Karlsruher Institut für Technologie

Zentrum für Angewandte Rechtswissenschaft

Einführung und Grundlagen

Dr. Christoph Werner

Vorlesung Datenschutzrecht
WS 2025/2026, UE 1/15

30.10.2025

Über mich

Seit 2019 als wiss. Mitarbeiter am ZAR
derzeit Postdoc im Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL)

Forschungsschwerpunkte:

- Datenschutzrecht,
- Datensicherheits- und IT-Sicherheitsrecht

Eigene Publikationen: https://it-security.law/veroeffentlichungen/

Bei Interesse werden auch Bachelor-/Masterarbeiten im Bereich der o.g. Forschungsschwerpunkte angeboten.

You‘ll never walk alone

Dr. Uwe K. Schneider

https://www.vogel-partner.eu/team/dr-uwe-k-schneider/
https://twitter.com/MedITRecht

Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Medizinrecht

Studium in Tübingen
Referendariat in Karlsruhe und Brüssel

Promotion an der Universität Tübingen zu
„Einrichtungsübergreifenden elektronischen Patientenakten – Zwischen Datenschutz und Gesundheitsschutz“

seit 2001 Betrieblicher Datenschutzbeauftragter
seit 2007 Rechtsanwalt

seit 2011 Partner bei Vogel & Partner in Karlsruhe

Handelsblatt
Deutschlands BESTE Anwälte
2024
Dr. Uwe K. Schneider
IT-Recht
13.06.2024
Best Lawyers

2 Dr. Uwe K. Schneider vogel—partner RECHTSANWÄLTE ZAR Zentrum für Angewandte Rechtswissenschaft www.kit.edu

Und Ihr?

Die Vorlesung ist primär für B.Sc.-Studierende folgender Fächer gedacht:

- **Wirtschaftsinformatik (i.d.R. im 5. Semester)**
  - Vertiefungsfach Recht / Geistes Eigentum und Datenschutz
  - Vorerfahrung mit Recht
  - Einführung in das Privatrecht
    - Wirtschaftsprivatrecht
    - Verfassungs- und Verwaltungsrecht
- **Informatik** (Ergänzungsfach, optional)
- **Digital Economics** (Pflichtfach, 1. Semester, keine Vorkenntnisse durch andere Rechtsvorlesungen)
- Altfälle Informationswirtschaft?

Alle Studierenden dieser Fächer sollen parallel die Vorlesung Geistiges Eigentum hören und die entsprechende Gesamtklausur/Modulprüfung „Geistes Eigentum und Datenschutz“ mitschreiben.

Geplante Themen im Überblick

Was schützt der Datenschutz?

Verfassungs- & unionsrechtliche Hintergründe des Datenschutzes

Was sind personenbezogene Daten?

Grundzüge der Datenschutz-Grundverordnung (DSGVO)
(Datenschutzgrundsätze, Rechtmäßigkeitstatbestände, Betroffenenrechte, Verantwortlichkeit, Datensicherheit, Datenschutz-Organisation & Aufsichtsbehörden, Öffnungsklauseln und verwandte Regelungen (u.a. KI-VO).

Gesetzestexte / Rechtsquellen

Sie benötigen (für Vorlesung und Klausur in der aktuellen Fassung):

- EU: Datenschutz-Grundverordnung (DSGVO, inkl. Erwägungsgründe)
- DE: Bundesdatenschutzgesetz (BDSG)
- DE: Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

Sie können dies im Internet abrufen (viele Quellen, gute Web-Ansicht: https://dsgvo-gesetz.de/) und für die Klausur aus folgenden Quellen ausdrucken:

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 (DSGVO)
- https://www.gesetze-im-internet.de/bdsg_2018/ (BDSG)
- https://www.gesetze-im-internet.de/ttdsg/BJNR198210021.html (TDDDG)

Oder ein käufliches Papierexemplar mitbringen (nächste Folie):

Textsammlung Datenschutzrecht

Datenschutzrecht und Datenwirtschaftsrecht: DatSchR

16. Auflage 2025
24,90€

„Bearbeitung“ der Gesetzestexte

Es gelten neben der Studien- und Prüfungsordnung die Klausurrichtlinien des Zentrums für angewandte Rechtswissenschaft (ZAR) in der jeweils aktuellen Fassung: **https://www.zar.kit.edu/pruefungen.php**
(Auszug hier mit Stand vom 15.10.2025)

Notierungen in Gesetzestexten: Unzulässig ist alles, was nicht ausdrücklich erlaubt ist!

