Teil I:
Analogien in der Risikokommunikation individueller und gesellschaftlicher Grundrechtsrisiken

Vollkörper-Airbags für Fußgänger:innen? – Zur Nutzung von Analogien in der Risikokommunikation im Datenschutz, oder: Wie mit guten Vergleichen über schlechte Lösungen aufgeklärt werden kann

Jörg Pohle und Maximilian Lukat

Zusammenfassung

Die Verarbeitung personenbezogener Daten ist allgegenwärtig. Für die Betroffenen ist jedoch oft unklar, wie diese Datenverarbeitung funktioniert und welche Auswirkungen sie haben könnte. Dieser Beitrag untersucht das Potenzial von Analogien für die Risikokommunikation im Datenschutz. Nach einer konzeptionellen Einführung werden die Funktionen von Analogien dargestellt und eine Abgrenzung zu verwandten Konzepten wie Metaphern, Modellen und Beispielen vorgenommen. Um darlegen zu können, dass der öffentliche Straßenverkehr und seine Regulierung als Zieldomäne für Analogien in der Risikokommunikation im Datenschutz geeignet sind, richtet sich der Blick zunächst auf die Ausgangsdomäne – das zugrunde liegende konsequentialistische Datenschutzverständnis des Beitrags. Vor diesem Hintergrund werden die relationalen Eigenschaften beider Bereiche erläutert und verbreitete Fehlbeschreibungen in der Risikokommunikation kritisiert. Letztendlich ist davon auszugehen, dass strukturell fundierte Analogien dafür geeignet sind, Missverständnisse über den Datenschutz und die Risiken der Verarbeitung personenbezogener Daten aufzudecken und ein angemesseneres Risikoverständnis zu fördern.

1. Einleitung

Die Verarbeitung personenbezogener Daten in Informatiksystemen ist allgegenwärtig. Häufig bleibt sie intransparent, oder jedenfalls wird sie so wahrgenommen. Nutzer:innen und Betroffene berichten von Herausforderungen, die Datenverarbeitung zu verstehen (Lukat u.a. 2025). Das liegt an komplexen Akteurskonstellationen – unterschiedliche Unternehmen wirken zusammen, um Inhalte bereitzustellen, Produkte zu bewerben oder

Werbeplätze zu vermitteln – und den hochentwickelten technischen Infrastrukturen, die dabei eingesetzt werden. Noch größer sind die Herausforderungen, wenn es darum geht, die Auswirkungen dieser Datenverarbeitungen auf individuelle wie kollektive Grundrechte und Freiheiten sowie gesellschaftliche Strukturen angemessen einzuschätzen.

Im Allgemeinen sowie im Gesetz werden diese Auswirkungen als Risiken adressiert. Bei genauerer Betrachtung des Begriffs wird außerdem deutlich, warum die Einschätzung von Auswirkungen so herausfordernd ist. Zunächst wird im rechtswissenschaftlichen Diskurs ein Risiko als eine nicht vollkommen einschätz- und abwägbare Gefahr angesehen. Dies steht anderen Definitionen entgegen, die ein Risiko als eine abschätzbare Gefahr sehen, die mit einer gewissen Wahrscheinlichkeit und Schwere eintreten kann (vgl. von Grafenstein 2018, S. 82f). Diese zweite Definition entspricht auch dem Verständnis des Gesetzgebers von einem Risiko, wie es in Erwägungsgrund 75 für die DSGVO als ein Schaden, der mit einer gewissen Wahrscheinlichkeit und Schwere eintreten kann, beschrieben wird. Die Tücke liegt darin, neben der Wahrscheinlichkeit und Schwere eines Risikos auch die jeweilige Risikoquelle identifizieren zu können, um passende und wirksame Schutzmaßnahmen umzusetzen. Was im Datenschutzrecht als ein Problem für Betreiber:innen und die Gestaltung und den Betrieb ihrer Systeme gesehen wird (vgl. Rost 2018, S. 80), gilt ebenso für Nutzer:innen, die nur ein begrenztes Maß an Informationen, Zeit und Handlungsmöglichkeiten innerhalb von IT-Systemen haben, um Risiken zu begegnen.

In Forschung und Praxis wurden bereits vielfältige Wege ausgelotet, wie Wissen über Datenverarbeitung besser vermittelt werden kann – von verständlichen Texten (vgl. Pardo/Le Métayer 2019) über grafische Darstellung (vgl. Kelley u.a. 2010; Efroni u.a. 2019) bis zu interaktiven Formaten (vgl. Morel u.a. 2025). Dennoch bleiben zwei zentrale Fragen oft unbeantwortet: Wie können Menschen nicht nur Datenverarbeitung besser verstehen, sondern auch Folgen und Risiken daraus ableiten? Und wie können Menschen wirklich dazu befähigt werden, Risiken nicht nur zu erkennen, sondern auch zu bewerten – und entsprechend zu handeln?

An dieser Stelle können Analogien zum Einsatz kommen. Dieser Beitrag zielt darauf ab, eine breite und fundierte Auseinandersetzung mit der Nutzung von Analogien in der Risikokommunikation im Datenschutz zu etablieren.

Analogien sind ein verbreitetes Mittel zur Wissensvermittlung und Verständnisgewinnung. Als besonders wertvoll gelten sie für die Vermittlung von schwierigen wissenschaftlichen Konzepten in Bereichen, die als solche

nicht direkt wahrnehmbar oder zugänglich sind. Sie werden dabei genutzt „to make the unfamiliar familiar" (Duit 1991). Vor allem in der naturwissenschaftlichen Bildung werden Analogien viel eingesetzt und sind dort auch im Hinblick auf ihre Möglichkeiten und Grenzen bereits gut untersucht (vgl. etwa Haider u.a. 2013).

Vor dem Hintergrund der Herausforderungen, moderne Datenverarbeitung zu verstehen, könnte erwartet werden, dass Analogien eine wichtige Rolle in der informatischen Bildung und der Informatikdidaktik einnehmen. Das ist jedoch nicht der Fall. Das ist durchaus überraschend, werden doch konzeptionell eng mit Analogien verwandte Modelle (vgl. Hesse 1963) sehr umfassend verwendet und diskutiert (vgl. Frank 2015), gerade auch in der Vermittlung von Wissen über Datenverarbeitung, Datenverarbeitungssysteme und -verfahren.

Im Datenschutzbereich sind Analogien ebenfalls noch nicht Gegenstand der wissenschaftlichen Auseinandersetzung. Auch hier überrascht das Fehlen einer wissenschaftlichen Auseinandersetzung mit Analogien, nicht zuletzt weil Analogien in der Praxis durchaus weite Verbreitung finden. Noch mehr gilt das für Metaphern, ein anderes mit Analogien verwandtes Konzept.

Ein Beispiel ist die sehr verbreitete Nutzung von Personen und ihrer Informationsverarbeitung beim Versuch, die Datenverarbeitung von Unternehmen verständlich zu machen. Die Datenerhebung und -verarbeitung von Google wird dann etwa problematisiert, indem sie verglichen wird mit: „Stell Dir vor, Deine Mutter findet heraus, dass…" Diese Problematisierung kann jetzt wahlweise als Modell, Metapher oder Analogie verstanden werden. Mit jedem dieser Verständnisse gehen leichte Unterschiede damit einher, was als gleich verstanden wird – und was sich unterscheiden kann, ohne dass diesen Unterschieden besondere Bedeutung für das zu vermittelnde Wissen oder Problemverständnis beigemessen wird. Zugleich zieht die Verwendung der drei Konzepte – Modell, Metapher und Analogie – jeweils unterschiedliche Verteilungen der Verantwortlichkeit nach sich: Müssen diejenigen, die diesen Vergleich nutzen, deutlich machen, was gleich und was ungleich ist? Oder müssen sich die Zuhörenden das selbst erschließen? Und was passiert, wenn sie daran scheitern? Wie der Beitrag zeigen wird, handelt es sich nicht um eine Analogie – zumindest um keine gute oder gut begründete. Und selbst als Metapher wäre diese Problematisierung nicht geeignet, um tatsächlich aufzuklären. Wie der Beitrag deutlich machen wird, vernebelt sie eher und entstellt, worum es im Datenschutz geht.

Der Beitrag ist wie folgt gegliedert. Nach dieser kurzen Einleitung gibt der Beitrag im zweiten Teil eine kurze Einführung zu Analogien und deren Nutzung zur Wissensvermittlung und zum Verständnisgewinn, grenzt sie von verwandten und benachbarten Konzepten ab und formuliert Anforderungen an die Auswahl und Gestaltung sowie den Einsatz von Analogien, denn: „Nicht alles, was hinkt, ist ein Vergleich." Im dritten Teil wird das dem Beitrag zugrunde gelegte Verständnis von Datenschutz kurz umrissen. Im vierten Teil des Beitrags werden der Bereich des öffentlichen Straßenverkehrs, seine Regulierung sowie die Rechtsdurchsetzung als Zieldomäne für Analogien für die Risikokommunikation im Datenschutz eingeführt, plausibilisiert und anhand von Beispielen diskutiert. Im fünften Teil des Beitrags werden Analogien sowie Metaphern, Vergleiche und, etwas allgemeiner, Beispiele eingeführt, die in der Risikokommunikation im Datenschutz verbreitet genutzt werden. Diese werden dann vor dem Hintergrund der Ausführungen in den vorhergehenden Teilen einer Kritik unterzogen. Der Beitrag schließt mit einem Ausblick und offenen Fragen für die weitere Forschung und Gestaltung von Analogien für die Risikokommunikation im Datenschutzbereich.

2. Analogien. Eine kurze Einführung

Im folgenden Teil gibt der Beitrag eine kurze konzeptionelle Einführung zu Analogien und deren Nutzung zur Wissensvermittlung und Verständnisgewinnung. Analogien werden im Verhältnis zu verwandten und benachbarten Konzepten verortet und von ihnen abgegrenzt, wie etwa Metaphern, Personifikationen, Vergleichen, Allegorien, Beispielen und Modellen. Daraus werden anschließend Qualitätsanforderungen an die Auswahl, die Gestaltung sowie den Einsatz von Analogien abgeleitet.

