

Datenschutz und Persönlichkeitsrechte

Von Jochen Koubek

Bei den derzeit sich überbietenden Meldungen über technische Sicherheitslücken, staatliche Abhörprojekte, illegale Datenspeicherungen und verfassungswidrige Überwachungsgesetze sind die Bürgerrechte derart in die Defensive geraten, dass bisweilen vergessen wird, in welcher Richtung die Legitimation eigentlich zu erfolgen hat. Denn nicht die Bewahrung von persönlichen Daten sollte permanent gerechtfertigt werden müssen, sondern ihre ausgreifende Erfassung, Speicherung und Verarbeitung.

Aber viele Bürgerinnen und Bürger wissen gar nicht, worin eigentlich ihr gutes Recht besteht und vor allem nicht, wie sie es vor sich und anderen begründen können, dass sie bestimmte Informationen gar nicht preisgeben wollen.

In diesem Beitrag soll ein kurzer historischer Überblick über die allgemeinen Persönlichkeitsrechte und über das Recht auf informationelle Selbstbestimmung gegeben werden, aus dem heraus sich bis heute die Argumente ableiten lassen, wer was von wem zu welcher Gelegenheit wissen darf.

Grundgesetz und allgemeines Persönlichkeitsrecht

Im Grunde beginnt unsere Geschichte – wie so viele Geschichten – im alten Griechenland, wo der Eid des Hippokrates jeden Arzt zur Verschwiegenheit im Umgang mit Patienteninformationen verpflichtete. Aber derart weit zurück will ich an dieser Stelle nicht gehen und überspringe einige Jahrhunderte der Kulturgeschichte des Geheimnisses, das neben Ärzten, Anwälten und Geistlichen auch auf Bürger ausgedehnt wurde, die seit der Frühen Neuzeit und noch stärker seit der Aufklärung zunehmend die soziale, kulturelle aber auch rechtliche Berücksichtigung ihrer individuellen Lebensumstände einfordern und die für sich und ihre Familien Rückzugsräume des privaten Lebens schufen (Aries; Duby). Zu diesen schutzwürdigen Bereichen zählte neben der persönlichen Ehre und der Wohnung auch die persönliche Korrespondenz. Das Briefgeheimnis versprach Joseph I. vor seiner Wahl zum römisch-deutschen König im Jahr 1690, »nachdem seine Verletzung schon mehrere Kriege verursacht hatte.« (Kittler, S. 8)

Nach der Auflösung des Römischen Reichs wurde im Deutschen Bund das Briefgeheimnis im Jahr 1831 in die Kurhessische Verfassung als ein Grundrecht aufgenommen. Hinzu kam in der zweiten Hälfte des 19. Jahrhundert »der Schutz gegen informationelle Eingriffe durch Private« (von Lewinski, S. 26), ein Recht, das sich vor allem gegen die Boulevardpresse richtete. Diese stöberte bevorzugt im Privatleben prominenter Einzelpersonen, gerne auch in den Grenzbereichen der persönlichen Ehre – eine journalistische Praxis, die sich bis heute bewahrt hat. Das Recht am eigenen Bild wurde 1907 im Anschluss an den Skandal um das Foto Otto von Bismarcks auf dem Sterbebett im Kunsturheberrecht (KunstUrhG) gesetzlich eingeräumt (Leffler, S. 42 ff.)

Dennoch sollte es noch bis zur Gründung der BRD dauern, ehe aus diesen disparaten Einzelregelungen ein systematisches, immaterielles Persönlichkeitsrecht gestaltet wur-

de. Die für uns heute relevanten Regelungen des privaten Lebens basieren auf der Erklärung der Menschenrechte aus dem Jahr 1948, laut deren Artikel 12 niemand willkürlichen Eingriffen in sein Privatleben, seine Familie, Heim oder seinen Briefwechsel ausgesetzt werden darf (UN 1948). Das Grundgesetz der Bundesrepublik Deutschland vom 23. Mai 1949 formuliert auf dieser Erklärung aufbauend die grundlegenden Abwehrrechte der Bürger gegenüber dem Staat und den Mitbürgern. Diese Rechte umfassen die unbedingt geltende und durch kein Gesetz einschränkbare Menschenwürde (Artikel 1), das Recht auf individuelle Selbstentfaltung, die allgemeine Handlungsfreiheit und die Freiheit der Person (Artikel 2), das Brief-, Post- und Fernmeldegeheimnis (Artikel 10) sowie die Unverletzlichkeit der Wohnung (Artikel 13). Daraus leiten sich die allgemeinen Persönlichkeitsrechte ab, die zwar »nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen.« (BVerfG 2008) Dazu gehören:

- Die persönliche Ehre, die insbesondere nicht durch Äußerungen, Berichterstattungen oder Veröffentlichungen beeinträchtigt werden darf.
- Das Recht auf Privatheit, oder das Recht, in Ruhe gelassen zu werden, ähnlich dem »right to be let alone«, das Warren und Brandeis in den USA bereits 1890 mit Blick auf das Hausrecht formuliert hatten (Warren; Brandeis 1890).
- Die Rechte am eigenen Namen, am eigenen Bild und am gesprochenen Wort. Niemand darf ohne mein Einverständnis unter meinem Namen auftreten und Aufnahmen in Bild oder Ton von mir anfertigen. Auch in der Schule gelten diese Rechte für alle Beteiligten, die Lehrer sind rechtlich vor heimlichen Mitschnitten ihres Unterrichts ebenso geschützt wie die Schüler Fotos von sich nicht auf der Schulhomepage dulden müssen.
- Die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Mit anderen Worten: Die persönlichen Lebenssachverhalte, alles, was jemand macht und sagt sowie alle Informationen, die ihn oder sie betreffen, sind zunächst einmal seine oder ihre Angelegenheit, über deren Bekanntgabe, Mitteilung oder Veröffentlichung er oder sie alleine bestimmen kann. Dieses Recht gilt für alle Menschen, in Schulen auch für Schüler, Lehrer, Eltern oder nicht-pädagogisches Personal, in einem Staat für alle Bürger. Die rechtshistorische Verwandtschaft zum Hausrecht legt eine analoge Legitimationsstrategie nahe: Niemand fühlt sich genötigt oder verpflichtet, die verschlossene Tür zu seinem Haus zu rechtfertigen. Im Gegenteil muss derjenige sich erklären, der die persönlichen Räume eines Anderen betreten möchte. So sollte es auch mit persönlichen Daten sein, was sich historisch durchaus abzeichnete.

Geschichte des Datenschutzrechts

Auch wenn sich die Persönlichkeitsrechte direkt aus dem Grundgesetz ableiten lassen, dauerte es noch über 40 Jahre, um das Recht auf Privatheit auch konsequent auf Daten

und Informationen auszuweiten. Die ersten 20 Jahre wurde das Problem der Datenverarbeitung nicht thematisiert. Ausgangspunkt der Überlegungen, dass Daten privat und damit schützenswert seien könnten, war eine Initiative der Bundesregierung Ende der 1960er-Jahren, bei der die wachsenden Möglichkeiten der Computertechnik genutzt werden sollten, um die Datenvorräte verschiedener Ämter und Verwaltungseinheiten zu einem zentralen Informations-System zusammen zu führen und in einer gemeinsamen Datenbank zu verwalten. Eine Missbrauchsgefahr wurde nicht gesehen, da die Daten ja nicht öffentlich zugänglich seien. Dieses in alter Tradition stehende Staatsverständnis, wonach der Regierung grundsätzlich zu trauen, der Bevölkerung hingegen zu misstrauen sei, wurde in den kommenden Monaten heftig diskutiert. Als Ergebnis der Diskussion wurde das Projekt einer Bundeszentraldatenbank zwar ausgesetzt, an den grundlegenden Vorstellungen darüber, wie Vertrauen und Legitimation in einem Staat zu verlaufen habe, änderte sich jedoch nichts. Den Sorgen der Bürger sollte aber begegnet werden, indem die Daten gesetzlich vor Missbrauch geschützt wurden. Am 7. Oktober 1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz, das im Kern forderte, dass die Ermittlung, Weiterleitung und Aufbewahrung von Daten durch Behörden durch personelle und technische Maßnahmen nicht von Unbefugten beeinflusst werden kann. Das im Jahr 1977 verabschiedete erste Bundesdatenschutzgesetz griff diesen Gedanken bereits im ersten Paragraphen auf, wonach es die Aufgabe des Datenschutzes sei, die schutzwürdigen Belange der Bürger vor Missbrauch bei der Datenverarbeitung zu schützen. Auf der anderen Seite bedeutete dies, dass eine staatliche Behörde, die sich in ihrem Handeln auf Gesetze und Verwaltungsvorschriften stützt, per definitionem gar nicht zu Missbrauch im Stande ist, der Bürger sich also nur vor unbefugten Dritten Sorgen zu machen habe.