Erlaubt sind:

- **Unterstreichungen**
- **farbliche** Hervorhebungen
- **Reiter (Lesezeichen):** Die Reiter müssen unbeschriftet sein! Keine Gesetzeszahlen, keine Wörter, keine Abkürzungen, nur der blanke Reiter!
- **Verweise** nur in Form von Gesetzesabkürzungen, Paragraphen und Artikeln (zulässig sind z.B.: § 433 I 2 BGB, §§ 44a ff. UrhG, Art. 53 GG).

  Die Verweise müssen am Rande einer Norm stehen und einen konkreten Bezug zu ihr haben. Verweise, die zusammenhanglos und ohne konkreten Bezug unter- oder oberhalb der bedruckten Bereiche einer Seite stehen, sind nicht zulässig.

  An jeder Norm dürfen höchstens 2 Verweise pro Absatz und Aufzählungspunkt stehen.

Literaturhinweise (optional)

- Kühling/Klar/Sackmann: Datenschutzrecht, 6. Auflage 2025. Ausleihbar in Bibliothek.
- Specht-Riemenschneider/Riemenschneider/Schneider: Internetrecht - Abschnitt „Datenschutzrecht“, S. 185 ff. Abrufbar via SpringerLink (KIT-VPN).
- Albrecht/Jotzo: Das neue Datenschutzrecht der EU. Abrufbar via beck-online (KIT-VPN).
- Simitis/Hornung/Spiecker gen. Döhmann: Datenschutzrecht, Kommentar, Abrufbar via beck-online (KIT-VPN).
- Petrlic/Sorge: Datenschutzrecht - Einführung in den technischen Datenschutz, Datenschutzrecht und Kryptographie. Abrufbar via SpringerLink (KIT-VPN).
- Themenspezifische Fachaufsätze (z.B. aus Zeitschrift für Datenschutz, MultiMediaRecht, usw.) werden im Rahmen der Vorlesung benannt.

Solche (Sekundär-)Literatur ist optional. Für die Klausur genügt die Teilnahme an der Vorlesung, die Wiederholung der Folien (ILIAS) und die Gesetzestexte.

ILIAS-Kurs und Kontaktdaten

- https://ilias.studium.kit.edu/goto.php/crs/2781190 (2424018 – Datenschutzrecht)

Dort findet ihr:

- Vorlesungsaufzeichnungen
- PDFs der Folien
- Abkürzungsverzeichnis (fortlaufend aktualisiert)
- Termine der Vorlesungen und der Klausur (letztere voraussichtlich: Mo. 09.03.2026)

Fragen, Anmerkungen oder Kritik zur Vorlesung gerne an
christoph.werner@kit.edu oder
us@vogel-partner.eu

Organisatorische Fragen
(Bescheinigungen, Prüfungsan- oder abmeldung, Anrechnung von Leistungen, etc.)
stefanie.fuchs@kit.edu

Digitale Mitarbeit

- **Testeinsatz für die nächsten 4 UE**
- Ermöglicht digitale Mitarbeit/Abstimmung
- Die Nutzung ist selbstverständlich freiwillig, es gilt die Datenschutzerklärung von wooclap.com [1] in der jeweils aktuellen Fassung.
  Empfehlung: alle Cookies ablehnen
- QR-Code ab nächster Vorlesung immer auf der ersten Folie

wooclap.com Code: REQQEP

[1] https://www.wooclap.com/en/privacy-policy/

Noch Fragen zur Vorlesung an sich?