2.1Geschichte und Konzept von Analogien

Für Analogien gibt es eine beachtliche Anzahl von unterschiedlichen Definitionen. Die Definitionen oszillieren zwischen dem Fokus auf Analogien als rhetorische Mittel und dem als kognitive Mittel. Jedenfalls sind sie nicht einfach Redewendungen, sondern eine Art des Denkens.

Analogien zählen zu den ältesten Denkformen der Menschheit und seit mindestens der Antike sowohl in Gebrauch als auch Gegenstand von wissenschaftlicher Auseinandersetzung (vgl. Hentschel 2010). Mit Analogien werden Ähnlichkeiten zwischen zwei verschiedenen Gegenstandsbereichen oder -objekten vermittelt: dem Quell- oder Basisbereich und dem Ziel-

oder Targetbereich (vgl. Gentner 1983). Dabei geht es nicht nur um gleiche oder vergleichbare Elemente in Quell- und Zielbereich oder Eigenschaften der Elemente oder Bereiche. Vor allem geht es nicht um punktuelle Vergleiche einzelner Attribute. Zentral ist stattdessen, dass es auch ähnliche Beziehungen zwischen den Elementen und Eigenschaften des Quellbereichs und denen des Zielbereichs gibt – oder ähnliche Beziehungen von Beziehungen. Analogien zeigen die Identität von Teilen der Strukturen an (vgl. Duit 1991).

An einem Beispiel wird deutlich, was es bedeutet, dass sich die Feststellung der Identität nicht auf Elemente, sondern auf Beziehungen zwischen den Elementen bezieht: Wenn eine Analogie zwischen Hand und Fuß gezogen wird, dann werden nicht alle Eigenschaften der Hand und des Fußes verglichen, sondern vielmehr die Beziehungen zwischen Hand und Fuß und ihren jeweiligen Innenflächen, nämlich die Handfläche einerseits und die Sohle andererseits.

Heutige Kognitionswissenschaftler:innen verwenden einen breit gefassten Analogiebegriff, der von Dedre Gentners „Structure Mapping Theory" eingerahmt wird (Gentner 1983). Nach dieser Auffassung hängt die Analogie zu einem kleineren Anteil von der Abbildung oder Entsprechung der Elemente von Quelle und Ziel ab, zu einem größeren jedoch von den Beziehungen von Objekten und den Beziehungen von Beziehungen:

> The central claims of the theory are that analogy is characterized by the mapping of relations between objects, rather than attributes of objects, from base to target; and, further, that the particular relations mapped are those that are dominated by higher-order relations that belong to the mapping (the systematicity claim). (Gentner 1983, S. 168).

Gentners „Structure Mapping" ist eine Theorie aus der Psychologie, die die psychologischen Prozesse beschreibt, die beim Denken durch Analogien und beim Lernen aus ihnen ablaufen. Hierfür zielt die Theorie darauf ab, zu beschreiben, wie vertrautes Wissen oder Wissen über einen Basisbereich – oder Quellbereich – genutzt werden kann, um das Verständnis einer Person für eine weniger vertraute Idee oder einen Zielbereich zu verbessern. Nach dieser Theorie betrachten Individuen ihr Wissen über Ideen oder Bereiche als zusammenhängende Strukturen. Das heißt, ein Bereich besteht aus Objekten, ihren Eigenschaften und den Beziehungen, die ihre Interaktion kennzeichnen. Der Prozess der Analogie – das Analogisieren – umfasst Folgendes: Erstens das Erkennen ähnlicher Strukturen zwischen Basis- und Zielbereich. Zweitens wird nach einer tieferen Ähnlichkeit gesucht, indem andere Beziehungen eines Basisbereichs auf den Zielbereich abgebildet

werden. Drittens erfolgt ein Abgleich dieser Erkenntnisse mit dem vorhandenen Wissen über den Zielbereich. Das Systematizitätsprinzip beschreibt die Feststellung, dass Menschen Analogien bevorzugen, bei denen die beiden Systeme in hohem Maße miteinander korrespondieren, das heißt zum Beispiel ähnliche Beziehungen zwischen den Domänen im Gegensatz zu ähnlichen Objekten innerhalb der Domänen, wenn Menschen versuchen, die Systeme zu vergleichen und zu kontrastieren.

2.2 Funktionen von Analogien

Analogien erfüllen in verschiedenen Kontexten unterschiedliche, aber verwandte Funktionen. Sie helfen beim Transfer von Wissen und fördern das Verständnis.

Analogien dienen dazu, unbekannte oder komplexe Konzepte verständlich zu machen, indem sie diese mit bekannten Konzepten in Beziehung setzen. Diese Verknüpfung kann außerdem dazu beitragen, dass die neuen und komplexen Konzepte besser gemerkt werden (Lehner 2018, S. 95). Außerdem können sie durch ihre strukturellen Relationen Wissen intra- und interpersonal in andere Wissensformen transformieren. Intrapersonal unterstützen Analogien beispielsweise den Kompetenzerwerb, indem sie prozedurales Wissen, also das Wissen, wie man etwas macht, auf neue Situationen übertragen können und so strukturelles Wissen gefestigt wird (Markauskaite/Goodyear 2014, S. 86; Hattie/Yates 2015, S. 126f). In ihrer interpersonalen Funktion sind sie besonders für die Pädagogik und die Organisationsforschung interessant. Dort wird vor allem ihre Rolle bei der Umwandlung von implizitem Wissen zu explizitem Wissen untersucht (Wiater 2007, S. 97ff). Ebenso ist es denkbar, dass sie eine Interdisziplinaritätsfunktion erfüllen, indem sie es ermöglichen, Verständnislücken zwischen verschiedenen Disziplinen zu schließen.

In der Argumentation können sie nachvollziehbare und überzeugende Argumente sein, da sie zulassen, auf Grundlage ähnlicher Beziehungen Schlüsse zu ziehen (Coenen 2002, S. 167ff).

2.3 Abgrenzung von ähnlichen Konzepten

Um verständlich zu machen, warum sich gerade Analogien dazu eignen, in der Risikokommunikation eingesetzt zu werden, müssen sie von ähnlichen

Konzepten wie Metaphern, Modellen, Beispielen, Vergleichen, Gleichnissen, Parabeln und Allegorien unterschieden werden. Eine vollständige Liste ähnlicher Konzepte an dieser Stelle anzubringen, ist kaum möglich, da diese in einer Vielzahl unterschiedlicher Disziplinen besprochen werden und in diesen Disziplinen auch unterschiedliche Bedeutungen haben können. Eine klare Grenze lässt sich daher nicht ziehen. Zur Abgrenzung der Structure-Mapping-Theorie von anderen, ähnlichen, geläufigen Konzepten sollte diese Ausführung aber genügen. Da es um eben diese theoretische Abgrenzung geht, wird auch auf Beispiele für die anderen Konzepte verzichtet.

Metaphern funktionieren nach Gentner u.a. (2001) auf eine ähnliche Art wie Analogien, nur dass die übertragenen Relationalitäten nicht ausgeführt, nicht expliziert werden. Hentschel (2010) beschreibt Metaphern als „unausgepackte Analogien", also als verkürzte Vergleiche. In der Folge muss bei der Benutzung von Metaphern das Bedeutungsfeld durch die Rezipient:innen selbstständig semantisch erschlossen werden. Gerade die Ausführung oder Explizierung der Relationalität bzw. spezifisch auch der Nichtrelationalität ist jedoch nach Brown und Salter (2010) gerade dann relevant, wenn ein didaktischer Anspruch verfolgt wird, um Misskonzeptionen zu vermeiden, insbesondere da Metaphern und Analogien auch als suggestive Sprachmittel verstanden werden können (vgl. Marzi/Renner 2024).

Modelle sind nach Herbert Stachowiaks Allgemeiner Modelltheorie (1973) vereinfachte oder abstrahierte Abbildungen komplexer Systeme, die bestimmte strukturelle oder funktionale Eigenschaften des Originals beibehalten (Saam 2009, S. 517), um Verständnis oder Vorhersagen zu ermöglichen. Dabei können sie in physischer oder formaler Form vorliegen (Hesse 2017, S. 299). Sie dienen in der Wissenschaft oft als heuristische Werkzeuge (Stachowiak 1980, S. 55), um Theorien zu entwickeln oder Phänomene zu erklären (Hesse 2017, S. 304). Während Analogien die Abbildung relationaler Strukturen von einem Basisbereich auf einen Zielbereich betonen, können Modelle auch Objektattribute ohne tiefere relationale Ordnung abbilden.

Auf einer abstrakteren Ebene bewegen sich *mentale Modelle*. Sie stellen nach dem kognitionswissenschaftlichen „instructional approach" das konzeptionelle Wissen und Verständnis über Domänen dar und sind somit eine abstraktere Form der Analogien. Die relationale Charakteristik der Analogien bleibt erhalten, wobei sich das Verständnis von konkreten Entsprechungen in der Außenwelt loslöst und in ein abstraktes Verständnis von Funktion und Zusammenhängen wandelt (Nitz/Fechner 2018, S. 75).

Analogien können also dazu beitragen, dass Wissen in mentale Modelle überführt wird.

Ein weiteres ähnliches Konzept sind *Beispiele*. Sie sind ein klassisches Mittel der allgemeinen Didaktik zur Wissensvermittlung. Grundsätzlich können komplexe Sachverhalte und Probleme in Beispielen kompakt dargestellt werden und grundlegende Eigenschaften verständlich werden (Klafki 2007, S. 143f), indem eine Verbindung zwischen dem Besonderen und dem Allgemeinen hergestellt wird (Zymner 1991, S. 15). In der pädagogischen Psychologie wird dies als inhaltliche Klarheit besprochen (Lipowsky 2020, S. 82). Durch die Komplexitätsreduktion, und im Falle von Problemen mit exemplarischen Lösungen, sind Beispiele einfach zu verstehen, da nicht zusätzlich nach einer Lösung gesucht werden muss (Renkl 2014, S. 5). Beispiele können Bestandteil von Analogien sein. Ein einzelnes Beispiel ist aber noch keine Analogie, da die Identifikation der Struktur und der Transfer der Eigenschaften in ein anderes Beispiel fehlt (Oberfell u.a. 2023, S. 430).

