Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Smart City! – Smart Citizens?

Quelle: BMI © GettyImages - miakievy

Keynote

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)

Inhalt

1. Smart City

a. KI
b. Autonomes Fahren
c. Vorgaben der DS-GVO

2. Smart Citizens

a. Transparenz
b. Skills of the 21-Century

3. Smart Privacy

Inhalt

1. Smart City

2. Smart Citizens

3. Smart Privacy

1. Smart City

Digitale Technologien helfen bei den urbanen Herausforderungen etwa in den Bereichen Umweltverschmutzung, demographischer Wandel, Bevölkerungswachstum, Verkehrssteuerung, (Energie-)Ressourcenverwendung, Städtebau, Wirtschaft oder Bürgerbeteiligung.

1. Smart City

Gera:

Digitalisierung als Weg zu einer effizienten, technologisch fortschrittlichen und sozial inklusiven Gesellschaft:

- **Starke Bürgerbeteiligung**: Raum und Werkzeug, den Prozess zu steuern.

- **Offenheit der Daten**: Transparenz und Opendata, digitale Teilhabe und E-Governement, Verwaltung öffnen, nicht abschotten, Zugang zu den Daten, die nicht personalisiert sind, wie bei Geodaten z.B., s.a. wie zuvor das Freifunkprojekt.

- **Förderung digitaler Projekte**, etwa autonomes (Bus-)Fahren oder das Freifunkprojekt.

- Förderung **energieautarker** und **klimagerechter** Stadtquartieren.

- **Förderung der Wirtschaft** durch die Ansiedelung beispielsweise von Softwareentwicklern.

- **Förderung des Wissenstransfers**, sowohl innerhalb der Kommune, aber auch zwischen Kommunen.

1. Smart City

Eine Smart City setzt voraus, dass möglichst viele Sensoren möglichst viele Daten der Stadtbewohner erfassen und auswerten und verfügbar machen.

Das setzt eine intakte IT-Struktur bei gegebener IT-Sicherheit voraus.

Unabhängig davon, ob es sich um Kommunikations- oder Informations-plattformen handelt, um intelligente Energienutzung (Smart Meters), um eine bessere Vernetzung von Behörden und Wirtschaft, um eGovernment, um Ratsinformationssysteme, um Bürgerbeteiligungsserver, um Apps für Information und Integration, um reale oder virtuelle IT-Experimentierfelder (digitale Bolzplätze), um Trainingsworkshops für Senioren, um Open Innovation (FabLabs), um Verkehrsplanung, um Citizen Sensing (Datengenerierung durch Bürgerinnen und Bürger) oder um e-b2c: Zumeist werden personenbezogene Daten verarbeitet.

Und das wirft <u>viele</u> Probleme auf: ⇨

1. Smart City

a. KI

Gutachten der Datenethikkommission (DEK) der Bundesregierung, Oktober 2019

Auftrag: Ethische Maßstäbe und Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter zu entwickeln.

Die DEK hat sich für ihr Gutachten an den folgenden **Leitgedanken** orientiert:

- **Menschenzentrierte** und werteorientierte Gestaltung von Technologie
- **Förderung digitaler Kompetenzen** und kritischer Reflexion in der digitalen Welt
- **Stärkung des Schutzes von persönlicher Freiheit, Selbstbestimmung und Integrität**
- Förderung verantwortungsvoller und gemeinwohl-verträglicher Datennutzungen
- Risikoadaptierte Regulierung und wirksame Kontrolle algorithmischer Systeme
- Wahrung und Förderung von Demokratie und gesellschaftlichem Zusammenhalt
- Ausrichtung digitaler Strategien an Zielen der Nachhaltigkeit
- Stärkung der digitalen Souveränität Deutschlands und Europas.

1. Smart City

a. KI

Zu den objektiven Anforderungen an jede verantwortungsvolle Nutzung von Daten gehören nach Auffassung der DEK die folgenden datenethischen **Grundsätze**:

- **Vorausschauende Verantwortung**: Bei der Sammlung, Verarbeitung und Weitergabe von Daten müssen mögliche Auswirkungen auf Einzelne oder die Allgemeinheit unter Berücksichtigung künftiger Akkumulations-, Netzwerk- und Skaleneffekte, technologischer Möglichkeiten und Akteurskonstellationen abgeschätzt werden.

- **Achtung der Rechte beteiligter Personen**: Akteure, die an der Generierung von Daten beteiligt waren – sei es als Subjekt der Information, sei es in einer anderen Rolle –, können Rechte in Bezug auf diese Daten zustehen, die zu achten sind.

- **Wohlfahrt durch Nutzen und Teilen von Daten**: Daten können als nicht-rivales Gut vervielfältigt und parallel von vielen Akteuren zu vielen verschiedenen Zwecken genutzt werden und damit das Gemeinwohl fördern.

- **Zweckadäquate Datenqualität**: Ein verantwortungsvoller Umgang mit Daten setzt die Sicherstellung einer dem jeweiligen Zweck angemessenen Datenqualität voraus.

- **Risikoadäquate Informationssicherheit**: Daten sind anfällig gegenüber Ausspähung und Verfälschung von außen und können, in andere Hände gelangt, nur schwer zurückgeholt werden. Es bedarf daher eines dem jeweiligen Risikopotenzial angemessenen Maßes an Informationssicherheit.

- **Interessenadäquate Transparenz**: Derjenige, der Daten als Verantwortlicher verarbeitet, muss bereit und in der Lage sein, dafür Rechenschaft abzulegen. Dies erfordert ein angemessenes Maß an Transparenz und Dokumentation des Handelns und ggf. auch entsprechende Haftungsregelungen.

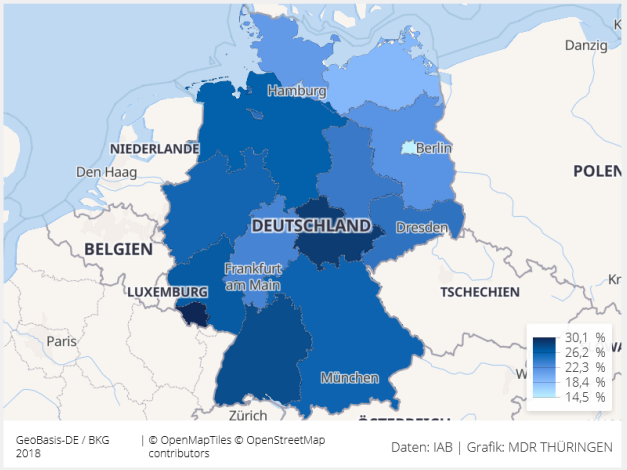
1. Smart City

Allgemeines zur KI:

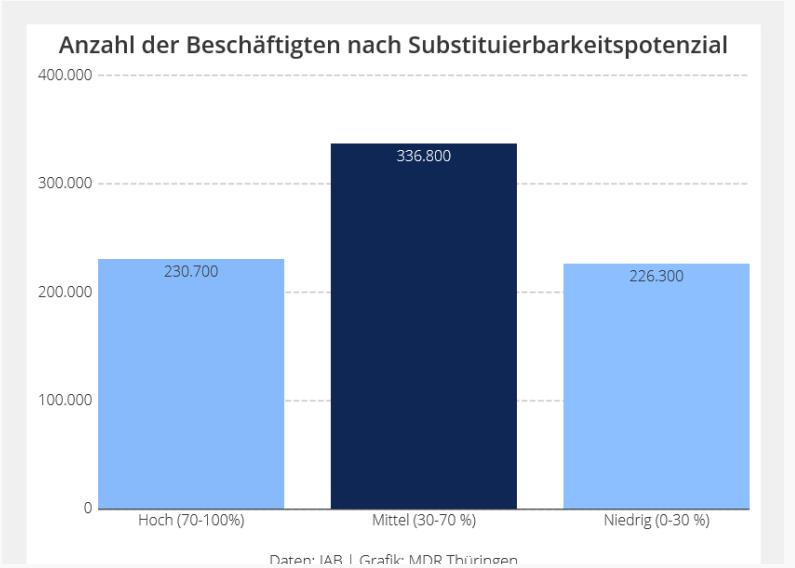
> *Zugleich entsteht oder erhöht sich durch die Digitalisierung die Nachfrage nach neuen Produkten oder Dienstleistungen. Welche Beschäftigungseffekte in der Summe entstehen, ist kaum vorhersehbar, aber es ist auf alle Fälle nicht nur das Wegfallen von Arbeitsplätzen.“*
>
> Dr. Per Kropp, IAB

Wie ist die Situation auf dem Thüringer Arbeitsmarkt?

In Deutschland liegt der Beschäftigtenanteil in stark substituierbaren Berufen zwischen 15 und 30 Prozent. In den Stadtstaaten Berlin und Hamburg sind die Werte am niedrigsten, über dem Bundesschnitt liegen Baden-Württemberg, das Saarland und auch **Thüringen mit 29,1 Prozent:**



Im Freistaat sind laut IAB etwa gleich viele Menschen in Berufen beschäftigt, die entweder stark oder nur gering substituierbar sind. Die Mehrheit hingegen arbeiten in Berufen mit mittlerer Substituierbarkeit:



Rund 10.000 der Beschäftigten (1,3 Prozent aller Beschäftigten) üben laut IAB Tätigkeiten aus, die bereits heute ganz von Computern oder computergesteuerten Maschinen übernommen werden könnten. Dabei handelt es sich um Fertigungs- und Fertigungstechnische Berufe wie Fachkräfte für Elektrotechnik oder Metallumformung und Dienstleistungs- und Logistikberufe wie Fachkräfte in der Steuerberatung und im Beruf Kranführer/Bediener Hebeeinrichtung.

Im Freistaat sind laut IAB etwa gleich viele Menschen in Berufen beschäftigt, die entweder stark oder nur gering substituierbar sind. Die Mehrheit hingegen arbeiten in Berufen mit mittlerer Substituierbarkeit:

mdr THÜRINGEN

19. Oktober 2019

mdr THÜRINGEN

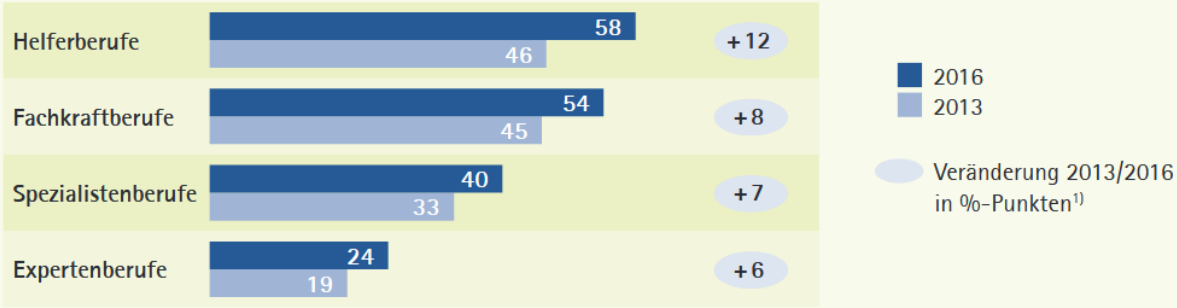
https://job-futuromat.iab.de/

Quelle: MDR THÜRINGEN/mm https://www.mdr.de/thueringen/immer-mehr-berufe-durch-computer-ersetzbar100.html#sprung4

19. Oktober 2019

Substituierbarkeitspotenzial nach Anforderungsniveau

Anteil der Tätigkeiten, die potenziell von Computern erledigt werden könnten, in Prozent



