Institut Sekundarstufe II
Fabrikstrasse 8, CH-3012 Bern
T +41 31 309 21 15, contactdesk@phbern.ch, www.phbern.ch

Unterricht und Recht

Reader

Richard Conrardy

1 Unterricht und Recht

Hinweis: Die Autoren sind keine Juristen.

Dieser Reader dient angehenden Lehrpersonen als Basis für ihr Wissen und Handeln in Bezug auf Datenschutz und Urheberrecht.

2 Datenschutz

Datenschutz ist ein breites Konstrukt, das je nach Kontext unterschiedlich verstanden und ausgelegt wird. Im Kern hat Datenschutz mit dem Bedürfnis nach Privatheit zu tun: Gesellschaften sind bereit, Restriktionen und Verpflichtungen im Umgang mit Daten in Kauf zu nehmen, um übergeordnete Interessen zu schützen (vgl. Rost 2013). Dieses Bedürfnis entsteht nicht im luftleeren Raum, sondern hat wesentlich mit Machtasymmetrien zu tun, etwa zwischen Staat und Bürgerinnen und Bürgern, aber auch zwischen Institutionen und Individuen.

Gerade der Staat ist darauf angewiesen, Informationen über Privatpersonen zu erheben und zu verarbeiten, um grundlegende Aufgaben erfüllen zu können: Steuern zu berechnen, Leistungen auszuzahlen, Bildung zu organisieren oder Sicherheit zu gewährleisten. Mit der Entwicklung der Informationstechnologien, insbesondere seit den 1970er Jahren, wurde es jedoch deutlich einfacher, Informationen zu speichern, auszutauschen, zusammenzuführen und über ursprünglich vorgesehene Zwecke hinaus zu nutzen.

Historisch ist Datenschutz als Schutzidee gegen einen „allwissenden“ Staat zu verstehen: Es besteht ein gesellschaftliches Interesse daran, dass staatliche Stellen Informationen nicht nach Belieben einsetzen können, etwa um Oppositionelle zu beobachten, Personen zu diskriminieren oder Verhalten zu steuern. Datenschutzrecht ist in diesem Sinne weniger ein „Technikgesetz“ als vielmehr ein Instrument zur Begrenzung von Macht.

Aus dieser Perspektive lässt sich Datenschutz als Anspruch formulieren, dass Menschen nachvollziehen können, wer wann was zu welchem Zweck über sie weiss – und was mit diesen Informationen geschieht. Dieses Bedürfnis hängt eng mit dem Konzept der informationellen Selbstbestimmung zusammen: Individuen sollen nicht vollständig die Kontrolle über „ihre“ Daten im Eigentumssinn haben, aber sie sollen in einer demokratischen Gesellschaft davor geschützt werden, dass Informationen über sie ohne rechtliche Grundlage, ohne Transparenz und ohne angemessene Grenzen verwendet werden.

Datenschutzrecht versucht deshalb einen Ausgleich zu schaffen. Es anerkennt, dass Datenbearbeitung notwendig ist, etwa für Verwaltung, Schule, Gesundheit oder Forschung, setzt dieser Bearbeitung aber Leitplanken. Diese Leitplanken lassen sich in wenigen Grundideen bündeln:

- Daten sollen nur für einen bestimmten Zweck erhoben werden;
- es sollen nur so viele Daten bearbeitet werden, wie tatsächlich notwendig sind;
- Betroffene sollen informiert werden;
- und es sollen organisatorische und technische Massnahmen verhindern, dass Daten unbefugt zugänglich werden oder in falsche Hände geraten.

Datenschutzrecht ist damit nicht bloss eine Sammlung von Verboten, sondern ein Regelwerk, das legitime Datenverarbeitung ermöglichen und zugleich Vertrauen sichern soll: Vertrauen darin, dass Institutionen ihre Aufgaben erfüllen können, ohne die Einzelnen schutzlos zu machen.