Daran anknüpfend können auch *Vergleiche* im Sinne der „Structure Mapping Theory" ein Bestandteil von Analogien sein. Mit ihnen können Ähnlichkeiten und Unterschiede zweier Domänen, zum Beispiel in ihren Merkmalen oder auch ihrer Struktur, herausgestellt werden (Gentner 1983, S. 159). Aber nicht alle Vergleiche sind Analogien, da Vergleiche sich nicht ausschließlich auf eine strukturelle Ähnlichkeit beziehen müssen (Oberfell u.a. 2023, S. 430).

Die folgenden drei Konzepte sind strukturell weiter von Analogien entfernt. Sie besitzen in erster Linie einen rhetorischen Charakter und stellen weniger kognitive Mittel dar.

In der antiken Rhetorik sind *Gleichnisse* kurze, bildhafte Erzählungen, die einen Vergleich anschaulich und eindrücklich, also konkret und verständlich, machen (Ueding/Steinbrink 2011, S. 287). Ihre Verständlichkeit entsteht durch die Erklärung anhand der Alltagswelt der Rezipient:innen (Lausberg 1960, S. 233). Gleichnisse betonen zwar relationale Strukturen, aber der Transfer ist oft auf einen zentralen Punkt, den „tertium comparationis", beschränkt. Dies wird auch daran deutlich, dass Gleichnisse aus einzelnen Wörtern entstehen können, die durch ein Vergleichswort verbunden sind (Ueding/Steinbrink 2011, S. 287). Bei Gentners Analogiebegriff werden hingegen immer mehrere Attribute und Teile von Strukturen miteinander verglichen.

Parabeln sind sprach- und literaturtheoretisch eng verwandt mit Gleichnissen. Sie sind ebenfalls kurze, bildhafte Erzählungen, die einen Vergleich

anschaulich und eindrücklich machen. Zugleich sind sie von Unbestimmtheit geprägt (Zymner 1991, S. 13f). Während ein Gleichnis in seiner Bedeutung und Intention selbsterklärend ist, ist dies bei Parabeln nicht der Fall (Zymner 1991, S. 72). Dies wirkt sich auch auf ihren pädagogischen oder didaktischen Nutzen aus. Da durch die Unbestimmtheit der Parabel die Erkenntnis nicht festgeschrieben ist, kann sie kein exaktes Wissen vermitteln, sondern allenfalls zum Nachdenken über einen bestimmten Bereich anregen. Weiter können Parabeln zwar zu relationalen Übertragungen einzelner struktureller Attribute führen, durch ihre Unbestimmtheit ist aber nicht eindeutig, was der Vergleichspunkt und die Zieldomäne sind (Zymner 1991, S. 117ff). Der „Vergleichspunkt" im Singular verdeutlicht zudem, dass es sich nicht um einen Vergleich mehrerer struktureller Attribute handelt.

Auch *Allegorien* stehen in Verbindung mit Gleichnissen und Parabeln. In der Literaturwissenschaft werden unter ihnen fiktionale Erzählungen verstanden, bei denen Figuren, Handlungen und Schauplätze stellvertretend für abstrakte Konzepte oder moralische Prinzipien stehen (Zymner 1991, S. 133). Strukturell sind sie aus literaturwissenschaftlicher und rhetorischer Sicht länger als Gleichnisse und Parabeln und als eine Aneinanderreihung von Metaphern konstituiert (Zymner 1991, S. 130; Ueding/Steinbrink 2011, S. 287). Im Vergleich zu Parabeln sind Allegorien etwas eindeutiger darin, welcher Zusammenhang zwischen Erzählung und möglicher Zieldomäne besteht, aber immer noch nicht konkret. Zudem geht aus ihnen ebenfalls nicht eindeutig hervor, was mit der Erzählung gemeint ist (Zymner 1991, S. 135; Ueding/Steinbrink 2011, S. 287). Während bei Allegorien immer ein Zusammenhang zwischen einer fiktionalen und der realen Situation hergestellt wird, ist das Fiktionale bei Analogien nicht zwingend erforderlich. Außerdem ist durch die weiterhin vorhandene Uneindeutigkeit der Allegorie nicht klar, was die intendierte Zieldomäne ist, während dies bei Analogien der Fall ist.

Aus der Betrachtung der verwandten Konzepte folgt, dass wir die Auswahl von Analogien als didaktisch sinnvolles Mittel darin begründen können, dass sie durch ihre Präzision und Verständlichkeit besser zur Wissensvermittlung geeignet sind, als die anderen besprochenen Konzepte. Zugleich folgt daraus das zentrale Qualitätskriterium für die Entwicklung und Auswahl von Analogien: Es muss explizit nachgewiesen oder hinreichend plausibilisiert werden, dass es sich bei ihnen auch tatsächlich um Analogien handelt.

3. Was verstehen wir unter Datenschutz?

Im folgenden Teil wird das dem Beitrag zugrunde gelegte Verständnis von Datenschutz kurz umrissen. Das ist notwendig, weil eines der wesentlichen Qualitätskriterien von Analogien darin liegt, ob sich nachweisen oder zumindest plausibilisieren lässt, dass die verglichenen Domänen (vgl. Duit 1991) über funktionsgleiche Strukturen verfügen. Bei der Betrachtung von Analogien genügt es daher nicht, nur die Zieldomäne zu beschreiben oder gar nur die einzelnen Analogien aufzulisten.

3.1 Datenschutz und Datenschutzrecht

Die erste und eine der wichtigsten Trennungen, die wir einführen, ist die zwischen Datenschutz und Datenschutzrecht. Datenschutz und Datenschutzrecht sind nicht äquivalent.

Datenschutzrecht ist immer eine historisch kontingente, von einem Gesetzgeber beschlossene und in Kraft gesetzte Menge von Datenschutznormen. Datenschutz hingegen bezeichnet den konzeptionellen Kern dessen, worum es geht (vgl. Pohle 2019).

Unter Datenschutz verstehen wir in Anlehnung an die Ausführungen in den „Grundfragen des Datenschutzes“ (Steinmüller u.a. 1972, S. 44) die „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung“. Datenschutz folgt demnach einem konsequentialistischen Verständnis: Problematisiert wird Informationsverarbeitung vor dem Hintergrund der Auswirkungen, die sie hat oder haben kann, nicht nach bestimmten inhärenten Eigenschaften. Der Fokus liegt dabei auf unerwünschten Auswirkungen, wobei die Kriterien für die Unerwünschtheit gesellschaftlich bestimmt sind: Unerwünscht sind Folgen von Informationsverarbeitung, wenn sie den gesellschaftlich konsentierten Vorstellungen zuwiderlaufen, wie sie in übergeordneten rechtlichen Werken wie Verfassungen niedergelegt sind – in Deutschland im Grundgesetz, auf der europäischen Ebene etwa in der EU-Grundrechtecharta (vgl. Steinmüller u.a. 1972, S. 44).

Im Datenschutzrecht ist der Datenschutz nach unserem Verständnis als Anwendung des Rechtsstaatsprinzips auf die gesamte Informationsverarbeitung umgesetzt, einschließlich der privaten. Datenschutzrecht ist, wie Steinmüller (1976, S. 14) formulierte, „die folgerichtige Weiterentwicklung

des rechtsstaatlichen Prinzips der Gesetzmäßigkeit der Verwaltung durch Ausdehnung auf den Bereich der privaten Informationsverarbeitung".

Im Kern problematisiert der Datenschutz demnach die Externalisierung von Risiken, die durch die Gestaltung, Umsetzung und Durchführung von Informationsverarbeitung erzeugt werden, von den Akteuren, die die Risiken erzeugen, auf diejenigen, die von ihnen betroffen sind. Und das Datenschutzrecht antwortet darauf mit einer Re-Internalisierung dieser externalisierten Risiken: Die Re-Internalisierungen werden dann in der Form von Compliance-Risiken den Datenverarbeitern, also den verantwortlichen Stellen einerseits und den Auftragsverarbeitern andererseits, aufgebürdet.

Diese Vorstellung von Datenschutz und Datenschutzrecht lässt sich nicht nur historisch herleiten (vgl. Pohle 2019), sondern ist auch so in der EU-Datenschutzgrundverordnung verkörpert, die in Artikel 1 den Gegenstand und die Ziele der Verordnung statuiert. In Absatz 1 heißt es: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten." Das heißt, Menschen – natürliche Personen im Recht – sollen *bei* der Verarbeitung personenbezogener Daten geschützt werden. Hierin zeigt sich die klar konsequentialistische Vorstellung, die dem zugrunde liegt. In Absatz 2 heißt es weiter: „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen" – als unerwünschte Auswirkungen werden hier also Risiken für die Grundrechte und Grundfreiheiten von Menschen problematisiert, und die Verordnung zielt darauf ab, vor diesen Risiken zu schützen.

Die Regelungsarchitektur des Datenschutzrechts, der die Datenschutzgrundverordnung folgt, ist durch drei zentrale Eigenschaften gekennzeichnet (vgl. Pohle 2022a).

Erstens werden Pflichten für die Verantwortlichen und die Auftragsverarbeiter formuliert, die nach objektiven Kriterien und unabhängig vom Wissen und Wollen der Betroffenen umgesetzt werden müssen, während die betroffenen Personen Rechte haben, hingegen keine Pflichten.

Zu den Pflichten der verantwortlichen Auftragsverarbeiter gehören zweitens ganz zentral Anforderungen an die Gestaltung, die Durchführung und den Betrieb von Verarbeitungstätigkeiten und die dafür eingesetzten Mittel, also sowohl die Organisationsstrukturen und -prozesse als auch die informationstechnischen Systeme.

Das dritte Merkmal der rechtlichen Umsetzung ist die Institutionalisierung der externen Aufsicht und Kontrolle in einer Behörde, die eigene Kontrollrechte hat, und nicht nur solche, die sich aus den Rechten der Betroffenen ableiten.

