis 2019 hat sich die Verwendung von leichten und schweren Drohnen mehr als verdoppelt (vgl. Buchholz 2019).

Ein Anwendungsbereich ist die Überwachung von großen Geländen und Anlagen (vgl. Third Element Aviation 2020). Auch die Polizei greift nun seit einiger Zeit auf den Einsatz von Drohnen zurück. Ein ganz aktueller Fall ist die Überwachung von Bürgern bezüglich ihrer Einhaltung der Corona-Regeln (vgl. Welt 2020). Neben der Kameratechnik sind diese Drohnen auch mit Lautsprechern ausgestattet, wodurch Menschenmengen auf ihr Fehlverhalten hingewiesen werden können und eine eventuelle Anfahrt einer Streife verhindert werden kann (vgl. TAZ 2020). Neben diesem aktuellen Thema nutzt die Polizei Drohnen auch zur Vermissten oder Verdächtigen Suche (vgl. Groneberg 2019). Ein weiteres Einsatzfeld ist das Nutzen im Verkehrswesen. Hier können beispielsweise Bilder eines Unfallorts aus der Vogelperspektive aufgenommen und ausgewertet werden. (vgl. Wagner 2020).

Unsere Sicherheit in 20 Jahren. Das Jahr 2040 - der Luftraum über den Städten beherrscht von Drohnen!

Bis 2030 wird ein Marktvolumen für kommerzielle Drohnen von 2,5 Mrd. € prognostiziert (vgl. Drone Industry Insights 2019). Mit Blick in die Zukunft, kann das Marktvolumen im Jahr 2040 3,9 Mrd. € betragen. Davon profitiert vor allem auch der Sicherheitssektor. Zu nennen sind hier die Unterstützung durch vollautonome Drohnen, so wie die Nutzung von persönlichen Daten in einem PRECOBS (Pre-Crime-Observation-System).

Drohnen unterstützen bei Waldbränden und Hochwasser um Personen zu erkennen und ihnen zu helfen. Sie werfen Atemmasken und Rettungsbojen ab, so dass die Person sich bis zum Ankommen der Helfer, selbst helfen kann. Diese Technik wird auch von der Wasserwacht benutzt um Verunfallte schnell und sicher aus einer Notlage zu befreien. Impfstoffe und Medikamente werden durch Wingcopter an abgelegene Orte wie Inseln oder kleine Dörfer transportiert. So auch für andere medizinische Transporte, wie Blut- und Gewebeproben. (vgl. Bundesministerium für Wirtschaft und Energie 2019)

Außerdem unterstützt die KI die Kriminalitätsbekämpfung, durch den Einsatz von Gesichtserkennungen und PRECOBS-Systemen. PRECOBS verwendet jüngste Deliktsdaten und prognostiziert in welchen „Bezirken" die nächsten Verbrechen stattfinden. (vgl. Stoldt 2017). Diese Technologien können ebenso in Verbindung mit Drohnen eingesetzt werden, indem Drohnen die prognostizierten Bezirke überwachen und mögliche Täter durch die Gesichtserkennung schnell identifizieren. Eine weitere Methode sind Nanodrohnen, mit denen Polizisten in geschlossene Räume eindringen können ohne erkennt zu werden. Dies ist dadurch möglich, dass sie sehr klein und kaum zu hören sind. (vgl. Hoppenstedt 2020)

Doch werden wir im Jahr 2040 die totale Überwachung haben? Wie lassen sich die Neuerungen unter ethischen Gesichtspunkten bewerten?

Wie bereits in der Einleitung erwähnt, sind besonders zwei Dinge wichtig: Faire Gesellschaft und Digitale Souveränität. Dazu gehören unter anderem die Meinungsfreiheit, Selbstbestimmtheit und die Privatsphäre.

Die Öffentlichkeit verliert ihre Meinungsfreiheit. Um Fakenews oder hetzerische Aussagen zu vermeiden, werden Uploadfilter eingesetzt, welche durch KI gestützt sind. Auf der anderen Seite jedoch sorgen vor allem Fakenews dazu, dass Unwahrheiten sich durch Social-Media schnell verbreiten und zu Unruhe in der Bevölkerung führen.

