

# Praxisbericht: Narrative als didaktisches Werkzeug in der Datenschutzbildung im Verwaltungsstudium

*Karoline Busse, Hochschule für Verwaltungswissenschaften Niedersachsen*

## *Zusammenfassung*

Die akademische Datenschutzbildung für Verwaltungskräfte an der Hochschule für Verwaltungswissenschaften Niedersachsen hat die Aufgabe, die Studierenden für den Umgang mit personenbezogenen Bürger\*innendaten aufzuklären und zu sensibilisieren. Gleichzeitig sollen die Studierenden als Privatpersonen über ihre Rechte und die Werkzeuge der DSGVO aufgeklärt und zur Durchsetzung dieser befähigt werden. In diesem Beitrag werden ausgewählte Narrative aus dem Bachelor-Modul „Datenschutzrecht“ vorgestellt, mit deren Hilfe diese Unterrichtsziele abgebildet werden.

## *1. Einleitung*

Das Datenschutzrecht und insbesondere die EU-Datenschutzgrundverordnung (DSGVO) haben in Deutschland einen schweren Stand. Immer wieder wird gerade die DSGVO als Sündenbock dargestellt, wenn es um Komplikationen in IT-Projekten und Verzögerungen in Digitalisierungsvorhaben geht, insbesondere im Bereich der öffentlichen Verwaltung.

Dass gerade Datenschutzerklärungen und Einwilligungsdialoge wie Cookie-Banner wenig zugänglich sind, liegt auch daran, dass sie nicht primär für die Nutzenden bzw. Kund\*innen von Plattformen und Diensten erstellt und gestaltet werden, sondern in erster Linie als Compliance-Instrument zwischen Datenverarbeiter und Aufsichtsbehörden, wie den Landesbeauftragten für Datenschutz verstanden werden (vgl. Schaub et al. 2017). Dies gibt Datenschutz als Sachthema einen schwierigen Stand.

Eine Möglichkeit, das Thema Datenschutz und insbesondere Datenschutzrecht zugänglicher in der Vermittlung zu machen, ist die Verwendung von Metaphern, Analogien und Narrativen. Während eine Metapher ein sprachliches Motiv von einem Bedeutungszusammenhang in einen anderen überträgt (z.B. „Datenautobahn“), handelt es sich bei einer Analogie

um eine Erläuterung eines Motivs mit Hilfe ähnlicher Verhältnisse in einem inhaltlich anderen Sachverhalt (z.B. Paketvermittlung im Postwesen und im Internet). Ein Narrativ hingegen stellt eine sinnstiftende Erzählung dar, die häufig auch Werte vermittelt (vgl. Turowski und Mikfeld 2013).

Auch wenn die Verwendung von Metaphern im größeren Kontext von Informationssicherheit und Privatheit nicht unumstritten ist (vgl. Demjaha et al. 2018), wurde sich für den Unterricht im Bereich Datenschutzrecht an der Hochschule für Verwaltungswissenschaften Niedersachsen dennoch bewusst für die Verwendung von Narrativen zur Vermittlung von Kontext und Inhalten des Datenschutzrechts (insbesondere DSGVO und NDSG) entschieden. Der erwartete Mehrwert dadurch ist ein besseres Verständnis der gesetzlichen Regelungen und wieso diese bestehen. Durch eine multiperspektivische Betrachtung des Datenschutzes sollen Studierende sowohl als Privatpersonen als auch als zukünftige Verarbeitende von personenbezogenen Daten im dienstlichen Kontext ihrer jeweiligen Behörden mit den rechtlichen Rahmenbedingungen in Kontakt gebracht werden. Außerdem wird eine gesteigerte Einprägsamkeit der Lerninhalte durch die Verwendung von zum Teil bewusst provokativen Metaphern und Narrativen angestrebt.

Dieser Praxisbericht soll die entsprechenden Narrative im Modul „Datenschutzrecht“ der Hochschule darlegen und begründen. Dazu werden zunächst der betreffende Studiengang und der zukünftige Praxiskontext der Studierenden dargestellt, bevor die Unterrichtsziele beschrieben werden. Schließlich werden vier ausgewählte Narrative aus dem Unterricht präsentiert und eingeordnet. Dadurch gibt dieser Beitrag neue Impulse für die Vermittlung von Datenschutz-Inhalten in der Bildungsarbeit, insbesondere in der höheren Bildung und Erwachsenenbildung. Die Wirksamkeit wird anhand anekdotischer Erfahrungen skizziert.

## *2. Rahmenbedingungen*

### *2.1 In der Hochschule: Das duale Studium Verwaltungswissenschaften*

Die Hochschule für Verwaltungswissenschaften Niedersachsen (HSVN) ist ein Teil des Niedersächsischen Studieninstituts für kommunale Verwaltung e.V. (NSI), einem gemeinnützigen Verein, dessen Mitglieder die Städte, Gemeinden und Landkreise des Landes Niedersachsen sowie die Region Hannover sind. Der Vereinszweck ist Aus-, Fort- und Weiterbildung, zu

diesem Zweck bietet das NSI außer dem Hochschulbetrieb auch Weiterbildungslehrgänge sowie Fortbildungen an.