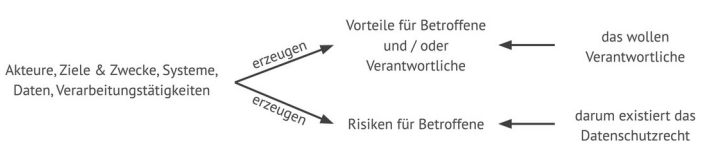
Das Problem besteht darin, dass diese konzeptionelle Orientierung an den Auswirkungen, die der Verordnung zugrunde liegt, im Regelungsdickicht der Einzelpflichten verschwindet. Das ist durchaus ein grundsätzliches Problem, das sich im Zusammenhang mit Prozeduralisierung immer wieder zeigt und das in der Rechtswissenschaft auch ausführlich diskutiert wird: Die Prozeduralisierung kann den materialen Kern des Rechts invisibilisieren (vgl. Eder 1987; Zalnieriute 2023).

3.2 Datenverarbeitung, Risiken und Risikobewältigung

Wenn wir uns den Zusammenhang von Datenverarbeitung und ihren Auswirkungen, sowohl den erwünschten als auch den unerwünschten, anschauen, dann müssen wir zwei Fälle unterscheiden: den abstrakten – oder allgemeinen – und den konkreten Fall.

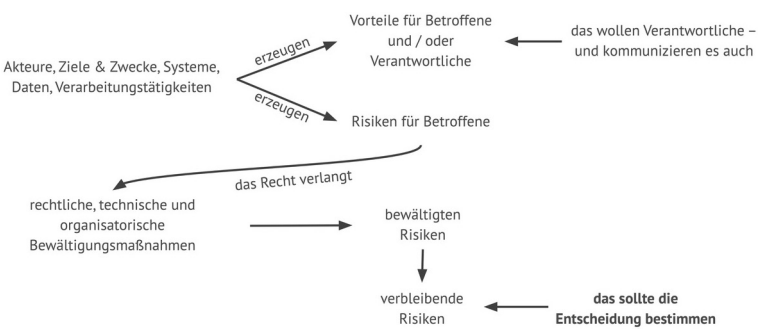
Generell unterscheidet das Datenschutzrecht zwischen Akteuren, den von ihnen verfolgten Zielen und Zwecken, den eingesetzten informationstechnischen Systemen, den verarbeiteten Daten sowie den Verarbeitungstätigkeiten. Das Recht nimmt wahr, dass zwei Arten von Auswirkungen erzeugt werden: Einerseits werden Vorteile erzeugt, erwünschte Auswirkungen, zumindest für die Verantwortlichen, möglicherweise auch für die Betroffenen. Andererseits werden unerwünschte Auswirkungen für die Betroffenen erzeugt. Im Verständnis der Datenschutzgrundverordnung handelt es sich dabei um Risiken für deren Grundrechte und Freiheiten. Die Vorteile sind es, um deren Willen die Verantwortlichen diese Datenverarbeitung typischerweise durchführen. Und sie sind es ganz oft auch, mit denen die Verantwortlichen gegenüber den Betroffenen dann die Durchführung der Datenverarbeitung rechtfertigen oder, wenn sie um Einwilligung bitten, auch damit werben. Die Risiken für Betroffene, die durch diese Verarbeitungstätigkeiten erzeugt werden, sind dann die Rechtfertigung für die Existenz des Datenschutzrechts (vgl. Abb. 1).

Abb. 1: Informationsverarbeitung und ihre Risiken: der allgemeine Fall



Grundsätzlich sieht das Bild ganz ähnlich aus, wenn wir uns eine einzelne, konkrete Informationsverarbeitung anschauen. Wir können die gleichen Strukturelemente identifizieren: die Akteure, ihre Ziele und Zwecke, die informationstechnischen Systeme, die Daten und die Verarbeitungstätigkeiten, die einzeln oder im Zusammenspiel Vorteile und Risiken erzeugen (vgl. Abb. 2). Und in diesem konkreten Fall findet das Datenschutzrecht dann schon Anwendung und erzwingt von den Verantwortlichen die Identifikation dieser Risiken für die Betroffenen und ihre Bewertung, aber vor allem auch ihre Bewältigung (vgl. Art. 24 Abs. 1 und 25 Abs. 1, Art. 35 Abs. 1 und 7 sowie, wenn auch beschränkt auf IT-Sicherheitsaspekte, Art. 32 Abs. 1 und 2 DSGVO). Diese Bewältigung soll dann durch die geeignete Auswahl und den Einsatz von rechtlichen, technischen und organisatorischen Schutzmaßnahmen erfolgen. Dieser Einsatz der Bewältigungsmaßnahmen führt dann dazu, dass mindestens ein Teil der Risiken wirksam bewältigt wird. Was dann nach der wirksamen Bewältigung von den Ursprungsrisiken übrig bleibt, sind die verbleibenden Risiken.

Abb. 2: Informationsverarbeitung und ihre Risiken: der konkrete Fall



Die Konsequenz daraus ist offenkundig: Vor dem Hintergrund der expliziten Zielsetzung der Datenschutzgrundverordnung sollten es gerade diese verbleibenden Risiken sein, die die Entscheidung für oder gegen die Datenverarbeitung bestimmen – für die Verantwortlichen, wenn sie sich auf ihr berechtigtes Interesse nach Artikel 6 Absatz 1 lit. f DSGVO als Rechtsgrundlage stützen, aber gerade auch für die Betroffenen, wenn es um ihre Einwilligung nach Artikel 6 Absatz 1 lit. a DSGVO und damit für oder gegen die Preisgabe personenbezogener Daten geht (vgl. Abb. 2).

4. *Der Straßenverkehr als Zieldomäne von Analogien in der Risikokommunikation im Datenschutz*

Im folgenden Teil wird der Beitrag den Bereich des öffentlichen Straßenverkehrs, seine Regulierung sowie die Rechtsdurchsetzung als Zieldomäne für Analogien für die Risikokommunikation im Datenschutz einführen, plausibilisieren und anhand von Beispielen diskutieren.

Der Zusammenhang zwischen Straßenverkehr und Straßenverkehrsrecht ist vielleicht nicht die erste Zieldomäne für Analogien im Datenschutzbereich, die sich aufdrängt. Naheliegender scheinen Analogisierungen von Datenschutz und Umweltschutz bzw. von Datenschutzrecht und Umweltschutzrecht – und diese finden durchaus Verbreitung. Hans-Peter Gassmann hat der modernen Informationsverarbeitung und insbesondere den internationalen Datenflüssen zugeschrieben, sie würden die „Gefahr der Verschmutzung unserer Informationsumwelt" bergen (Gassmann 1976). Kenneth Cukier hat in einer ähnlichen Bildsprache den Gegenstand, der zu regulieren sei, als „data exhaust" bezeichnet (Economist 2010). Vor allem hat die Forderung nach Übertragung von Konzepten aus dem einen in das andere Rechtsgebiet eine größere Zahl von Anhänger:innen gefunden (vgl. etwa Hirsch 2006; Froomkin 2015; Pohle 2020).

Der Straßenverkehr ist in der Vergangenheit mindestens einmal ganz explizit als Zieldomäne von Analogien im Datenschutz benutzt worden, als Rudolf Schomerus 1981 einen Beitrag in der Zeitschrift für Rechtspolitik veröffentlichte, der schon im Titel die Frage aufwarf, was das Regulierungsziel sein solle: „Datenschutz oder Datenverkehrsordnung?" (Schomerus 1981). Schomerus lehnte jedenfalls eine Konzeption des Datenschutzrechts als „ein Recht zur Regelung von Informationsbeziehungen" (Schomerus 1981, S. 294) vehement ab. Abgesehen von diesem Beispiel scheint es keine Arbeiten zu geben, die Analogien zwischen Datenschutz und Straßenverkehr herstellen oder diskutieren.

4.1 Gemeinsamkeiten und Unterschiede von Straßenverkehr und moderner Datenverarbeitung

Der Straßenverkehr und die Datenverarbeitung weisen in ihrer Entwicklung und gesellschaftlichen Bedeutung einige strukturelle Parallelen, aber auch deutliche Unterschiede auf.

Beide Bereiche sind stark technisiert. Die Technisierung des Straßenverkehrs ist materiell gebunden – Straßen, Fahrzeuge, Ampeln und andere

Verkehrszeichen sind ihre materialisierten Formen – und auch deshalb deutlich wahrnehmbar. Die Technisierung der Datenverarbeitung vollzieht sich hingegen deutlich weniger sichtbar, ob in Prozessoren oder Arbeitsspeichern, Algorithmen oder Software, Cloud-Systemen oder anderen vernetzten Infrastrukturen, auch wenn die Prozessoren, Computer oder Kabel natürlich materielle Objekte sind.

In beiden Bereichen besteht eine hohe gesellschaftliche Erwünschtheit. Mobilität gilt als Grundvoraussetzung für individuelle Freiheit und wirtschaftliche Aktivität. Ganz ähnlich wird die moderne Datenverarbeitung als Motor für Effizienz, Innovation und Komfort betrachtet.

Die Risiken scheinen sich in ihrer Art zu unterscheiden: Der Straßenverkehr erzeugt unmittelbare, direkt wahrnehmbare Probleme wie Unfälle, Abgas- und Lärmbelastung, deren Verursacher meist eindeutig benennbar sind. Demgegenüber scheinen die Risiken der Datenverarbeitung eher unsichtbar und systemisch zu sein – gängige Diskurse framen die Risken dann als „Überwachung" (vgl. Christl 2014; Newell 2023), „algorithmische Diskriminierung" (vgl. Cofone 2019), „Verhaltenssteuerung" (vgl. Christl/Spiekermann 2016) oder als gesellschaftliche Abhängigkeiten von globalen Tech-Infrastrukturen (vgl. Lambach/Oppermann 2022).

In beiden Gegenstandsbereichen besteht ein Spannungsverhältnis zwischen Nutzen und Risiken. Im Straßenverkehr scheint es erfolgreich eingehegt. Im Hinblick auf die Datenverarbeitung scheint eine solche Einhegung eher fragwürdig.