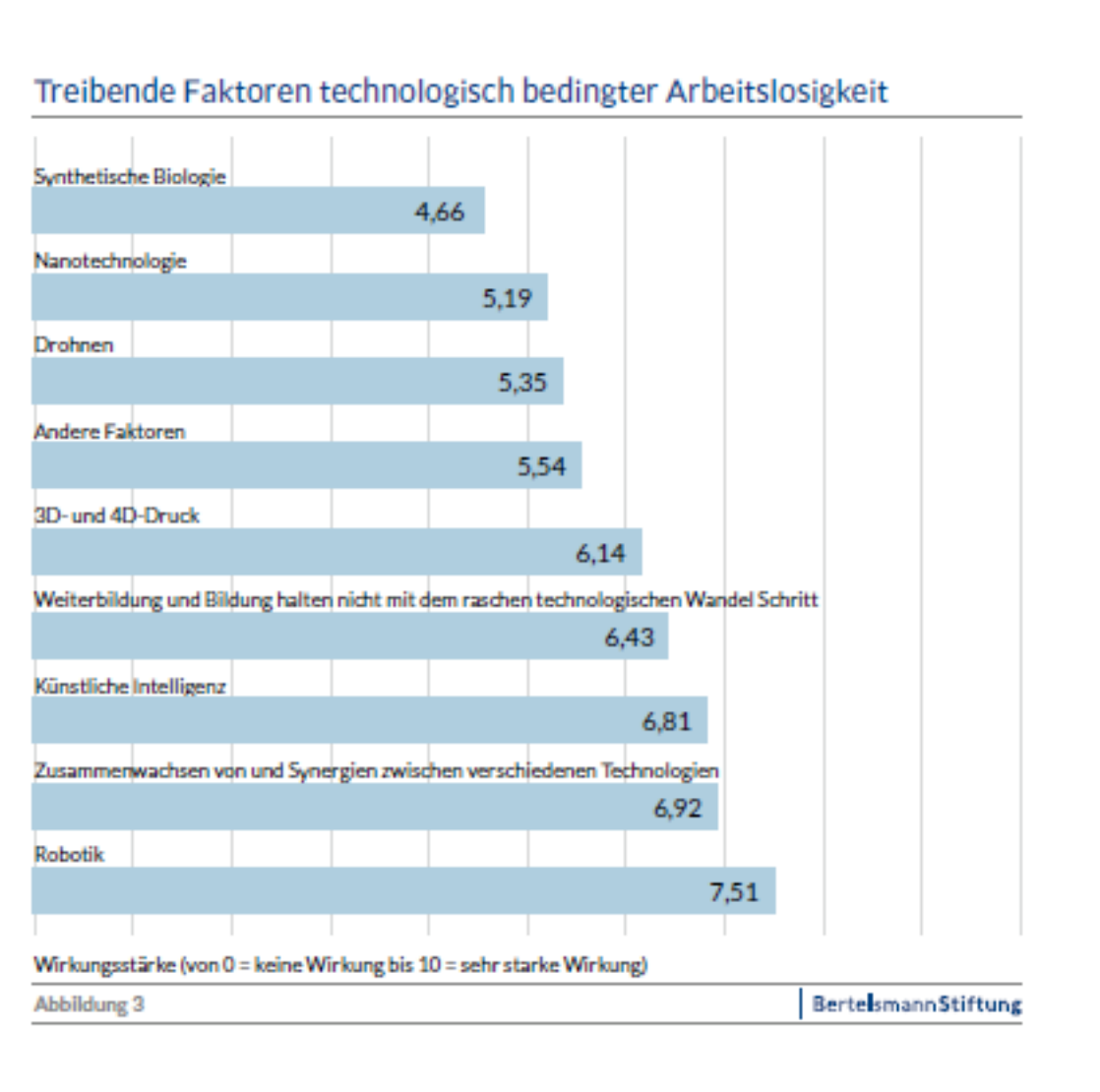
1) Abweichungen zu den Differenzen kommen durch Rundung zustande.

Quelle: Eigene Berechnungen, Dengler/Matthes (2015), BERUFENET (2013, 2016).

aus IAB-Kurzbericht 4/2018

Abbildung 1

2050: Die Zukunft der Arbeit



Befragung der Bundesbürger Nov. 2017

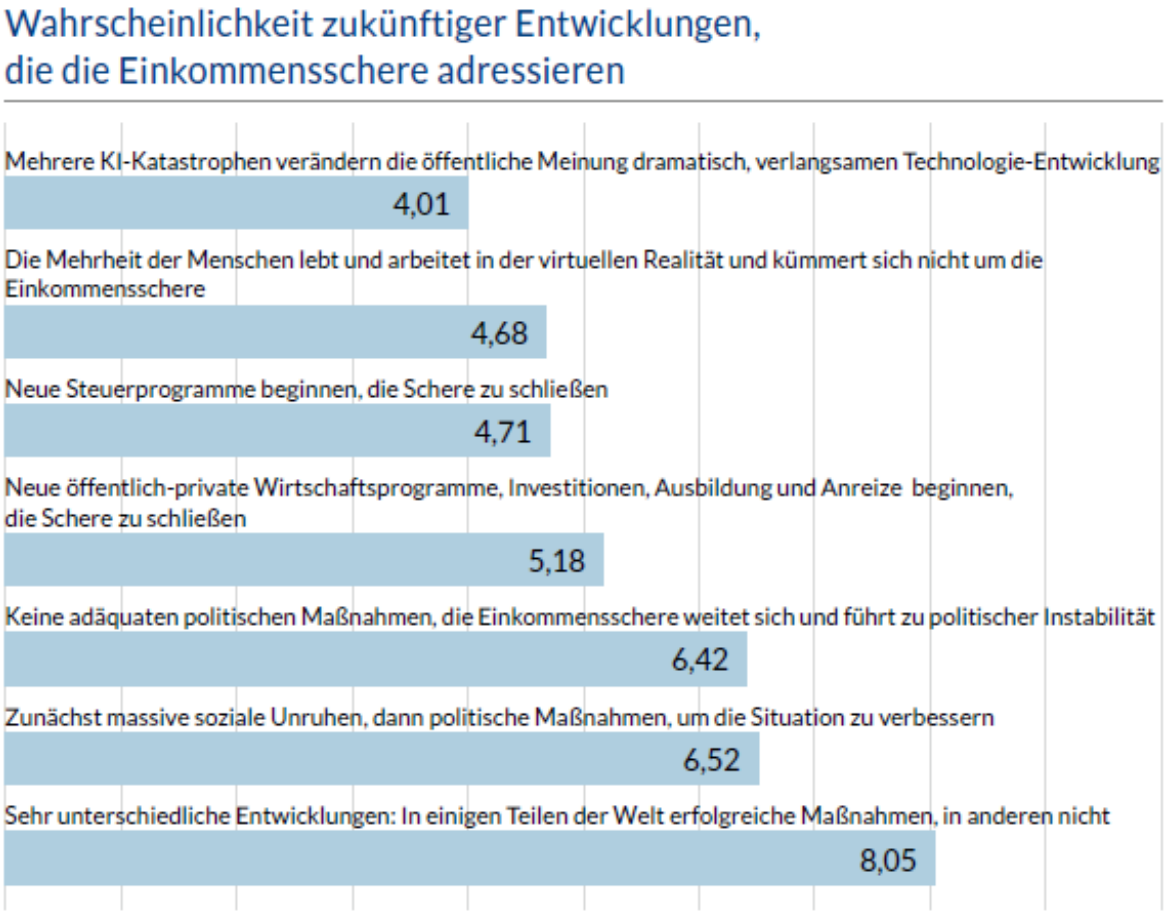
Befragung der Bundesbürger Nov. 2017

2050: Die Zukunft der Arbeit

Mögliche Zukunftsberufe:

- Innenausstatter für virtuelle Räume
- Kreativitätscoach
- Persönlicher Gesundheitsberater
- Empathie-Interventionist
- Algorithmen-Versicherer
- Biosignal-Trainer
- Bildungs-Portfolio-Optimierer
- Extrem-Genetiker / Syn-Biologe
- Metaversum-Hausmeister
- Übersetzer Mensch-Maschine & Maschine-Mensch
- Freizeit-Gestalter / Beschäftigungsbeschaffer
- Virtueller Team-Assistent
- Persönlicher Lerncoach
- Ethik-Algorithmiker
- Wohnort-Makler für Wissensarbeiter
  (Quelle: Bertelsmann Stiftung)

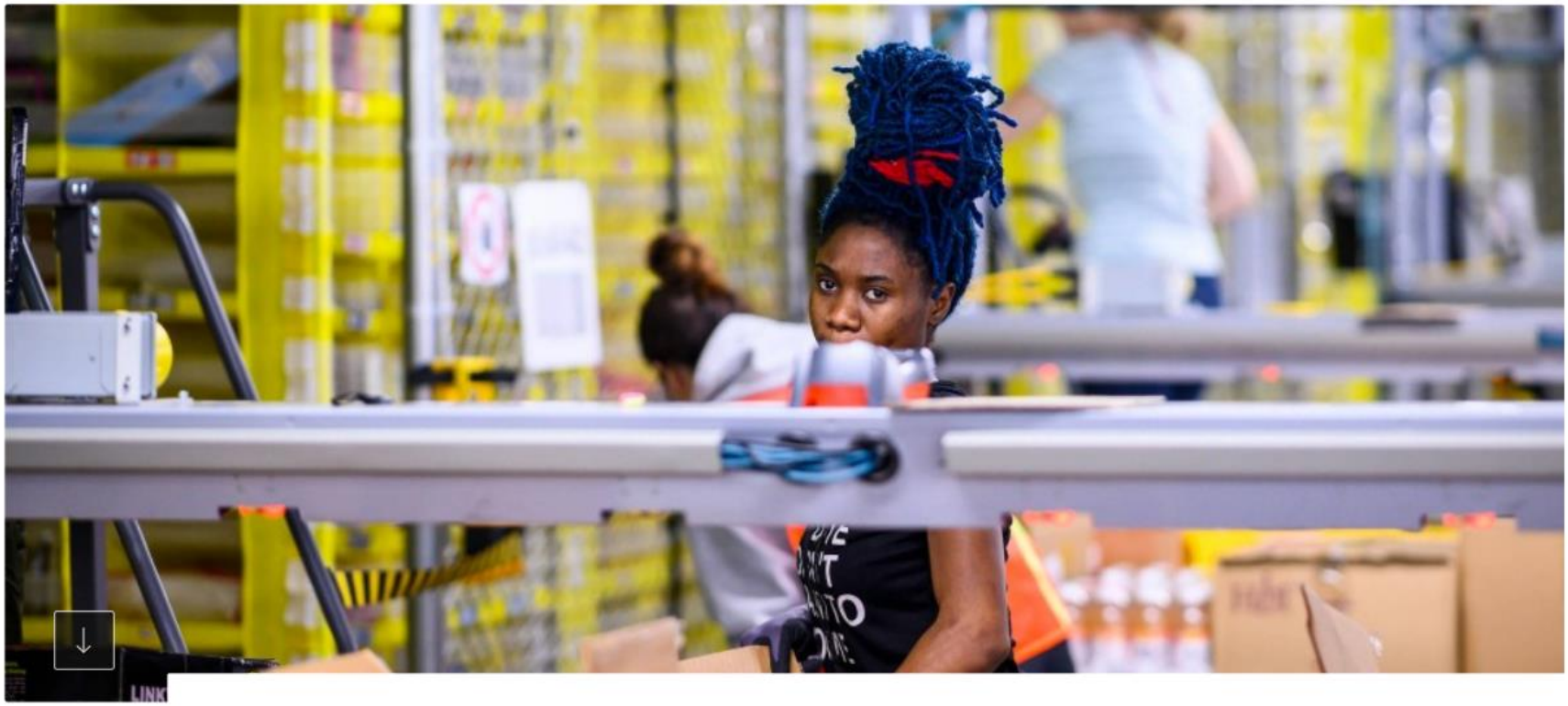
2050: Die Zukunft der Arbeit



NEUE PACK-ROBOTER

Wie Amazon seine Angestellten durch Maschinen ersetzt

VON GUSTAV THEILE - AKTUALISIERT AM 14.05.2019 - 13:28



700 Päckchen verpacken in einer Stunde – das schafft nur eine Maschine. In den ersten Logistikzentren setzt Amazon jetzt auf Pack-Maschinen. Für die Angestellten gibt es dagegen neue Anreize, Paketlieferant zu werden.

https://www.faz.net/aktuell/wirtschaft/diginomics/wie-amazon-seine-angestellten-durch-pack-maschinen-ersetzt-16186353.html?utm_source=pocket-newtab

- Amazon: Algorithmus kontrolliert Arbeitsleistung und entscheidet (mit) über Entlassung.
- Arbeitshandschuh registriert Fehlgriffe des Arbeitnehmers.

Datenschutz

Österreichs Jobcenter richten künftig mit Hilfe von Software über Arbeitslose

In Österreich teilt ab nächstem Jahr ein Algorithmus alle Jobsucher in Kategorien. Wer schlecht abschneidet, dem werden Zukunftschancen verbaut. Die Behörden bejubeln das als Effizienzsteigerung mit modernsten technischen Mitteln. Experten warnen hingegen vor automatisierter Diskriminierung.