Die HSVN bietet den dualen Studiengang Verwaltungswissenschaften an, der sich in die Studienzweige Kommunal-, Landes- und Kirchenverwaltung gliedert. Die Studierenden sind ausschließlich Anwärter\*innen in der Beamnt\*innenlaufbahn im Dienst der öffentlichen Verwaltung in Niedersachsen. Pro Jahr beginnen etwa 800 Studierende ihr duales Studium an der HSVN, die aus organisatorischen Gründen in Kursgruppen von etwa 30 Studierenden unterrichtet werden. Des Weiteren bietet die HSVN zwei berufsbegleitende Masterstudiengänge an, Kommunales Verwaltungsmanagement und Öffentliches Digitalisierungsmanagement. Im Folgenden soll es jedoch ausschließlich um den Unterricht im Bachelorstudium gehen.

Das Studienjahr an der HSVN ist in drei Trimester unterteilt, eines dieser Trimester ist in jedem Studienjahr ein Praxistrimester, die anderen zwei werden an der Hochschule verbracht. Der Schwerpunkt des Studiums ist Rechtsanwendung im kommunalen Umfeld, da die Studierenden nach ihrem Abschluss ein Teil der exekutiven Gewalt des Staates sein werden. Im Gegensatz zu einem rechtswissenschaftlichen Universitätsstudium wird in den Verwaltungswissenschaften an der HSVN also ein engerer Fokus auf den unterrichteten Rechtsgebieten als auch in Bezug auf die methodische Kompetenz gelegt. Ergänzend zu den Studieninhalten im Bereich Rechtsanwendung werden Soziologie und Arbeitspsychologie, Öffentliches Management und ökonomische Kompetenzen vermittelt. Nach ihrem Abschluss sollen die Studierenden flexibel von ihren Behörden eingesetzt werden können.

Das Datenschutzrecht ist Thema im dritten Studienjahr des Bachelorstudienganges Verwaltungswissenschaften. In dem 0,5 ECTS-Leistungspunkte umfassenden Teilmodul des Moduls Europarecht (zukünftig ein 1-LP Teilmodul des neu eingerichteten Pflichtmoduls Verwaltungsdigitalisierung) liegt der Fokus auf der Vermittlung der verwaltungsbezogenen Kerninhalte der DSGVO, insbesondere den Grundsätzen aus Artikel 5 sowie den Betroffenenrechten aus Artikel 12ff. Das Modul wird in Kap. 3 genauer beschrieben.

## 2.2 In der Praxis: Kommunalverwaltung in Niedersachsen

Die Kommunalverwaltung in Niedersachsen gliedert sich in zwei Ebenen, Städte und Gemeinden bilden die eine Ebene und Landkreise die andere.

Die beiden Ebenen sind für unterschiedliche Aufgaben zuständig, wobei die acht kreisfreien Städte des Landes die Aufgaben beider Ebenen bündeln. Die Region Hannover als Kommunalverband besonderer Art übernimmt dabei großteils die Aufgaben eines Landkreises.

Kommunalverwaltung zeichnet sich durch ein äußerst abwechslungsreiches Arbeitsfeld aus, das sich aus einer Vielzahl an Aufgaben (auch Verwaltungsleistungen genannt) niederschlägt. Allein rund 300 Verwaltungsleistungen stehen auf der Liste der zu digitalisierenden Dienste des Online-Zugangsgesetzes (OZG), dazu gesellen sich eine große Anzahl Pflichtleistungen, die nicht zu digitalisieren sind (beispielsweise die Eheschließung), sowie in der Regel mehrere Dutzende freiwillige, sprich in eigener Gestaltung erhobene Leistungen, z.B. Beratungsangebote oder über das Kommunalabgabengesetz festgelegte Steuern, beispielsweise auf Hotelübernachtungen. Nimmt man die internen Tätigkeiten wie IT-Betrieb, Buchhaltung und Gebäudedienste mit dazu, kommt eine Kommunalverwaltung schnell auf eine vierstellige Anzahl an Geschäftsprozessen. In der Mitarbeitendenzahl vergleichbare kleine und mittelständische Unternehmen kommen hingegen nur auf ein Zehntel oder gar ein Hundertstel dieser Prozesse. Da im Rahmen des Datenschutzmanagements prinzipiell jeder Geschäftsprozess auf die Verarbeitung personenbezogener Daten hin untersucht werden muss, ergibt sich für Kommunalverwaltungen ein substanzieller Aufwand.

