# Von der Lochkarte zum Mobile Computing

## 20 Jahre Datenschutz in der Schweiz

**Herausgegeben durch**
**Datenschutz-Forum Schweiz**

Schulthess § 2012

# Das Bauchgefühl im Datenschutz

David Rosenthal*

**Inhaltsübersicht**



## 1. Einleitung

### 1.1 Viele Wertentscheide …

Wozu wird in der Schweiz heute Datenschutz betrieben? Die Frage muss gelegentlich gestellt werden, auch wenn sie die Gefahr birgt, den Fragenden in die Ecke der Naiven oder jener zu stellen, die die Privatsphäre der anderen für den

* Lic. iur., Konsulent einer Anwaltskanzlei in Zürich, Lehrbeauftragter der juristischen Fakultät der Universität Basel und der Eidg. Technischen Hochschule (ETH) Zürich

eigenen Profit zu opfern bereit sind. Die Frage muss gestellt werden, weil kaum eine Rechtsmaterie von ihren Anwendern derart häufig Wertentscheide abverlangt, um die Rechtmässigkeit eines bestimmten Tuns beurteilen zu können. Das gilt jedenfalls im Bereich der Datenbearbeitung durch Private, die nicht wie Behörden für jede Datenbearbeitung eine gesetzliche Grundlage benötigen[1] und sich damit nicht auf vorweg vom Gesetzgeber – zumindest teilweise – getroffene Wertentscheide abstützen können.

Wertentscheide erfordert schon die Anwendung der Bearbeitungsgrundsätze des Datenschutzgesetzes (DSG). Dies gilt nicht nur für den Grundsatz der Bearbeitung von Personendaten nur nach Treu und Glauben[2], sondern auch für die anderen Bearbeitungsgrundsätze. Zwar erscheinen der Zweckbindungsgrundsatz[3] und der Grundsatz der Transparenz[4] auf den ersten Blick als frei von jeglicher Wertung, da beide Bestimmungen letztlich nur die Erkennbarkeit einer Datenbearbeitung bzw. -erhebung und gewisser Parameter verlangen. Doch schon die Frage, wie deutlich eine Information erfolgen muss, damit sie hinreichend erkennbar ist, ist bereits eine Frage der Wertung, über die sich trefflich streiten lässt. Dasselbe gilt für die Frage, welche datenschutzrechtlichen Parameter erkennbar sein müssen und in welchem Detail. Liegt keine spezifische Information des Datenbearbeiters vor, sondern lediglich eine Erkennbarkeit aus den Umständen, was nach Art. 4 Abs. 3 DSG genügt, so stellt sich wiederum die Wertungsfrage, von welchen Bearbeitungszwecken bezüglich ihrer Personendaten die betroffene Person aufgrund der konkreten Umstände in guten Treuen ausgehen durfte und musste, als sie deren Beschaffung ermöglichte bzw. als diese stattfand. Auch dies ist in letzter Konsequenz eine Frage der Wertung der Umstände.

Auch der Grundsatz der Verhältnismässigkeit[5] verlangt in verschiedener Hinsicht Wertungen, etwa bezüglich der Frage, welche Personendaten für einen bestimmten Zweck tatsächlich erforderlich oder geeignet sind. Dies gilt erst Recht für die Frage, ob eine bestimmte Bearbeitung für eine betroffene Person zumutbar ist, also die Verhältnismässigkeit im engeren Sinne gegeben ist. Der Grundsatz der Richtigkeit der Daten[6] verlangt Wertentscheide bezüglich der Frage, wie weit dieses Erfordernis im Einzelfall tatsächlich gehen muss, da Richtigkeit nur aber immerhin verlangt, dass eine Tatsache mit Bezug auf die

**1** Art. 17 DSG.
**2** Art. 4 Abs. 1 DSG.
**3** Art. 4 Abs. 3 DSG.
**4** Art. 4 Abs. 4 DSG.
**5** Art. 4 Abs. 2 DSG.
**6** Art. 5 Abs. 1 DSG.

betroffene Person im Hinblick auf den Verwendungszweck sachgerecht wiedergegeben wird.

Der Grundsatz der Datensicherheit wiederum erfordert nur «angemessene» technische und organisatorische Massnahmen, um eine unbefugte Datenbearbeitung zu verhindern[7]. Diese sind zwar in der Verordnung zum Datenschutzgesetz näher ausgeführt, doch werfen die dortigen Präzisierungen noch mehr Wertungsfragen auf und stellen überdies klar, dass die Angemessenheit der Massnahmen periodisch zu überprüfen ist[8], also regelmässig zu kontrollieren ist, ob die einst getroffene Wertung noch zutrifft.