Heutige Agenda (Grundlagen)

A. Allgemeine juristische Grundlagen:

1. Normenhierarchie
2. Auslegung und Subsumtion

B. Hinführung zum Datenschutzrecht

3. Diskussion um das Dateneigentum
4. Persönlichkeitsrechte vs. Datennutzung
5. Risikobeispiel Microtargeting
6. Nutzungsbeispiel Live Traffic Information
7. Gesellschaftliche Wahrnehmung des Datenschutzes

Vorab: Umfrage

1. Normenhierarchie

Europäische Stufen	*Erläuterung/Beispiele*
1. Europäisches Primärrecht	Europäische Verträge (EUV, AEUV) Grundrechtecharta (GRC)
2. Europäisches Sekundärrecht	DSGVO, EPrivacy-RL (siehe Art. 288 AEUV)
Nationale Stufen	
1. Verfassungen	Grundgesetz und Landesverfassungen
2. Bundes- und Landesgesetze	BDSG und LDSG
3. Rechtsverordnung	KritisV (oder die Corona-Verordnungen der Länder)
4. Satzung	von Selbstverwaltungsträgern (Gemeinden, Unis)

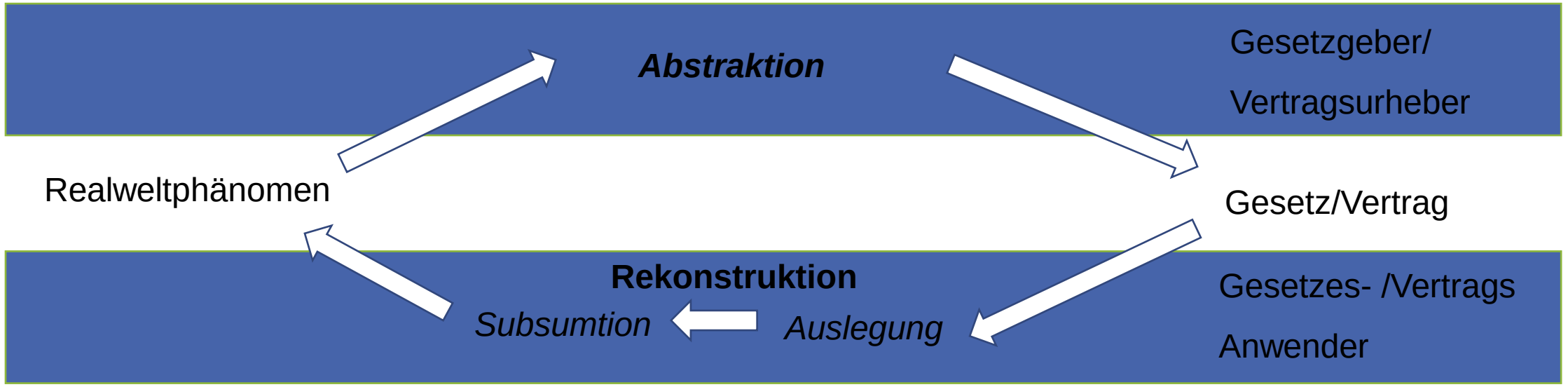
Bundesrecht bricht Landesrecht

Zu den nationalen Stufen: Lepsius, JuS 2018, 950

2. Auslegung und Subsumtion

Vorfrage: Was ist juristische Auslegung und warum wird ausgelegt?

Ein Gesetz (oder auch ein Vertrag) ist stets notwendigerweise eine Abstraktion.
Die Auslegung ist (Teil der) Rekonstruktion



2. Auslegung und Subsumtion (Beispiel 1)

Einfaches Beispiel:

Realweltphänomen: Menschen beschädigen vorsätzlich Eigentum anderer (Vandalismus: z.B. Scheiben einwerfen, Wände beschmieren, Autos zerkratzen), dass soll unterbunden werden.

Abstraktion

§ 303 StGB: Wer rechtswidrig eine fremde Sache **beschädigt oder zerstört**, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Rekonstruktion

Realweltphänomen (Fall): T hat an einem Auto die Luft aus den Reifen gelassen, hat er es **beschädigt**?