13.10.2018 um 09:00 Uhr - Alexander Fanta - 18 Ergänzungen

Netzpolitik.Org: Arbeitslose im Berlin der 1920er-Jahre. Sie hätten sich wohl nicht träumen lassen, dass eines Tages Maschinen die Verteilung von Ressourcen beeinflussen könnten. CC-BY-SA 3.0 Wikimedia/Bundesarchiv

Einzelne Bereiche

- Bewerbung:
  - (Hoch-)Schul-Vita-Daten von Schul-Plattformen?
  - Big-Data-Profil (soziale Netzwerke)
  - USA: Facebook-Profile erwünscht
  - Die Eingabemasken werden mit den Bewerbungsdaten befüllt und eine lernende Verarbeitungskomponente kann automatisiert eine Eignungsempfehlung abgeben *(Quelle: Bitkom - Entscheidungsunterstützung mit Künstlicher Intelligenz, s. S. 19).*

- Die Talanx-Versicherung analysiert mit der Software „Precise“ anhand der Stimme die Persönlichkeit eines Bewerbers in 10 Minuten – der Algorithmus kann 42 Dimensionen einer Persönlichkeit messen *(Quelle: Tagesspiegel, 02.02.2018).*

Einzelne Bereiche

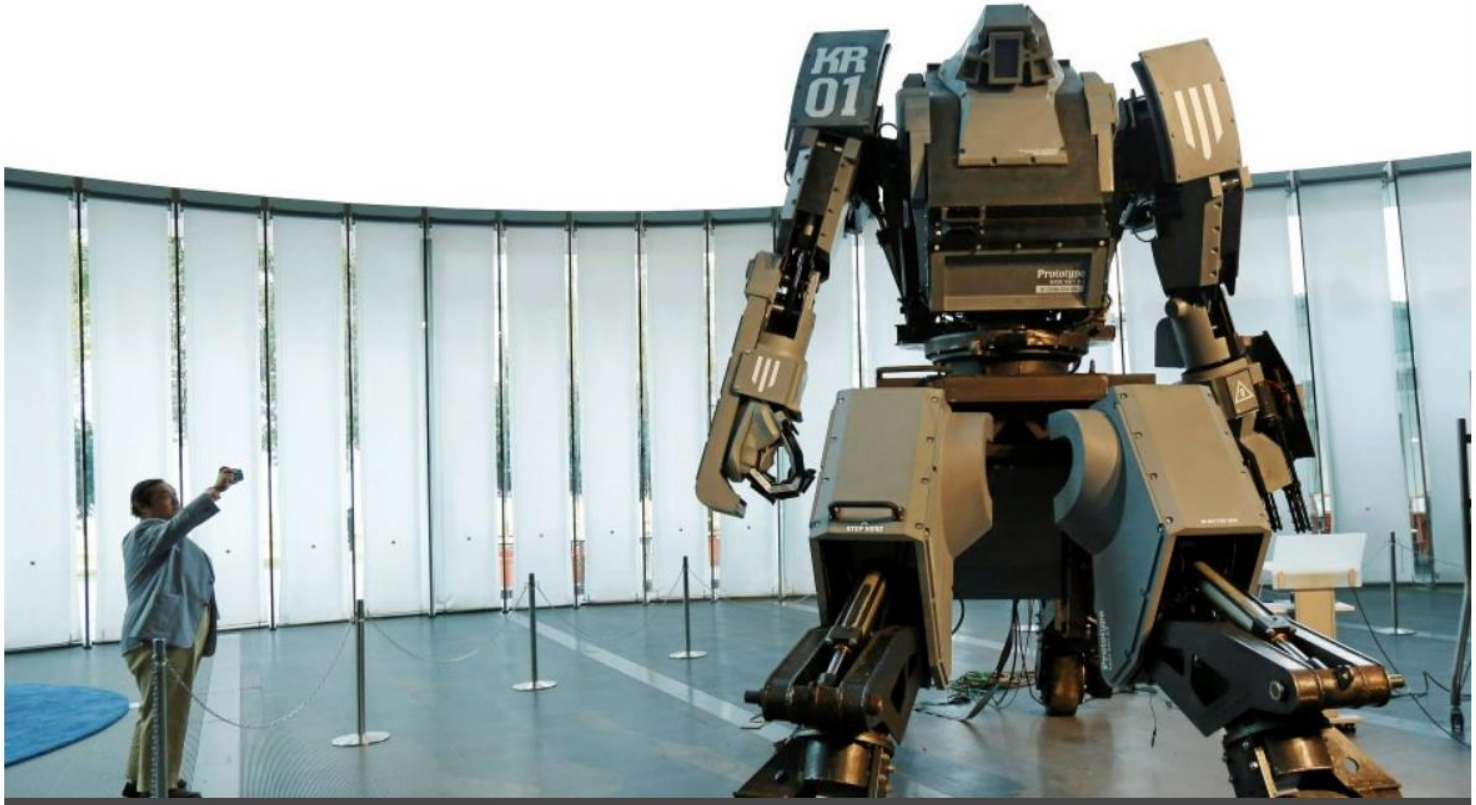
Job:

- **Leistungskontrolle** durch Tracking und Video
- Handy-App, die Schlaf-Daten an Arbeitgeber sendet
- Handy-Fitness-Tracker; **Interesse der Krankenversicherer und Arbeitgeber** an Daten
- Walmart will mit Audiosensoren im Kassenbereich die „Effizienz der Bezahlvorgänge erhöhen“:

  - Aufzeichnung der Piep-Geräusche:
  - Bewertung der Mitarbeitereffizienz.
  - Aufzeichnung und Auswertung von Kunden- und Mitarbeitergesprächen:
  - Bewertung des Gemütszustands und des Umgangs mit Kunden (Kuketz, iT-Security, Blog).

Umstrittenes Google-Militär-Projekt: Was dürfen Roboter?

Christian Unger 06.06.2019 - 05:36 Uhr



Ein Mann fotografiert den Roboter „Kuratas“ auf einer Messe in Tokio – vier Meter hoch, tonnenschwer und bewaffnet.
Foto: REUTERS / KIM KYUNG-HOON / Reuters

TA, 6. Juni 2019

Wer macht was?

China:

China will bis 2030 führend in KI sein.

Erster chinesischer Roboter, Xiao Yi, hat im Herbst 2017 die nationale Medizinprüfung bestanden. *(TA Erfurt, Seite 6, 17. August 2018)*

Sozialkredit-System zur Steigerung der Aufrichtigkeit in Regierungsangelegenheiten, der kommerziellen Integrität, der sozialen Integrität und der gerichtlichen Glaubwürdigkeit:

- Erfasst werden staatliche und private Datenbanken; Kooperation mit Alibaba Group (chin. Amazon), Baidu (chin. Google) und Tencent (chin. Facebook und WhatsApp (chin. Wechat)).
- Ausgehend von 1000 Punkten, werden bei positivem Verhalten Punkte addiert, bei negativem subtrahiert; gleiches gilt für die persönlichen Beziehungen.

1, 4 Milliarden Menschen in 3 Sekunden an jedem Ort zu identifizieren; 2020 fertig

Wer macht was?

China:

- „Bereits heute müssen Internetnutzer sämtliche Accounts - bei sozialen Netzwerken und anderen Onlinediensten - mit ihrer Handynummer verknüpfen. Sie dient den Behörden als digitale Identifikationsnummer. Fast jede Onlineaktivität kann so im Bruchteil einer Sekunde einer Person zugeordnet werden. Das beginnt bei so banalen Dingen wie dem Eintippen einer Suchanfrage. …Universitäten kontrollieren so, wer den Campus betritt. Und mithilfe eines landesweiten Netzwerks aus bald 600 Millionen Kameras werden Menschen auf der Straße identifiziert, …“

Quelle: SZ online,

https://www.sueddeutsche.de/politik/china-ueberwacht-ueberall-1.4646259,

18. Oktober 2019

- Folgen:

– Öffentliche Bekanntgabe der Personen, die sich positiv oder negativ verhalten im Netz und auf Bildschirmen, z.B. an der Bushaltestelle (digitaler Pranger).

– Positiver oder negativer Einfluss auf Reisemöglichkeiten, Karriere, Internetgeschwindigkeit, Teilnahme an öffentlichen Ausschreibungen, Höhe der Steuern, Zugang zu Krediten, Zugang der Kinder zu Bildungseinrichtungen.

Thüringer Allgemeine (Ilmenau)

„Wie kann ich Ihnen helfen?“

Service-roboter verändern den Einzelhandel. Eine Elektronikkette setzt nun auf den Humanoiden Alex, der direkt an Kunden verkaufen soll

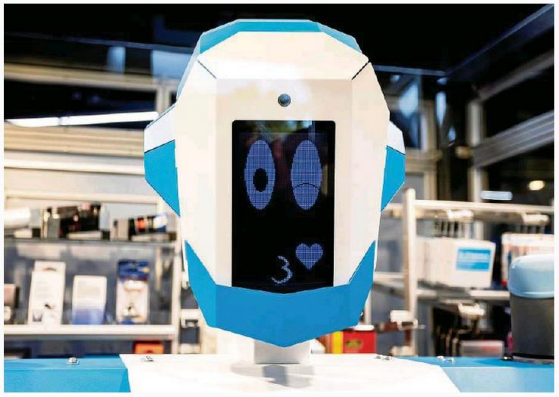
18 Okt. 2019 +44 mehr Von Wolfgang Mulke

Berlin. Alex kann freundlich mit seinen großen Kulleraugen blinzeln oder Kunden höflich heranwinken. Beweglich ist der blauweiß verkleidete Roboter auch. Sein rechter Arm greift weit hinter seinem Rücken eine Packung mit Batterien und legt sie auf ein kleines Fließband, das die Akkus zum wartenden Käufer transportiert. „Alle haben den Roboter am Ende lieb“, sagt der Chef der Elektronik-handelskette Conrad, Jürgen Groth.

Der neue Verkäufer aus Stahl und Chips soll die Berliner fortan rund um die Uhr an sieben Tagen in der Woche mit den nötigsten elektronischen Kleinteilen versorgen. Im Minilager hinter seinem Rücken lagern die Teile, die Verbraucher auch am Abend oder am Wochenende schnell brauchen können: Batterien, Powerbanks, Adapter oder Einwegkameras. Bestellt und bezahlt wird über ein Display.

Groth hätte dafür wohl auch einen einfachen Automaten installieren können. Doch der Familienunternehmer aus dem bayerischen Hirschau will sich als Technologieführer beweisen. „Der Einzelhandel muss sich zurückbesinnen“, sagt er und meint damit dessen Stärken gegenüber dem Geschäft im Internet. Die Waren seien verfügbar, und in den Läden würden Kunden noch von Menschen beraten.

In anderen Filialen der Kette sind auch schon Roboter im Einsatz. Sie weisen den Kunden allerdings lediglich im Laden den Weg zur gesuchten Produktgruppe. Alex hingegen ist schon zum Verkäufer weiterentwickelt worden. Offenkundig nehmen Kunden den Humanoiden mit menschlichen Zügen mittlerweile an. Zwölf Mimiken kann dieser darstellen, zum Beispiel zwinkern, sich schlafend stellen oder einen leicht verwirrten Gesichtsausdruck aufsetzen. Filialleiter Jochen Mädler betont, dass es hier nicht um den Ersatz von echten Verkäufern gehe. Es werde in den Läden auch künftig immer Ansprechpartner aus Fleisch und Blut geben, sagt Mädler.



Der neue humanoide Kollege Alex verkauft in der Conrad-filiale in Berlin-schöneberg direkt an Kunden. Während seine Vorgänger nur den Weg weisen konnten, kann er Wünsche erfüllen und Produkte anreichen.

Die Brüder und Schwestern von Alex arbeiten in den Autofabriken. Dort setzen sie Schweißpunkte oder heben Karosserieteile auf das Band. Den elektronischen Werksarbeitern fehlt dabei allerdings das fröhliche Grinsen.

Aus dieser Branche bringt der Entwickler des Verkaufsbots seine Kenntnisse mit. RoboterPionier Matthias Krinke führt die Firma pi4_robotics mit 50 Beschäftigten in Berlin. Die nächsten Schritte bei der Digitalisierung des Einzelhandels hat er schon im Kopf. Im kommenden Jahr sollen „click-and-collect-einkäufe“möglich werden. Die Kunden bestellen ihre Waren im Internet, fahren dann zur nächsten Filiale, wo ein Roboter ihnen die gekauften Produkte aushändigt.

Einzelne Bereiche

Medizin:

- Chatbot gegen Depressionen:
  - Psychologische Beratung mit Hilfe von Sprachrobotern.
  - Impetus: Rationalisierung, ökonomische Interessen – Aber auch: zeitnahe Beratung, die gar nicht so schlecht sein soll für Millionen Bürger bei geringem Entgelt.

- Roboter werden bereits als Operateure eingesetzt. Absehbar ist, dass Roboter Chirurgen ersetzen können *(Quelle: Bitkom-Entscheidungsunterstützung mit Künstlicher Intelligenz, s. S. 52)*

- In der Diagnose erkennt „IBM Watson Oncology“ ein Lungenkarzinom mit 90 % Wahrscheinlichkeit, ein Radiologe nur mit 50 %. *(Quelle: Bitkom-Entscheidungsunterstützung mit Künstlicher Intelligenz, s. S. 60)*

GOOGLE-COMPUTER GEWINNT GO-DUELL

Was der Sieg der Maschine für den Menschen bedeutet

von Oliver Voß
15. März 2016

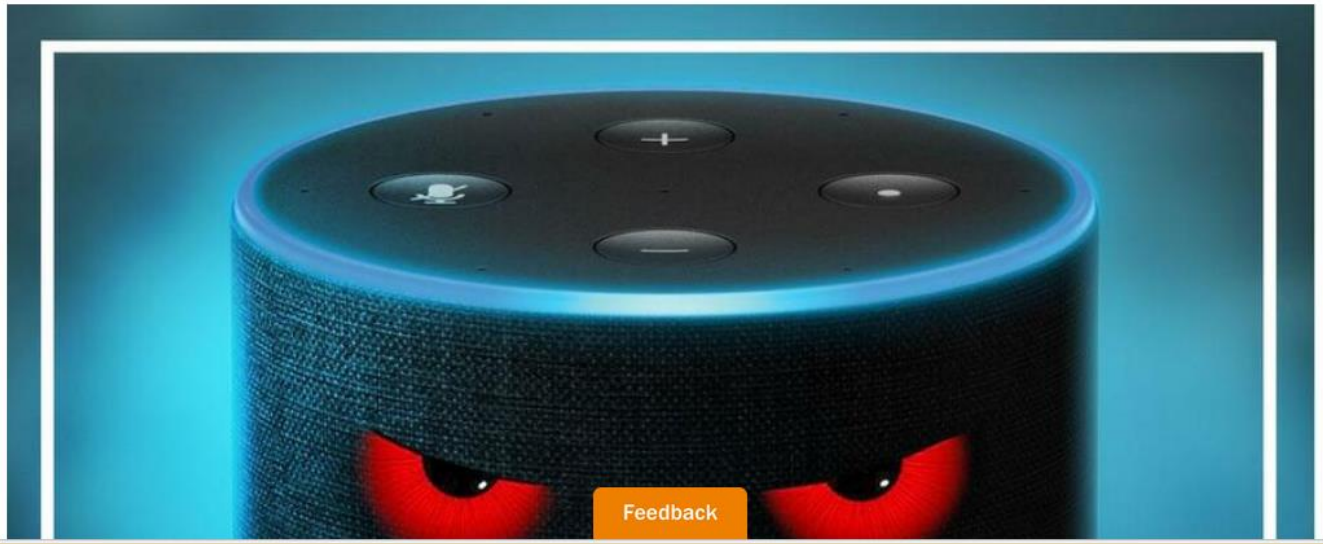
Googles Computerprogramm AlphaGo hat den Meister des Brettspiels Go, Lee Sedol, vernichtend geschlagen. Die Technologie soll künftig noch ganz andere Probleme lösen: Vom Krebs bis zum Klimawandel.