Wertentscheide erfordert auch die Frage der Rechtfertigung gemäss Art. 13 Abs. 1 DSG. Offenkundig ist dies im Falle der Interessenabwägung, aber auch die Rechtfertigung durch Einwilligung des Verletzten basiert letztlich auf gewissen Wertentscheiden, jedenfalls soweit die Gültigkeit der Einwilligung[9] zu beurteilen ist: Ist eine Einwilligung tatsächlich freiwillig erfolgt und nach angemessener Information? Für beide Aspekte können zwar Regeln und Grundsätze definiert werden, die dem Rechtsanwender eine gewisse Leitlinie in der Vornahme seiner Entscheide geben können. Ohne Wertungen kommt er jedoch auch hier nicht aus.

## 1.2 … und wenig Hilfestellung

So zahlreich die Wertentscheide sind, die das Datenschutzgesetz dem Rechtsanwender abverlangt, so gering sind die Hilfestellungen, die sich ihm dabei bieten (wobei mit Rechtsanwender vorliegend nicht nur Richter und Datenschutzbehörden, sondern auch all jene privaten Praktiker gemeint sind, welche in ihrem Alltag datenschutzrechtliche Fragestellungen zu beurteilen haben).

In einigen wenigen Fällen wird der Rechtsanwender auf Spezialisten anderer Disziplinen zurückgreifen können, so etwa im Bereich der technischen Datensicherheit. Allerdings ist dies eine trügerische Hilfe. Der Jurist vertraut in technischen Sicherheitsfragen zwar zu Recht gerne dem Informatik- oder IT-Sicherheitsexperten und lässt diesen daher zum Beispiel selbst entscheiden, ob und wann welche Verschlüsselungsstandards zum Einsatz kommen, wie Personen beim Netzwerkzugriff sicher identifiziert werden und welchen Standards ein Passwort genügen muss. Dies darf jedoch nicht darüber hinwegtäuschen, dass auch diese Spezialisten letztlich dieselben Wertungen vornehmen müssen, mit denen auch die Rechtsanwender konfrontiert sind. Sie haben zwar ein

**7** Art. 6 Abs. 1 DSG.
**8** Art. 8 Abs. 3 VDSG.
**9** Art. 4 Abs. 5 DSG.

technisches Fachwissen in Fragen der IT-Sicherheit. Dafür fehlt ihnen oftmals das Verständnis für die bearbeiteten Daten und deren Verwendungszweck – ein Verständnis, das für die Beurteilung der Angemessenheit einer Sicherheitsmassnahme nach Art. 6 Abs. 1 DSG genauso wichtig ist wie das Wissen über den Stand der Technik. Somit ist das Grundproblem des einer jeden solchen Massnahme zugrundeliegenden Wertentscheids nicht wirklich gelöst, sondern lediglich von einer Person an eine andere delegiert, wobei beide immer nur eine Seite der Medaille kennen. Der Unterschied besteht in der Praxis daher oftmals darin, dass IT-Sicherheitsexperten sich eher zutrauen, den nötigen Entscheid zu treffen, weil sie auf eine breitere Basis an «Best Practices» zurückgreifen können.

Der Jurist hat es da schwieriger. So hilft auch die Fachliteratur dem Rechtsanwender im Bereich des Datenschutzes erfahrungsgemäss wenig, wenn es darum geht, eine konkrete datenschutzrechtliche Wertentscheidung zu treffen. Zwar gibt es etliche Aufsätze und Bücher zum Thema Datenschutz. Allerdings beschränken sich viele Beiträge darauf, die bestehende Rechtslage zu beschreiben, manchmal auch sie zu kritisieren oder zu zeigen, warum im Alltag weit verbreitete Verhaltensweisen nach Ansicht der Autoren rechtswidrig sind, ohne jedoch praktikable Lösungsvorschläge aufzuzeigen. Sie können so zwar einen wertvollen Diskussionsbeitrag zur Weiterentwicklung des Datenschutzes leisten, doch dem Rechtsanwender helfen sie wenig.

Nicht sehr ergiebig ist diesbezüglich auch die Praxis der Gerichte, jedenfalls, wenn es um die Bearbeitung von Personendaten durch Private geht. Es gibt in der Schweiz viel zu wenig Gerichtsentscheide, als dass der Praktiker aus den wenigen Ausnahmen klare und einigermassen zuverlässige Leitlinien für seine datenschutzrechtlichen Wertentscheide ableiten könnte. Die Entscheide sind häufig ohnehin stark einzelfallbezogen, sodass sie sich für die Rechtsentwicklung im Bereich des Datenschutzes schon deswegen nur beschränkt eignen. Da sind die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) publizierten Stellungnahmen in aller Regel grundsätzlicherer Natur; auf seiner Website und in seinen Jahresberichten finden sich wertvolle Stellungnahmen zu zahlreichen Themen des Alltags. Allerdings ändert auch seine vergleichsweise eher pragmatische Haltung nichts daran, dass er in seiner Rolle vor allem die Interessen des Datenschutzes und der betroffenen Personen zu vertreten hat und seine Ansichten daher naturgemäss oft etwas einseitig sind.