Zudem wird in der Kommunalverwaltung eine hohe Bandbreite an Kategorien personenbezogener Daten (pbD) verarbeitet, insbesondere eine große Anzahl von pdD mit besonderem Schutzbedarf nach Art. 9 DSGVO. In diesem Artikel werden explizit Daten wie Gesundheitsdaten, Biometrie, Angaben zur sexuellen Orientierung, zur religiösen Überzeugung oder zur Gewerkschaftszugehörigkeit genannt, für die besondere Auflagen hinsichtlich ihres Schutzes gelten. Beispielhaft sind hier im kommunalen Kontext die Leistungen des öffentlichen Gesundheitsdienstes (Gesundheitsdaten) oder der Ein- und Austritt aus Kirchensteuer einziehenden Religionsgemeinschaften (religiöse Überzeugungen). Wenn es zudem um den Betrieb von beispielsweise Frauenhäusern und Möbelschutzräumen geht oder um Fälle von Kindeswohlgefährdung, verarbeiten Kommunalverwaltungen zudem pbD der höchsten Schutzstufe gemäß des Schutzstufenkonzepts der zuständigen Aufsichtsbehörde, des Landesbeauftragten für Datenschutz Niedersachsen (vgl. Tabelle 1). Hierunter fallen alle personenbezogenen Daten, die ein Risiko für Leib und Leben der betroffenen Personen darstellen, sollten diese Daten in falsche Hände geraten oder unbeabsichtigt veröffentlicht werden.

Während in der Privatwirtschaft üblicherweise eine Verarbeitung auf Grundlage einer Einwilligung (bspw. durch ein Cookie-Banner) geschieht, begründet sich die Datenverarbeitung in der öffentlichen Verwaltung zum Großteil aus gesetzlichen Aufträgen. Auch dieser Aspekt führt zu einer hohen Komplexität des Datenschutzmanagements in der Kommunalverwaltung. Für eine saubere Datenschutzdokumentation muss demnach jedes Fachgesetz nach einer Grundlage für die Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. c DSGVO gesichtet werden.

Durch die DSGVO haben die Aufsichtsbehörden maßgeblich an Einfluss gewonnen, das dabei stärkste Werkzeug gegen rechtswidrige Verarbeitung personenbezogener Daten ist die Verhängung von Bußgeldern, die bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr betragen kann (vgl. Art. 83 Abs. 5 DSGVO). Die niedersächsische Landesaufsichtsbehörde für Datenschutz hat dieses Mittel jedoch nicht gegenüber Kommunalverwaltungen, da nach § 20 Abs. 5 NDSG keine Bußgelder von der Aufsichtsbehörde gegen öffentliche Stellen verhängt werden können.

### *3. Ziele des Unterrichts*

Da zum Zeitpunkt der Erstellung dieses Artikels das neue Datenschutzrecht-Modul noch nicht durchgeführt wurde, wird sich im Folgenden auf das auslaufende Teilmodul bezogen. Da sich die Unterrichtsinhalte grundsätzlich eher erweitern statt fundamental verändert werden, ist davon auszugehen, dass die vorgestellten Narrative und Inhalte ihre Gültigkeit in Zukunft behalten werden.

Das Teilmodul „Grundlagen des Datenschutzrechts“ umfasst 0,5 ECTS-Leistungspunkte und damit vier Vorlesungstermine à 90 Minuten Dauer. Das Qualifikationsziel des Teilmoduls besteht darin, dass die Studierenden die zentralen Regelungsgrundsätze des Datenschutzrechts auf einfache praxisrelevante Sachverhalte anwenden können. Außerdem werden grundsätzliche Aspekte der Zulässigkeit des Umgangs mit personenbezogenen Daten im beruflichen Kontext vermittelt.

Die Inhalte des Moduls setzen sich zusammen aus der historischen Entwicklung des Datenschutzrechts, der Bedeutung des Datenschutzrechts für die öffentliche Verwaltung, den Rechtsquellen des Datenschutzrechts mit besonderem Fokus auf DSGVO und NDSG, den Grundprinzipien

des Datenschutzrechts, sowie der rechtlichen Bewertung einfacher datenschutzrechtlicher Sachverhalte.

Die davon abgeleiteten didaktischen Ziele des Unterrichts sind einerseits, den Studierenden ein Bewusstsein für die in der öffentlichen Verwaltung verarbeiteten personenbezogenen Daten von Bürger\*innen und die damit einhergehende Verantwortung zu schärfen. Hierzu gehören ebenfalls der Umgang mit von der Datenverarbeitung betroffenen Personen und deren Rechten bezüglich Transparenz, Auskunft, Korrektur und Löschung der eigenen pbD nach Art. 12-17 DSGVO und die Bearbeitung von damit zusammenhängenden Ersuchen. Andererseits handelt es sich bei den Studierenden selbst auch um Unionsbürger\*innen, sodass das zweite didaktische Ziel des Teilmoduls darin besteht, den Studierenden ihre eigenen Rechte und Möglichkeiten im Zusammenhang mit ihren eigenen personenbezogenen Daten aufzuzeigen.