Außerdem werden ethische Entscheidungen durch Maschinen getroffen. Durch autonomes Fahren und KI-gestütztem Straßenverkehr werden ethische Entscheidungen nicht mehr von Menschen übernommen. Die KI entscheidet folgendermaßen, ob ein Leben mehr Wert ist als ein anderes. Sol in Konfliktsituation eher ein Kind überfahren wird oder ein älterer Mann? Wenn man sich jedoch die derzeitige Situation anschaut, ist leicht zu erkennen, dass 95% der Unfälle nicht durch technischem, sondern durch menschlichem Versagen verursacht werden. Dies verdeutlicht, dass die meisten Fehler durch den Menschen zustande kommen und die KI entsprechende Gefahrensituationen löst.

Das Wichtigste ist jedoch, dass jeder Bürger so viele Daten von sich preisgeben wird, wodurch er so gut wie keine Privatsphäre mehr besitzt. Der Bürger wird „gläsern" sein. Diese Daten werden nicht nur für staatliche Organisationen sichtbar sein, sondern auch für private Unternehmen, da die Bevölkerung ihre Daten freiwillig weitergibt. Umso wichtiger ist es also, dass eine digitale Souveränität geschaffen wird, indem gesetzliche Grundlagen die Nutzung und Speicherung der Daten regeln. Auch sollte der Öffentlichkeit bereits in jungen Jahren gelehrt werden, wie mit persönlichen Daten umzugehen ist. Denn die Nutzung der Daten ist enorm wichtig um die Welt sicherer zu machen, Verbrechen schneller aufzuklären und vorher zu bekämpfen.

Gesundheit im Jahr 2040 – Personalisierte Behandlungen oder Sanktionssysteme?

Wearable-Computers, kurz Wearables, bauen auf dem Konzept des „Internet of Things" auf. Wearables sind dabei technologische Hilfsmittel, welche einfach am Körper getragen werden können.

(vgl. Hiremath 2014) Zu den Wearables gehören beispielsweise heute schon erhältliche Fitnesstracker oder Silikonpflaster. Diese können mit auf der Haut angebrachte Sensoren Vitaldaten erheben (vgl. Emprechtinger 2018). Mit Hilfe dieser Technologien und deren Weiterentwicklung könnte sich das Gesundheitswesen für den Bürger im Jahr 2040 stark ändern. Durch angebrachte Sensoren und Tracker am Handgelenk können jederzeit Vitaldaten des Bürgers eingelesen und Rückmeldungen gegeben werden. Durch diese ständige Überwachung der Werte wird sich die Häufigkeit an Arztbesuchen deutlich reduzieren. Außerdem haben auch Krankenkassen jederzeit Einblick in diese Daten und können ihre Angebote und Kundenbeiträge so positiv an ihre Patienten anpassen. (vgl. Strauß 2019) Daneben bieten diese Technologien und dadurch erhobene Daten einen Mehrwert für die Forschung verschiedener Krankheiten. Für Parkinson wird davon ausgegangen, dass es bis 2040 12,9 Millionen Fälle gibt, was mehr als doppelt so viele Betroffene sind als 2015. Durch die bis dahin erhobenen Daten und Forschungen wird die Behandlung von Parkinson im Jahre 2040 viel angenehmer für die Patienten gestaltet und im besten Fall steht bis dahin eine Heilung in Sicht. (vgl. Boroojerdi 2019). Diese Verbesserungen werden sich bis 2040 auf viele weitere, noch nicht weit genug erforschte Krankheiten ausbreiten. Insgesamt kann zu den Wearables gesagt werden, dass sie das Gesundheitswesen bis in das Jahr 2040 stark beeinflussen werden. (vgl. Health Informatics 2019). Die Entwicklung führt aktuell über eine unterstützende Funktion der Wearables, hin zu einer klaren Empfehlung der Wearables zu einem besseren Lebensstil.

Doch sorgt die Sammlung an Vitaldaten in der Zukunft für eine bessere Gesundheit oder überwiegen die negativen ethischen Aspekte?