Für den schulischen Kontext ist diese Grundidee besonders relevant. Schule ist eine staatliche Institution mit einem Bildungsauftrag, und sie arbeitet zwangsläufig mit sensiblen Informationen: Leistungsdaten, Entwicklungsbeobachtungen, Gesprächsnotizen, Absenzen, Unterstützungsbedarfe oder Hinweise aus

der Zusammenarbeit mit Eltern und Fachstellen. Gerade weil Schule einerseits Nähe und Beziehung lebt, andererseits aber als Institution handelt, ist der Umgang mit Daten nicht nur eine administrative Nebenfrage. Er ist Teil professioneller Verantwortung: Lernende sollen sich darauf verlassen können, dass Informationen über sie nicht beliebig zirkulieren, nicht unnötig gespeichert werden und nicht in Kontexte gelangen, die ihnen schaden oder sie stigmatisieren könnten.

2.1 Datenschutzrecht

Datenschutzrecht ist in der Schweiz nicht einfach „ein Gesetz", sondern eine abgestufte Ordnungsidee: Oben steht die Bundesverfassung als Grundrechtsrahmen, darunter folgen Ausführungsgesetze, die festlegen, wie dieses Grundrecht im Alltag von Behörden und Privaten konkret umgesetzt werden soll. Der verfassungsrechtliche Ausgangspunkt ist Art. 13 BV (Schutz der Privatsphäre). Dort wird nicht nur das Privat- und Familienleben sowie die Vertraulichkeit der Kommunikation geschützt, sondern ausdrücklich auch der Anspruch auf Schutz vor Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV). Neben dem Grundrechtsschutz aus Art. 13 BV ist für das Datenschutzrecht der verfassungsrechtliche Rahmen des staatlichen Handelns entscheidend. Art. 5 BV hält fest, dass Grundlage und Schranke staatlichen Handelns das Recht ist. Staatliche Stellen, und damit auch öffentliche Schulen, dürfen Personendaten nicht „einfach weil es praktisch ist" bearbeiten, sondern brauchen dafür eine rechtliche Grundlage und müssen ihr Handeln an den rechtsstaatlichen Prinzipien ausrichten. Datenschutz wird damit nicht nur als individuelles Schutzrecht verstanden, sondern auch als Ausdruck eines Rechtsstaats, der seine Macht an Regeln bindet.

Aus diesem Verfassungsauftrag ergeben sich in der Gesetzgebung zwei grosse Linien, die für angehende Lehrpersonen wichtig sind. Einerseits gibt es das Bundesgesetz über den Datenschutz (DSG), das regelt, wie Personendaten im Zuständigkeitsbereich des Bundes und im privaten Sektor bearbeitet werden. Andererseits haben die Kantone eigene Datenschutzgesetze für ihre Behörden – im Kanton Bern ist das das Datenschutzgesetz (KDSG, BSG 152.04). Für den Schulalltag ist diese Unterscheidung zentral: Eine öffentliche Schule in Bern ist typischerweise Teil der kantonalen/kommunalen Verwaltung und fällt deshalb primär unter das KDSG; das DSG ist dennoch wichtig, weil es als Referenzrahmen dient und weil viele digitale Diensteanbieter (EdTech, Plattformen, Clouds) als Private dem DSG unterstehen.

Das DSG sagt klar, an wen es sich richtet. In Art. 2 DSG wird festgehalten, dass das Gesetz für die Bearbeitung von Personendaten natürlicher Personen gilt durch (a) private Personen und (b) Bundesorgane. Das bedeutet: Unternehmen, Vereine, Plattformbetreiber, aber auch Bundesstellen müssen die Vorgaben einhalten.