Der Unterricht besteht inhaltlich aus vier Teilen, die im Lehrgespräch mit Unterstützung eines Foliensatzes, einer Analyse des Gesetzestextes sowie weiteren Quellen und Übersichten vermittelt werden. Das Modul beginnt mit der historischen Entwicklung des Datenschutzrechts in Deutschland und Europa, klärt anschließend die Grundbegriffe wie personenbezogene Daten, Anonymisierung und Pseudonymisierung, die Kernprinzipien und Betroffenenrechte nach DSGVO, sowie die praktische Umsetzung des Datenschutzmanagements in der Kommunalverwaltung nach entwickelten best practices. Auch ein Exkurs in technisch-organisatorischen Maßnahmen im Bereich der Informationssicherheit ist Teil des Moduls.

Im Themenfeld des Datenschutzmanagements in der Kommunalverwaltung wird Bezug genommen auf das Schutzstufenmodell des niedersächsischen Landesbeauftragten für Datenschutz (LfD) (siehe Tab. 1) sowie auf die von der Arbeitsgruppe kommunaler Datenschutz des Instituts für Datenschutz und Digitalisierung am NSI entwickelten Materials zum Datenschutzmanagements.

Tabelle 1: Übertragung der Schwere des möglichen Schadens auf das niedersächsische Schutzstufenkonzept (LfD Niedersachsen 2018)

| Schutzstufe | Personenbezogene Daten,                                                                                                                                                                | zum Beispiel                                                                                                                                                                         | Schwere eines möglichen Schadens |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| A           | die von den Betroffenen <i>frei zugänglich</i> gemacht wurden                                                                                                                          | Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien                                                            | Geringfügig                      |
| B           | deren unsachgemäße Handhabung zwar <i>keine besondere Beeinträchtigung</i> erwarten lässt, die aber von den Betroffenen <i>nicht frei zugänglich</i> gemacht wurden                    | beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien                                                       | Geringfügig                      |
| C           | deren unsachgemäße Handhabung den Betroffenen in <i>seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen</i> beeinträchtigen könnte („Ansehen“)            | Einkommen, Grundsteuer, Ordnungswidrigkeiten                                                                                                                                         | Überschaubar                     |
| D           | deren unsachgemäße Handhabung den Betroffenen in <i>seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen</i> erheblich beeinträchtigen könnte („Existenz“) | Anstaltsunterbringung, Strafbarkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DSGVO | Substantiell                     |
| E           | deren unsachgemäße Handhabung <i>Gesundheit, Leben oder Freiheit</i> des Betroffenen beeinträchtigen könnte                                                                            | Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm                                                                                  | Groß                             |

#### 4. Narrative und Analogien im Unterricht

Im Folgenden sollen zentrale Narrative im Unterricht des Datenschutzrechts im dualen Bachelorstudium an der HSNV vorgestellt werden.

##### 4.1 Die Kultur von Datenschutz und Privatheit gegenüber dem Staat in Deutschland: Das Narrativ des Vertrauensbruchs

Im Vergleich mit anderen EU-Ländern herrscht in Deutschland eine stark kritische zivilgesellschaftliche Haltung gegenüber der Datenverarbeitung durch die staatliche Exekutive. Um bei den Studierenden ein Bewusstsein für die Haltung der Öffentlichkeit ihrem zukünftigen Handeln gegenüber

zu schaffen und gleichzeitig bereits früh im Modulverlauf eine desillusierte Haltung zu vermeiden, beginnt die historische Aufarbeitung des Datenschutzrechts mit einer Sondierung der Beziehung zwischen Bevölkerung und Staat.

In skandinavischen Ländern wird der Staat generell als „Kümmerer“ und „Fürsorger“ gesehen, wie am Beispiel der finnischen Willkommenspakete für Neugeborene illustriert wird (vgl. Zips 2015). Doch warum ist dies in Deutschland anders? Hierzu wird ein Blick in die deutsche Geschichte geworfen. Bereits zweimal gab es hier innerhalb der letzten 100 Jahre tiefgreifende und folgenschwere Vertrauensbrüche zwischen Staat und Gesellschaft, die auch heute noch die öffentliche Haltung zur staatlichen Datenverarbeitung prägen und als Argumentation gegen geplante Maßnahmen der Bundespolitik herangezogen werden, bspw. im Kontext einer geplanten Novelle des Psychisch-Kranken-Gesetzes (DGSP 2025; Verlag Dashöfer 2025).

In den 30er und 40er-Jahren des 20. Jahrhunderts hat die Diktatur der NSDAP systematisch Menschengruppen erfasst, dokumentiert und letztendlich systematisch vernichtet. Es ist nicht übertrieben, dass hier die staatliche Verarbeitung personenbezogener Daten mehrere Millionen Menschen in Deutschland und Europa das Leben gekostet hat. Auch wenn heute die wenigsten Bürger\*innen diese Ereignisse selbst erlebt haben, stecken die Folgen doch intergenerational weiterhin in unserer Gesellschaft.

Der zweite einschneidende Vertrauensbruch in der deutschen Geschichte geschah einige Jahrzehnte später, in der DDR. Hier hat das Ministerium für Staatssicherheit (Stasi) durch gesamtstaatliche, tiefgehende Datensammlung und -auswertung in Verbindung mit Zensur, Repressalien, Haft und Folter ein psychologisches Schreckensregime etabliert, dessen Folgen auch heute noch gesellschaftlich nachhallen.