Wenn wir über Gesundheit und Ethik sprechen, sind uns vor allem die Werte Privatsphäre, Chancengleichheit und Selbstbestimmtheit wichtig. Am Beispiel der Vitaldatenübermittlung an die Krankenkassen kann es für den gläsernen Bürger zu Nachteilen bei allen Werten kommen. Als Beispiel kann ein Bürger an Blutdruckproblemen leiden und deshalb gewisse Aufgaben zur Besserung auferlegt bekommen. Die Einhaltungen der Vorgaben können nun von der Krankenkasse selbst überwacht werden. Wird der Krankenkasse nun vor Augen geführt, dass sich ihre Kunden nicht an Vorgaben der Ärzte halten, können sie durch die eindeutigen Daten kurzerhand die Krankenkassenbeiträge dieser Kunden erhöhen. Aufgrund dessen könnte die Chancengleichheit im Gesundheitssystem zukünftig nicht mehr gegeben sein, da Menschen mit der gleichen Krankheit bzw. Behandlung unterschiedliche Beiträge leisten müssen. Jedoch kann dieses System entgegen dem Sanktionssystem auch als Belohnungssystem gesehen werden, aus welchem der Bürger nicht nur finanzielle, sondern auch gesundheitliche Vorteile zieht. Gegenüber vielen Krankheiten raten Ärzte zu einer abwechslungsreicheren und gesünderen Ernährung sowie mehr Sporteinheiten. Aus diesen Empfehlungen werden durch das neue System der Krankenkassen nun Verpflichtungen, wenn der Bürger keine finanziellen Nachteile erfahren möchte. Der Zwang, sich an diese Empfehlungen zu halten, schränkt den Bürger in seiner Selbstbestimmtheit bezüglich Ernährung und Sport ein. Zuletzt wird in diesem Szenario durch das Weiterleiten der Vitaldaten, welche sonst nur den zuständigen Ärzten zur Verfügung stehen, tief in die Privatsphäre eingegriffen. Umgekehrt können durch diese Datenerhebungen aber auch, wie bereits oben erwähnt, mehr nützliche Daten zur Erforschung unheilbarer Krankheiten gesammelt werden. Damit sich der gläserne Bürger 2040 nicht vom Staat überwacht fühlt, sondern die positiven Punkte dieser Eingriffe im Vordergrund sieht, wird hier auf die digitale Souveränität in den Empfehlungen verwiesen.

Unsere Empfehlungen

Die Zukunft der Datennutzung bietet uns viele neue Möglichkeiten, den Alltag neu und effizienter zu gestalten. Jedoch ist auch der Datenkapitalismus weiter auf dem Vormarsch, immer wieder berichten die Nachrichten über Daten-Leaks, Sicherheitsprobleme oder auch Datenmissbräuche. Persönliche Informationen und digitale Profile sind heute mehr denn je handelbare Waren. An dieser Sachlage gibt es jedoch ebenso öffentliche Kritik, welche in politischen Debatten um Datenschutzregulierungen oftmals aufgegriffen werden. Um eine positive Zukunft der Datennutzung zu ermöglichen, müssen daher im Vorfeld grundlegende Problemstellungen aufgezeigt und geklärt werden. Eine dieser Problemstellungen ist die Frage danach, was getan werden muss, damit eine Synergie zwischen der Nutzung und dem Schutz der Daten gewährleistet werden kann. Um diese Frage beantworten zu können, werden im Folgenden mehrere Empfehlungen in Hinblick auf soziale als auch persönliche Aspekte ausgesprochen.

Digitale Souveränität bedeutet: Europäische Gesetze und Verordnungen bestärken!
Damit ein Best Case Szenario für das Jahr 2040 erreicht werden kann, muss die Administration Europas den Datenschutz der Zukunft bestärken und gegebenenfalls erweitern. Eine Bestärkung kann zum einen durch eine strikte Durchsetzung der aktuellen Datenschutzgrundverordnung (DSGVO), als auch durch eine Stärkung der Aufsichtsbehörden mittels neuer Technologien oder der Erhöhung des Personals erfolgen. Die Erweiterung des Datenschutzes hingegen, kann durch die Ergänzung weiterer Verordnungen erfolgen. Ein gutes Beispiel hierfür ist die ePrivacy-Verordnung der EU, welche in naher Zukunft verabschiedet werden soll und sich unter anderem mit dem Tracking auf Webseiten über Cookies und anderen Aspekten der Datennutzung näher befasst. (vgl. Hildebrandt 2017).

Digitale Souveränität bedeutet: Aspekte der Datennutzung in den Mittelpunkt der Gesellschaft rücken!
Um eine bessere Datenzukunft zu arrangieren, muss am Beispiel von Deutschland das Bundesministerium für Bildung und Forschung die ökonomischen sowie sozialen Aspekte der heutigen und zukünftigen Datennutzung näher in den Blick der Gesellschaft rücken. Dadurch wird es ermöglicht, ethische Fragen zur Nutzung der Daten besser beantworten zu können, als auch die digitale Souveränität der Gesellschaft zu fördern. Dabei spielt die Nutzung der Daten für das Gemeinwohl sowie die Beobachtung der Marktmacht einzelner wirtschaftsstarker Unternehmen eine wichtige Rolle. Bei der näheren Betrachtung dieser Aspekte ist es besonders wichtig, ebenso die Auswirkungen der Datenökonomie auf marginalisierte Gruppen stärker in den Blick zu nehmen, damit keine Chancenungleichheit entstehen kann.