Auf kantonaler Ebene setzt das KDSG Bern denselben Grundgedanken fort, aber für die Behörden im Kanton. Es dient „dem Schutz von Personen vor missbräuchlicher Datenbearbeitung durch Behörden" (Art. 1 KDSG). Damit ist die Zielrichtung deutlich: Nicht „Datenverarbeitung verhindern", sondern Datenverarbeitung in staatlichen Strukturen so begrenzen, dass sie

- rechtmässig (Art. 5 Abs. 1 KDSG),
- zweckgebunden (Art. 5 Abs. 2 und 4 KDSG)
- und verhältnismässig (Art. 5 Abs. 3 BV) bleibt.

Für angehende Lehrpersonen ist die Konsequenz praktisch: Sobald du im Rahmen einer öffentlichen Schule handelst (Notenführung, Erhebung von Allergien, Kommunikation mit Eltern, Foto-/Videoeinsatz in schulischen Kontexten), bearbeitest du Personendaten als Teil einer Behörde/öffentlichen Aufgabe und damit gelten die kantonalen Regeln.

Damit man überhaupt weiss, wovon die Gesetze sprechen, braucht es die Begriffe. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 2 Abs 1 KDSG), das DSG hingegen bezieht sich ausschliesslich auf natürliche Personen. Das ist bewusst weit: Name, Kontaktdaten, ein Foto, eine Lernstandsnotiz oder auch eine ID in einem Lernsystem. Im KDSG wird zudem betont, dass „Bearbeiten" sehr breit zu verstehen ist: Es umfasst jeden Umgang mit Personendaten, etwa Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten.

Für die Schule ist das wichtig, weil Datenschutz nicht erst beim „Veröffentlichen“ beginnt, sondern bereits beim Sammeln, Ablegen, Teilen im Kollegium oder Speichern in Tools.

Besonders relevant ist die Kategorie der besonders schützenswerten Personendaten. Sie meint Daten, bei deren Bearbeitung eine erhöhte Gefahr besteht, die Persönlichkeit der betroffenen Person zu verletzen, nicht nur wegen der Datenkategorie selbst, sondern oft auch wegen Kontext, Zweck und Kombination. Das DSG (Art. 5c) und KDSG (Art. 3) benennen solche Datenkategorien ausdrücklich:

Tabelle 1: Datenklassifikation in DSG und KDSG

DSG	KDSG Bern
Besonders schützenswerte Personendaten:1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,3. genetische Daten,4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,6. Daten über Massnahmen der sozialen Hilfe;	Besonders schützenswerte Personendaten sind Angaben übera die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit;b den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand;c Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung;d polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.

Man merkt schnell, warum das im Schulalltag nicht exotisch ist. „Gesundheit“ beginnt nicht erst bei Diagnosen, sondern umfasst z.B. Therapien, psychische Belastungen oder Hinweise aus Abklärungen. „Massnahmen der sozialen Hilfe“ kann berührt sein, wenn Unterstützungsleistungen, finanzielle Härtefälle oder sozialdienstliche Themen in Gesprächen und Akten auftauchen. Und „Intimsphäre“ kann bereits tangiert sein, wenn Vorfälle, Konflikte oder persönliche Lebensumstände dokumentiert werden. Gerade deshalb ist die zentrale praktische Konsequenz weniger juristisch als professionell: Solche Daten gehören besonders strikt zweckgebunden, zugriffsbeschränkt und zurückhaltend bearbeitet.

Wenn man diesen verfassungsrechtlichen und gesetzlichen Rahmen zusammennimmt, ergibt sich für die Schule eine einfache Orientierung: Datenschutzrecht will nicht, dass Schule „nichts mehr darf“, sondern dass die Schule bewusst entscheidet, warum sie Daten braucht, welche Daten wirklich nötig sind und wie sie so bearbeitet werden, dass Missbrauch, Zufallsweitergaben und unnötige Risiken möglichst ausgeschlossen sind.