Diese Tiefpunkte der deutschen Geschichte zeigen den Studierenden, woher sich die heutige Stimmungslage der Zivilgesellschaft gegenüber staatlicher Datenverarbeitung speist und weshalb ein spezieller Druck auf den Mitarbeitenden der öffentlichen Verwaltung liegt, möglichst datensparsam, stets rechtlich korrekt und verantwortungsbewusst mit den personenbezogenen Daten von Bürger\*innen umzugehen. Nach persönlicher Wahrnehmung kann somit erreicht werden, dass die Studierenden inhaltlich Interesse am Fach behalten, ohne von den Auflagen und Pflichtaufgaben, die aus dem Datenschutzrecht erwachsen, demotiviert zu werden.

## 4.2 Verarbeitung von personenbezogenen Daten der Studierenden im Privatleben

Um Datenschutzkompetenz in Bezug auf die eigenen personenbezogenen Daten zu entwickeln, werden im Unterricht an geeigneten Stellen immer wieder Analogien in die private Sphäre gezogen. Anstatt hier jedoch auf Kategorien von personenbezogenen Daten mit hoher Schutzstufe gemäß Gesetz bzw. der für Kommunalverwaltungen verbindlichen Risikoeinstufung (vgl. Tab. 1) einzugehen, wird stattdessen auf personenbezogene Daten mit hohem persönlichem Bezug eingegangen. Da sich 61 % der Menschen zwischen 16 und 29 auf Online-Datingplattformen wie Tinder nach sexuellen und/oder romantischen Partnerschaften umsehen (Bitkom Research, 2025) und 25 % der Menschen zwischen 16 und 24 bereits einmal erotische Bilder von sich selbst per Messenger an Partner\*innen versendet haben (Kaspersky 2024), wird die umgangssprachlich „Auberginenbilder“ (nach der verbreiteten popkulturellen Symbolik des Auberginen-Emoji  als visuelle Metapher für einen Phallus) betitelte Analogie für diese Art Dating-bezogener personenbezogener Daten im Unterricht verwendet und an geeigneten Stellen aufgegriffen. Die für den hochschulischen Kontext ungewöhnliche und spontane Überbrückung der professionellen Distanz zwischen Lehrenden und Lernenden in die private Sphäre in Kombination mit der suggerierten geteilten Erfahrung schafft nach persönlicher Beobachtung zusätzliche Aufmerksamkeit unter den Studierenden, sowohl für diese Art personenbezogener Daten, den allgemeinen Schutzbedarf personenbezogener Daten, als auch für die Verarbeitung dieser Daten durch unterschiedliche Verantwortliche (Datingplattformen, Messenger-Anbieter) und mit unterschiedlichen technisch-organisatorischen Maßnahmen wie Ende-zu-Ende-Verschlüsselung. Es wird hier also weniger ein voll ausgestaltetes Narrativ verwendet, sondern mehr eine Metapher bzw. ein konkretes Datenbeispiel, um den Begriff der personenbezogenen Daten mit persönlichem Bezug zu versehen. Der weitere Kontext von pbD im Online-Dating wie Plattformökonomie oder die Auswirkungen von Datenlecks auf Betroffene wird im Rahmen des Unterrichts aus Gründen der zeitlichen Kapazität nicht weitergehend diskutiert.

#### 4.3 Verarbeitung von personenbezogenen Daten durch Studierenden im Ehrenamt: Der Sportverein als Datenverarbeiter

Ein anderes Narrativ bzw. eine Perspektive mit hohem potenziellem Bezug zum Alltag der Studierenden ist die Verarbeitung personenbezogener Daten im Kontext eines (Sport-)Vereins, also einer juristischen Person. Im Gegensatz zur Verarbeitung von pbD im Privatkontext (vgl. Art. 2 Abs. 2 lit. c DSGVO) müssen hier die gesetzlichen Regelungen beachtet werden, beispielsweise der Transparenzgrundsatz, der zur Offenlegung der Kategorien der verarbeiteten Daten und der jeweiligen Verarbeitungszwecke verpflichtet (Art. 5 DSGVO), oder die Notwendigkeit zur Einwilligung in die Verarbeitung personenbezogener Daten im Vereinskontext (Art. 6 Abs. 1 lit. a DSGVO) im Rahmen der Mitgliedschaftserklärung. Durch diese Analogie wird neben der Verarbeitung durch die öffentliche Verwaltung auch die Verarbeitung durch juristische Personen anschaulich erläutert und durch die Wahl eines Vereins als Datenverarbeiter – im Gegensatz zu den häufig als Beispiel verwendeten multinationalen Konzernen – auch eine gewisse Nähe zum Alltag der Studierenden aufgezeigt. Da die Studierenden sich sowohl als Vereinsmitglieder als auch als ehrenamtlich Tätige (beispielsweise als Trainer\*innen) in dieser Konstellation wiederfinden können, soll ein multiperspektivisches Verständnis für das Datenschutzrecht sowohl aus Betroffenen- als auch aus Verarbeitendensicht geschaffen werden. Die den Studierenden bereits bekannte Unterscheidung zwischen juristischen und natürlichen Personen im Kontext der Rechtsanwendung wird durch diese Analogie nochmals wiederholt und mit einem Praxisbeispiel unterfüttert, sodass deutlich wird, dass für die Handlungen einer natürlichen Person im Kontext einer juristischen Person eine andere Perspektive der Rechtsanwendung gilt. Dies ist auch dann der Fall, wenn sich die tatsächliche Verarbeitungstätigkeit kaum von der mit einer Ausnahme von der DSGVO belegten Verarbeitung personenbezogener Daten zu ausschließlich privaten Zwecken (vgl. Art. 2 Abs. 2 lit. c DSGVO) unterscheiden lässt.