Dieses staatlich verordnete Vertrauen in die Obrigkeit wurde Anfang der 80er Jahre auf die Probe gestellt, als eine geplante Volkszählung von verschiedenen Interessengruppen massiv kritisiert wurde. Der Streit gipfelte in einer Klage vor dem Bundesverfassungsgericht, das in seinem historischen Urteil vom 15. Dezember 1983 den Schutz von personenbezogenen Daten aus den Persönlichkeitsrechten ableitete (BVerfG 1983). Der entscheidende Passus der Urteilsbegründung soll hier umfänglich zitiert werden, finden sich darin doch alle wesentlichen Argumente, die in den vergangenen 30 Jahren an Relevanz noch gewonnen haben (s. Kasten, Hervorhebungen von mir).

Das **Recht auf informationelle Selbstbestimmung** wurde 1990 im Bundesdatenschutzgesetz umgesetzt. Der wesentliche Grundsatz ist die Tatsache, dass persönliche Daten grundsätzlich zur Person gehören, die über ihren Verbleib entscheiden kann. Ausnahmen bedürfen bei nicht-öffentlichen Stellen der freiwilligen Zustimmung oder bei öffentlichen Stellen einer gesetzlichen Regelung. Für alle gilt, Datensammlungen so weit wie möglich zu vermeiden. Wo dies nicht möglich ist – z.B. bei Verwaltungsaufgaben – müssen sie in einem angemessenen Verhältnis zu den Anforderungen stehen und dürfen nur zweckbestimmt verwendet werden. Die Betroffenen müssen über den gesamten Vorgang informiert werden, sie haben das Recht auf Einsicht, Korrektur und ggfs. Löschung ihrer Daten. Informationstechnische Systeme müssen darüber hinaus so gestaltet werden, dass diese Prinzipien eingehalten und umgesetzt werden können. Die

...

Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. [...] Es umfaßt [...] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, **grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden**

Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar Person [...] technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekanntem Weise die Möglichkeiten einer Einsichtnahme und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.

Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. **Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.** Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten. Dies würde nicht nur die **individuellen Entfaltungschancen** des Einzelnen beeinträchtigen, sondern auch das **Gemeinwohl**, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfaßt. **Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.**

Begründung dafür leitete das Gericht unmittelbar aus den Persönlichkeitsrechten des Grundgesetzes ab und nicht mehr aus einer Sorge vor Missbrauch, der im Zweifel erst einmal zu beweisen wäre.

Herausforderungen

Noch einmal: Das Recht auf informationelle Selbstbestimmung ist als allgemeines Persönlichkeitsrecht den Grundrechten des Grundgesetzes gleichgestellt. Nicht seine Inanspruchnahme sollte daher der Rechtfertigung bedürfen, sondern seine Einschränkung. Personenbezogene Daten sind ein immaterielles Gut und als solches eine Art Eigentum.

Doch wie alle Immaterialgüter steht es vor der prinzipiellen Herausforderung, dass sich viele der mittelbar Betroffenen nicht richtig darum kümmern, diejenigen nämlich, die zwar Interesse, aber keine Rechte an den Daten haben. Die unautorisierte Erfassung, Vervielfältigung oder Verwertung wird allzu oft nicht als Schaden gesehen, billigend in Kauf genommen oder bewusst ignoriert. Das ist beim unbefugten Kopieren von Film- und Musikdaten der Unterhaltungsindustrie nicht anders als beim Plagiierten von Hausarbeiten im Bildungssystem und dort nicht anders als beim Erfassen und Speichern von personenbezogenen Daten im öffentlichen und nicht-öffentlichen Bereich: Die Informationen sind verfügbar, ihre Erfassung ist leicht, ihre Speicherung billig und ihre Verarbeitung wird immer komfortabler. Doch während sich die Unterhaltungsindustrie noch mit allen redlichen und unredlichen Mitteln gegen die Daten-Erosion wehrt, das Bildungssystem zumindest den Ehrenkodex hochhält, wonach Informationen nicht einfach ungekennzeichnet vervielfältigt werden dürfen, steht es um den Schutz personenbezogener Daten schlechter:

- Die Eigentümer, die Personen, deren Daten geschützt werden sollen, gehen freimütiger denn je damit um. Das Recht auf informationelle Selbstbestimmung ist keine Pflicht, es umfasst auch das Recht auf Datenpromiskuität, bei der eigene Daten in Form von Äußerungen, Fotos oder Videos in großem Umfang öffentlich gemacht werden.
- Produkte wie Facebook, Google, Smartphones und ihre Apps sind hinter Geschäftsbedingungen mit Diensten und Datenaggregationen verbunden, die mit dem Recht auf informationelle Selbstbestimmung eigentlich ausgeschlossen werden sollten, durch die Zustimmung der Nutzer aber rechtlich vielfach nicht zu beanstanden sind.
- Nationale und internationale Gesetzgebungen sind nur bedingt kompatibel. In Zeiten, in denen problemlos Informations-Angebote ausländischer Dienstleister angenommen werden können, stellt sich die Frage nach der Zuständigkeit und der Gültigkeit rechtlicher Regelungen.
- Durch Cloud-Computing entstehen Meta-Daten über das Nutzungsverhalten der Primärdaten. Der Gebrauch von Medien-Streaming-Diensten führt dazu, dass der anbietende Konzern weiß, wann ich welche Musik höre, welchen Film sehe, welches Buch lese oder welches Spiel spiele.
- Regelmäßige Datenskandale, bei denen Millionen von Kundendaten ins Netz sickern, werden wie unvermeidliche Naturkatastrophen zur Kenntnis genommen

ohne dass auch nur die Suche nach einer nachhaltigeren Infrastruktur in Sicht wäre.

- Weder stehen ausreichende Mittel zur Durchsetzung von Datenschutzbestimmungen bereit noch werden im Falle von ertappten Überschreitungen ernsthafte Sanktionen verhängt.

Auf der einen Seite gehen die Nutzer mit ihrem Grundrecht auf Datenhoheit sehr sorglos um. Auf der anderen Seite stehen die erfassenden und verarbeitenden Stellen, die ebenfalls nicht allzu fokussiert auf den Schutz der ihnen anvertrauten Daten erscheinen. Und der für die Aufstellung und Durchsetzung von Schutzrechten verantwortliche Staat steckt in diesen Fragen derzeit in einer Vertrauenskrise, deren Ausmaß nur durch die Gleichgültigkeit überboten wird, mit der sie von nahezu allen Beteiligten wahrgenommen und diskutiert wird.

Die ehemaligen Verfassungsrichter Hans-Jürgen Papier und Wolfgang Hoffmann-Riem haben es am 22.05.2014 in einer Anhörung vor dem NSA-Untersuchungsausschuss auf den Punkt gebracht (Krempel 2014):

1. Das massenhafte Abhören von Kommunikationen und Verbindungsdaten ist ähnlich einzustufen wie die flächendeckende, vorsorgliche und anlasslose Vorratsdatenspeicherung. Deren Unvereinbarkeit mit den Persönlichkeitsrechten und dem Grundgesetz haben verschiedene Gerichte – u.a. das BVerfG und der EuGH – wiederholt bestätigt.
2. Die Grundrechtseinschränkung ist auch dann verfassungswidrig, wenn sie durch Ausländer, aber auf deutschem Boden mit Billigung und Duldung der deutschen Behörden erfolgt.
3. Es ist die Pflicht der Bundesregierung, alles in ihrer Macht stehende zu unternehmen, um ihre Bürger vor der massenhaften Verletzung ihrer Grundrechte zu schützen. Sie hat eine grundrechtswahrende Informationsinfrastruktur und gesetzliche Regelungen zu schaffen, um die Grundrechte der Bürger zu wahren.

Durch Schweigen, Verharmlosen, Vertuschen oder Verzögern beim Durchsetzen dieser notwendigen Schutzmaßnahmen handelt die Bundesregierung entgegen ihres verfassungsgemäßen Auftrags. Es würde auch nicht ausreichen, das Abhören auf eine gesetzliche Grundlage zu stellen, wurden derartige Gesetze in der Vergangenheit doch regelmäßig im Kern als verfassungswidrig eingestuft.