2.2 DSG

Neben dem kantonalen Datenschutzrecht, das für öffentliche Schulen als staatliche Akteure gilt, spielt im schulischen Umfeld auch das Bundesgesetz über den Datenschutz (DSG) eine wichtige Rolle. Das hängt damit zusammen, dass Schule heute kaum noch ohne private Dienstleister auskommt: Lernplattformen, Kommunikations-Apps, Cloudspeicher, digitale Übungs- und Diagnosetools oder KI-Anwendungen werden häufig von privaten Unternehmen betrieben. Diese Anbieter unterstehen als „private Personen“ dem DSG (Art. 2 DSG).

In dieser privaten Sphäre herrscht ebenfalls informationelle Selbstbestimmung: Wer einen Dienst nutzt, schliesst einen Vertrag und akzeptiert die dortigen Bedingungen oder entscheidet sich für alternative Anbieter. Das Obligationenrecht geht dabei von Vertragsfreiheit aus, betont aber gleichzeitig, dass sie nur innerhalb der Schranken des Gesetzes gilt (Art. 19 Abs. 1 OR). Genau hier setzt das DSG als solcher Rechtsrahmen an: Es definiert Mindeststandards dafür, wie private Unternehmen Personendaten bearbeiten dürfen, wenn sie in der Schweiz tätig sind (Art. 2 DSG).

Für EdTech-Anbieter sind dabei drei Pflichten besonders zentral. Erstens müssen sie Personendaten nach Grundsätzen der Bearbeitung handhaben: Datenbearbeitung muss rechtmässig, zweckgebunden

und verhältnismässig sein (Art. 6 DSG). Zudem müssen Betroffene in der Regel angemessen informiert werden, insbesondere bei der Beschaffung von Personendaten (Art. 19 DSG).

Zweitens statuiert das DSG ein Auskunftsrecht (Art. 25 DSG): Betroffene sollen erfahren können, ob und welche Daten über sie bearbeitet werden (und in welchem Rahmen). Das ist im Schulkontext relevant, weil EdTech nicht nur Stammdaten, sondern oft auch Nutzungs- und Leistungsdaten erzeugt.

Drittens verlangt das DSG angemessene Datensicherheit (Art. 8 DSG): Unternehmen müssen durch geeignete technische und organisatorische Massnahmen Personendaten vor unbefugter Bearbeitung schützen.

Datenschutzrecht lässt sich damit auch als Antwort auf Machtasymmetrien verstehen: Es schützt einzelne Personen davor, dass Staaten und Unternehmen aufgrund ihrer Ressourcen, ihres Informationsvorsprungs und ihrer organisatorischen Möglichkeiten beliebig Wissen über Menschen anhäufen und nutzen. Datensicherheit zielt demgegenüber stärker auf die umgekehrte Schutzrichtung: Sie soll verhindern, dass Dritte, seien es einzelne Individuen, kriminelle Gruppen oder „Hacker“, unbefugt auf Daten zugreifen, diese ändern oder löschen, und schützt damit Institutionen und Unternehmen (und mittelbar auch die Betroffenen) vor Angriffen von aussen.

3 Urheberrecht

Datenschutzrecht und Urheberrecht wirken im Schulalltag auf den ersten Blick wie zwei getrennte Baustellen: hier der Schutz von Personen und ihren Daten, dort der Schutz von Werken und kreativen Leistungen. In der Praxis hängen beide aber eng zusammen, weil Unterricht heute fast immer digital vermittelt ist und damit zwei Arten von „Schutzgütern“ berührt. Wenn Lehrpersonen kommunizieren, dokumentieren, beurteilen oder digitale Tools einsetzen, geht es um Personendaten und um die Frage, wer was über wen wissen darf. Wenn Lehrpersonen Materialien suchen, kopieren, teilen, präsentieren oder auf Lernplattformen bereitstellen, geht es um fremde Werke und um die Frage, wer was mit wessen Inhalten tun darf. Beide Rechtsgebiete reagieren damit auf ähnliche Grundspannungen: Auf der einen Seite steht das legitime Interesse von Schule, Unterricht zu organisieren und Lernen zu ermöglichen; auf der anderen Seite stehen Rechte, die nicht einfach „im Namen der Praktikabilität“ aufgehoben werden dürfen.