Digitale Souveränität bedeutet: Schutzmaßnahmen für personenbezogene Daten der Bevölkerung näherbringen!
Der Schutz personenbezogener Daten sollte nicht ausschließlich durch behördliche Regelungen und Verordnungen stattfinden, sondern muss ebenso durch ihre Eigentümer erfolgen. Dementsprechend sollte die Administration Europas ihren Bürgern die Schutzmaßnahmen persönlicher Daten schon im frühen Alter näherbringen. Dabei kann im Allgemeinen zwischen zwei verschiedenen Schutzmaßnahmen unterschieden werden. Die reaktiven Schutzmaßnahmen bieten dem Dateneigentümer die Möglichkeit, seine Datenfreigabe besser zu kontrollieren und gegebenenfalls zu reduzieren. Zu diesen Schutzmaßnahmen zählen unter anderem die Verwendung von datenschutzkonformen Kommunikationswegen, Suchmaschinen und Betriebssystemen, der

Gebrauch von Technologien wie Virtual-Private-Network (VPN), The-Onion-Router (TOR), Advertising- und Trackingblocker, als auch das Löschen oder Unterbinden von Webseiten-Cookies. Die proaktiven Schutzmaßnahmen hingegen dienen als Präventionsmaßnahmen, welche unbewusste Datenfreigaben minimieren oder gänzlich verhindern sollen. Diese Schutzmaßnahmen können durch frühzeitige Schulungen unterstützt werden, welche zur Förderung des öffentlichen Bewusstseins für den Umgang mit personenbezogenen Daten beitragen.

Digitale Souveränität bedeutet: Entwicklung technischer Lösungen und Innovationen zum Datenschutz!
Bei der Entwicklung neuer Methoden zur Gewinnung von personenbezogenen Daten scheuen Unternehmen keine Kosten. Um dem entgegen zu wirken, müssen Forschungsinstitute sowie Unternehmen auch in Zukunft die Forschung an Anonymisierungstechniken fortführen. Dabei ist es wichtig, sowohl technische Lösungen, als auch Innovationen zu entwickeln, die den Datenschutz beständig gewährleisten können.

Im Hinblick auf die allgemeine Empfehlung sollte sich letztlich jeder, der Daten über sich im Internet preisgibt, klar vor Augen führen, dass diese sein Eigentum sind und somit seiner Privatsphäre angehören. Im Endeffekt liegt es in unserer Entscheidungsmacht, ob wir die aufgezeigten Empfehlungen umsetzen und damit das beschriebene Best-Case-Szenario im Jahr 2040 in sichtbare Nähe zu rücken. Durch die Aussprache der Empfehlungen könnte eine Basis dafür geschaffen werden, welche dazu dient, die digitale Souveränität der Gesellschaft zu fördern!

Quellen:

Bründl, Simon (2016): Daten als Geschäft — Rollen und Wertschöpfungsstrukturen im deutschen Markt für persönliche Daten, in: *Wirtschaftsinformatik & Management*, [online] https://link.springer.com/article/10.1007/s35764-016-0124-5?error=cookies_not_supported&code=49b20ada-8fd5-4531-a429-95d60ef3be38 [28.06.2020].

Boroojerdi, Babak (2019): Können sogenannte „Wearables" (tragbare Sensoren) einen Mehrwert für Parkinson-Patienten schaffen? | UCB, in: *UCB*, [online] https://www.ucb.de/medien/ucb-storys/detail/a/K%C3%B6nnen-sogenannte-Wearables-tragbare-Sensoren-einen-Mehrwert-f%C3%BCr-Parkinson-Patienten-schaffen [28.06.2020].

Buchholz, Katharina (2019): More Countries Are Using Drones, in: *Statista Infographics*, [online] https://www.statista.com/chart/17021/number-of-countries-using-drones/ [28.06.2020].

Buduma, Nikhil / Nicholas Locascio (2017): *Fundamentals of Deep Learning: Designing Next-Generation Machine Intelligence Algorithms*, 1. Aufl., Sebastopol, USA: O'Reilly Media.