2. Auslegung und Subsumtion (Beispiel 1)

- Auslegung nach dem Wortlaut

  Ergründung der üblichen oder fachspezifischen Bedeutung eines Begriffs
  Beschädigen, Schaden: Substanz- oder Funktionsbeeinträchtigung

- Systematische Auslegung

  Begriff bzw. Norm nicht isoliert, sondern in Gesamtschau mit anderen Vorschriften betrachten

- Historische Auslegung

  Ermittlung des (subjektiven) Willens des historischen Gesetzgebers mit Blick auf vorherige Gesetze, Gesetzgebungsmaterialien und Erwägungsgründe

- Teleologische Auslegung

  Ermittlung des objektiven Sinn & Zwecks der Vorschrift im aktuellen Anwendungskontext

  Geschützt ist das Interesse des Eigentümers an der Nutzung seines Eigentums, diese muss damit zumindest nicht unerheblich gestört sein

Am Ende der Auslegung steht eine Definition, unter die der Fall „subsumiert“ werden kann.

2. Auslegung und Subsumtion (Beispiel 1)

Am Ende der Auslegung steht eine Definition, unter die der Fall „subsumiert“ werden kann.

Definition „Beschädigung“ (stark vereinfacht): jede nicht unerhebliche Substanz- oder Funktionsbeeinträchtigung

Subsumtion:

Auto mit leeren Reifen:

- ist zwar nicht in seiner Substanz beeinträchtigt
- Aber Funktionsbeeinträchtigung (+)

- Erheblich?
  - Aufpumpen an sich leicht wieder möglich („wenn dies unmittelbar an einer Tankstelle geschieht, die die Reifen für den Besitzer mühelos und kostenfrei wieder aufpumpt“)
  - Aber gilt das auch an entlegenen Orten?

BGH, Beschluss vom 14. 7. 1959 - 1 StR 296/59 (NJW 1959, 1547)

2. Auslegung und Subsumtion (Beispiel 2)

Art. 32 DSGVO – Sicherheit der Verarbeitung

Maßnahmen zur Gewährleistung der Datensicherheit schließen ggf. u.a. folgendes ein:

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und **Resilienz** [Belastbarkeit] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Wortlaut	Systematik	Historie	Telos
lat. resilire: abprallen, zurückspringen; Psychologie: Widerstandsfähigkeit ggü. widrigen Ereignissen	Eine Anforderung von **Systemen und Diensten**, zur Gewährleistung der Datensicherheit	Nicht in vorheriger DS-RL enthalten Datensicherheits-vorgaben aus Sicht des Gesetzgebers wohl ergänzungsbedürftig	Umgang mit neu auftretenden, ungewissen Herausforderungen (z.B. durch komplexe Systeme oder KI-Einsatz)

Resilienz: Fähigkeit eines Systems, mit ungewissen Ereignissen umzugehen (Definition, Auslegungsergebnis)

https://doi.org/10.5771/9783748947523

2. Auslegung und Subsumtion (Beispiel 2)

Art. 32 DSGVO – Sicherheit der Verarbeitung

Maßnahmen zur Gewährleistung der Datensicherheit schließen ggf. u.a. folgendes ein:

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und **Resilienz** [Belastbarkeit] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Resilienz: Fähigkeit eines Systems, mit ungewissen Ereignissen umzugehen (Definition, Auslegungsergebnis)

Subsumtion: Zu ergreifende Maßnahmen (Realweltphänomen) zur Herstellung von Resilienz

- Anomalieerkennungssysteme
- Automatische Segmentierung von Netzwerken, Aktivierung von Redundanzen
- Vorbereitete Wiederherstellungsroutinen

https://doi.org/10.5771/9783748947523

B. Hinführung zum Datenschutzrecht

3. Diskussion um Dateneigentum

Personenbezogene Daten sind „meine Daten“

- **§ 903 BGB (Sacheigentum):** Der Eigentümer einer Sache kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen.
- Bundesverfassungsgericht (BVerfG) zu Art. 14 GG: Jedes vermögenswerte Recht [*Bezahlen mit Daten*], das die Rechtsordnung dem Einzelnen zur ausschließlichen Nutzung im eigenen Interesse zuweist.