Urheberrecht ist im Schulalltag weniger eine „Bremse“ als eine rechtliche Konstruktion, die überhaupt erst möglich macht, dass mit fremden Texten, Bildern, Musik oder Filmen gearbeitet werden kann, ohne jedes Mal individuell Rechte einholen zu müssen. Das Urheberrechtsgesetz (URG) schützt die schöpferische Leistung der Urheberinnen und Urheber, geht aber gleichzeitig davon aus, dass Bildung auf Nutzung beruht. Deshalb kennt das Gesetz Schranken, die Unterricht ausdrücklich privilegieren. Zentral ist dabei die Verwendung zum Eigengebrauch: Als Eigengebrauch gilt nicht nur die private Nutzung, sondern ausdrücklich auch „jede Werkverwendung der Lehrperson für den Unterricht in der Klasse“ (Art. 19 Abs. 1 lit. b URG). Damit ist rechtlich „eingepreist“, dass Schule mit geschützten Werken arbeitet. Und auch ökonomisch ist das kein blinder Fleck: In der Schweiz werden viele schulische Nutzungen über Verwertungsgesellschaften und entsprechende Vergütungsmechanismen kollektiv abgegolten, die Idee dahinter ist, dass Urheber:innen entschädigt werden, ohne dass Unterricht in unpraktikable Einzelbewilligungen zerfällt.

Aus dieser optimistischen Perspektive ist Urheberrecht im Kern ein Fairness-Deal: Unterricht darf viel, aber nicht grenzenlos. Entscheidend ist der schulische Rahmen „in der Klasse“ (Art. 19 URG). Sobald Nutzung in Verbreitung kippt, also über den Unterrichtskontext hinausgeht oder dauerhaft für grössere Kreise zugänglich wird, wird Urheberrecht wieder strenger, weil dann nicht mehr nur Lernen ermöglicht, sondern potenziell ein Markt ersetzt oder ein Werk öffentlich zugänglich gemacht wird.

Typische schulische Handlungen lassen sich vor diesem Hintergrund gut einordnen:

- Im Unterricht zeigen/abspielen: Musik hören, Lieder singen, Geschichten lesen und bearbeiten oder Filme anschauen ist im Klassenunterricht grundsätzlich zulässig (Eigengebrauch/Unterrichtsnutzung).

- Kopieren/Scannen von Materialien: Auszüge kopieren oder einzelne Kapitel verwenden ist typischerweise unproblematischer als „ganze Werke“ zu vervielfältigen. Gerade beim Kopieren gibt es aber Grenzen – z.B. wird das vollständige oder weitgehend vollständige Kopieren im Handel erhältlicher Exemplare als nicht zulässig dargestellt.
- Material auf die Lernplattform stellen: Für die eigene Klasse kann das didaktisch naheliegend sein, rechtlich ist aber wichtig, ob damit nur der Unterricht in der Klasse organisiert wird oder ob faktisch ein dauerhafter, weitergehender Zugang entsteht (z.B. klassenübergreifend, öffentlich, ohne Zugriffsbeschränkung).
- Bilder aus dem Internet für Arbeitsblätter/Präsentationen: „Online auffindbar“ heisst nicht frei. Wenn Bilder eingesetzt werden, hilft eine saubere Quellenangabe und, wo möglich, die Nutzung von klar lizenzierten Inhalten (z.B. Creative Commons) als professionelle Routine.
- Elternabend, Schulhomepage, Social Media: Hier verlässt man schnell den geschützten Unterrichtsrahmen. Was im Klassenzimmer zulässig ist, ist nicht automatisch für öffentliche oder halböffentliche Anlässe bzw. Publikationen gedeckt, insbesondere bei Aufnahmen von Aufführungen oder bei weiterverbreiteten Inhalten.