Wo stehen wir nun? Es gibt ein historisch gewachsenes und sowohl durch Rechtsnormen ausformuliertes als auch durch die Urteilspraxis ausgeformtes Persönlichkeitsrecht, das insbesondere den Umgang mit personenbezogenen Daten umfasst. Wir haben Firmen, denen dieses Recht gleichgültig ist, weil sie in ihrer Selbstwahrnehmung gar nicht im deutschen Rechtsraum operieren. Wir haben eine Regierung, der dieses Recht gleichgültig ist, wenn es um die Wahrung ihrer eigenen Interessen geht. Und wir haben Bürger, denen dieses Recht ebenfalls gleichgültig ist, wenn es mit Einschränkungen der

persönlichen, digitalen Lebensgestaltung einhergeht oder wenn zu seiner Durchsetzung politische Aktivierung erforderlich wäre.

Insofern ist George Orwells Roman *1984* nicht die richtige Metapher, um die digitale Gesellschaft in diesem Fall zu beschreiben. Orwells Menschen litten unter den Repressionen eines autoritären Regimes und versuchten, sich dagegen zur Wehr zu setzen. Die geeignetere Dystopie ist Huxleys *Brave New World*, dessen Bürger freiwillig und affirmativ auf Teile ihrer Grundrechte verzichten, in der Überzeugung, dass der Staat nur so ein für sie besseres Leben garantieren kann.

Trotz dieser düsteren Metaphorik darf aber nicht übersehen werden, dass sich der Überwachungsstaat nicht entlang der literarischen Vorbildern ausgestaltet. Solange kritische Veröffentlichungen nicht zensiert werden oder ihre Autoren verschwinden, ist politische Willensbildung noch möglich. Solange die Regierung noch versucht zu vertuschen, anstatt zu verbieten, ist sie sich über die prinzipielle Fragwürdigkeit ihres Verhaltens zumindest im Klaren. Auch Papier und Riem haben nicht die für Absetzung der Regierung plädiert, was ein wahrhaft revolutionärer Akt gewesen wäre, sondern sie vielmehr zu konsequentem Handeln aufgefordert. Es besteht also noch Hoffnung, dass sich der Rechtsstaat in diesen Fragen irgendwann wieder seiner Wurzeln besinnt. Das aber bedarf auch Bürgerinnen und Bürger, denen ihre digitalen Grundrechte am Herzen liegen. Die Schule kann und sollte ein Ort sein, in denen diese Rechte vermittelt, eingeordnet und diskutiert werden, wo das notwendige Selbstbewusstsein gestärkt wird, das für eine Leben in der Informationsgesellschaft erforderlich ist.

Quellen

Alle URLs wurden im Juni 2014 auf ihre Erreichbarkeit überprüft.

ARIES, PHILIPPE; DUBY, GEORGES (1993): Geschichte des privaten Lebens. 5 Bde. Fischer.

BVERFG (1983): BVerfG · Urteil vom 15. Dezember 1983 · Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil). URL: <http://openjur.de/u/268440.html>

BVERFG (2008): BVerfG 1 BvR 370/07, 1 BvR 595/07 (Erster Senat) - Urteil vom 27. Februar 2008. URL: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

KITTLER, WOLF (1990): Das Posthorn. Signal und Symbol. In: *Kultur und Technik* 3/1990, S. 6-9. URL: <http://www.deutsches-museum.de/fileadmin/Content/data/Insel/Information/KT/heftarchiv/1990/14-3-6.pdf>

KREMPL, STEFAN (2014): Ex-Verfassungsrichter: Staat muss vor NSA-Ausspähung schützen. URL: <http://www.heise.de/newsticker/meldung/Ex-Verfassungsrichter-Staat-muss-vor-NSA-Ausspaehung-schuetzen-2195942.html>

Erscheint in LOG IN Heft Nr. 178/179 (2014), S. 21-26.

VON LEWINSKI, KAI (2012): Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: Jan-Hinrik Schmidt / Thilo Weichert (Hrsg.): *Datenschutz. Grundlagen, Entwicklungen und Kontroversen*. Bonn: bpb.

LEFFLER, RICARDA (2012): Der strafrechtliche Schutz des Rechts am eigenen Bild vor dem neuen Phänomen des Cyber-Bullying. Frankfurt: Lang.

UN (1948): Allgemeine Erklärung der Menschenrechte.
<http://www.un.org/depts/german/menschenrechte/aemr.pdf>

WARREN, SAMUEL; BRANDEIS, LOUIS (1890): The Right to Privacy. In: Harvard Law Review, Vol. IV/5, 15.12.1890.
http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html