- Kern des Eigentums (auch des geistigen wie des Urheberrechts (UrhR)):
  - **Nutzung nach Belieben** innerhalb eines weiten sozialen/rechtlichen Rahmens
  - **Ausschließlichkeit**: Eigentümer kann (rechtlich) andere von Nutzung ausschließen
  - **Transferierbarkeit**: Eigentum kann aufgeben und übertragen werden
    (bei Daten theoretisch möglich, aber praktisch eher irrelevant)

3. Diskussion um Dateneigentum

<u>Kein</u> Eigentum an (auch nicht-personenbezogenen/nicht-pb) Daten

Da zwei entscheidende Unterschiede zum Sacheigentum:

1. **Nicht-Rivalität im Konsum**, leicht zu kopieren und zumeist zu geringen (Grenz-)Kosten

2. **Zuweisungsfrage**: Daten stehen wirtschaftlich nicht zwingend (nur) der Person zu, die sie erhebt: Daten bilden die soziale Wirklichkeit ab, an der viele Stellen beteiligt sind (z.B. Smartwatch)

Außerdem Verbindung mit Persönlichkeitsrecht…

3. Diskussion um Dateneigentum

- **Eigentum an pb. Daten wird (auch) durch Verbindung mit Persönlichkeitsrecht ausgeschlossen:**
  - Personenbezogene Daten sagen immer etwas über die betroffene Person aus
  - Ihre Verbreitung hat Folgen für die betroffene Person
    - Zunächst abstrakt: Informationen über sich selbst werden an andere weitergegeben
    - Mittelbare (mögliche) Folgen:
      - Zugang und Personalisierung einer digitalen Dienstleistung/Werbung, gewollte Kommunikation,
      - aber auch: Manipulation (Filter Bubble), Ablehnung von Verträgen, soziale Ausgrenzung und Diskriminierung (ggf. auch in Verbindung mit Datenleaks)
  - Grundrechtliche Absicherung über das Recht auf informationelle Selbstbestimmung (im Detail UE 3/15)
  - Daher *kein* bloßes vermögenswertes Gut i.S.d. Art. 14 GG, trotz „Bezahlens mit Daten“

4. Persönlichkeitsrechte vs. Datennutzung

4. Persönlichkeitsrechte vs. Datennutzung

Personenbezogene Daten als Abbild realer Vorgänge und Zustände
(z.B. Gesundheitsdaten, Verkehrsdaten, Bankdaten, etc.)

Personenbezogene Daten als Ausdruck sozialer Kommunikation

- Menschen kommunizieren („Man kann nicht nicht kommunizieren.“ Paul Watzlawick)
  - Analog: explizit (Sprache) oder implizit (Kleidung, Styling, Mobilitätsform, Besuchen von Ereignissen)
  - Digital: explizit (Chats, Posts, Likes) oder implizit (Surfverhalten, Nutzung bzw. Nicht-Nutzung von Apps, unbewusstes Standort-Tracking)

- Kommunikation löst i.d.R. soziales Feedback aus und trägt maßgeblich zur Identitäts- und Charakterbildung bei

- Das Feedback kann (anders in der analogen Welt) auch in einer technischen Veränderung der eigenen digitalen Welt liegen (Personalisierung)

4. Persönlichkeitsrechte vs. Datennutzung

Risiken für Persönlichkeitsrechte:

- **Manipulation** durch personalisierte digitale Welt (Vorfilterung von Informationen, Filter Buble)
- **Chilling-Effects**

  Vermeidung bestimmter (digitaler) Kommunikation aus Angst vor Nachverfolgbarkeit und Repressionen
- **Soziale Ausgrenzung, Diskriminierung** bspw. infolge geleakter Gesundheitsdaten

Risiken für sonstige Rechte:

- **Ökonomische Nachteile**

  Versicherungen, z.B. Pay-as-you-drive oder private Krankenkassen

4. Persönlichkeitsrechte vs. Datennutzung

Möglichkeiten der Datennutzung:

- Forschung und Entwicklung z.B. von Medizinprodukten oder KI-Systemen
- Effizienterer Informationszugang durch Personalisierung
- Effizientere Ressourcennutzung (z.B. smarter ÖPNV, smarte Stromnetze)
- ***(****Mehr Wirtschaftswachstum durch personalisierte Werbung****)***

4. Persönlichkeitsrechte vs. Datennutzung

Risiken für Persönlichkeitsrechte

Möglichkeiten der Datennutzung

Regulierung durch Datenschutzrecht

5. Risikobeispiel Microtargeting

- **Microtargeting**: Anpassung von digitalen Angeboten auf individuelle Person anhand umfassenden Profilings (Systematische Erfassung und Bewertung persönlicher Verhältnisse, Verhaltensmuster, etc.)