Insgesamt zeigt sich: Das URG ist für die Schule nicht primär ein System von Verboten, sondern eine Struktur, die Unterrichtsnutzung rechtlich ermöglicht und finanziell (über kollektive Vergütungssysteme) mitträgt solange Lehrpersonen den Unterschied zwischen didaktischer Verwendung im Klassenrahmen und Publikation/Verbreitung im Blick behalten.

3.1 Freie Lizenzen und GenAI

Freie Lizenzen sind eine praktische Professionalisierung im Umgang mit Unterrichtsmaterialien. „Frei“ heisst dabei nicht automatisch „gratis“, sondern dass Nutzungsrechte nachhaltig und endnutzerfreundlich sind. Das ist im Schulalltag besonders wertvoll, weil Lehrpersonen ständig vor der gleichen Frage stehen: Darf ich dieses Material nur für mich nutzen oder auch weitergeben? Freie Lizenzen geben darauf eine eindeutige Antwort und reduzieren den „Graubereich“ auf ein Minimum.

In Anlehnung an Richard Stallman wird die Idee des „Freien“ oft über vier Grundfreiheiten für Software beschrieben, die sich gut auf Bildungsmaterialien übertragen lassen:

- Freiheit 0: Das Werk für jeden Zweck verwenden.
- Freiheit 1: Das Werk studieren und verstehen können (bei Software: Zugang zum Quelltext; übertragen auf Materialien: nachvollziehbare Grundlage und Bearbeitbarkeit).
- Freiheit 2: Das Werk kopieren und weitergeben dürfen.
- Freiheit 3: Das Werk verändern/verbessern und die bearbeitete Version weiterverbreiten dürfen.

Im Bildungsbereich sind Creative-Commons-Lizenzen (CC) der gängigste Weg, solche Freiheiten konkret und standardisiert zu regeln. Sie funktionieren modular über Bausteine, die auf einen Blick zeigen, was erlaubt ist und welche Bedingungen gelten. Das wichtigste Element ist fast immer BY (Namensnennung):

- SA (ShareAlike): Bearbeitungen müssen wieder unter derselben Lizenz weitergegeben werden.
- NC (NonCommercial): Nutzung nur nicht-kommerziell, dies schliesst gewinnorientierte Privatschulen aus.
- ND (NoDerivatives): Teilen ist erlaubt, Bearbeitung jedoch nicht.

Bei Creative Commons gehört die Attribution zwingend dazu: In der Praxis heisst das mindestens Name des Urhebers/der Urheberin, ein Link zur Originalquelle, die Lizenzbezeichnung inkl. Link (z.B. „CC BY 4.0“). CC-Lizenzen können das Zitatrecht nicht ein einschränken, zitieren ist als gesetzliche Schranke immer erlaubt.

Ein Spezialfall, der in Schulen zunehmend relevant wird, sind KI-generierte Inhalte (GenAI). Hier ist die Rechtslage weniger stabil, und sie verändert sich schnell: Es bestehen Unsicherheiten, etwa welche Rechte an Outputs im Einzelfall gelten, wie stark Outputs bestehenden Werken ähneln dürfen, wie

Trainingsdaten rechtlich bewertet werden oder welche Nutzungsbedingungen einzelne Tools in ihren AGB festlegen.

4 Reality Check

Eine Facette von Demokratiebildung ist ein *shared sense of reality*, also die Fähigkeit, eine gemeinsame Realitätswahrnehmung herzustellen, auf deren Grundlage man überhaupt sinnvoll diskutieren kann. Dieser Abschnitt will genau dafür eine Basis legen. Gesetze sind normativ gedacht. Sie sollen einen gesellschaftlichen Mindestkonsens ausdrücken. In der Praxis zeigt sich jedoch, dass dieser Konsens brüchig ist. Genau deshalb lohnt sich ein Reality Check: Er macht Zielkonflikte und strukturelle gesellschaftliche Probleme sichtbar, die zwischen rechtlichem Anspruch und Praxis entstehen. Erst wenn diese Reibungen benannt sind, lassen sich im nächsten Schritt Handlungsoptionen und Empfehlungen formulieren.