Der große Lauschangriff – Wie Amazon, Apple und Google ihre Kunden aushorchen

Die Affäre um den Sprachassistenten Alexa zeigt, wie weit wir Internetkonzerne in unser Leben gelassen haben. Höchste Zeit für ein paar Spielregeln.

 Christof Kerkmann  Sebastian Matthes  Christian Rickens

02.05.2019 - 19:25 Uhr • 87 x geteilt



https://www.handelsblatt.com/technik/vernetzt/datenschutz-der-grosse-lauschangriff-wie-amazon-apple-und-google-ihre-kunden-aushorchen/24247016.html?ticket=ST-3560146-7BfcPY9rneT2n27dgZdj-ap2

Die Vermessung des Kunden

Die Londoner Oxford Street im Dezember: "Viele Unternehmen glauben, dass Kunde gleich Kunde ist. Aber das stimmt nicht." (Foto: REUTERS)

Immer mehr US-Unternehmen lassen sich von Spezialisten berechnen, wie viel ihnen ein Konsument bis zum Tod einbringen wird. Wer viel wert ist, wird beim Einkauf hofiert - der Rest ignoriert.

Von Claus Hulverscheidt, New York

https://www.sueddeutsche.de/wirtschaft/konsum-die-vermessung-des-kunden-1.4264260

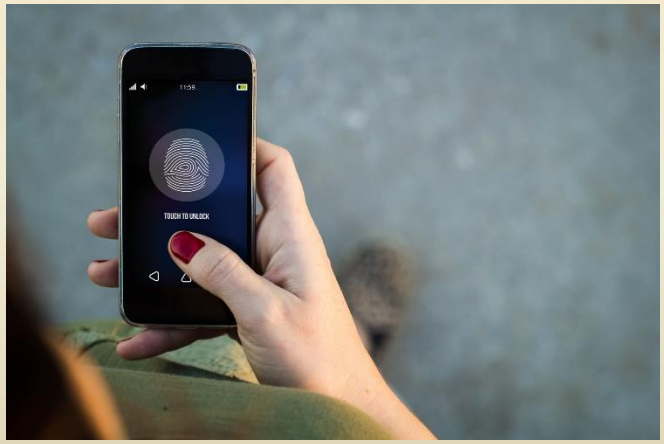
CLV, das steht für "customer lifetime value", zu Deutsch: "Kundenlebenszeitwert" - ein neues machtvolles Marketinginstrument, das Unternehmen in den Vereinigten Staaten so elektrisiert wie es Verbraucherschützer alarmiert, denn einen ähnlich groß angelegten Angriff auf die Privatsphäre von Millionen Flug-, Telefon-, Einzelhandels- und sonstigen Kunden dürfte es selbst in der US-Wirtschaftsgeschichte mit ihren dauernden Datenskandalen bisher nicht gegeben haben. Immer mehr Firmen lassen anhand Dutzender, Hunderter, gar Tausender persönlichen Daten berechnen, wie viel ihnen ein einzelner Käufer über sein gesamtes "Kundenleben" wohl in Dollar und Cent einbringen wird. Kommt jemand auf einen hohen CLV, wird er umgarnt und gepflegt, erhält Rabatte, Hochstufungen, persönliche Hotline-Ansprechpartner und andere schicke Sonderleistungen. Ist der Wert dagegen niedrig, fristet der meist ahnungslose Konsument fortan ein Leben in der Telefonschleife.

https://www.sueddeutsche.de/wirtschaft/konsum-die-vermessung-des-kunden-1.4264260

Smartphone

Auf und Ab des Smartphones beim Gehen →

- KI kann Handlung Parkinson identifizieren
- Ok, ABER wer hat die Daten?



© georgejmclittle - Woman walking smartphone fingerprint - Fotolia

Fragen:

- Dürfen wir automatisierte Entscheidungsprozesse (ADM: automated-decision-making) (fehlerhaften) Algorithmen überlassen?
- Sind wir auf dem Weg in eine automatisierte Demokratie?
- Ein Staat ohne eigene Ressourcen ist auf die Privatwirtschaft angewiesen – besteht die (konkrete) Gefahr der Vermischung von Staat und Wirtschaft?
- Ist KI auch intelligent?
- Kann KI sozial sein?
- Wie ist die demokratische Kontrolle algorithmischer Entscheidungssysteme zu bewerkstelligen?

Was ist zu tun?

- Das Bildungssystem muss sich revolutionieren. Technologische Kompetenzen sind dringend zu vermittelnde Basis-Kompetenzen, um den Algorithmen nicht hilflos gegenüber zu stehen.
  (Quelle: Bertelsmann Stiftung, 2050: Die Zukunft der Arbeit (2016), S. 10)

- Microsoft hat den amerikanischen Kongress aufgefordert, den Einsatz von Gesichtserkennungs-Algorithmen zu regulieren, um die Freiheit des amerikanischen Volkes und die Daten seiner Bürger zu schützen!!! *(Quelle: SZ v. 18.07.18)*

Wer macht‘s?

Erschreckend ist die verbreitete Skepsis gegenüber den politischen Institutionen, die in systemischer Trägheit und der Orientierung an kurzfristig populären Maßnahmen gefangen sind. *(Quelle: Bertelsmann Stiftung, 2050: Die Zukunft der Arbeit (2016), S. 28)*

Vieles wird an der Macht der Lobbyisten scheitern. *(Quelle: Bertelsmann Stiftung, 2050: Die Zukunft der Arbeit (2016),S. 25)*

Ausblick:

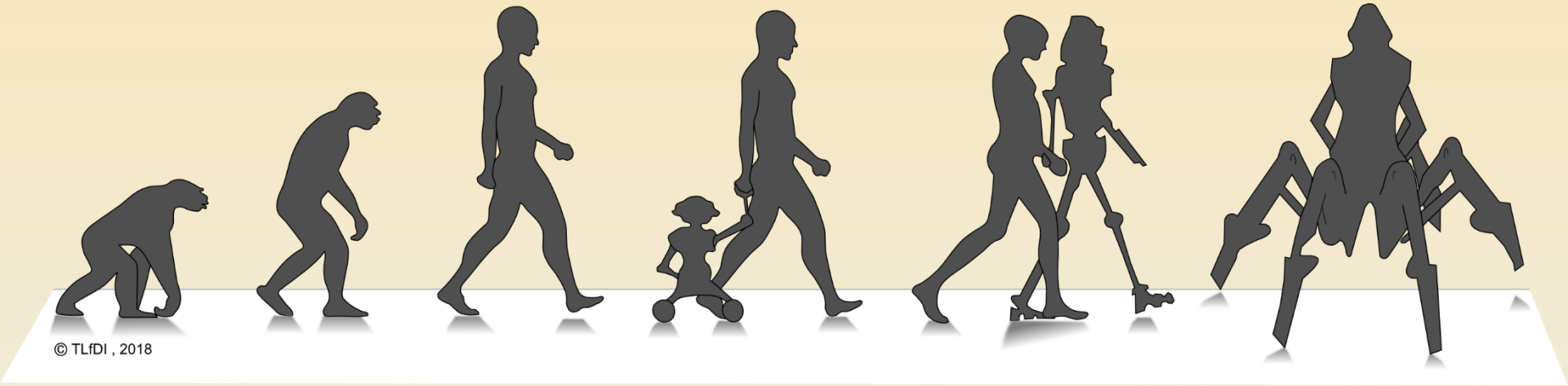
Ethik-Rat, 27.06.2018

Yuval Noah Harari
Hacking humans

Künstliche Intelligenz übertrifft den Menschen längst.

Menschliche Entscheidungen beruhen auf Wahrnehmungen, die zu einem emotional und rational gesteuerten Entschluss führen. Diese Mechanismen werden derzeit entschlüsselt und können gegen den Menschen eingesetzt werden.

Gefährlich ist menschliche Ignoranz und Selbstüberschätzung, wenn sie die Gefahren der Entwicklung unterschätzt.


© TLfDI , 2018

1. Smart City

b. Autonomes Fahren

Video Erfurter Kreisel

Quelle: https://www.youtube.com/watch?v=A29OihNF-OU

1. Smart City

b. Autonomes Fahren

„We kill people based on metadata.“
- Michael Hayden, früherer NSA- und CIA-Direktor

„Wir kennen jeden Autofahrer, der die Verkehrsregeln bricht. Und wir wissen, wo und wie jemand das tut.“
– Jim Farley, Marketingchef Ford, Consumer Electronics Show 2014

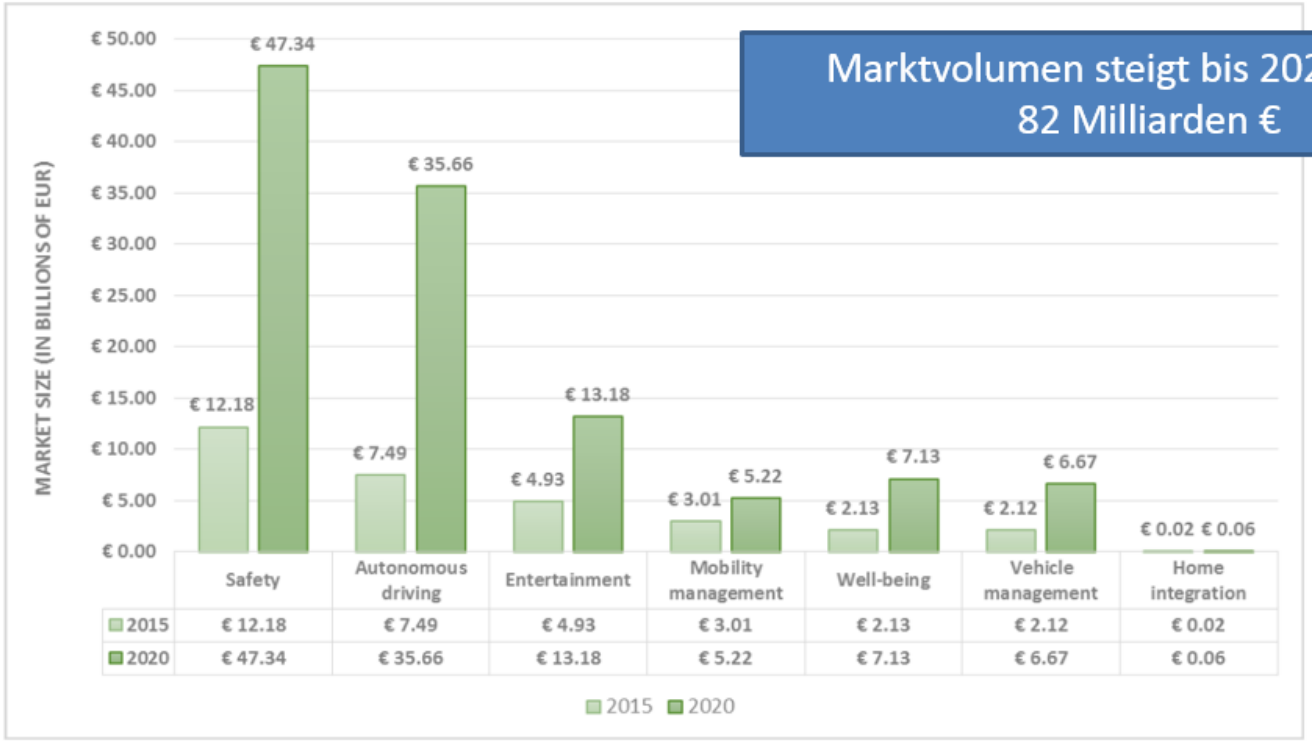
„Es gibt eine Menge Dinge, die wir gern tun würden, aber leider nicht tun können, weil sie illegal sind. Weil es Gesetze gibt, die sie verbieten. Wir sollten ein paar Orte haben, wo wir sicher sind. Wo wir neue Dinge ausprobieren und herausfinden können, welche Auswirkungen sie auf die Gesellschaft haben.“
- Larry Page, CEO Google Inc.

„Daten sind der Rohstoff der Zukunft“
– Angela Merkel, Wirtschaftstag 2015

1. Smart City

b. Autonomes Fahren

Figure 3: Market size and potential of the connected car trend (2015-2020), per market segment.