4.2 Gemeinsamkeiten von Straßenverkehrsrecht und Datenschutzrecht

Die Parallelen zwischen den beiden Gegenstandsbereichen sind tatsächlich bemerkenswert – und sie erstrecken sich auch auf deren Regulierung. In beiden Bereichen geht es um gesellschaftlich erwünschte Tätigkeiten – Mobilität einerseits, Informationsverarbeitung andererseits –, die aber potenziell negative Folgen erzeugen können und deshalb einer Risikoregulierung unterliegen. Sowohl die Straßenverkehrsordnung als auch das EU-Datenschutzrecht verfolgen den Ansatz, diese Risiken nicht erst im Nachhinein zu sanktionieren, sondern durch präventive Anforderungen zu begrenzen. Im Straßenverkehr geschieht dies durch Verhaltensnormen wie vorausschauendes Fahren, Rücksichtnahme und die Pflicht, Gefährdungen möglichst zu vermeiden (vgl. § 1 Abs. 1 und 2 StVO). Im EU-Datenschutzrecht wird ein strukturell ähnliches Prinzip angewendet: Verantwortliche

müssen Risiken für Grundrechte und Grundfreiheiten der Betroffenen identifizieren und bewerten, geeignete Schutzmaßnahmen wählen und ihre Systeme so gestalten, dass Risiken möglichst gar nicht erst entstehen oder zumindest minimiert werden (vgl. Art. 24, 25 und 35 DSGVO). Beide Regime verlangen also Umsicht, Verantwortungsbewusstsein und technische wie organisatorische Vorkehrungen, um die aus der jeweiligen Tätigkeit resultierenden Risiken zu reduzieren. Nur mit dieser Risikoreduzierung können die gesellschaftlich erwünschten Tätigkeiten auch tatsächlich gesellschaftlich akzeptabel gemacht werden (vgl. Podlech 1988).

Das Straßenverkehrsrecht versteht Risiken dabei als objektive Merkmale dieser Form von Mobilität, nicht nur als Folge von subjektiven Fehlern von Teilnehmenden am Verkehr. Das Straßenverkehrsrecht ist geprägt durch objektives Recht, nicht durch subjektive Rechte, etwa von Verkehrsteilnehmenden. Die Durchsetzung der Straßenverkehrsordnung erfolgt in erster Linie durch Dritte – die Polizei –, nicht durch Selbstregulierung der Verkehrsteilnehmenden. Sie erfolgt auch nicht durch zivilrechtliche Durchsetzung von Abwehr- oder Schutzrechten, etwa durch die Fußgänger:innen, die Schwächsten im Verkehr. Das Straßenverkehrsrecht folgt grundsätzlich einem risikobasierten Ansatz, genau wie die EU-Datenschutzgrundverordnung. Danach werden einem größeren Fahrzeug oder einer höheren Geschwindigkeit größere Risiken zugeordnet oder zugetraut, und das geht mit mehr und höheren Pflichten einher.

Es gibt eine konzeptionelle Unterscheidung zwischen Selbst- und Fremdschutz, das heißt zwischen dem Schutz von Fahrer:innen und anderen Insassen, etwa bei einem Unfall, und dem Schutz von Dritten. Ersteres ist vergleichbar mit der IT-Sicherheit, letzteres hingegen, das dem Schutz vor den Fahrer:innen dient, entspricht dem Datenschutzrecht. Und beide, der Schutz der Fahrer:innen und anderen Insassen sowie der Schutz vor den Fahrer:innen, führen zu möglicherweise konfligierenden Maßnahmen.

Das Straßenverkehrsrecht enthält auch Regelungen, deren Äquivalent im Datenschutzrecht als „Verbot mit Erlaubnisvorbehalt“ bezeichnet wird: § 2 Abs. 1 StVG („Fahrerlaubnis und Führerschein“) und § 21 StVG („Fahren ohne Fahrerlaubnis“) finden ihre Entsprechung in Art. 6 Abs. 1 DSGVO („Rechtmäßigkeit der Datenverarbeitung“). Danach dürfen personenbezogene Daten nur dann verarbeitet werden, wenn die Verantwortlichen nachweisen können, dass die Datenverarbeitung rechtmäßig ist. Nach dem Straßenverkehrsgesetz darf man nur dann – jedenfalls mit einem Fahrzeug – am Straßenverkehr teilnehmen, wenn man eine Fahrerlaubnis hat, also

nachgewiesen hat, dass man in der Lage ist, sicher und vorausschauend am Straßenverkehr teilzunehmen.

Der wesentliche Unterschied zwischen Straßenverkehr und „Datenverkehr" liegt weniger im Prinzip der Regulierung als in der Natur der Risiken selbst, die dann wiederum Auswirkungen auf die Erfüllung der gesetzlichen Vorgaben und deren Durchsetzung, vor allem aber auch auf die Wissensvermittlung und Handlungsbefähigung haben: Während die Gefahren im Straßenverkehr konkret, lokal und seit Langem verstanden sind, sind die Risiken der Datenverarbeitung oft abstrakter, global verteilt und dynamisch, was die Umsetzung – und Durchsetzung – der eigentlich ähnlichen Grundlogik der Vorsorge komplizierter macht. Zwar sind beide Rechtsbereiche Formen der präventiven Risikoregulierung, die auf vorausschauendes Handeln und die Minimierung unvermeidbarer Belastungen setzen, aber die fehlende Konkretheit und die Nicht-direkte-Wahrnehmbarkeit von Datenverarbeitung und ihren Risiken verhindert eine direkte Übertragung in lebensnahe Aufklärung sowie Handlungsvorgaben – oder kann leicht in die Irre führen, wenn eine solche Übertragung dennoch vorgenommen wird.

Die zunehmende Zahl von Elektrofahrzeugen bedeutet, dass einige der traditionellen Methoden zur Risikoerkennung und -bewertung nicht mehr so gut funktionieren wie früher. Dazu gehören etwa die auf Geräuschen basierenden Methoden, die auf der Annahme basieren, dass etwas, das lauter ist, auch schneller oder schwerer ist – und dass beides dann indiziert, dass es sich um risikoreichere Verkehrsteilnehmer handelt. Das lässt sich jetzt nicht mehr in der gleichen Art und Weise aufrechterhalten, weil Elektrofahrzeuge ungleich leiser sind als Fahrzeuge mit Verbrennungsmotoren. Und das heißt, dass wir auch im Straßenverkehr – obwohl extrem materiell – durch den Einsatz von Elektrofahrzeugen eine Verschiebung zu nicht mehr direkt wahrnehmbarer Riskanz sehen. In der Folge wird sich auch die Aufklärung zu den Risiken im Straßenverkehr darauf einstellen müssen.

Im Ergebnis zeigt sich, dass sich in den Gegenstandsbereichen Straßenverkehr und Datenverarbeitung sowie in den Regulierungsbereichen Straßenverkehrsrecht und Datenschutzrecht nicht nur Entsprechungen zwischen einer Vielzahl von Elementen finden lassen, sondern gerade auch zwischen den Beziehungen von Elementen zueinander – den Strukturen der Bereiche. Dazu zählen zuvorderst die Beziehungen zwischen der Gestaltung und dem Gebrauch der technischen Artefakte und den dabei erzeugten Risiken, aber auch die Beziehungen zwischen den abstrakten bzw. generellen Risiken in den jeweiligen Bereichen insgesamt und den konkre-

ten Risiken, die kontext- und praxisabhängig sind. Dazu zählen aber auch die Beziehungen zwischen den Elementen der Gegenstandsbereiche und ihren Gegenstücken in den Regulierungsbereichen: Schutz von Dritten, tendenziell Schwächeren, die von der konkreten Fahrweise eine:r Fahrer:in oder Verarbeitungstätigkeit eine:r Verantwortlichen betroffen sind, Anforderungen an die sowohl prospektive wie präventive – also vorausschauende wie Folgen verhütende – Gestaltung und Praxis, aber auch Aufsicht und Kontrolle durch von den Risikoverursacher:innen unabhängige Stellen. Es ist demnach äußerst plausibel, dass sich der Straßenverkehr und seine Regulierung als Zieldomäne für Analogien im Bereich des Datenschutzes und des Datenschutzrechts sowie der entsprechenden Risikokommunikation eignen.

5. Verbreitete Fehlbeschreibungen und schlechte Analogien in der Risikokommunikation zum Datenschutz

Im folgenden Teil des Beitrags werden überblicksartig verbreitete Analogien sowie Metaphern, Vergleiche, Personifikationen und, etwas allgemeiner, Beispiele eingeführt, die in der Risikokommunikation im Datenschutz eine gewisse Verbreitung haben. Diese werden dann vor dem Hintergrund der im dritten Teil ausgeführten Vorstellungen zum Datenschutz und der im vierten Teil ausgeführten Plausibilisierung für die Nutzung des öffentlichen Straßenverkehrs als Zieldomäne für Analogien einer Kritik unterzogen.

5.1 Negativbeispiele

Sehr weit verbreitet ist die Verwendung von Begriffen mit stark negativer Konnotation. Da wird etwa von „Missbrauch“ gesprochen, wenn es um die Verarbeitung von Daten geht, von „Datenmissbrauch" oder „Missbrauch von Daten“ (Zehl 2025). Da werden die Erhebung und Verarbeitung von Daten als „Überwachung“ bezeichnet, wenn dabei technische Mittel eingesetzt werden (Marx 2002). Da ist von „Angriffen“ und „Angreifer:innen“ die Rede (differenzierend und kritisch: Hansen u.a. 2022). Selbst dort, wo die Begriffe Termini technici sind (vgl. Pohle 2022b), vermitteln sie nicht, dass es um alltägliche Risiken von alltäglichen Datenverarbeitungen geht, sondern sie transportieren bestimmte Formen von Datenverarbeitung als Ausnahmezustand.

Das gilt nicht nur für die Datenverarbeitung als Tätigkeit oder Prozess, sondern auch für die Benennung oder Beschreibung derjenigen Akteur:innen, die als Verursacher:innen oder Auslöser:innen von Risiken in diesem Bereich, also als Risikoquelle, identifiziert werden. Das sind dann etwa „Hacker", „Cyberkriminelle", „Identitätsdiebe" oder „Datenkraken". Dass die meisten Risiken nicht von solchen externen, gar noch böswillig agierenden Einzelpersonen erzeugt werden, wie etwa Zehl (2024) glauben macht, sondern von den datenverarbeitenden Organisationen selbst (vgl. Rost 2017; Hansen u.a. 2022), wird damit ausgeblendet.