4.1 Datenschutz

Auch im Datenschutz zeigt sich der Unterschied zwischen Ideal und Realität besonders deutlich. Verfassungsrechtlich ist der Rahmen eigentlich klar: Staatliches Handeln ist an Recht und Gesetz gebunden; „Grundlage und Schranke staatlichen Handelns ist das Recht“ (Art. 5 Abs. 1 BV). Die Realität in Schulen ist jedoch oft weniger sauber, weil sich Datenschutz im Alltag nicht als „ein grosser Verstoss“, sondern als Summe kleiner Routinen zeigt, in denen Informationen unnötig breit zirkulieren. Dass Lehrpersonen miteinander sprechen, ist selbstverständlich und in den meisten Lehrerzimmern wird frei heraus über personenbezogene Daten von Schülerinnen und Schülern geredet.

Daneben gibt es weitere Alltagsszenarien, die fast überall vorkommen:

- Eine Klassenlehrperson bittet das Kollegium, alle Noten zentral in ein Google-Sheet einzutragen, weil es praktisch ist.
- Notenlisten liegen im Kopierraum, bleiben am Beamer hängen oder werden als Foto geteilt („nur schnell, damit niemand es vergisst“).
- Für Webseiten, Umfragetools oder Lernapps werden Klarnamen und ganze Klassenlisten hochgeladen, obwohl für den Zweck Pseudonyme oder Minimallösungen reichen würden.
- In Mails an Eltern werden Empfänger im „An“-Feld sichtbar gemacht.
- Lehrpersonen erheben die Religion der Lernenden um zu wissen wer kein Schweinefleisch isst.
- In BNE sollen die Lernenden ihre Weltanschauung analysieren.
- Die Lehrperson verlangt den Grund eines Nachteilsausgleichs zu erfahren.
- Die Kommunikation über Diagnosen verläuft per Mail.

Konsequenzen gibt es selten. Hacker haben 1.2 Terabyte an Daten vom Basler Erziehungsdepartement erbeutet, darunter Abklärungsberichte und schulpsychologische Diagnosen SRF (2023). Die Reaktion von Regierungsrat Conradin Cramer: „Es sind sehr viele Baslerinnen und Basler betroffen – viele Kinder. Wir können nichts tun, ausser zu hoffen, dass niemand diese Daten missbraucht.“ (SRF 2023).

Hinzu kommt eine nüchterne Anreizstruktur: Lehrpersonen werden nicht „pro Stunde“ bezahlt, sondern stehen unter einem permanenten Effizienzdruck. Gleichzeitig ist das Risiko, für alltägliche Datenschutzverstösse tatsächlich „erwischt“ zu werden, gering, und viele Praktiken sind sozial normalisiert („das machen alle so“). Dadurch verschiebt sich der Massstab: Was objektiv problematisch ist, wirkt subjektiv routinemässig und damit harmlos.

4.2 DSG

Um Datenbearbeitung im privaten Bereich ist es nicht besser bestellt. Der Rechtsrahmen funktioniert im Alltag oft nicht so, wie es die Idee informationeller Selbstbestimmung nahelegt. Ein eindrückliches Beispiel liefern Bouhoula et al. (Bouhoula u. a. 2024): In ihrer grossangelegten automatisierten Analyse von Cookie-Bannern zeigen sie, dass viele Websites die Cookie-Entscheidungen der Nutzerinnen und Nutzer ignorieren. Die Studie macht damit sichtbar, dass „Zustimmung“ im Web häufig eher als Interface-Inszenierung erscheint, denn als tatsächlich respektierte Entscheidung.