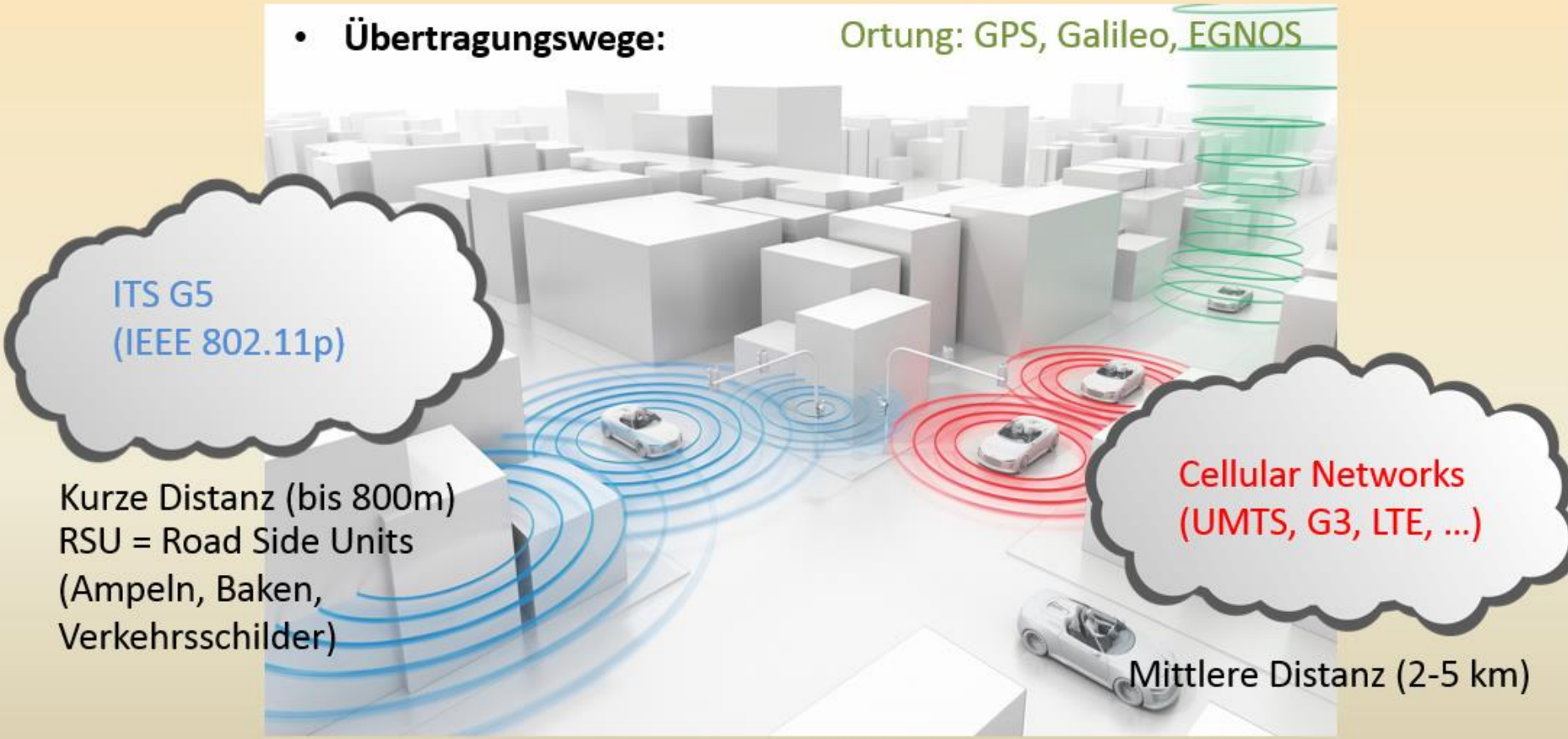
Source: Strategy& (2014). Racing ahead – The Connected C@r 2014 study

Marktvolumen steigt bis 2020 um ca. 82 Milliarden €

Quelle: European Commision , Business Innovation Observatory, Internet of Things, Connected Cars, Case Study 43

1. Smart City

b. Autonomes Fahren

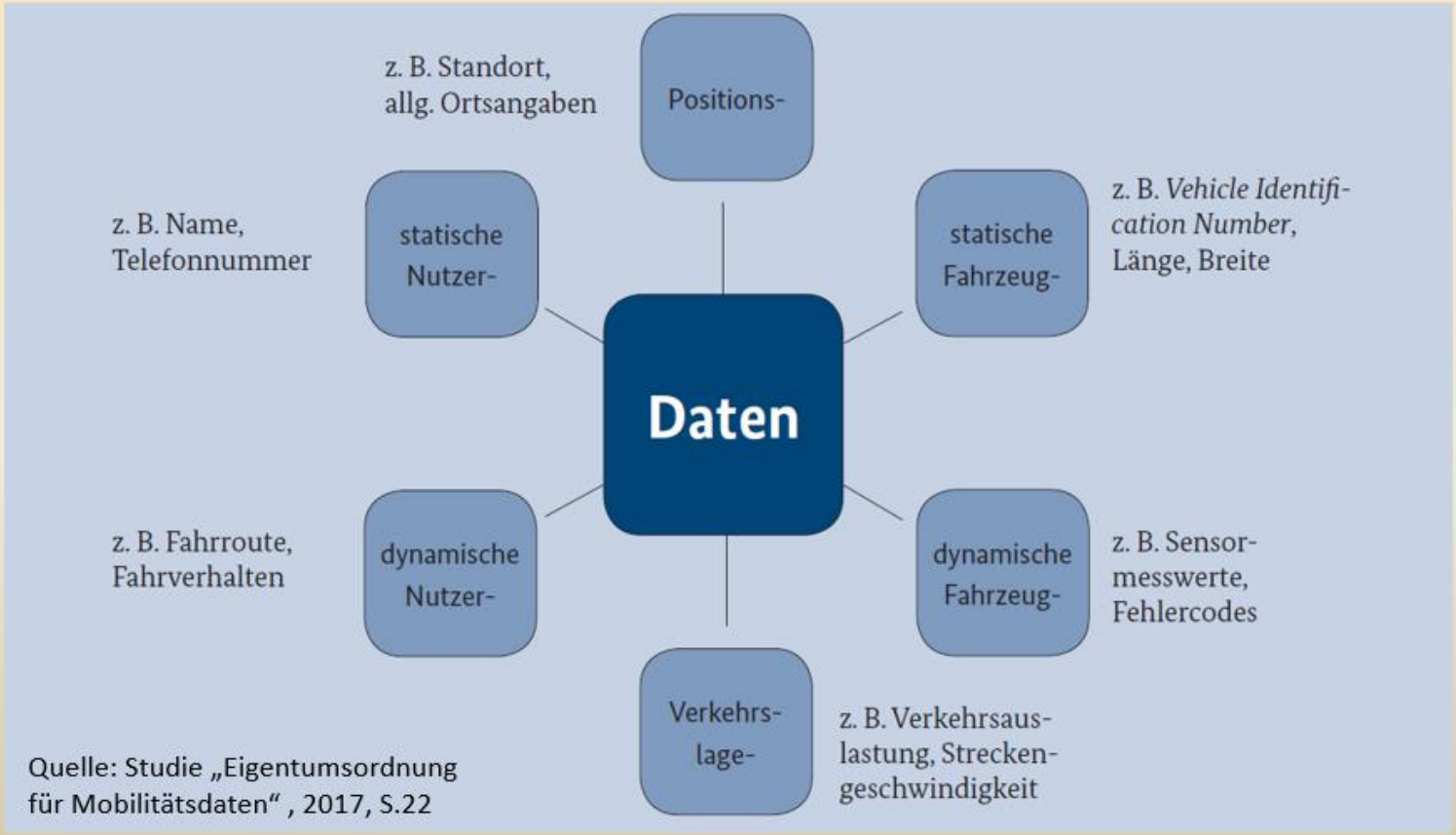


Quelle: Audi AG

1. Smart City

b. Autonomes Fahren

Welche Daten fallen im Auto an?



Quelle: Studie „Eigentumsordnung für Mobilitätsdaten“ , 2017, S.22

1. Smart City

b. Autonomes Fahren

BMW sagt gegen Fahrer aus:

- Urteil vom 14. April 2016 beim LG Köln (117 KLs 19/15)
  - Verurteilter wegen fahrlässiger Tötung eines Radfahrers verurteilt
  - Im BMW war ein CMS Modul zur Abrechnung wegen Car-Sharing verbaut
  - Daraus war Bewegungsprofil ableitbar ➔ BMW konnte auch die Hinterradgeschwindigkeit zum Tatzeitpunkt ermitteln (77 km/h)
  - ➔ die Beweislast genügte zur Verurteilung

➔ Datenschutzproblem: Anwender haben keine Kenntnis, welche Daten vom Automobil gespeichert werden

1. Smart City

b. Autonomes Fahren

Welche Sensoren gibt es? Was ist (u.a.) deren Funktion?

Sensor	Funktion	Zusatzfunktion ☺
Gurtschlosssensor	Scharfschalten Airbag	Insassen zählen
Sitzeinstellungen	Ergonomie	Fahrerwechsel
Blinker	Sicherheit	Fahrstil
GPS Position	Navigation	Fahrzeugtracking
Stromverbrauch	Defekte Birne	Nutzerprofile (genutzte Geräte)
Regensensor	Scheibenwischer	Wetterbedingungen
Radio	Radio hören	Profilbildung (Lieblingssender, -sendungen)
Klimaanlage	Heizen / Kühlen	Profilbildung
Kamera	Müdigkeitserkennung	z.B. Alter, Geschlecht, Identität, Laune…

Problem: Daten sind personenbezogen

1. Smart City

b. Autonomes Fahren

Gesellschaftliche Auswirkungen bei Nicht-Beachtung

- Belohnungssysteme könnten gewünschtes Verhalten honorieren und damit die gesellschaftliche Entwicklung beeinflussen
  - Bsp.: Telematik-Versicherungen motivieren zum „**Normfahrer**“
- Sanktionssysteme könnten unerwünschtes Verhalten unterbinden und dadurch die Gesellschaft beeinflussen
  - **StVO-Verstöße**, die durch „Road-Side-Units“ **automatisch registriert** werden
- Wird eine Telematik-Versicherung aus wirtschaftlichem Zwang heraus abgeschlossen, kann die „Freiwilligkeit“ der Einwilligung entfallen

➔ Soziale Implikation: finanziell schwächer Gestellte müssen mit ihren Daten zahlen

1. Smart City

b. Autonomes Fahren

Nicht nur mit dem neuen Telematik-Versicherungstarif „Pay **how** you drive“ sind Profilbildungen möglich, die nicht nur zur Bestimmung des Versicherungstarifs dienen. Aus den Daten über Fahrweise, Gesetzestreue, Lebensweise, Freizeit- und Konsumverhalten, Berufstätigkeit und Arztbesuche lassen sich detaillierte Persönlichkeitsbilder generieren. Diese nehmen an Deutlichkeit zu, wenn sie etwa mit Gesundheitsdaten (vom Fitness-Tracker) oder weiteren Daten, etwa aus den sogenannten Sozialen Netzwerken, angereichert werden.

1. Smart City

c. Vorgaben der DS-GVO

1.1. Thüringer Verfassung

Artikel 6

(2) Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen.

(3) Diese Rechte dürfen nur auf Grund eines Gesetzes eingeschränkt werden. Den Belangen historischer Forschung und geschichtlicher Aufarbeitung ist angemessen Rechnung zu tragen.

1. BVerfGE 65,1 – Volkszählungsurteil (15. Dezember 1983) = wichtigstes Urteil für den Datenschutz in Deutschland

- BVerfG hat eine Ausprägung des Persönlichkeitsrechts neu definiert: Aus dem Grundrecht der Menschenwürde (Art. 1 Abs. 1 GG) und dem Grundrecht auf allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) hat BVerfG ein Recht auf informationelle Selbstbestimmung herausgebildet.

Auszug aus dem Urteil:

„Mit dem Recht auf informationelle Selbstbestimmung wäre […] eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst." (…)

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

„…, insoweit gibt es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr."

1. Smart City

c. Vorgaben der DS-GVO

2.2. DS-GVO

Personenbezogene Daten

b) Legaldefinition in Art. 4 Nr. 1 DS-GVO:

1. „Personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Erwägungsgrund 26
Keine Anwendung auf anonymisierte Daten*

[1]Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. [2]Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. [3]Um festzustellen, ob eine natürliche Person **identifizierbar** ist, sollten alle **Mittel** berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen **wahrscheinlich genutzt werden**, um die natürliche Person **direkt** oder **indirekt** zu identifizieren, wie beispielsweise das Aussondern. [4]Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die **Kosten** der Identifizierung und der dafür erforderliche **Zeitaufwand**, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. [5]Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. [6]Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

* Dieser Titel ist eine inoffizielle Beschreibung des Erwägungsgrundes.

Personenbezogene Daten

a) Legaldefinition in Art. 4 Nr. 1 DS-GVO:

- Natürliche Person (= betroffene Person):
  - Nicht: juristische Personen, es sei denn, Daten zur juristischen Per-son machen die natürliche Person identifizierbar
  - Nicht: Verstorbene (EG 27), es sei denn Daten zum Verstorbenen lassen Schlüsse auf Daten von natürlichen Personen zu (z. B. durch Schlüsse aus dem veröffentlichten Gencode eines Verstorbenen auf den (defekten) Gencode seines Nachfahren)
  - Nicht: anonyme Daten ➔ personenbezogene Daten wurden in einer Weise anonymisiert, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (EG 26)

Zum Beispiel reine Sach- oder Prozessdaten:

Datenflüsse im IoT (Internet of Things) oder in/ zwischen (selbst)fahrender Autos oder Maschinen.