## 1.3 Das Bauchgefühl als Rettungsanker

Dies führt dazu, dass der Rechtsanwender andere Wege finden muss, um den «richtigen» Wertemassstab für die Beurteilung datenschutzrechtlicher Konstellationen zu finden. Die dabei am häufigsten eingesetzte Methode ist das

Bauchgefühl. Über das Bauchgefühl wird in der Fachliteratur in der Regel kein einziges Wort verloren. Auch manche Datenschutzexperten werden nur hinter vorgehaltener Hand zugeben, dass sie in ihrem Alltag regelmässig und oft ziemlich blind ihrem Bauchgefühl vertrauen. Erst in einem zweiten Schritt werden sie eine rationale Begründung für ihr Bauchgefühl suchen und in aller Regel auch entwickeln können. Da erfahrungsgemäss sehr viele Personen im Bereich des Datenschutzes auf die Methode «Bauchgefühl» setzen, liefert sie überall dort, wo Menschen mit ähnlichem kulturellem Hintergrund und Gedankengut und in einer ähnlichen Situation sie einsetzen, auch entsprechend ähnliche Resultate. Sie erscheint damit jedenfalls auf den ersten Blick auch als vergleichsweise zuverlässig.

Die Methode «Bauchgefühl» ist daher trotz fehlender wissenschaftlicher Basis keineswegs abzulehnen, wenn es darum geht, zum Beispiel die Schwere eines Persönlichkeitseingriffs zu beurteilen (Fragen wie «Wie fände ich es, wenn dies mit meinen eigenen Daten geschehen würde?») oder wenn das Gewicht eines Rechtfertigungsgrundes (Fragen wie «Habe ich wirklich mein Bestes versucht, die Datenbearbeitung auf ein vernünftiges Mass zu reduzieren?») festgelegt werden muss. Einen offenkundigen Nachteil hat die Methode «Bauchgefühl» freilich: Sie ist der Subjektivität des Rechtsanwenders ausgeliefert.

So kann es sich lohnen, für einmal die üblichen Pfade der Rechtswissenschaft zu verlassen und die für den Datenschutz allem Anschein nach so wichtige Methode des «Bauchgefühls» etwas näher zu untersuchen. Namentlich stellt sich die Frage, ob sie tatsächlich so subjektiv ist, wie es auf den ersten Blick den Anschein macht. Oder anders formuliert: Es stellt sich die Frage, ob es nicht Methoden, Strategien und Konzepte gibt, mit denen sich die für datenschutzrechtliche Wertentscheidungen im Alltag erforderlichen Wertmassstäbe mit etwas mehr Objektivität und Systematik ermitteln und anwenden lassen, als bloss dem subjektiven Bauchgefühl zu vertrauen.

Um es vorwegzunehmen: Eine mathematische Formel, mit welcher sich Wertentscheidungen im Einzelfall objektiv und schematisch treffen lassen, wird auch hier keine präsentiert werden. Zwar lassen sich methodische Vorgehensweisen definieren, wie beispielsweise Interessenabwägungen, die im Rahmen einer datenschutzrechtlichen Rechtfertigung durchgeführt werden müssen. Auch der Autor der vorliegenden Zeilen hat das ausführlich getan. Allerdings führt kein Weg an der Erkenntnis vorbei, dass der Rechtsanwender irgendwann im Prozess immer an einen Punkt gelangt, an welchem er die verschiedenen gegenläufigen Interessen gewichten muss. Diese Gewichtung ermittelt letztlich jeder nach seinem Gefühl. Die Tatsache, dass ein guter Datenschutzjurist jedes solche Gefühl rational mehr oder weniger im Rahmen einer Darlegung der relevanten Werte und Interessen überzeugend sachlich begründen kann, ändert

nichts daran, dass es letztlich ein Gefühlsentscheid bleibt. Wie schwer wiegt zum Beispiel der Eingriff in die Privatsphäre eines Mitarbeiters, wenn eine von einem Unternehmen beauftragte Anwaltskanzlei seine E-Mail zu einem bestimmten Thema anschaut? Ändert der Anlass für die Untersuchung etwas an der Schwere des Eingriffs? Oder ob die Untersuchung durch andere Mitarbeiter des Unternehmens durchgeführt wird? Die Antworten auf diese vermeintlich einfachen Fragen werden je nach befragter Person erfahrungsgemäss sehr unterschiedlich ausfallen. Dabei kann keineswegs nur zwischen solchen Personen unterschieden werden, die normalerweise die Rechte von Arbeitnehmern vertreten und solchen, die primär für Unternehmen tätig sind. Die Antworten werden auch innerhalb der klassischen Interessenlager unterschiedlich ausfallen – und damit auch die Interessenabwägung.

Trotz allem gibt es methodische Hilfen, mit denen datenschutzrechtliche Wertentscheidungen etwas objektiver getroffen werden können. Das Ziel dieses Beitrags ist es, einige davon zu erläutern und zur kritischen Diskussion zu stellen.