Zugleich werden Risiken oft sehr eng beschrieben. Wenn Beteiligte in einer kollaborativen Datenschutz-Folgenabschätzung nach „privacy risks" gefragt werden, dann darf man sich eigentlich nicht wundern, wenn den Beteiligten nur Risiken für die Privatsphäre einfallen (so aber Friedewald u.a. 2022) – das Framing invisibilisiert ganz explizit die Risiken jenseits der Privatsphäre. An vielen Stellen ist zu fragen, ob es sich überhaupt um echte Risikobeschreibungen handelt – oder nicht einfach nur um Anschlusshandlungen. Das sind Handlungen, die dadurch ermöglicht werden, dass vorher etwas getan wurde oder passiert ist. Ein Beispiel ist: „Jemand kann etwas über Dich herausfinden." Das ist – außerhalb eines sehr engen Geheimnisverständnisses, das aber leider weit verbreitet ist und sehr offensiv kommuniziert wird (vgl. etwa Zehl 2025) – erst einmal keine Risikobeschreibung, denn in den meisten Fällen werden die eigentlichen Risiken wiederum erst als Folgen des Geheimnisbruchs verstanden (vgl. Seiling u.a. 2024). Diese Vermischung von Anschlusshandlungen und dem, was dann als die eigentlichen Risiken ausgeflaggt werden, führt zu einer Risikoflut, die sich von Angstmache nicht unterscheiden lässt. Das kann auf die Betroffenen lähmend wirken und die Handlungsfähigkeit effektiv einschränken.

Darüber hinaus werden Organisationen oft personifiziert (vgl. Lukat/Sayman 2025). So wird etwa die Datenverarbeitung durch Unternehmen wie KI-Anbieter beschrieben als: „Stell dir vor, du hast einen neuen Mitbewohner. [...] Jetzt stell dir vor, dieser Mitbewohner schaut dir bei allem zu…" (Wieland 2025). Einerseits ist das problematisch, weil es die Risiken möglicherweise kleiner darstellt, als sie es vielleicht sind. Immerhin bleibt es ja sprachlich in einem familiären Rahmen. Auf der anderen Seite wird hier in der Risikobeschreibung auf Personen verwiesen. Dabei wird jedoch die Datenverarbeitung, die vom KI-Anbieter vorgenommen wird, überhaupt gar nicht mit Hilfe von Menschen durchgeführt. Stattdessen sind es einzig und allein Computer – Maschinen, Software, Algorithmen –, die irgendwelche Daten erheben, speichern, verarbeiten und nutzen. Indem

dann der KI-Anbieter – oder ein anderes Unternehmen, das Daten verarbeitet, oder bestimmte Apologeten (vgl. Posner 2005) – darauf verweist, dass es eben gerade nicht Menschen sind, die irgendetwas herausfinden, sondern rein maschinelle Verarbeitungsschritte, wird einer möglicherweise berechtigten Kritik an bestimmten Verarbeitungen oder ihren Auswirkungen der Boden unter den Füßen weggezogen.

Eine andere verbreitete Metapher ist die des Selbstschutzes, im Datenschutzbereich oft „Selbstdatenschutz" genannt. Andere durchaus gängige Bezeichnungen sind „digitale Selbstverteidigung", „Datenachtsamkeit" oder auch „digitale Mündigkeit". Unter Verwendung dieser Metaphern werden Pflichten, die laut Gesetz die Verantwortlichen treffen, fälschlicherweise auf die Betroffenen verlagert (Pohle 2022a). Vordergründig werden die Betroffenen mit derart gelabelten Materialien dabei unterstützt, sich selbst zu schützen (siehe etwa Digitalcourage o.J.), aber zugleich wird dadurch deutlich kommuniziert, dass es eine Pflicht zum Selbstschutz gebe. Diese Pflichtenverschiebung findet auch statt, wenn für bestimmte Werkzeuge, damit geworben wird, dass diese Werkzeuge Menschen helfen, sich selbst zu schützen. Das gilt etwa für manche Werkzeuge aus dem Bereich der „Privacy-Enhancing Technologies" (vgl. Karaboga u.a. 2014).

Nicht zuletzt werden Daten mit fließendem Wasser oder fließendem Geld verglichen. Es wird von Datenflüssen gesprochen (früh schon McGuire 1979), manchmal auch: „Daten wollen fließen". Letzteres ist zugleich eine Personalisierung, eine Unterstellung von Intentionalität und eine „Naturalisierung" der Daten (vgl. Ueberschär 2018). Leider ist es auch eine falsche Beschreibung, eine unpassende Metapher und eine schlechte Analogie.

5.2 Kritische Reflektion

Im Folgenden nutzen wir Analogien zum Straßenverkehr und seiner Regulierung, um diese Falschdarstellungen und Missinterpretationen zu kritisieren.

Verursacher oder Auslöser von Risiken, die mit der Datenverarbeitung einhergehen, als Hacker, Cyberkriminelle oder Identitätsdiebe zu bezeichnen ist vergleichbar damit, als Hauptverursacher von Verkehrsrisiken Autobomber und Amokfahrer zu identifizieren – und nicht etwa rücksichtslose Autofahrer oder ausbeuterische Arbeitsbedingungen, die zu überlasteten, übermüdeten und damit unvorsichtigen Fahrern führen.

Pflichten auf Betroffene zu verlagern, die eigentlich Verantwortliche erfüllen müssten, insbesondere die Pflicht, sich selbst zu schützen, ist so, als würde von Fußgänger:innen verlangt werden, Vollkörper-Airbags zu tragen, und ihnen, wenn sie das unterlassen, die Schuld dafür geben, dass sie sich selbst gefährden (vgl. zur Responsibilisierung, Gray 2009).

Die Rollenvermischung, in der von den Nutzer:innen verlangt wird, dass sie „Digital Literacy" oder „Data Literacy" besitzen oder erwerben müssen, etwa in Form eines „Internetführerscheins", ist durchaus vergleichbar mit der Forderung nach einem Führerschein für Fußgänger:innen.

Die Forderung nach Selbstregulierung, die immer wieder erhoben wird (zur Diskussion über die unterschiedlichen Maße von „Selbst" in „Selbstregulierung", siehe Hornung 2018), ist nicht nur problematisch, weil sie denjenigen, die die Risiken auslösen, auch noch Macht darüber gibt, zu bestimmen, wie die Risiken adressiert werden sollen. Der direkte Vergleich mit dem Straßenverkehr zeigt, dass natürlich insbesondere nicht die Raser:innen darüber bestimmen dürfen, was als Verkehrsverstoß zu werten ist und was nicht.

Die in Datenschutzerklärungen von Webseiten- und -dienstanbietern sehr häufig zu findende Aussage, wonach die Verantwortlichen die Regeln der Datenschutzgrundverordnung einhalten, vermittelt eine vergleichbare Botschaft wie Aufkleber, die Transportunternehmen auf die Rückseite ihrer Lkws kleben, auf denen steht: „Wir halten die Regeln der Straßenverkehrsordnung ein." Und IT-Sicherheitsmaßnahmen, die ausschließlich getroffen werden, um die Datenverarbeitung vor externen Angreifer:innen zu schützen, als Datenschutzmaßnahmen zu verkaufen, ist gerade so, als würden Überrollbügel in Fahrzeugen als Mechanismen zum Schutz von Fußgänger:innen dargestellt werden.

Und nicht zuletzt sind Informationen und Warnungen selbst noch keine Maßnahmen zur Risikobewältigung: Ein Aufkleber auf einem Lkw, „Vorsicht, Lkw!", ändert an der Riskanz des Lkws rein gar nichts.

6. Abschluss und Ausblick

Der Beitrag hat gezeigt, dass Analogien ein sinnvolles Mittel für die Risikokommunikation im Datenschutzbereich sind. Hierfür wurde das Konzept der Analogien eingeführt und von anderen, ähnlichen Konzepten abgegrenzt. Vor dem Hintergrund der Darstellung dessen, was Datenschutz ist, wozu er dient und wie er im europäischen Datenschutzrecht umgesetzt ist,

hat der Beitrag gezeigt, dass es eine Vielzahl konzeptioneller und relationaler Ähnlichkeiten zwischen dem Sachverhalt und der rechtlichen Regelung zwischen Datenschutz und Datenschutzrecht einerseits und dem öffentlichen Straßenverkehr und dem Verkehrsrecht andererseits gibt. Es zeigt sich, dass der öffentliche Straßenverkehr und seine Regulierung, jedenfalls im deutschen Recht, eine geeignete Zieldomäne für Analogien aus dem Bereich des Datenschutzes und seines Rechts ist. Das gilt gerade auch für die Risiken, die die jeweils gesellschaftlich erwünschten Techniken und Praktiken erzeugen können, und die daran anschließende Risikokommunikation. Im Folgenden werden vier offene Forschungsfragen formuliert.

Die erste betrifft Legal Design Patterns (vgl. Koulu u.a. 2021; Koulu/Pohle 2024) und die Frage, ob diese ein geeignetes Instrument zur Nachweisführung sind, dass konkret gewählte Analogien tatsächlich über funktionsgleiche Strukturen zwischen Gegenstands- und Regulierungsbereich verfügen. Die These könnte hier lauten, dass Quell- und Zieldomäne in diesem Fall von den gleichen rechtlichen Entwurfsmustern geprägt werden. Zugleich ließe sich damit untersuchen, wie weit die Analogisierung von Datenverarbeitung und Straßenverkehr, ihren Risiken und ihren Risikobewältigungsansätzen trägt, wo sie an ihre Grenzen stößt, und welche Aspekte auf der Seite der Datenverarbeitung dadurch möglicherweise nicht hinreichend oder passgenau erfasst werden können.