Aber: Weisen diese Daten Personenbezug auf (durch Fahrzeug-ID oder Smart-Home-ID) unterfallen personenbezogene Daten der DS-GVO.

Personenbezogene Daten

a) Legaldefinition in Art. 4 Nr. 1 DS-GVO:

- Nicht: anonymisierte Daten:.
- Anonymisierung etwa durch nicht reanonymisierbare Verschlüsselung (kritisch), Löschung, Aggregation von personenbezogenen Daten.
- Identifizierte Person: Identität ergibt sich unmittelbar aus der Information
  - Name, Steuer-ID, Iris-Scan, Fingerabdruck, biometrische Merkmale (Video: Gesicht, Gang), Kontext (Judas-Kuss); Übergang zur identifizierbaren Person fließend.
- Identifizierbare Person
  - Art. 4 Nr. 1 DS-GVO:

    Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Personenbezogene Daten

- Ein Datum (Puzzle-Teil) genügt nicht, um eine Person identifizieren zu können. Es besteht jedoch die legale Möglichkeit, dass auch unter Einbeziehung Dritter weiter Daten (Puzzle-Teilchen) verknüpft werden können, sodass die natürliche Person identifizierbar ist (Puzzle-Bild). Dann ist jedes Datum (Puzzle-Teil) personenbezogen.
- Pseudonymisierung

  Art. 4 Nr. 5 DS-GVO
- (5) „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
  - Pseudonymisierung etwa durch: Verschlüsselung, Datentrennung, ID-Management, Treuhändermodelle

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

1. Personenbezogene Daten müssen

   a) auf **rechtmäßige Weise**, nach **Treu und Glauben** und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

   b) für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („**Zweckbindung**“);

   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);

   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);

   e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);

   f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).

Art. 6 DS-GVO Rechtmäßigkeit der Verarbeitung

(1) [1]Die Verarbeitung ist nur rechtmäßig, wenn **mindestens eine der nachstehenden Bedingungen** erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines **Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung **öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten **erforderlich**, **sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein **Kind** handelt.

*2 Unterabsatz 1: Buchstabe f **gilt nicht für die von Behörden** in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.*

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 **Buchstaben c und e** beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) [1]Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 **Buchstaben c und e** wird festgelegt durch

Unionsrecht oder

das **Recht der Mitgliedstaaten**, dem der Verantwortliche unterliegt.

[2]Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. [3]Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. [4]Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

Rechtmäßigkeit der Datenverarbeitung

Einwilligung: Definition Art. 4 Abs. 11 DS-GVO

(11) „Einwilligung“ der betroffenen Person: jede **freiwillig** für den **bestimmten Fall**, in **informierter Weise** und **unmissverständlich** abgegebene Willensbekundung in Form einer **Erklärung** oder einer **sonstigen eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Freiwilligkeit:

Freiwilligkeit setzt eine selbstbestimmte Entscheidung voraus, ob der Betroffene einwilligen will oder nicht. Damit geht regelmäßig die **Wahl des Betroffenen zwischen mindestens zwei Möglichkeiten einher** – auch im Fall der Nicht-Einwilligung muss dem Betroffenen eine Alternative offenstehen, die ihn nicht derart unter Druck setzt, dass er unfreiwillig – doch einwilligt (vgl. EG 42 a. E.).

Keine Freiwilligkeit bei:

Drohung, monopolartiger Position des Verantwortlichen, wirtschaftlicher oder sozialer Schwäche des Betroffenen, Verleitung des Betroffenen zur Einwilligung durch übermäßige Anreize.

Freiwilligkeit bei: Sozialen Netzwerken, da Alternativen zur Verfügung stehen (WhatsApper sicherlich a. A., da Gefahr der Vereinsamung => unfreiwillige Einwilligung ☺).

Art. 7 DSGVO Bedingungen für die Einwilligung

1. Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

2. [1]Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in **verständlicher** und **leicht zugänglicher Form** in einer **klaren und einfachen Sprache** so erfolgen, dass es von den anderen Sachverhalten **klar zu unterscheiden** ist. [2]Teile der Erklärung sind dann **nicht verbindlich**, wenn sie einen Verstoß gegen diese Verordnung darstellen.

3. [1]Die betroffene Person hat das Recht, ihre Einwilligung **jederzeit zu widerrufen**. [2]Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. [3]Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. [4]Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

4. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Art. 32 DSGVO Sicherheit der Verarbeitung

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

   a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
   b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
   c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;
   d) ein **Verfahren zur regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen **zur Gewährleistung der Sicherheit der Verarbeitung**.

a.a. KI

Art. 22 DSGVO Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

1. Die betroffene Person hat das Recht, **nicht einer ausschließlich auf einer automatisierten Verarbeitung** – einschließlich **Profiling – beruhenden Entscheidung unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

2. Absatz 1 gilt nicht, wenn die Entscheidung
   a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
   b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
   c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

3. In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

4. Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

a.a. KI

Art. 13 DSGVO Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

1. Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
   a) den Namen und **die Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines Vertreters;
   b) gegebenenfalls die **Kontaktdaten des Datenschutzbeauftragten**;
   c) die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
   d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
   e) gegebenenfalls die **Empfänger** oder Kategorien von Empfängern der personenbezogenen Daten und
   f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

a.a. KI

Art. 14 DSGVO Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

1. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:
   a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
   b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
   c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
   d) die Kategorien personenbezogener Daten, die verarbeitet werden;
   e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
   f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.
2. **Zusätzlich** zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:
   a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
   b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
   c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
   d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
   e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
   f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
   g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

a.a. KI

Art. 15 DSGVO Auskunftsrecht der betroffenen Person

1. **Die betroffene Person hat das Recht**, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:
   a) die Verarbeitungszwecke;
   b) die Kategorien personenbezogener Daten, die verarbeitet werden;
   c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
   d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
   e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
   f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
   g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
   h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
2. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.
3. [1]Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. [2]Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. [3]Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.
4. Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

a.a. KI

Art. 17 DSGVO Recht auf Löschung ("Recht auf Vergessenwerden")

1. **Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden**, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:
   a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
   b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
   c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
   d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
   e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
   f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.
2. Hat der Verantwortliche die personenbezogenen Daten **öffentlich gemacht** und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten **angemessene Maßnahmen**, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, **darüber zu informieren**, dass eine betroffene Person von ihnen die **Löschung** aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten **verlangt hat**.

a.a. KI

Art. 21 DSGVO Widerspruchsrecht

1. [1]Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. [2]Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.
3. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.
4. Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.
5. Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.
6. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

a.a. KI

Art. 24 DSGVO Verantwortung des für die Verarbeitung Verantwortlichen

1. [1]Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung **gemäß dieser Verordnung** erfolgt. [2]Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
2. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.
3. Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

a.a. KI

Art. 35 DSGVO Datenschutz-Folgenabschätzung

1. [1]Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich **ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. [2]Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Art. 36 Vorherige Konsultation

1. Der **Verantwortliche konsultiert** vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche **keine Maßnahmen zur Eindämmung des Risikos trifft**.

b.b. Autonomes Fahren

Grundbegriffe und wichtige Regelungen der DSGVO:

Definition personenbezogene Daten DSGVO Art. 4 :

1. **"personenbezogene Daten"** alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person (im Folgenden "betroffene Person") beziehen

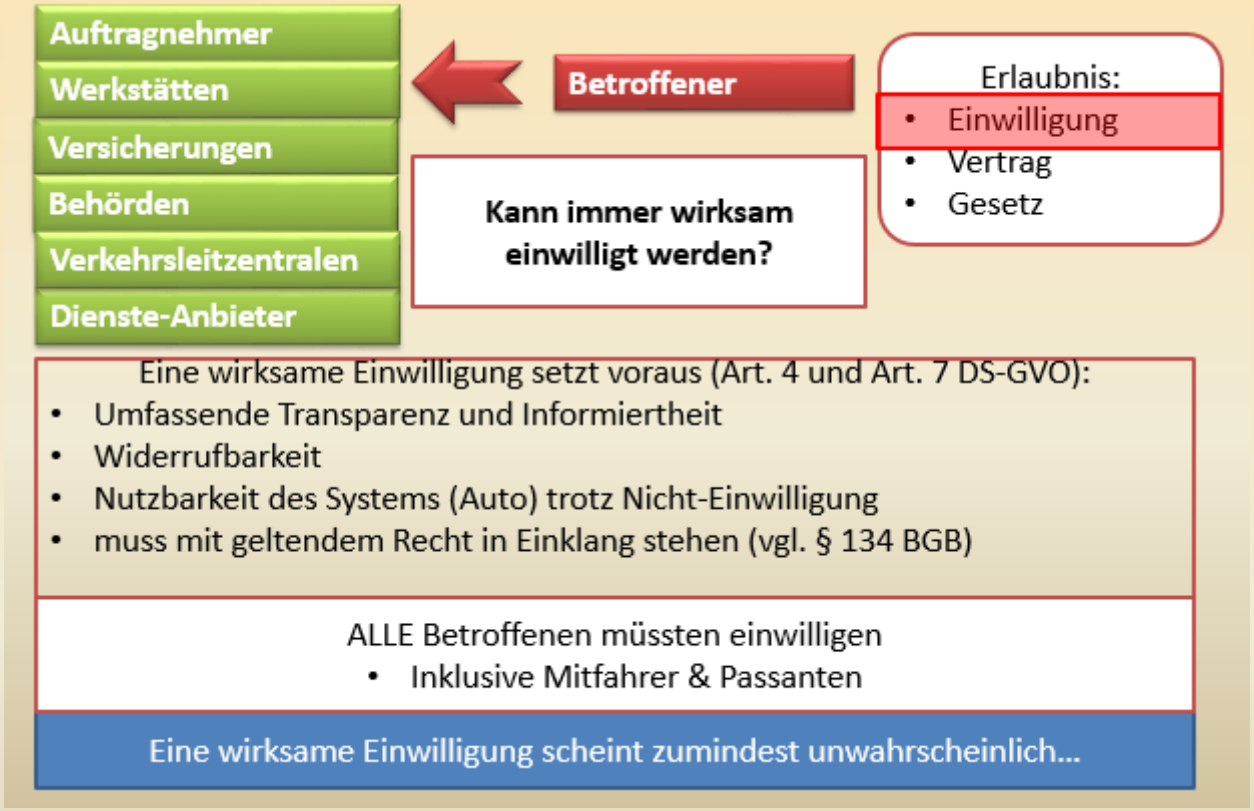
= ist eine Person, wenn das Datum selbst einen unmittelbaren Rückschluss auf die Identität des Betroffenen zulässt, z.B.:

- Name
- Telefonnummer

= ist eine Person, wenn sie zwar durch das Datum selbst noch nicht allein bzw. eindeutig identifizierbar ist, aber mit Hilfe weiterer Informationen (Zusatzhinweise) der Bezug herstellbar ist, z.B.:

- **Fahrzeugidentifikationsnummer (insbesondere beim eCall)**
- Smartphone-ID, Lokalisation

b.b. Autonomes Fahren



b.b. Autonomes Fahren

- Nutzer muss erkennen, welche Daten **ohne Einwilligung** verarbeitet werden (Gesetze)
- Nutzer soll im Fahrzeug alle personenbezogenen Daten(-kategorien) einsehen können
- Verarbeitung der Daten nur im Notwendigen umfang (auch bei Car-to-Car)
- keine Speicherung im reinen Fahrbetrieb (nicht-automatisch) notwendig, sonst verschlüsseln – auch beim Datentransport
- Ist zum Verarbeitungszweck kein Personenbezug erforderlich → anonymisieren
- Umgebungsaufnahmen sind nach der Verarbeitung zu löschen
- Zugriff auf Datenkategorien muss **selektiv** gewährbar bzw. sperrbar sein
- Privacy-by-default Einstellung in jedem Fahrzeug
- Fahr- und Komfortfunktionen müssen – wenn technisch möglich – ohne externe Datenverbindung möglich sein
- Löschen von personenbezogenen Daten muss durch den Fahrzeug**nutzer** möglich sein
- unbefugter Zugriff muss verhindert werden (inkl. Schutz vor Cyberangriffen)

Quelle: Forderungen der BfDI vom 1. Juni 2017

b.b. Autonomes Fahren

39. Internationale Konferenz der Datenschutzbeauftragten
Hong Kong, 25.- 29. September 2017
Entschließung zum Datenschutz beim automatisierten und vernetzten Fahren

Übersetzung sinngemäß:
Hersteller, Behörden und Anbieter fahrzeugbezogener Dienste sind aufgefordert:

1. Auskunft zu geben, welche Daten gesammelt werden,
2. Anonymisierungsmaßnahmen zu nutzen,
3. Datensparsamkeit zu beachten und Daten nach gewisser Zeit zu löschen,
4. Technische Mittel bereitzustellen, um persönliche Daten beim Verkauf des Autos zu löschen,
5. Einfache Datenschutzeinstellungen für den Benutzer bereitzustellen,
6. Technische Mittel bereitzustellen, um Datensammlungen zu unterbinden,

b.b. Autonomes Fahren

b.b. Autonomes Fahren

„Eigentumsordnung“ für Mobilitätsdaten?