## 2. Neun Regeln für objektivere Wertentscheidung

### 2.1. Regel 1: Es kommt nicht nur auf den Einzelfall an

Juristen neigen dazu, sich im Rahmen von rechtlichen Beurteilungen nur vom spezifischen Einzelfall leiten zu lassen. Das ist verständlich und hat auf den ersten Blick auch seine Richtigkeit, ist es doch im Rahmen einer Wertentscheidung regelmässig erforderlich, alle relevanten Umstände zu berücksichtigen. Diese ergeben sich aber nur aus dem spezifischen Einzelfall und sind in ihrer Gesamtheit jedes Mal anders. Das Ergebnis ist eine Einzelfallgerechtigkeit, die zwei Probleme mit sich bringt:

Erstens wird sie stark vom subjektiven Eindruck, den die beteiligten Personen auf den Betrachter hinterlassen, geprägt. Dieser ist oft unweigerlich vom Bedürfnis beeinflusst, die beteiligten Personen entsprechend ihrer Schutzwürdigkeit und Sympathie zu qualifizieren. Jeder erfahrene Prozessanwalt weiss: Nebst den nüchternen Fakten und sachlichen Rechtserwägungen zählt selbst bei erfahrenen Richtern letztlich immer der subjektive Eindruck, den eine Partei hinterlässt. Wer die Sympathien des Gerichts auf seiner Seite hat, hat zwar nicht den Prozess gewonnen, es in den materiellen Fragen aber leichter. Wem es gar gelingt, den Gegner gegenüber dem Gericht direkt oder über die Öffentlichkeit erfolgreich zu dämonisieren, hat einen noch besseren Stand, wenn es um Wertentscheidungen geht. Im Datenschutz gilt dies ganz speziell.

Zweitens birgt das Streben nach Einzelfallgerechtigkeit die Gefahr, dass die falschen Wertmassstäbe entwickelt werden. Wertmassstäbe sind zwar dazu da, auf einen konkreten Einzelfall angewandt zu werden. Entwickelt werden müssen sie jedoch vor dem Hintergrund, dass sie über den konkreten Einzelfall hinaus generell Geltung haben können und damit übertragbar sind. Wertmassstäbe sind letztlich Ausdruck einer Grundhaltung und nicht der wertmässigen Beurteilung des Einzelfalls. Dies ist zugegebenermassen keine leichte Aufgabe, da eine Vielzahl von Konstellationen berücksichtigt werden und das Ergebnis trotzdem auch im Einzelfall «stimmen» muss. Leider wird aber häufig gar nicht erst der Versuch unternommen, die dazu erforderliche gesamtheitliche Betrachtung vorzunehmen. Stattdessen wird ergebnisorientiert entschieden.

Wer vor einer datenschutzrechtlichen Wertentscheidung steht, kann sich zwar durchaus vom Einzelfall und allen Umständen inspirieren lassen. Aber er sollte in der Lage sein zu zeigen, dass der von ihm angewandte Wertmassstab – wie beispielsweise die Gewichtung der verschiedenen Interessen – nicht fallspezifisch ist. Namentlich sollte er aufzeigen können, dass der Wertmassstab auch dann zu «richtigen» Ergebnissen führt, wenn er auf vergleichbare Datenbearbeitungen, deren Zulässigkeit oder Unzulässigkeit allgemein anerkannt ist, angewandt wird. Das ist Regel 1. Es darf also z.B. nicht möglich sein, Aussagen zu treffen wie «wenn dies als gerechtfertigt beurteilt wird, müsste auch … als gerechtfertigt beurteilt werden, was aber niemand vernünftigerweise behaupten kann». Das ist nicht immer eine leichte Übung, doch wer der Meinung ist, es gäbe keine vergleichbaren Sachverhalte, auf welche sich ein bestimmter, ins Auge gefasster Wertmassstab anwenden liesse, ist vermutlich bereits im Abseits.

## 2.2 Regel 2: Immer mit gleicher Elle messen

Dass Wertmassstäbe nicht nur vor dem Hintergrund eines spezifischen Falls entwickelt werden dürfen, bedeutet natürlich nicht, dass alle auf den ersten Blick ähnlichen datenschutzrechtlichen Sachverhalte in einen Topf geworfen werden sollten. Es muss jedoch sichergestellt werden, dass immer mit der gleichen Elle gemessen wird. Das ist Regel 2. Diese setzt nicht gleiche Sachverhalte voraus, sondern lediglich Sachverhalte, die in den datenschutzrechtlich relevanten Parametern vergleichbar sind. Relevant sind tatsächliche, wertfreie Faktoren wie beispielsweise die möglichen Konsequenzen einer Datenbearbeitung. Wie schwerwiegend der betreffende Datenschutzverstoss gemeinhin erachtet wird, ist hingegen eine Wertungsfrage und darf für die vorliegenden Zwecke gerade kein Kriterium sein, um die Vergleichbarkeit zweier Sachverhalte zu beurteilen.