Die zweite Frage lautet, ob sich der Vermittlungsansatz über die Analogien auch verwenden lässt, um damit ganz grundsätzlich zu zeigen, dass wir uns von einer Fixierung auf inhärente Eigenschaften von Datenverarbeitungen lösen sollten und die Auswirkungen in den Mittelpunkt der Aufmerksamkeit stellen müssen. Es sollte also nicht mehr um die Datenverarbeiter, die Verantwortlichen, bestimmte Zwecke oder die verarbeiteten Daten oder bestimmte Verarbeitungsformen gehen, etwa die Nutzung von „KI“ oder den Verweis auf bestimmte Pflichten von Verantwortlichen. Stattdessen muss das Datenschutzrecht ganz explizit als Umsetzung eines konsequentialistischen Ansatzes verstanden werden. In diesem Ansatz geht es im Kern darum, wie Risiken aus den inhärenten Eigenschaften der Datenverarbeitung für Grundrechte und Grundfreiheiten entstehen und inwieweit diese Risiken dann wieder bewältigt werden .

Die dritte Frage betrifft die Wahrnehmung sprachlicher Bilder durch verschiedene Zielgruppen, beispielsweise durch Nutzer:innen und Expert:innen, Jüngere und Ältere, aber auch Menschen in verschiedenen sozialen Bereichen. Damit Analogien und andere sprachliche Bilder ihre verständnisgenerierende Wirkung entfalten können, müssen sie von den Rezipi-

ent:innen interpretiert und verstanden werden. Dabei könnten sie je nach Zielgruppe durchaus unterschiedlich interpretiert werden, sodass unterschiedliche Schlüsse daraus gezogen werden. Bestimmte Arten von sprachlichen Bildern könnten auch besser für bestimmte Zielgruppen geeignet sein, wenn diese sie eher verstehen. Eine systematische, übergeordnete Untersuchung zur Wahrnehmung sprachlicher Bilder durch verschiedene Zielgruppen gibt es jedoch bisher nicht, wäre aber sehr wünschenswert.

Und zuletzt stellt sich viertens die Frage, wie für den Bereich des Datenschutzes nicht nur kritisierende Analogien oder die Kritik an bestehenden Analogien formuliert, sondern auch praktische und lebensnahe Handlungsanleitungen abgeleitet werden können. Das ist eine der Fragen, denen sich das Projekt „Sicher im Datenverkehr" (SID) widmet. Auf der Basis einer Sammlung, Systematisierung und Kritik gängiger Narrative zu Datenverarbeitung, Personalisierung und Datenschutz sollen in Zusammenarbeit mit Expert:innen aus der Medienbildung Narrative entwickelt werden, die phänomenologisch passender und zugleich handlungsbefähigender sind als die derzeit im Umlauf befindlichen. Die Narrative werden Teil eines interaktiven Entscheidungsbaums, der zum einen bestehende Verständnisse hinterfragen hilft und zum anderen Handlungsoptionen und -alternativen transparent und verständlich macht. Die Wahl dieses Formats ist konzeptionell begründet: Einerseits lässt sich der analogische Charakter in die Struktur eines Entscheidungsbaums integrieren und visuell darstellen, etwa durch explizite Verbindungen zwischen den Domänen. Andererseits ermöglicht der interaktive Charakter des Formats den Nutzer:innen, verschiedene Handlungsoptionen explorativ zu erproben und deren Konsequenzen nachzuvollziehen.

Danksagung

Wir danken Elena Eulitz für Ihre tatkräftige Unterstützung bei der Recherche und der Aufbereitung des Materials für den Theorieteil (2) sowie für die kritische Durchsicht des Manuskripts und viele Vorschläge zur Verbesserung. Ebenso danken wir den anonymen Reviewer:innen für ihre kritisch-konstruktiven Kommentare. Alle verbleibenden Fehler sind unsere eigenen.

Förderung / Interessen

Die diesem Beitrag zugrunde liegenden Arbeiten wurden vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) als Teil des Projekts „Sicher im Datenverkehr (SID)", Förderkennzeichen 16KIS1968, gefördert. Im Übrigen erklären die Autoren, dass sie keine konkurrierenden Interessen haben.

Literatur

Brown, Simon und Salter, Susan (2010): Analogies in science and science teaching. *Advances in Physical Education 34*(4). S. 167-169. https://doi.org/10.1152/advan.00022.2010.

Christl, Wolfie (2014): Kommerzielle digitale Überwachung im Alltag. Studie im Auftrag der österreichischen Bundesarbeitskammer. Wien: Cracked Labs – Institut für Kritische Digitale Kultur.

Christl, Wolfie und Spiekermann, Sarah (2016): *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: facultas Universitätsverlag.

Coenen, Hans Georg (2002): *Analogie und Metapher. Grundlegung einer Theorie der bildlichen Rede*. Berlin: DeGruyter.

Cofone, Ignacio N. (2019): Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*, 70(6), S. 1389–1443.

Digitalcourage (o. J.): Digitale Selbstverteidigung. Anleitung zur Selbsthilfe. https://digitalcourage.de/digitale-selbstverteidigung (besucht am 14.12.2025).

Duit, Reinders (1991): On the role of analogies and metaphors in learning science. *Science education*, 75(6), S. 649–672.

Economist (2010): Data, Data Everywhere: A Special Report on Managing Information. Interview with Kenneth Cukier. In: The Economist. London. 25. Februar 2010. URL: http://www.economist.com/node/15557443.

Eder, Klaus (1987): Die Autorität des Rechts: eine soziale Kritik prozeduraler Rationalität. *Zeitschrift für Rechtssoziologie*, 8(2), S. 193–230.

Efroni, Zohar; Metzger, Jakob; Mischau, Lena und Schirmbeck, Marie (2019): Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. *European Data Protection Law Review*, 5(3), S. 352–366. https://doi.org/10.21552/edpl/2019/3/9.

Frank, Ulrich (2015): Modelle und die Hoffnung auf eine bessere Welt. *Erwägen Wissen Ethik*, 26(3), S. 372–375.

Friedewald, Michael; Schiering, Ina; Martin, Nicholas und Hallinan, Dara (2022): Data Protection Impact Assessments in Practice. In: Katsikas, Sokratis u.a. (Hg.): *Computer Security. ESORICS 2021 International Workshops*. Cham: Springer, S. 424–443. https://doi.org/10.1007/978-3-030-95484-0_25.

Froomkin, A. Michael (2015): Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, S. 1713–1790.

Gassmann, Hans-Peter (1976): Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa. In: Dierstein, Rüdiger; Fiedler, Herbert und Schulz, Arno (Hg.): *Datenschutz und Datensicherung*. Köln: J. P. Bachem Verlag, S. 11–26.

Gentner, Dedre (1983): Structure-Mapping: A Theoretical Framework for Analogy. *Cognitive Science*, 7(2), S. 155–170.

Gentner, Dedre; Bowdle, Brian F.; Wolff, Phillip und Boronat Consuelo (2001): Metaphor Is Like Analogy. In: Gentner, Dedre; Holyoak, Keith J. und Kokinov, Boicho K. (Hg.): *The Analogical Mind: Perspectives from Cognitive Science*. Cambridge: MIT Press, S. 199–253.

Gray, Garry C. (2009): The responsibilization strategy of health and safety: neo-liberalism and the reconfiguration of individual responsibility for risk. *The British Journal of Criminology*, 49(3), S. 326–342. https://doi.org/10.1093/bjc/azp004.

Haider, Michael; Keck, Marika; Haider, Thomas und Fölling-Albers, Maria (2013): Analogiemodelle als didaktisches Mittel zur Unterstützung naturwissenschaftlicher Lernprozesse. In: Fischer, Hans-Joachim; Giest, Hartmut und Pech, Detlef (Hg.): *Der Sachunterricht und seine Didaktik. Bestände prüfen und Perspektiven entwickeln*. Bad Heilbrunn: Verlag Julius Klinkhardt, S. 147–154.

Hansen, Marit; Bieker, Felix und Bremert, Benjamin (2022): Datenschutz und Privatheitsschutz durch Gestaltung der Systeme. In: Roßnagel, Alexander und Friedewald, Michael (Hg.): *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt*. Wiesbaden: Springer, S. 259–300.

Hattie, John und Yates, Gregory C. R. (2015): *Lernen sichtbar machen aus psychologischer Perspektive*. Baltmannsweiler: Schneider Hohengehren.

Hentschel, Klaus (2010): Die Funktion von Analogien in den Naturwissenschaften, auch in Abgrenzung zu Metaphern und Modellen. In: Hentschel, Klaus (Hg.): *Analogien in Naturwissenschaften, Medizin und Technik*. Acta Historica Leopoldina Nr. 56, S: 13–66.

Hesse, Mary B. (1963): *Models and Analogies in Science*. Notre Dame: University of Notre Dame Press.

Hesse, Mary B. (2017): Models and Analogies. In: William H. Newton-Smith (Hg.): *A Companion to the Philosophy of Science*. Malden, Massachusetts: Blackwell. https://doi.org/10.1002/9781405164481.ch44.

Hirsch, Dennis D. (2006): Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law. *Georgia Law Review*, 41(1), S. 1–63.

Hornung, Gerrit (2018): Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything". In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*. Wiesbaden: Springer Vieweg, S. 315–336. https://doi.org/10.1007/978-3-658-23727-1_18.

Karaboga, Murat; Masur, Philipp; Matzner, Tobias; Mothes, Cornelia; Nebel, Maxi; Ochs, Carsten; Schütz, Philip und Fhom, Hervais Simo (2014): Selbstdatenschutz. White Paper. 2. Auflage. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. URL: https://plattform-privatheit.de/p-prv-wAssets/Assets/Veroeffentlichungen_WhitePaper_PolicyPaper/whitepaper/WP_2014_Selbstdatenschutz_2.Auflage.pdf.

Kelley, Patrick Gage; Cesca, Lucian; Bresee, Joanna und Cranor, Lorrie Faith (2010): Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. New York: Association for Computing Machinery, S. 1573–1582. https://doi.org/10.1145/1753326.1753561.

Klafki, Wolfgang (2007): *Neue Studien zur Bildungstheorie und Didaktik. Zeitgemäße Allgemeinbildung und kritisch-konstruktive Didaktik*. Weinheim: Beltz Verlag.