- **Gedanken de lege ferenda**:
  Kopplung von Investition und der Verfügungsgewalt an Daten:
  - Derjenige, als dessen **Verdienst die Generierung von Daten** anzusehen ist, erhält die **Verfügungsgewalt** an diesen Daten und hat Anspruch auf Datenschutz; **er** ist der **„Dateneigentümer“;**
  - die Investitionstätigkeit wird im Vorfeld der Datenerstellung durch den **Eigentümer des Kfz mittels Kaufpreises abgegolten**, **wenn** der Eigentümer des Kfz die **Datenverfügungsbefugnis erlangen will**.

- Übertragung der Gedanken auf **Gesundheitsdaten**

c.c. Freifunkprojekt

Das Freifunknetz Gera ist eine Ansammlung von Richtfunkstrecken, die einzelne WLAN-Hotspots zu einem stadtweiten Netzwerk zusammenschließt. Das Netz wird durch Server unterstützt, auf denen interne Dienste laufen (z.B. Adressvergabe, Routing usw.) und welche dieses Netz mit dem Internet verbinden. Personenbezogene Daten fallen an – beim Besuch einer Website, bei der Vergabe von IP Adressen – theoretisch auch sehr grobe Bewegungsmuster, wann welcher Nutzer an welchem Netzknoten angemeldet ist. Wie sicher das Netz ist, wie Nutzer gegeneinander abgeschirmt sind, ob schädliche Inhalte geblockt werden und Sicherheitsmaßnahmen gegen Attacken der IT-Infrastruktur vorhanden sind, ist fraglich. Wir sollten reden.

Inhalt

1. Smart City

2. Smart Citizens

3. Smart Privacy

a. Transparenz

Akzeptanz durch **Transparenz**, Information, Einbindung, Tools: Bürgerinnen und Bürger nicht als Objekte der Digitalisierung, sondern als deren aktive Mitgestalter sehen.

Das Thüringen Transparenzgesetz (ThürTG), tritt am 01.01.2020 in Kraft, löst das bisherige Thüringer Informationsfreiheitsgesetz (ThürIFG) ab, das den Zugang zu amtlichen Informationen regelt.

Das Thüringer Transparenzgesetz stellt einen Paradigmenwechsel dar, da von **öffentlichen Stellen Informationen von allgemeinen Interesse** für die Öffentlichkeit, die das Ergebnis oder den Abschluss eines Verwaltungsvorgangs dokumentieren und nach Inkrafttreten dieses Gesetzes entstanden, bestellt oder beschafft worden sind, **öffentlich zugänglich gemacht werden** sollen - § 5 Abs. 1 ThürTG. **Zudem müssen öffentlichen Stellen** des Landes und die Landesregierung bestimmte amtliche Informationen (der sog. Veröffentlichungskatalog § 6 Abs. 3 ThürTG) **von sich aus im Transparenzportal veröffentlichen**, z.B. Gutachten und Studien, soweit sie von den öffentlichen Stellen in Auftrag gegeben wurden und in die Entscheidung bereits eingeflossen sind; Kabinettbeschlüsse; Übersichten über Zuwendungen ab einer Fördersumme von 1.000 Euro. Die Nutzung des Transparenzportals ist für Bürger kostenlos.

Neu ist, dass der TLfDI nun auch Ombudsstelle für das Thüringer Umweltinformationsgesetz (ThürUIG) ist. Bürger können sich nun auch bei Umweltinformationen an den TLfDI wenden.

Kommunen sind nicht verpflichtet Informationen des Veröffentlichungskatalogs (§ 6 Abs. 3 ThürTG) im Transparenzportal zugänglich zu machen.

Kommunen sollen lediglich Informationen nach § 5 Abs. 1 ThürTG veröffentlichen. Die Regelung stellt keine Verpflichtung dar. Bürger interessiert jedoch besonders Informationen die einen lokalen Bezug haben z.B. Bauprojekte, Förderungen usw.

Im Rahmen eines Modellprojekts soll geklärt werden, inwieweit Kommunen im Transparenz-portal Informationen zugänglich machen müssen. Das Zuständige Ministerium kann Näheres durch Verwaltungsvorschrift regeln.

§ 16 Abs. 2 ThürTG

„Das für die Informationsfreiheit zuständige Ministerium unterstützt die Kommunen bei der Teilnahme am Transparenzportal und bietet ein Modellprojekt zur Klärung von rechtlichen, organisatorischen und technischen Fragen aus spezifisch kommunaler Sicht an. Es kann Näheres, insbesondere zu Teilnehmern, Dauer, Vorgehens- und Verfahrensweise und Obliegenheiten, **durch Verwaltungsvorschrift** regeln."

Bereits heute veröffentlicht die Stadt Jena von sich aus Informationen proaktiv https://opendata.jena.de/. Dennoch soll ein Modellprojekt die proaktive Veröffentlichung klären.

Einen zeitlichen Rahmen für das Modellprojekt regelt das ThürTG nicht. In den Übergangsbestimmungen ist lediglich im § 23 Abs. 4 ThürTG geregelt: „Das für die Informationsfreiheit zuständige Ministerium unterrichtet den für die Informationsfreiheit zuständigen Ausschuss des Landtags jährlich zum Modellprojekt nach § 16 Abs. 2."

Der TLfDI bedauert, dass die Kommunen nicht von der Veröffentlichungspflicht erfasst sind.

b. Skills of the 21-Century

– Skills oft the Twenty-First-Century:

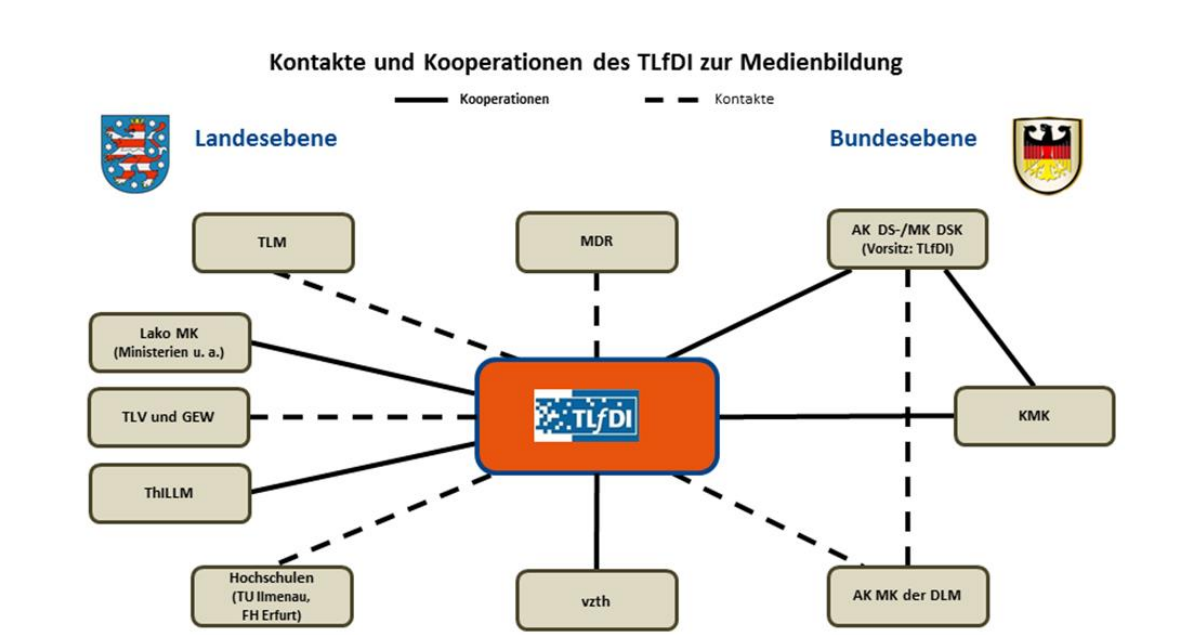
- Kritisches Denken.
- Kreativität.
- Zusammenarbeit.
- Kommunikation.
- Informationskompetenz.
- Medienkompetenz.
- Technologiekompetenz.
- Flexibilität.

Der TLfDI ist auch Bundesvorsitzender von zwei Arbeitskreisen:

AK Schulen und Bildungseinrichtungen

AK Datenschutz-/ Medienkompetenz der Datenschutzkonferenz

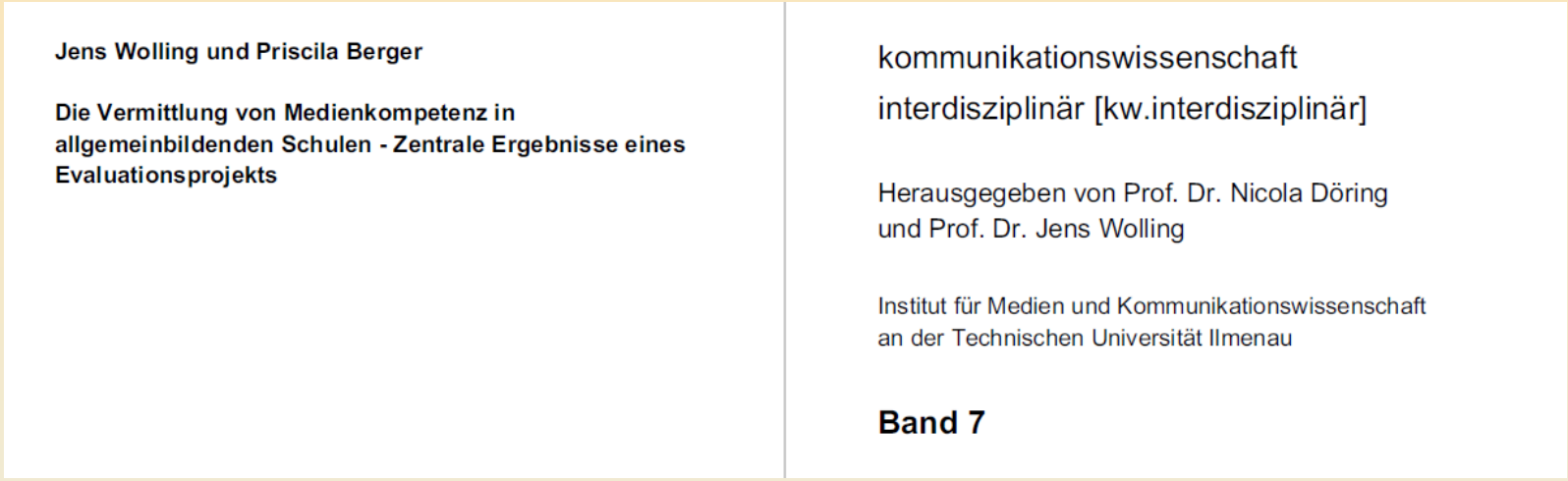
Daher dazu Folgendes:



Der TLfDI ist auch Bundesvorsitzender von zwei Arbeitskreisen:

AK Schulen und Bildungseinrichtungen
AK Datenschutz-/ Medienkompetenz der Datenschutzkonferenz

Im Weiteren:



In den letzten beiden Jahrzehnten hat sich das Medienumfeld, in dem Kinder und Jugendliche aufwachsen, grundlegend verändert. Diese Veränderungen konfrontieren nicht nur die Eltern, sondern auch die Schulen mit völlig neuen Herausforderungen bei der Vermittlung von Medienkompetenz. Ein pädagogischer Ansatz, um die Heranwachsenden auf diese neue Medienwelt vorzubereiten, besteht in der Integration medienbezogener Inhalte in den Fachunterricht. Im Rahmen der vorliegenden Untersuchung wurde die Umsetzung eines solchen integrativen Konzepts in Thüringen evaluiert. In einer aus verschiedenen qualitativen und quantitativen Teilstudien bestehenden Untersuchung wurde die Praxis der Medienkompetenzvermittlung und ihre Bestimmungsfaktoren analysiert. Kernstück der Untersuchung ist eine repräsentative Befragung von Lehrenden sowie von Schulleiterinnen und Schulleitern des ganzen Bundeslandes. Die Befunde verdeutlichen, welche Faktoren die erfolgreiche Umsetzung des Konzepts begünstigen und welche sich als hinderlich erweisen. Auf der Grundlage der erzielten Ergebnisse wurden Empfehlungen entwickelt, wie das integrative Konzept weiterentwickelt werden sollte und welche Maßnahmen notwendig sind, um die Rahmenbedingungen für eine erfolgreiche Vermittlung von Medienkompetenz zu verbessern.

17. Juli 2018

Quelle: https://www.db-thueringen.de/servlets/MCRFileNodeServlet/dbt_derivate_00041138/ilm1-2018100036.pdf

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Pressemitteilung

Kurs Medienkunde endlich wissenschaftlich evaluiert - ! Weichenstellungen in der (Hoch-)Schule notwendig !