Kommt es bezüglich der Wertung der Persönlichkeitsverletzung durch Verletzung von Art. 12 Abs. 2 Bst. b DSG beispielsweise darauf an, ob eine klar nicht

für die Öffentlichkeit bestimmte Information über den Mitarbeiter einer Firma von (a) seinem eigenen Arbeitgeber, (b) einem Kollegen oder (c) einem Journalisten auf dem Internet gegen den Willen des Mitarbeiters publiziert wird? Während der Verrat durch den eigenen Arbeitgeber gemeinhin als besonders gravierend empfunden werden dürfte, wird die Publikation durch einen Journalisten je nach Fallkonstellation noch als akzeptabel gelten. Die Fälle erscheinen jedenfalls auf den ersten Blick nicht vergleichbar. Doch auf den zweiten Blick wird klar, dass bezüglich der Wertung der Schwere einer durch die öffentliche Zugänglichkeit einer Information bewirkte Persönlichkeitsverletzung die Person des Verletzers keine Rolle spielen darf. Denn öffentlich zugänglich ist öffentlich zugänglich, ganz gleich, wer dafür verantwortlich ist. Damit sind alle drei Fälle jedenfalls bezüglich dieser Frage bei Lichte betrachtet vergleichbar und nach demselben Wertmassstab zu beurteilen.

Mit anderen Worten: Bevor die erwähnte Preisgabe einer Information durch den Arbeitgeber als eine besonders gravierende Persönlichkeitsverletzung beurteilt wird, sollte sich der Rechtsanwender fragen, ob dieselbe Datenpublikation als genauso schwerwiegende Verletzung eingestuft werden müsste, wäre sie durch einen Kollegen oder einen Journalisten begangen worden. Nur wer dies ernsthaft bejahen kann, wendet einen einheitlichen Wertmassstab an und misst mit gleicher Elle. Das bedeutet natürlich nicht, dass die Person des Verletzers irrelevant ist; relevant ist sie jedoch in anderem Zusammenhang, etwa bezüglich einer Treueverletzung, einer allfälligen Rechtfertigung oder eines Verschuldens.

## 2.3 Regel 3: Abwarten, bis sich die Wogen glätten

Mit gleicher Elle zu messen, ist unter anderem deshalb schwierig, weil der Mensch ein «Gewohnheitstier» ist. Mit Bekanntem findet er sich über Zeit grundsätzlich ab, Neues ist hingegen tendenziell verdächtig und gefährlich. Das ist auch im Datenschutz so, und es soll an dieser Stelle als Fakt nicht kritisiert werden. Der Rechtsanwender sollte sich dieses Mechanismus jedoch bewusst sein, wenn er den «richtigen» Wertmassstab für eine datenschutzrechtliche Beurteilung sucht.

Zunächst kommt diesem Mechanismus eine Schutzfunktion zu. Wird einer neuen Form der Datenbearbeitung mit Misstrauen begegnet, so darf dies erfahrungsgemäss nicht als endgültige Wertung betrachtet werden. Das Misstrauen dient vielmehr dazu, Schäden durch etwaige Kinderkrankheiten und anfängliche Missbräuche in Grenzen zu halten. Es sorgt zudem dafür, dass all jene, die mit neuen Entwicklungen – zum Beispiel im Bereich des Internets – auf den Markt kommen wollen, im Bereich des Datenschutzes normalerweise

höhere Anstrengungen unternehmen und strengere Standards erfüllen müssen als bereits etablierte Datenbearbeiter in anderen Branchen. Letztere haben das Vertrauen der Kundschaft bereits.

Für den Rechtsanwender, der sich mit einer solchen neuen Anwendung beschäftigen muss, bedeutet dies, dass er negative aber auch positive Äusserungen zu solch einer neuen Entwicklung mit Vorsicht geniessen muss und warten sollte, bis sich eine erste Aufregung im Guten wie im Schlechten gelegt hat, bevor er darauf abstellt, wie beispielsweise die Öffentlichkeit auf eine ihr bis dato unbekannte Form der Datenbearbeitung reagiert. Dies ist Regel 3. Sie wird im Eifer des Gefechts, wenn eine neue Form der Datenbearbeitung die Wogen hoch gehen lässt, leider häufig missachtet. Wer sich jedoch an Regel 1 hält, wird kaum in diese Falle tappen.

## 2.4 Regel 4: Soziale Akzeptanz reflektiert öffentliches Interesse

Hat sich eine bestimmte Form der Datenbearbeitung erst einmal etabliert, wird ihr in unserer Gesellschaft selten mit Ablehnung begegnet. Das gilt notabene auch für Datenbearbeitungen, die sich nach Gesetz auf den ersten Blick ohne Weiteres als rechtswidrige Handlungen qualifizieren lassen aber gesellschaftlich letztlich akzeptiert sind, weil sie im Alltag andauernd und überall vorkommen. Dem hat der Rechtsanwender auch in rechtlicher Hinsicht Rechnung zu tragen.