- Laut einer Studie der Universität Cambridge aus 68 „neutralen“ Likes auf Facebook (es wurden die Daten von 80.000 Nutzer:innen analysiert) mit überwiegender Wahrscheinlichkeit ermittelt werden
  - Hautfarbe, Homosexualität, Wahlverhalten (USA), Religionszugehörigkeit, Rauschmittelkonsum, Trennung der Eltern vor 20. Geburtstag. [1]

- Unterfall **Emotional Targeting**: „das US-Werbeunternehmen MediaBrix [hat] ein System entwickelt, das in Echtzeit die Emotionen von Computerspieler:innen analysiert und diese dann in besonders geeigneten Momenten (während sog. Breakthrough Moments) direkt durch personalisierte Werbung anspricht.“ [2]

- Unterfall **Politisches Microtargeting**
  Cambridge Analytica im US-Wahlkampf:
  Individuelle Ansprache von vorher identifizierten potenziellen Wähler:innen

[1] Kosinski/Stillwell/Graepel PNAS 110 (2013), 5802; Youyou/Kosinski/Stillwell PNAS 112 (2015), 1036.[2] Ebers/Heinze/Krügel/Steinrötter KI, 1. Aufl. 2020, § 3 Rn. 117 m.w. N.;

5. Risikobeispiel Microtargeting

Problematische Auswirkungen:

- **Individuell extreme Macht- und Informationsasymmetrie** [1]
  Betroffene Person überblickt i.d.R. nicht, was das Werbeunternehmen über sie weiß;
  das Werbeunternehmen kennt hingegen die betroffene Person und ihre „Schwächen“ genau
  (Grundrechtlich: freie Entfaltung möglich?; zivilrechtlich: Privatautonomie?)

- **Gesellschaftlich: Möglichkeit z.B. der Wahlmanipulation durch politisches Microtargeting**

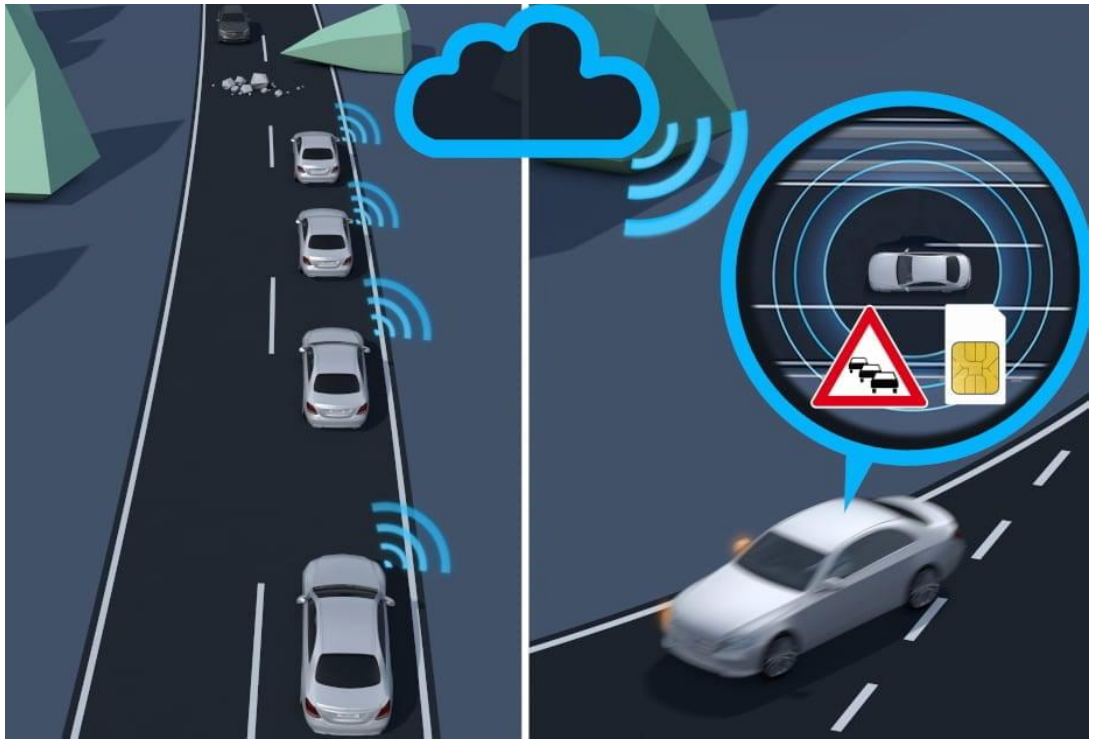
  Europäische Reaktion: Verbot der politischen Werbung auf Basis von Profiling:
  Art. 18 Abs. 1 lit c) **VO 2024/900**