#### 4.4 Verarbeitung von personenbezogenen Daten durch Studierenden als Mitarbeitende der öffentlichen Verwaltung: Die 15-17-15-Kombo

Der Großteil der Vorlesung Datenschutzrecht bezieht sich auf die Anwendung der DSGVO im dienstlichen Kontext. Hier ist es zentral, ein Bewusstsein für die personenbezogenen Daten von Bürger\*innen in den Händen

der öffentlichen Verwaltung und den Umgang mit ihnen zu schaffen. Da die meisten Verarbeitungstätigkeiten in der öffentlichen Verwaltung auf der Durch- und Umsetzung von Gesetzen basieren und damit anstelle der im privaten Kontext verbreiteten Einwilligung (vgl. Abschnitt 4.3) die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (vgl. Art. 6 Abs. 1 lit. c DSGVO) zum Zuge kommt, liegt sowohl im Unterricht als auch in der kommunalen Datenschutzpraxis der Fokus stärker auf der Recherche nach gesetzlicher Legitimation für eine Verarbeitung anstatt der Gestaltung von Einwilligungen.

Das wohl markanteste Narrativ in diesem Zusammenhang ist die sogenannte „15-17-15-Kombo“ im Themenfeld der Betroffenenrechte. Es geht hier im Kern um die Beantwortung von Bürger\*innenanliegen nach Artikel 12 ff. DSGVO durch die Behörde. Die genannte „Kombo“ besteht aus drei verketteten Anliegen einer betroffenen Person: Ein Auskunftersuchen über gespeicherte personenbezogene Daten der anfragenden Person nach Art. 15 DSGVO, gefolgt von einem Löschersuchen bezüglich dieser Daten nach Art. 17 DSGVO um eine Löschung von nicht mehr benötigten Daten zu erzielen, und einem anschließenden erneuten Auskunftersuchen nach Art. 15 DSGVO um diese Löschung gewissermaßen zu kontrollieren. Ein mächtiges Werkzeug für die anfragende Person und gleichzeitig eine logistische Herausforderung für eine Organisation, denn für ein allgemeines Artikel-15-Ersuchen müssen alle Prozesse und deren Datenhaltungen nach personenbezogenen Daten der betroffenen Person durchsucht und die Ergebnisse anschließend aufbereitet werden. Wie in Abschnitt 2.2 bereits dargelegt, finden in einer Kommunalverwaltung sehr viele Prozesse auf personenbezogenen Daten von Bürger\*innen statt, die in solch einem Fall nach der betroffenen Person zu durchleuchten sind. Auch das Gebot der Mitwirkung (vgl. ErwG 63 S.7 DSGVO), das dem Datenverarbeiter die Möglichkeit gibt, ein Auskunftersuchen mit einer Bitte um Präzisierung zu beantworten, kann hier nur bedingt helfen, da die anfragende Person auch bei einer Aufforderung zur Konkretisierung ihres Ersuchens darauf bestehen kann, eine Kopie aller sie betreffenden personenbezogenen Daten des Verarbeitenden zu erhalten. Ein einzelnes Artikel-15-Ersuchen kann daher bereits eine signifikante Herausforderung für eine Kommunalverwaltung darstellen, insbesondere wenn diese intern kein vollständiges Bild über die Verarbeitungstätigkeiten und zugehörigen IT-Services besitzt. Das folgende Artikel-17-Ersuchen stellt eine Herausforderung an die korrekte Führung des Verzeichnisses der Verarbeitungstätigkeiten, insbesondere der hier hinterlegten Löschfristen. Da der Großteil der Datenverarbeitung einer