Bundesministerium für Wirtschaft und Energie (2019): Umbemanntes Fliegen im Dienst von Mensch, Natur und Gesellschaft, in: *BMWI*, [online] https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/drohnen-unbemanntes-fliegen.pdf?__blob=publicationFile&v=14 [28.06.2020].

Drone Industry Insights (2019): Drohnen - Nachfrageentwicklung in Deutschland 2030, in: *Statista*, [online] https://de.statista.com/statistik/daten/studie/972655/umfrage/prognose-der-entwicklung-der-nachfrage-auf-dem-drohnenmarkt-in-deutschland/ [28.06.2020].

Emprechtinger, Franz (2018): Wie Wearables die klassische Medizin revolutionieren, in: *Lead Inovation*, [online] https://www.lead-innovation.com/blog/wie-wearables-die-klassische-medizin-revolutionieren [28.06.2020].

Groneberg, Frank (2019): Verschwunden: Mit der Polizei-Drohne auf Vermisstensuche, in: *MOZ.de*, [online] https://www.moz.de/landkreise/oder-spree/eisenhuettenstadt/artikel0/dg/0/1/1704167/ [28.06.2020].

Health Informatics (2019): Big Data and Wearable Health Monitors: Harnessing the Benefits and Overcoming Challenges, in: *Health Informatics Online Masters | Nursing & Medical Degrees*, [online] https://healthinformatics.uic.edu/blog/big-data-and-wearable-health-monitors-harnessing-the-benefits-and-overcoming-challenges/#:%7E:text=A%20Wealth%20of%20Health%20Data&text=Generally%20speaking%2C%20E-marketer%20estimates,will%20own%20a%20wearable%20device [28.06.2020].

Hildebrandt, Christian / Arnold, René (2017): Wirtschaftliche Auswirkungen der Regelungen der ePrivacy-Verordnung auf die Online-Werbung und werbefinanziertedigitaleGeschäftsmodelle, in: *ZBW*, [online] http://www.zbw.eu/econis-archiv/bitstream/handle/11159/2801/2017_ePrivacy-BMW.pdf?sequence=1 [11.06.2020].

Hiremath, Shivayogi (2014): Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare - IEEE Conference Publication, in: *IEEE Xplore*, [online] https://ieeexplore.ieee.org/document/7015971 [28.06.2020].

Hoppenstedt, Max (2020): EU geht mit Drohnen auf Einbrecherjagd, in: Süddeutsche.de, [online] https://www.sueddeutsche.de/panorama/kriminalitaet-eu-geht-mit-drohnen-auf-einbrecherjagd-1.4863948 [25.06.2020].

Stoldt, Till-R. (2017): Polizei startet Verbrecherjagd mit Prognose-Software, in: *DIE WELT*, [online] https://www.welt.de/regionales/nrw/article133396024/Polizei-startet-Verbrecherjagd-mit-Prognose-Software.html [28.06.2020].

Strauß, Kathrin (2019): Wearables und Fitness-Apps – Spione im Kleinformat, in: *datenschutzexperte.de*, [online] https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/wearables-und-fitness-apps-datenschutzrisiko/ [28.06.2020].

TAZ (2020): Drohnen-Einsatz in der Coronakrise: Die Polizei mahnt von oben, in: *TAZ Verlags- und Vertriebs GmbH*, [online] https://taz.de/Drohnen-Einsatz-in-der-Coronakrise/!5677868/ [28.06.2020].

Third Element Aviation (2020): Überwachung durch Drohnen, in: *Third Element Aviation*, [online] https://3rd-element.com/ueberwachung-durch-drohnen/ [28.06.2020].

Wagner, Hannah (2020): Drohneneinsätze: Überwachung und Hilfe, in: *heise online*, [online] https://www.heise.de/newsticker/meldung/Drohneneinsaetze-Ueberwachung-und-Hilfe-4701315.html [28.06.2020].

Welchering, Peter (2019): Autonome Waffen - KI-Systeme im Militär, in: *Deutschlandfunk*, [online] https://www.deutschlandfunk.de/autonome-waffen-ki-systeme-im-militaer.676.de.html?dram:article_id=459749 [28.06.2020].

Welt (2020): Regeln in der Corona-Krise: Wo die Polizei die Ausgangssperre per Drohne kontrolliert, in: *DIE WELT*, [online] https://www.welt.de/vermischtes/article207183545/Regeln-in-der-Corona-Krise-Wo-die-Polizei-die-Ausgangssperre-per-Drohne-kontrolliert.html [28.06.2020].