  national: **Politische-Werbung-Transparenz-Gesetz (PWTG)** im Entwurfsstadium

[1] Ebers/Heinze/Krügel/Steinrötter KI, 1. Aufl. 2020, § 3 Rn. 117 m.w. N.;

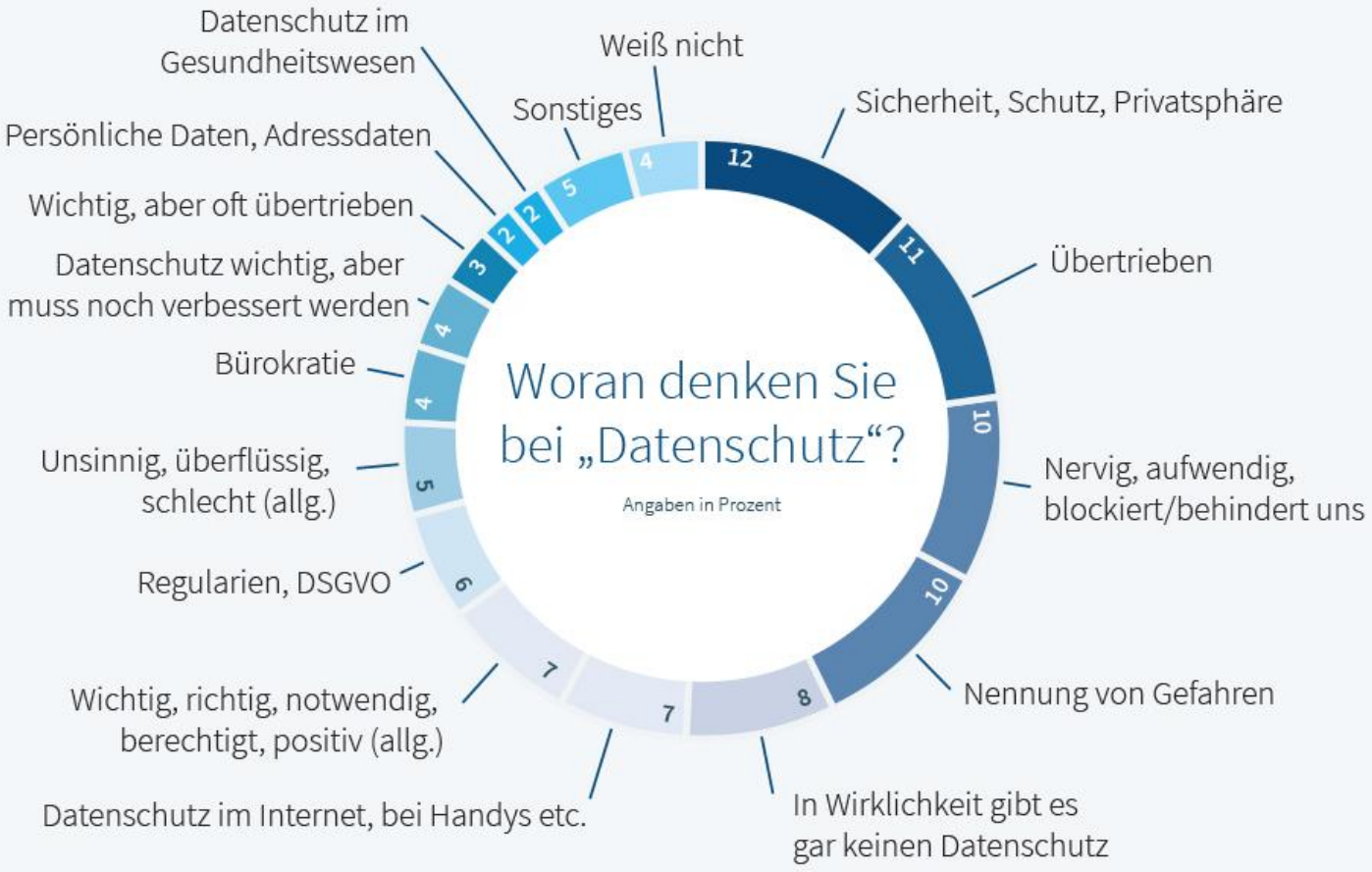
6. Nutzungsbeispiel Live Traffic Information