Kommunalverwaltung auf gesetzlichen Grundlagen gemäß Art. 6 Abs. 1 lit. c DSGVO basiert (vgl. Abschnitt 2.2), müssen ebendiese Gesetze im Zuge der Erstellung des Verzeichnisses gründlich nach Aufbewahrungsfristen durchsucht werden. Doch nur die wenigsten Fachgesetze weisen diese Fristen explizit auf, zudem gibt es Ausnahmen und Ermessensspielräume im Kontext des Archivwesens (Bundesarchiv/BfDI 2023). Das abschließende Artikel-15-Ersuchen fungiert als Prüfmechanismus des vorangegangenen Löschersuchens und macht die Umsetzung von Artikel 17 transparent. Die betroffene Person kann durch den Abgleich mit den Ergebnissen des ersten Artikel-15-Ersuchens genau ermitteln, welche Daten in Folge des Artikel-17-Ersuchens gelöscht wurden. Des Weiteren kann die betroffene Person anhand der Ergebnisse abgleichen, ob möglicherweise Daten, die hätten gelöscht werden müssen, nicht gelöscht wurden. In diesem Falle läge eine widerrechtliche Datenverarbeitung vor, die eine Grundlage für zivilrechtliche Schadensersatzansprüche gegen die entsprechende Kommunalverwaltung bildet. Während im privatwirtschaftlichen Bereich noch das Risiko eines Bußgelds durch den Landesbeauftragten für Datenschutz (LfD) besteht, ist dies in Niedersachsen nach § 20 Abs. 5 NDSG jedoch nicht gegenüber Behörden möglich. Der LfD Niedersachsen hat dennoch verschiedene Hebel gegen eine Kommunalverwaltung, die sich von der Einsichtnahme in die Datenschutzdokumentation wie dem Verzeichnis der Verarbeitungstätigkeiten bis hin zu Untersagungen bestimmter Datenverarbeitungsprozesse erstrecken. Zudem bindet ein Gerichtsverfahren bezüglich privaten Schadensersatzes Kräfte und Ressourcen in der Kommunalverwaltung und stellt ein Risiko für das Außenbild der Verwaltung dar.

*Abbildung 1: Das zur Illustration der 15-17-15-Kombo verwendete Bild aus den Unterrichtsfolien. Public Domain via Wikimedia Commons*



Die 15-17-15-Kombo stellt also eine signifikante organisatorische Herausforderung und einen scharfen Prüfmechanismus für die Konformität der Datenverarbeitung personenbezogener Daten dar. Sie gibt dem Individuum, der von Datenverarbeitung „betroffenen Person“ ein Werkzeug, um die Machtasymmetrie im Kontext der Datenverarbeitung zumindest punktuell herauszufordern. Entsprechend wird das Szenario in der Datenschutzrecht-Vorlesung mit einer Kampfsportszene illustriert (siehe Abb. 1), denn Kampfsport erfordert genau wie ein effektives Datenschutzmanagementsystem eine gute Kenntnis der Techniken und Methoden sowie eine schnelle Reaktionszeit im Falle einer „Attacke“. Wenn eines dieser Elemente nicht funktioniert, besteht in beiden Sphären – Kampfsport und Datenschutzmanagement – ein signifikantes Risiko einer schmerzhaften Folge. Aus der Perspektive der ihre Rechte ausübenden Person wird durch das martialische Narrativ verdeutlicht, welche Wirkmacht eine Einzelperson durch die Ausübung ihrer Rechte selbst gegenüber einem als übermächtig wahrgenommenen Datenverarbeiter entfalten kann, wenn sie die richtigen Techniken, also die Ersuchen nach Artikel 15 und 17 DSGVO kennt. Wiederkehrende Beispiele für diese Datenverarbeiter im Unterrichtsgespräch

sind neben Social Media-Plattformen auch die eigene Hochschule. In den Wiederholungs- und Feedbackeinheiten der Datenschutzrecht-Vorlesung an der HSVN taucht insbesondere das Narrativ der 15-17-15-Kombo regelmäßig als markante Erkenntnis des Unterrichts auf.

## 5. Fazit

Das Vorlesungsmodul „Datenschutzrecht“ an der Hochschule für Verwaltungswissenschaften in Niedersachsen nutzt Risikonarrative maßgeblich auf zwei verschiedene Weisen. Einerseits soll durch das in Abschnitt 4.1 dargestellte Narrativ über die historisch begründete Kultur des Misstrauens gegenüber dem Staat und daraus resultierender starker Datenschutzkultur in Deutschland ein Verständnis für die Gesetzgebung in ihrer aktuellen Form erzeugt werden, andererseits soll über das bewusst martialische Narrativ zur Ausübung von Betroffenenrechten sowohl die organisatorische Perspektive seitens eines fast allumfassenden Datenverarbeiters – der Kommunalverwaltung – als auch die Wirkmacht dieser Rechte, wenn sie von Einzelpersonen wahrgenommen werden, deutlich gemacht werden. Die vorgestellten Narrative verwenden bewusst markante Bilder und Metaphern (vgl. Abschnitt 4.2), damit sie sich von den üblichen Unterrichtsinhalten in rechtswissenschaftlichen Fächern abheben und den Studierenden auch über die Laufzeit des Moduls – und vielleicht gar des Studiums – hinaus prägnant im Gedächtnis bleiben. Somit bilden sie ein vielversprechendes Instrument in der Bildungsarbeit des Datenschutzrechts.