Noch grundlegender wird das Spannungsfeld dort, wo digitale Dienstleistungen nicht nur Daten bearbeiten, sondern Zugang zu zentralen Lebensbereichen vermitteln. Cloud- und Plattformunternehmen können Accounts willkürlich sperren und setzen sich über Gerichtsbeschlüsse hinweg (Friedrich 2022), selbst Richter sind nicht von solchen Massnahmen sicher (Kirchner 2025). Betroffene verlieren damit nicht nur einen Login, sondern den Zugang zu E-Mails, gekauften Programmen, privaten Dateien und Logins bei verbundenen Diensten.

Auf internationaler Ebene verschärft sich dieses Bild durch politischen Druck auf Verschlüsselung. Immer wieder wird gefordert, starke Ende-zu-Ende-Verschlüsselung zugunsten staatlicher Zugriffsmöglichkeiten aufzuweichen (Gnehm 2025), was aus Sicherheitsperspektive paradox ist: Jede „Hintertür", die für Behörden gedacht ist, ist auch eine strukturelle Schwächung, die missbraucht werden kann.

Vor diesem Hintergrund ist auch die aktuelle Debatte um internationale Cloudanbieter in der öffentlichen Hand ein Symptom derselben Grundspannung: Privatim (Konferenz der schweizerischen Datenschutzbeauftragten) äussert Zweifel, ob grosse US-Cloud-SaaS-Lösungen unter Schweizer Anforderungen zuverlässig rechtkonform betrieben werden können (Privatim 2025). Dass solche Einschätzungen in der Praxis oft wenig „Effekt" haben, zeigt wiederum ein strukturelles Muster: Rechtliche Rahmen existieren, aber Marktmächte und Bequemlichkeit erzeugen eine Realität, in der formale Regeln nicht automatisch zu tatsächlicher Selbstbestimmung führen.

4.3 Urheberrecht

Das Internet ist also kein rechtsfreier Raum, es scheint jedoch ein teilweise rechtsdurchsetzungsfreier Raum zu sein.

4.3 Datensicherheit

Bouhoula, Ahmed, Karel Kubicek, Amit Zac, Carlos Cotrini, und David Basin. 2024. «Automated Large-Scale Analysis of Cookie Notice Compliance». *33rd USENIX Security Symposium (USENIX Security 24)*, 1723–39.

Friedrich, Greta. 2022. «Automatisierte Scans: Microsoft sperrt Kunden unangekündigt für immer aus». In *c't Magazin*. Https://www.heise.de/hintergrund/Automatisierte-Scans-Microsoft-sperrt-Kunden-unangekuendigt-fuer-immer-aus-7324608.html.

Gnehm, Claudia. 2025. «Kampf um Regulierung: Schweizer Techfirma protestiert gegen <<Überwachung>> und investiert fortan im Ausland». In *Tages-Anzeiger*. Https://www.tagesanzeiger.ch/techfirma-proton-kehrt-der-schweiz-den-ruecken-126325644688.

Kirchner, Malte. 2025. «Digitaler Rückfall in die 90er: US-Sanktionen treffen französischen Richter». In *heise online*. Https://www.heise.de/news/Wie-ein-franzoesischer-Richter-von-den-USA-digital-abgeklemmt-wurde-11087453.html.

Privatim. 2025. *Publikation: Resolution zur Auslagerung von Datenbearbeitungen in die Cloud – privatim*.

Rost, Martin. 2013. «Zur Soziologie Des Datenschutzes». *Datenschutz und Datensicherheit*, Nr. 2: 85–91.

Sokolov, Daniel. 2023. «Basler Schulnetz gehackt, Schülerdaten im Darknet». In *heise online*. Https://www.heise.de/news/Gescheiterte-Erpresser-posten-Daten-Basler-Schueler-9056730.html.

SRF. 2023. «Grosser Cyberangriff - Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt». News in *Schweizer Radio und Fernsehen (SRF)*. Https://www.srf.ch/news/schweiz/grosser-cyberangriff-kinder-betroffen-daten-des-basler-erziehungsdepartements-gehackt.