Koulu, Riikka; Peters, Amadeus und Pohle, Jörg (2021): Finding design patterns in law: An exploratory approach. HIIG Discussion Paper No. 2021-03. https://doi.org/10.2139/ssrn.3814234.

Koulu, Riikka und Pohle, Jörg (2024): Legal Design Patterns: New Tools for Analysis and Translations Between Law and Technology. *Digital Society*, 3, Artikel-Nr. 22. https://doi.org/10.1007/s44206-024-00109-y.

Lambach, Daniel, & Oppermann, Kai (2022): Narratives of digital sovereignty in German political discourse. *Governance*, 36(3), S. 693–709. https://doi.org/10.1111/gove.12690.

Lausberg, Heinrich (1960): *Handbuch der literarischen Rhetorik*. München: Hueber.

Lehner, Martin (2018): *Erklären und Verstehen. Eine kleine Didaktik der Vermittlung*. Bern: UTB.

Lipowsky, Frank (2020): Unterricht. In: Wild, Elke und Möller, Jens (Hg.): *Pädagogische Psychologie*. Berlin, Heidelberg: Springer. S. 69–118.

Lukat, Maximilian und Sayman, Volkan (2025): Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren. In: Friedewald, Michael; Roßnagel, Alexander; Geminn, Christian L. und Karaboga, Murat (Hg.): *Freiheit in digitalen Infrastrukturen*. Baden-Baden: Nomos, S. 243–262. https://doi.org/10.5771/9783748953371-243.

Lukat, Maximilian; Sayman, Volkan; Guagnin, Daniel und Pohle, Jörg (2025): *Zwischen Bauchgefühl und Fachwissen: Risiken personalisierter Werbung im Internet. Eine Annäherung aus Sicht von Nutzer*innen und Expert*innen.* Berlin: HIIG. https://doi.org/10.5281/zenodo.16651958.

Markauskaite, Lina und Goodyear, Peter (2014): Professional Work and Knowledge. In: Stephen Billett, Christian Harteis und Gruber, Hans: *International Handbook of Research in Professional and Practice-based Learning.* Dordrecht: Springer. S. 79–106.

Marx, Gary T. (2002): What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society*, 1(1), S. 9–29.

Marzi, Thomas und Renner, Manfred (2024). Metaphern, Analogien und Modellübertragungen. In: Marzi, Thomas und Renner, Manfred: *Das Weltbild der Circular Economy und Bioökonomie: Vorbild Natur?*. Berlin: Springer Spektrum, S. 217–233.

McGuire, Richard P. (1979): The Information Age: An Introduction to Transborder Data Flow. *Jurimetrics*, 20(1), S. 1–7. http://www.jstor.org/stable/29761693.

Morel, Victor; Iwaya, Leonardo Horn und Fischer-Hübner, Simone (2025): AI-Driven Personalized Privacy Assistants: A Systematic Literature Review. *IEEE Access*, 13, S. 160982–161002. https://doi.org/10.1109/ACCESS.2025.3609188.

Newell, Bryce Clayton (2023): Surveillance as information practice. *Journal of the Association for Information Science and Technology*, 74(4), S. 444–460. https://doi.org/10.1002/asi.24734.

Nitz, Sandra und Fechner, Sabine (2018): Mentale Modelle. In:*Theorien in der naturwissenschaftsdidaktischen Forschung*. Berlin, Heidelberg: Springer. S. 69–86.

Oberfell, Heiko; Lohrmann, Katrin und Hartinger, Andreas (2023): Lernen aus Beispielen – eine Studie zu Vergleichsprozessen von Schülerinnen und Schülern zum Hebelgesetz. *Zeitschrift für Grundschulforschung* 16. S. 427–447. https://doi.org/10.1007/s42278-023-00174-1

Pardo, Raúl und Le Métayer, Daniel (2019): Analysis of Privacy Policies to Enhance Informed Consent. Research Report n° 9262. Saint Ismier: Inria. *arXiv preprint arXiv:1903.06068*. https://doi.org/10.48550/arXiv.1903.06068.

Podlech, Adalbert (1988): Unter welchen Bedingungen sind neue Informationssysteme gesellschaftlich akzeptabel? In: Steinmüller, Wilhelm (Hg.): *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*. Frankfurt am Main: Fischer Taschenbuch Verlag, S. 118–126.

Pohle, Jörg (2019): Zu den gesellschaftlichen Auswirkungen zunehmender Verdatung und Automation: Erkenntnisse aus der Frühzeit und Hochphase der Datenschutzdebatte. In: Burzan, Nicole (Hg.): *Komplexe Dynamiken globaler und lokaler Entwicklungen. Verhandlungen des 39. Kongresses der Deutschen Gesellschaft für Soziologie in Göttingen 2018*. URL: https://publikationen.soziologie.de/index.php/kongressband_2018/article/view/1157

Pohle, Jörg (2020): On Measuring Fundamental Rights Protection: Can and Should Data Protection Law Learn From Environmental Law? In: The Global Constitutionalism and the Internet Working Group (Hg.): *Don't Give Up, Stay Idealistic and Try to Make the World a Better Place – Liber Amicorum for Ingolf Pernice*. Berlin: HIIG, S. 71–79.

Pohle, Jörg (2022a): Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In: Verbraucherzentrale NRW e.V. (Hg.): *Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung*. URL: https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-05-pohle-datenschutz-rechtsstaatsmodell-oder-neoliberale-responsibilisierung_0.pdf.

Pohle, Jörg (2022b): Framing follows business models: How major private data processors frame the privacy problem. HIIG Discussion Paper Nr. 2022/04. Berlin: HIIG. https://dx.doi.org/10.2139/ssrn.4082029.

Renkl, Alexander (2014): Toward an instructionally oriented theory of example-based learning. *Cognitive science, 38*(1). S. 1-37.

Rost, Martin (2017): Bob, es ist Bob! *FIfF-Kommunikation*, 34(4), S. 63–66.

Rost, Martin (2018): Risiken im Datenschutz. *vorgänge–Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 57*(2), S. 79-92.

Saam, Nicole J. (2009): Modellbildung. In: Stephan Kühl, Petra Strodtholz und Andreas Taffertshofer. (Hg.): *Handbuch Methoden der Organisationsforschung.* Wiesbaden: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_25.

Schomerus, Rudolf (1981): Datenschutz oder Datenverkehrsordnung? *Zeitschrift für Rechtspolitik*, S. 291–294.

Seiling, Lukas; Gsenger, Rita; Mulugeta, Filmona; Henningsen, Marte; Mischau, Lena und Schirmbeck, Marie (2024): Beware: Processing of Personal Data—Informed Consent Through Risk Communication. *IEEE Transactions on Professional Communication*, 67(1), S. 4–25. https://doi.org/10.1109/TPC.2024.3361328.

Stachowiak, Herbert (1973): *Allgemeine Modelltheorie*. Wien: Springer.

Steinmüller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph; Harbort, Uwe; Kolb, Gerhard und Schneider, Jochen (1972): Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern. BT-Drs. VI/3826, Anlage 1.

Steinmüller, Wilhelm (1976): Informationsrecht und Informationspolitik. In: Steinmüller, Wilhelm (Hg.): *Informationsrecht und Informationspolitik*. München: Oldenbourg Verlag, S. 1–20.

Steinmüller, Wilhelm (1985): Soziale Beherrschbarkeit offener Netze. In: Spies, Peter Paul (Hg.): *Datenschutz und Datensicherung im Wandel der Informationstechnologien*. Berlin: Springer-Verlag, S. 237–249.

Ueberschär, Ellen (2018): Den Atemraum der Freiheit schützen: Wie wir die Digitalisierung angstfrei nutzen können. *Böll.Thema*, 1/2018, URL: https://www.boell.de/de/2018/01/24/den-atemraum-der-freiheit-schuetzen-wie-wir-die-digitalisierung-angstfrei-nutzen-koennen (besucht am 14.12.2025).

Ueding, Gert und Steinbrink, Bernd (2011): *Grundriß der Rhetorik: Geschichte–Technik–Methode*. Stuttgart: J.B. Metzler.

von Grafenstein, Maximilian (2018): *The principle of purpose limitation in data protection laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.* Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.

Wiater, Walter (2007): *Wissensmanagement: Eine Einführung für Pädagogen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Wieland, Ron (2025): KI und Datenschutz: Wie künstliche Intelligenz unsere Privatsphäre herausfordert – und was wir dagegen tun können. deDATA.de. https://dedata.de/ki-und-datenschutz-wie-kuenstliche-intelligenz-unsere-privatsphaere-herausfordert-und-was-wir-dagegen-tun-koennen (besucht am 14.12.2025).

Zalnieriute, Monika (2023): Against Procedural Fetishism: A Call for a New Digital Constitution. *Indiana Journal of Global Legal Studies*, 30(2), S. 227–263.

Zehl, R. (2024): Der Wolf bleibt draußen. Lassen sich komplexe Themen wie Datenschutz schon kleinen Kindern vermitteln? Und ob! Und zwar, liebe Eltern, mit überraschenden Verbündeten. *Golem* vom 29. September 2024. URL: https://glm.io/187945 (besucht am 14.12.2025).

Zehl, R. (2025): Rotkäppchen und die Inferenz-Attacke. Datenschutz ist kinderleicht – wenn ein Märchen als Erklärung reicht. *Golem* vom 23. November 2025. URL: https://glm.io/201475 (besucht am 14.12.2025).

Zymner, Rüdiger (1991): *Uneigentlichkeit. Studien zu Semantik und Geschichte der Parabel*. Paderborn: Ferdinand Schöningh.

Über die Autoren

Dr. Jörg Pohle
ist Leiter des Forschungsprogramms „Daten, Akteure, Infrastrukturen: Governance datengetriebener Innovation und Cybersicherheit“ am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin. E-Mail: joerg.pohle@hiig.de

Maximilian Lukat, M.A.
ist wissenschaftlicher Mitarbeiter im Forschungsprojekt „Sicher im Datenverkehr: Alltagsnahe Veranschaulichung von Grundrechtsrisiken“ am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin. E-Mail: maximilian.lukat@hiig.de