- Nutzung von (ggf. auch anonymisierten bzw. pseudonymisierten) Echtzeit-Verkehrsdaten für Warnungen und Routenführungen
- Sowohl in Navigationsapps als auch integrierten Navigationslösungen in Fahrzeugen
- Z.B. Meldungen für Staus oder Baustellen inkl. optimierter Routenvorschläge.



https://www.kunzmann.de/de/services/lexikon/live-traffic-information/

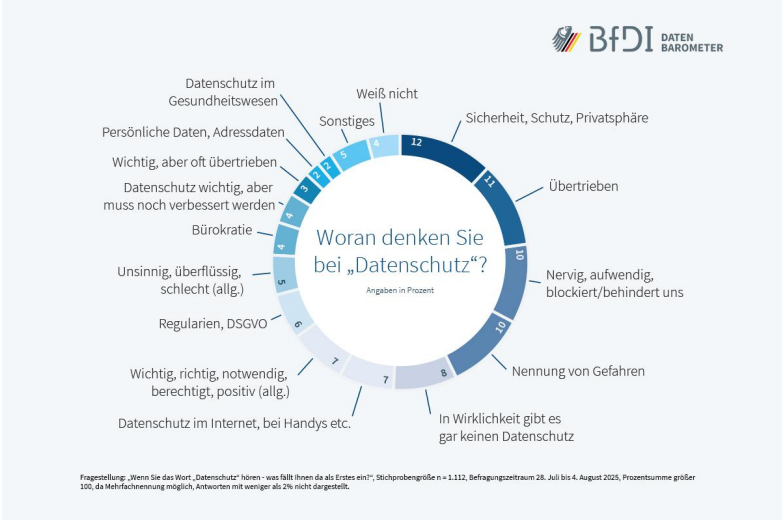
7. Gesellschaftliche Wahrnehmung des Datenschutzes



Fragestellung: „Wenn Sie das Wort „Datenschutz“ hören - was fällt Ihnen da als Erstes ein?“, Stichprobengröße n = 1.112, Befragungszeitraum 28. Juli bis 4. August 2025, Prozentsumme größer 100, da Mehrfachnennung möglich, Antworten mit weniger als 2% nicht dargestellt.

https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/15_Datenbarometer.html

7. Gesellschaftliche Wahrnehmung des Datenschutzes



Zusammenfassung:

- 22% der Assoziationen sind positiv
  (z.B. Sicherheit, Schutz, Privatsphäre)
- 35% neutral oder ambivalent
  (z.B. wichtig, aber muss noch verbessert werden)
- 37% negativ
  (z.B. übertrieben, unsinnig, bürokratisch, illusorisch)

https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/15_Datenbarometer.html

7. Gesellschaftliche Wahrnehmung (Umfrage in der Vorlesung)

Referenz:

Positiv: 22%

Neutral: 35%

Negativ: 37%

Anhang: Wichtigste Lerninhalte der UE

- Normenhierarchie (Europarecht (primär/sekundär), Grundgesetz, Bundesrecht, Landesrecht
- Juristische Auslegung (Wortlaut, Systematik, Historie, Telos) und Subsumtion
- Es gibt kein Eigentum an (personenbezogenen) Daten, sondern personenbezogene Daten sind immer auch Ausdruck der eigenen Persönlichkeit und deshalb gesondert geschützt.
- Datenschutzrecht dient dem Ausgleich zwischen den mit der Datenverarbeitung einhergehenden Risiken für Persönlichkeitsrechte und den Chancen der Datennutzung
  (zu den dahinterstehenden Rechtsgütern nächste UE)