Es gibt jedoch auch Aspekte der DSGVO, für die weitere Narrative hilfreich wären, beispielsweise den für nicht-Jurist\*innen schwer greifbaren Grundsatz der Datenverarbeitung nach Treu und Glauben (vgl. Art. 5 Abs. 1 lit. a DSGVO). Des Weiteren handelt es sich bei den in diesem Text beschriebenen Wirkungseindrücken zu den dargestellten Narrativen lediglich um anekdotische Evidenz. Eine wissenschaftliche und methodisch fundierte Evaluierung der kurz- und langfristigen Wirksamkeit dieser Narrative stellt daher einen wichtigen nächsten Schritt zu diesem Praxisbericht dar.

Derzeit wird das Modul zu Datenschutzrecht im Rahmen einer neuen Studienordnung an der HSVN überarbeitet, dabei soll auch die Strategie der Hochschule zu den Themen Blended Learning und Flipped Classroom berücksichtigt werden. Diese Umstellung böte eine gute Gelegenheit für eine empirische Analyse der Wirkung dieser Narrative unter den Studierenden, beispielsweise mit Hilfe einer qualitativen Methodik.

Literatur

- Bitkom Research (2025): *Online-Dating: 6 von 10 suchen im Netz nach weiteren Infos zu ihrem Match*. 24.03.2025, <https://bitkom-research.de/news/online-dating-6-von-10-suchen-im-netz-nach-weiteren-infos-zu-ihrem-match>.
- Das Bundesarchiv und Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2023): *Archivrecht und Datenschutz: Erläuterungen zur Abgabe von Archivgut an das Bundesarchiv*. März 2023. [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?\\_\\_blob=publicationFile&v=11](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?__blob=publicationFile&v=11).
- Schaub, Florian; Balebako, Rebecca; Cranor, Lorrie Faith (2017): "Designing Effective Privacy Notices and Controls," in IEEE Internet Computing, vol. 21, no. 3, S. 70-77, doi: 10.1109/MIC.2017.75.
- Demjaha, Albese; Spring, Jonathan; Becker, Ingolf; Parkin, Simon und Sasse, Angela (2018): „Metaphors Considered Harmful? An Exploratory Study of the Effectiveness of Functional Metaphors for End-to-End Encryption“. Conference paper presented auf Workshop on Usable Security, San Diego, CA. *Proceedings 2018 Workshop on Usable Security*, Internet Society, 2018. <https://doi.org/10.14722/usec.2018.23015>.
- Der Landesbeauftragte für den Datenschutz Niedersachsen (2018): *Schutzstufenkonzept des LfD Niedersachsen*. <https://www.lfd.niedersachsen.de/download/137188>.
- Deutsche Gesellschaft für Soziale Psychiatrie (Hrsg.) (2025): *Registrierung psychisch erkrankter Menschen: Die Deutsche Gesellschaft für Soziale Psychiatrie (DGSP e. V.) mahnt zu politischer und historischer Sensibilität*. Pressemitteilung, 16.01.2025. [https://www.dgsp-ev.de/images/Stellungnahmen/2025/251016\\_PM%20Registrierung.pdf](https://www.dgsp-ev.de/images/Stellungnahmen/2025/251016_PM%20Registrierung.pdf).
- Kaspersky (2024): *The Naked Truth. How intimate image sharing is reshaping our world*. 22.07.2024. <https://media.kasperskydaily.com/wp-content/uploads/sites/86/2024/07/15164921/The-Naked-Truth-Kaspersky.pdf>.
- Turowski, Jan; Mikfeld, Benjamin (2013): *Gesellschaftlicher Wandel und politische Diskurse – Überlegungen für eine strategieorientierte Diskursanalyse*. Denkwerk Demokratie & Hans Böckler Stiftung, September 2013.
- Verlag Dashöfer (Hrsg.) (2025): *Keine „Lebensakte Trans\*“ im Melderegister*. Online-Artikel, 20.10.2025. <https://www.dashoefer.de/dasgleichstellungswissen/newsletter/artikel/keine-lebensakte-trans-im-melderegister.html>.
- Zips, Martin (2015): Kind in der Kiste. Süddeutsche Zeitung Online vom 15. August 2015. <https://www.sueddeutsche.de/leben/familie-partnerschaft-junge-schachtel-1.2603885>.

*Über die Autor\*in*

Dr. Karoline Busse

unterrichtet an der Hochschule für Verwaltung Niedersachsen und dem Niedersächsischen Studieninstitut für kommunale Verwaltung in den Bereichen Informationssicherheit, Datenschutz, Verwaltungsdigitalisierung und Mensch-Computer-Interaktion. Zuvor hat Dr. Busse an der Rheinischen Friedrich-Wilhelms-Universität Bonn im Bereich Usable Security and Privacy zur Wahrnehmung von Sicherheit promoviert. Seit August 2024 ist Karoline Busse zu 50% abgeordnet an das Niedersächsische Ministerium für Inneres, Sport, und Digitalisierung und begleitet dort die Transformation der Sicherheitsarchitektur der Landesverwaltung hin zum Zero-Trust-Paradigma. E-Mail: karoline.busse@nsi-hsvn.de