Man nehme das Beispiel des Kaffeeklatsches: Der dabei im Büro, im privaten Umfeld oder sonst stattfindende Austausch von mitunter intimen und – naturgemäss – oft auch peinlichen Informationen über ebenfalls naturgemäss nicht anwesende Dritte wird häufig ohne Weiteres als Verletzung von Art. 12 Abs. 2 Bst. c DSG zu qualifizieren sein. Trotzdem ist dem Autor kein einziger Fall bekannt, in welchem nur schon erwogen wurde, wegen einer solchen Klatschrunde den Richter anzurufen, auch wenn eine solche dem Ruf einer Person sehr viel abträglicher sein kann als andere Bekanntgaben besonders schützenswerter Personendaten oder Persönlichkeitsprofilen.

Woran liegt das? Ist es letztlich nur eine Frage der Kosten, Opportunität und Praktikabilität, dass solche Persönlichkeitsverletzungen rechtlich nicht verfolgt werden? Auch wenn sich kein privater Kläger für einen solchen Prozess finden würde, so wären an sich alle Voraussetzungen für eine Popularklage des EDÖB nach Art. 29 DSG erfüllt. Trotzdem wird niemand vom EDÖB ernsthaft verlangen, einen Musterprozess gegen die Beteiligten an einem Kaffeeklatsch durchzuführen. Daher stellt sich die womöglich provokative Frage, ob ein Verhalten, das zwar die Persönlichkeit der betroffenen Personen regelmässig verletzt, trotz allem zulässig sein kann, weil es allgemein akzeptiert und überall so praktiziert wird.

Ein Datenschutzexperte mit professionellem Selbstrechtfertigungstrieb dürfte diese Frage tendenziell mit dem Hinweis verneinen, dass es keine Gleichbehandlung im Unrecht gibt und die Tatsache, dass eine Persönlichkeitsverletzung häufig vorkommt, diese nicht zu rechtfertigen vermag. Eine solche Antwort ist jedoch zu kurz gegriffen, denn auch hier geht es letztlich um die Frage der Wertung und damit der Werte, auf die im Rahmen der rechtlichen Beurteilung solcher Vorfälle abgestellt werden muss.

Wer aber definiert diese Werte? Ist es die Gesellschaft an sich, die das tut, ist der Kreis geschlossen und die Antwort auf die aufgeworfene Frage offenkundig: Falls die Gesellschaft das Interesse an der Möglichkeit des Kaffeeklatsches als gewichtiger bewertet als jenes der davon betroffenen Personen, muss die damit verbundene Persönlichkeitsverletzung im Rahmen der Interessenabwägung von Art. 13 Abs. 1 DSG gerechtfertigt und damit erlaubt sein. Zu beachten ist, dass es hier bloss um soziale Akzeptanz geht und nicht darum, ob die Gesellschaft den Austausch von Klatsch für besonders wertvoll erachtet. Es genügt, dass die Gesellschaft ihn nicht missen möchte, obwohl er unstreitig negative Auswirkungen haben kann, sich kaum jemand offen dazu bekennen wird und manche sich nicht einmal daran beteiligen. Ob dabei auf ein überwiegendes öffentliches oder ein überwiegendes privates Interesse abgestellt wird, ist eine Formalie und hier daher irrelevant. Der Kaffeeklatsch ist auch nur ein Schulbeispiel, um das der datenschutzrechtlichen Rechtfertigung zugrunde liegende Wertsystem zu illustrieren. Das Beispiel ist austauschbar, das Konzept immer dasselbe: Es geht nicht um eine Gleichbehandlung im Unrecht, sondern darum, dass die soziale Akzeptanz einer Persönlichkeitsverletzung im bestehenden Datenschutzgesetz letztlich dazu führen kann, dass diese Verletzung auch rechtlich kein Unrecht (mehr) darstellt.

Eine solche Erkenntnis birgt freilich einiges an Konfliktpotenzial. Denn die Relevanz der sozialen Akzeptanz zur Beurteilung der Rechtfertigung von Persönlichkeitsverletzungen kann im Ergebnis dazu führen, dass – negativ ausgedrückt – die Rechte des Einzelnen vor dem Hintergrund der als überwiegend erachteten Interessen des Kollektivs oder eines Teils davon geopfert werden. So kann es im Zeitalter der Informationsgesellschaft zu einem schleichenden Verlust der Privatsphäre kommen, falls und wenn die Gesellschaft die Vorteile und Chancen der Bearbeitung von immer mehr Personendaten beispielsweise durch Internet-Anbieter als grösser einschätzt als die Nachteile und Risiken einer solchen Bearbeitung. Aber auch der umgekehrte Vorgang kann eintreffen: Widerfährt einem Unternehmen beispielsweise eine grosse, schlagzeilenträchtige Datenschutzpanne, wird regelmässig der Ruf nach strengeren Datenschutzgesetzen laut, um die betroffenen Personen vermeintlich besser vor den Folgen solcher Pannen zu schützen. So können Vorkehrungen zum Datenschutz, die

vor einigen Jahren noch als angemessen erachtet wurden, aufgrund veränderter gesellschaftlicher Ansichten plötzlich den Anforderungen des Datenschutzes nicht mehr genügen und damit kann geltendes Recht verletzt sein. Dass eine Datenschutzpanne systembedingt nicht ein Problem der fehlenden materiellen Regelung darstellt, sondern eines derer fehlenden Einhaltung ist, ändert nichts daran, dass auch der Datenschutz einem gesellschaftlichen Wertewandel unterliegt, der rationale wie irrationale Ursachen haben kann. Dieser Wandel wiederum ist in der Anwendung des Datenschutzes angemessen zu berücksichtigen, wenn wie etwa im Rahmen der Rechtfertigung Wertentscheidungen zu treffen sind.