Nun ist es raus (MDR): In Thüringer (Hoch-)Schulen knirscht es in Sachen Medienkompetenzentwicklung. Dass es da nicht so rund läuft wie auf dem Papier, war auch bisher schon der nachhaltige Eindruck des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Und er ließ der Sache keinesfalls ihren Lauf, denn in unserer datenzentrierten Welt gehört zu kompetentem Medienumgang auch der kompetente Umgang mit personenbezogenen Daten. Die (schüler)eigenen Daten stehen da ganz vorn! Der Nachdruck des TLfDI u. a. gegenüber den Verantwortlichen im TMBJS und beim „Runden Tisch Medienkompetenz“ hat dazu beigetragen, dass Medienkunde seit 2017 evaluiert wurde. Eine **mutige Entscheidung von Frau Staatssekretärin Ohler**! Auch die Beteiligung des TLfDI an diesem Evaluationsprozess war nichtselbstverständlich. Nun bleibt abzuwarten, wie die Weichen nach den aufrüttelnden Ergebnissen der TU Ilmenau gestellt werden. Wird der integrative Ansatz endlich durch ein **eigenes Unterrichtsfach** ergänzt? Wie gelingt es, hierfür genügend **Lehrkräfte aus-und fortzubilden**? Klar, dass der TLfDI auch hier am Ball bleibt und unterstützt. Die „Landeskooperation zur nachhaltigen Weiterentwicklung von Medienkompetenz“ bietet eine gute Plattform für Überlegungen des TLfDI gemeinsam mit Landesministerien, ThILLM, TLM und weiteren Partnern. Dr. Hasse: “Nun wissen wir: Es gibt viel zu tun -handeln wir also!“

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Häßlerstraße 8, 99096 Erfurt
www.tlfdi.de

Wo stehen wir? …

Medienbildung und Informatikunterricht sollen das notwendige Wissen vermitteln.

- **Soll:** KMK Beschluss von 2016*, u.a.
  - integrativer Ansatz zum Erreichen von digitaler Medienkompetenz (Kap. 1, S.11, Nr.1)
  - Schulen anforderungsgerecht ausstatten (Kap. 2.2.3)
  - es werden verbindliche Kompetenzbereiche in der Ausbildung benannt (Kap. 2.2.1)
    - u. a. Kompetenz 4.2 „Persönliche Daten und Privatsphäre schützen“
  - zum Erreichen der Kompetenzen:
    - müssen die Lehrpläne der Länder analysiert und ergänzt werden
    - muss die Lehrerausbildung im Bereich des Studiums, des Vorbereitungsdienstes und der Fortbildung angepasst werden

* vgl. Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“, Dez. 2016, neu gefasst 07.12.2017

Abhilfe?

(Erste) Unterstützungsangebote der Landesdatenschutzbehörden

- **Beispiel 1:**
  - Jugendportal www.youngdata.de

    - Federführung: LfDI Rheinland Pfalz
    - Thüringen: Videoüberwachung, Informationsfreiheit
  - Veröffentlichungen, u. a.
    - z. B. zu Sozialen Netzwerken, Orientierungshilfe Lernplattformen
    - In Arbeit: Orientierungshilfe Apps auf privaten Geräten der Lehrer
  - Vorbereitung von Entschließungen der DSK, z. B. Datenschutz als Bildungsaufgabe
- **Beispiel 2**: Initiativen einzelner Datenschutzbehörden, z. B.:
  - Mecklenburg-Vorpommern: Projekt „Medienscouts“
  - Rheinland-Pfalz: Workshops mit Studenten / Lehrern
  - Thüringen: Überarbeitung des Moduls „Datenschutz“ bei Klicksafe
  - Thüringen: Angebot des TLfDI an TMBJS: Mitwirkung bei Umsetzung der „Digitalstrategie Thüringer Schule“ (DiTS)

Abhilfe?

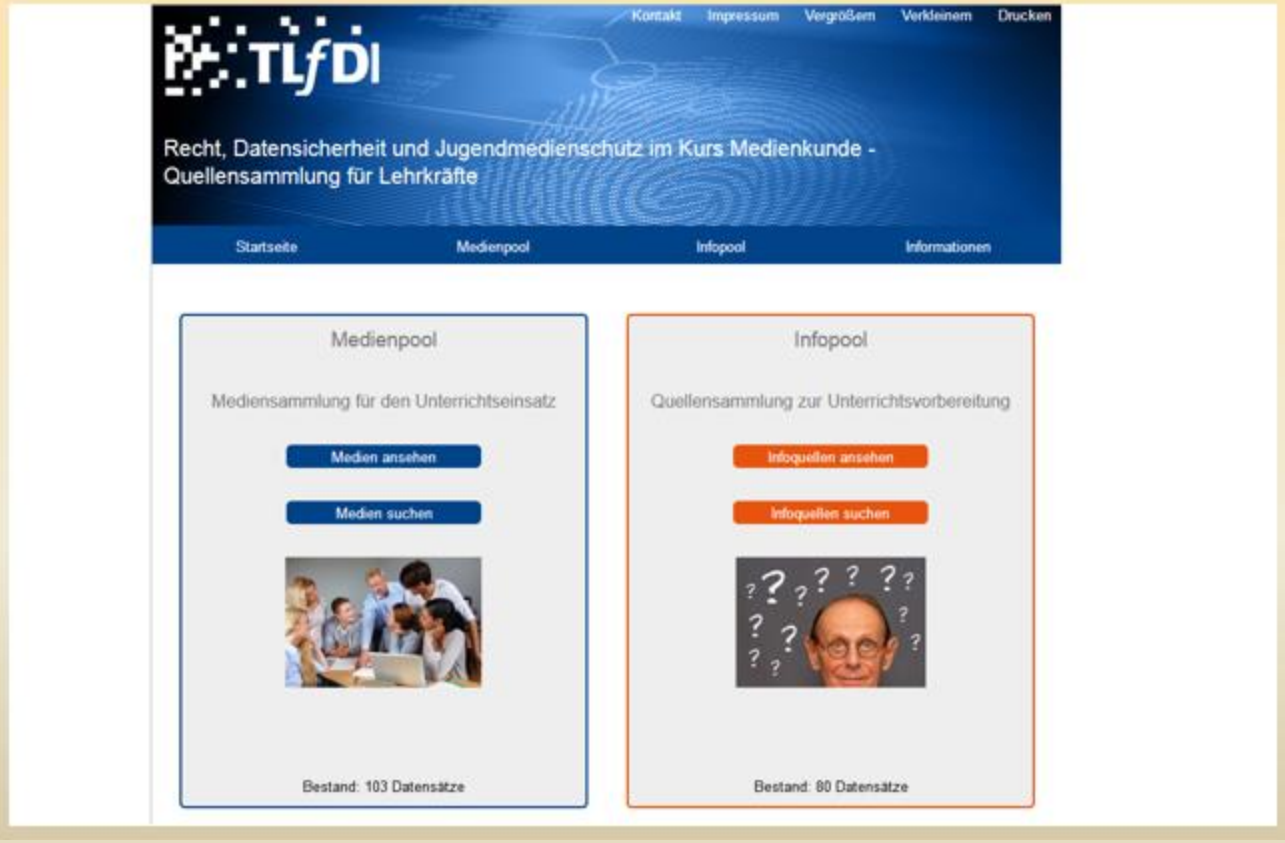
➢ **Beispiel 3: Mediendatenbank zu DS+DS-Themen**

- „Medienpool“ (Linksammlung) für den direkten Einsatz im Unterricht
- „Infopool“ für Lehrer zur individuellen Vorbereitung/Vertiefung
- Zielgerichtet recherchierbar

➢ **Beispiel 4: Unterrichtsmaterial „Videoüberwachung in Ordnung oder nicht?“**

- Zur integrativen Umsetzung des Kurses Medienkunde im Fach Sozialkunde am Gymnasium, Klassenstufen 9 – medienspezifische Unterrichtsstunden)
- Unterrichtskonzept u. Materialpaket, u. a. mit Video, Handreichung, Gesetzestexten, Powerpoint für Lehrer, Arbeitsvorlagen für Schüler
- Video zum Thema Einsatz von Drohnen (Copyright MDR 360 Grad)

Überarbeitung auf Basis DSGVO/ThürDSG geplant!


Kontakt
Impressum
Vergrößern
Verkleinern
Drucken
TLfDI
Recht, Datensicherheit und Jugendmedienschutz im Kurs Medienkunde - Quellensammlung für Lehrkräfte
Startseite
Medienpool
Infopool
Informationen
Medienpool
Mediensammlung für den Unterrichtseinsatz
Medien ansehen
Medien suchen
Bestand: 103 Datensätze
Infopool
Quellensammlung zur Unterrichtsvorbereitung
Infoquellen ansehen
Infoquellen suchen
Bestand: 80 Datensätze

- Lehrer**fort**bildungen
  - … in Kooperation mit dem ThILLM oder eigenständig, z. B.:
    E-Mail-Verschlüsselung mit PGP,
    Datenschutzrecht in schulischem Kontext,
    Smartphone-Einstellungen,
    Browsereinstellungen (Firefox),
    Datenträgerverschlüsselung mit Veracrypt

- Lehrer**aus**bildung
  - Inhaltliche Konzeption des TLfDI zu Themen Datenschutz und Datensicherheit für **Zweite Phase der Lehrerbildung**

- Betreuung von Seminarfacharbeiten

Inhalt

1. Smart City

2. Smart Citizens

3. Smart Privacy

3. Smart Privacy

Der TLfDI ist oberste Datenschutzaufsichtsbehörde:

a. Kooperation statt Bußgeld

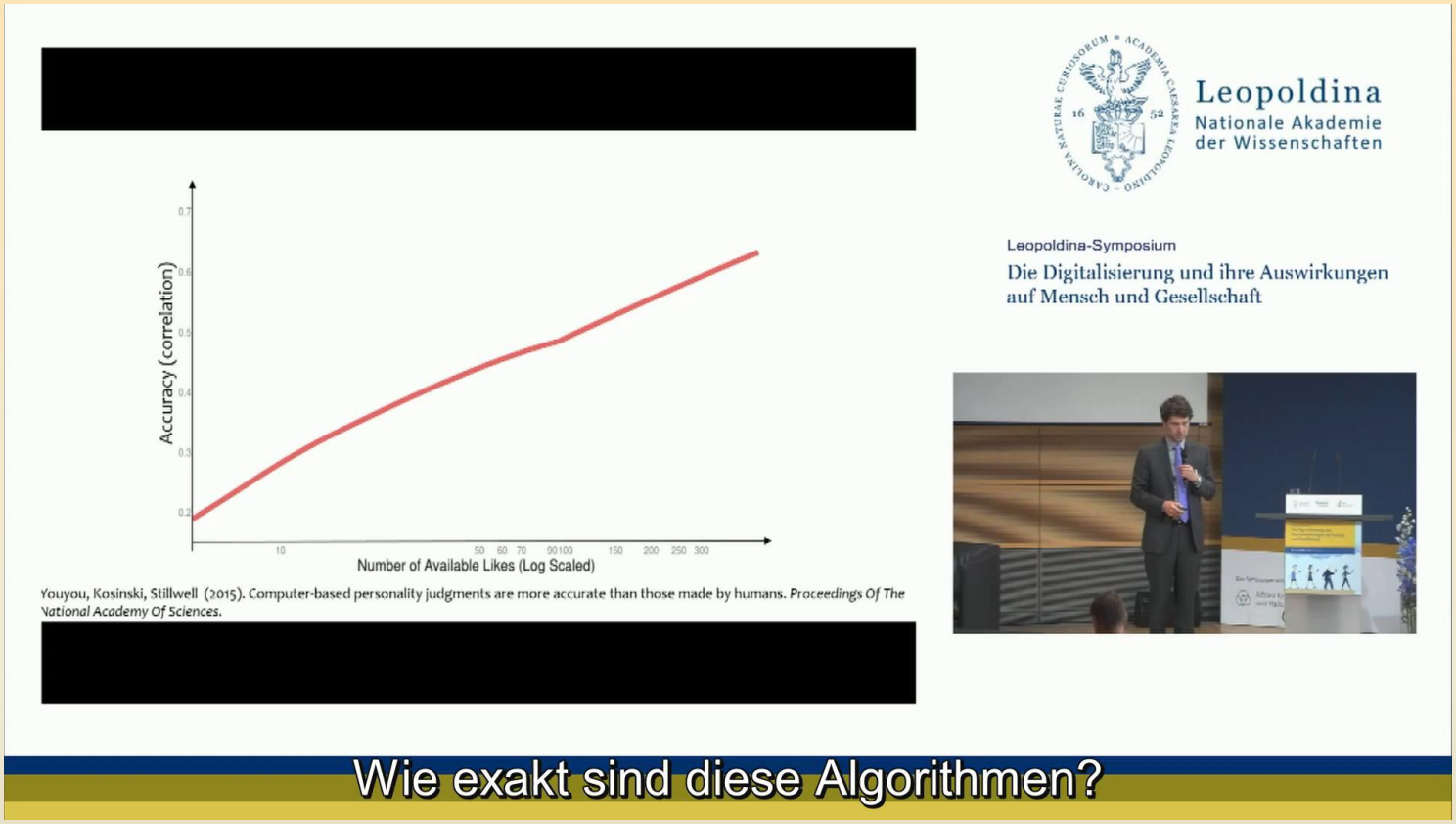
b. Datensicherheit

– Zertifizierung (Art. 42, 43 DS-GVO)

• Zertifizierung durch Aufsichtsbehörde und akkreditierte Stelle mit Zertifizierungsverfahren, Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass die DS-GVO eingehalten wird.

• Zertifiziert werden Verarbeitungsvorgänge, nicht Stellen.

Kosinski: Charakterschätzung über Facebook-Likes



Michal Kosinski - Schafft Digitalisierung eine eigene Dynamik in der Meinungsbildung?

Smart City – Smart Citizens – Smart Privacy