Der Gesetzgeber hat sich diesem Konflikt bisher «entzogen»: Er hat es tunlichst vermieden, bezüglich der Bearbeitung von Personendaten durch Privatpersonen entsprechende Wertentscheide zu treffen. Stattdessen sah er das in Art. 13 Abs. 1 DSG geregelte Verfahren der Abwägung aller auf dem Spiel stehenden Interessen vor. Nicht einmal die in Art. 13 Abs. 2 DSG beispielshaft aufgeführten Fallkonstellationen legen verbindlich fest, ob ein überwiegenden privates Interesse besteht. Ein überwiegendes privates Interesse des Datenbearbeiters ist in den exemplarisch aufgezählten Fällen lediglich «in Betracht» zu ziehen. Auch der Hinweis in der bundesgerichtlichen Rechtsprechung, wonach ein überwiegendes Interesse an einer Datenbearbeitung nur zurückhaltend angenommen werden darf[10], besagt letztlich nur, dass die Datenschutzinteressen auch einer einzelnen Person als gewichtig erachtet werden müssen. Die Interessenabwägung wird damit nicht vorweggenommen, und sie ist binär: Ist das Interesse an der Durchführung einer bestimmten Datenbearbeitung grösser als jenes gegen ihre Durchführung, ist das Erfordernis der Rechtfertigung erfüllt – und sonst nicht. Oder bildlich ausgedrückt: Es genügt, wenn das Gewicht des Interesses des Datenbearbeiters und der Öffentlichkeit das Datenschutzinteresse der betroffenen Person um ein Gramm übertrifft; ein Kilogramm an Differenz braucht es nicht. Wie schwer das Datenschutzinteresse einer betroffenen Person gegen eine Datenbearbeitung wiegt und wie schwer jenes dafür, besagt das Datenschutzgesetz aber nicht. Diese Wertung hat der Gesetzgeber bewusst nicht vorgenommen und damit das Datenschutzgesetz wandelnden Wertvorstellungen gegenüber offen gehalten.

Der Ball liegt somit wiederum beim Rechtsanwender, der versuchen muss, die Interessenabwägung nach möglichst objektiven Kriterien in jedem Fall von Neuem vorzunehmen. Er kann zwar den Datenschutzinteressen betroffener Personen mit Hinweis auf die bundesgerichtliche Rechtsprechung ein gewisses Gewicht zusprechen. Er kann ihnen mit Hinweis auf den grundrechtlichen

**10** BGE 136 II 508, Erw. 6.3.3.

Kerngehalt des Persönlichkeitsschutzes sogar einen gewissen Minimalschutz zuweisen. Doch das System des Datenschutzgesetzes verlangt, dass im Rahmen einer Interessenabwägung zwecks Rechtfertigung einer Persönlichkeitsverletzung zwingend alle legitimen Interessen angemessen zu berücksichtigen sind, also nicht nur die Datenschutzinteressen der betroffenen Personen. Auch kann die Gewichtung Letzterer nicht so ausgestaltet sein, dass das Ergebnis der Abwägung dadurch vorweggenommen ist, dass das Datenschutzinteresse in der Praxis praktisch immer überwiegt. Ansonsten würde das Instrument der Interessenabwägung seines Sinngehalts beraubt, was dem Willen des Gesetzgebers widersprechen würde, der das System der Rechtfertigung einer Verletzung nicht nur in Art. 13 Abs. 1 DSG, sondern schon in der Grundnorm von Art. 28 Abs. 2 ZGB vorgesehen hat. Auch der erwähnte grundrechtliche Kerngehalt des Persönlichkeitsschutzes wird in Anbetracht der bundesgerichtlichen Rechtsprechung[11] eher eng verstanden werden müssen.

Im Ergebnis bedeutet dies, dass der Rechtsanwender im Rahmen der Interessenabwägung nicht um die Gretchenfrage der sozialen Akzeptanz herumkommt, d.h. wie weit die Gesellschaft zu gehen bereit ist, den Persönlichkeitsschutz des Einzelnen zu gewährleisten und inwieweit sie bereit ist, Verletzungen desselbigen hinzunehmen, um bestimmte Datenbearbeitungen im Interesse anderer Werte zu ermöglichen. Diese Frage muss sich der Rechtsanwender stellen, wenn er die Wertordnung ermitteln will, mit welcher er die auf dem Spiel stehenden Interessen gewichten will. Das ist Regel 4.

## 2.5 Regel 5: Die stille Masse gibt den Takt

Die Antwort auf die Frage gemäss Regel 4 können allerdings weder Politiker, noch Datenschützer, noch die Medien geben, auch wenn sich diese üblicherweise am lautesten Gehör verschaffen, wo und wie Datenschutz praktiziert werden sollte oder nicht. Es ist stattdessen die «stille Masse», an welcher sich der Rechtsanwender orientieren muss. Sie ist es auch, die letztlich mit dem Ergebnis leben muss: Über sie werden Daten bearbeitet, und ihr kommt die Bearbeitung der Daten in der einen oder anderen Form zugute oder eben nicht. Damit ist Regel 5 definiert.

Die Frage ist dabei nicht, ob die Bevölkerung bereit ist, die Rechte eines Einzelnen zugunsten des Kollektivs zu opfern, sondern umgekehrt, wie weit

**11** Vgl. etwa BGE 136 III 401 betr. eine Vereinbarung über erotische Fotos im Internet. Das Bundesgericht befand, dass die Veröffentlichung von (zulässigerweise aufgenommenen) Fotos der Intimsphäre einer Person nicht (mehr) den höchstpersönlichen Kern deren Persönlichkeit tangiere (Erw. 5.4.2).

der Einzelne bereit ist, Eingriffe zu akzeptieren, wenn er im Gegenzug das erhält, was die Datenbearbeitung ihm an Vorteilen und Chancen verspricht, auch wenn er sie letztlich nicht selbst beanspruchen kann, sondern sie nur dem Kollektiv zugutekommen.

Es ist absehbar, dass diese Ansicht in Datenschutzkreisen nicht unbedingt geteilt werden wird. Es dürfte insbesondere argumentiert werden, dass auf die Ansicht der «stillen Masse» deshalb nicht abgestellt werden könne, weil sie gar nicht verstehe, was mit ihren Daten geschieht und welche Risiken sich hinter einer Datenbearbeitung verbergen können. Das mag je nach Fallkonstellation sogar zutreffen. Die Frage muss jedoch erlaubt sein, ob die mangelnde Sachkunde bezüglich der Konsequenzen einer Datenbearbeitung überhaupt relevant ist, wenn es darum geht zu ermitteln, welches Gewicht die Gesellschaft dem Schutz der Privatsphäre in einem bestimmten Bereich beimisst.

Mangelnde Sachkunde kann in einer solchen Situation sogar ein Indiz dafür sein, dass das Datenschutzinteresse in diesem Bereich eher tief ist, dem Datenschutz seitens der potenziell betroffenen Personen also ein eher geringes Gewicht beigemessen wird. Dies wäre wiederum im Rahmen der Interessenabwägung zu berücksichtigen. Die Erfahrung zeigt nämlich, dass jedenfalls ein grosser Teil der Schweizer Bevölkerung den eigenen Daten bei weitem nicht den Wert zumisst, der ihnen nach Ansicht der Datenschützer zuteilwerden sollte. Nicht ohne Grund sind Konsumenten nachwievor mehrheitlich bereit, einem Händler ihre persönlichen Kaufinteressen zur Auswertung und Verwendung für beinahe beliebige Zwecke im Gegenzug für ein «Butterbrot» anzuvertrauen; die zahlreichen Kundenkartenprogramme des Schweizer Detailhandels belegen dies deutlich.

Doch wenn dem so ist, ist es dann Sache des Datenschutzgesetzes und seiner Anwender, die Schweizer Bevölkerung vor ihrer eigenen «Geringschätzung» in Bezug auf ihre eigenen Personendaten und Datenschutzinteressen zu schützen? Oder müsste nicht genau diese Erkenntnis im Wertmassstab berücksichtigt werden, der für die Gewichtung der Interessen im Rahmen derer Abwägung massgeblich ist? Wenn Letzteres nicht der Fall ist, was ist dann der relevante Massstab? Sind es die Werte, welche die Gesellschaft dem Persönlichkeitsschutz vernünftigerweise zumessen sollte, auch wenn sie es in Tat und Wahrheit nicht tut? Und wer entscheidet, was vernünftig ist?

## 2.6 Regel 6: Informationelle Selbstbestimmung ist wertneutral

Die vorstehende Diskussion zeigt, dass sich der Datenschutz nicht an theoretischen Wunschvorstellungen, sondern an denjenigen Werten orientieren muss, welche ihm die Gesellschaft zum jeweiligen Zeitpunkt tatsächlich beimisst. Sie

macht aber auch deutlich, dass es nicht darum gehen kann, die Interessen des Kollektivs einfach über jene des Individuums zu stellen, zumal der Schutz des Einzelnen für sich einen wichtigen gesellschaftlichen Grundwert darstellt, den es zu bewahren gilt.

Was der «Schutz des Einzelnen» in datenschutzrechtlichen Fragen tatsächlich verlangt, bedarf freilich der näheren Betrachtung. Die Antwort darauf ergibt sich aus dem Ziel des Datenschutzes, wie ihn Art. 13 Abs. 2 BV definiert: Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Damit ist das Recht auf informationelle Selbstbestimmung gemeint, also das Recht einer Person über die Bearbeitung sie betreffender Daten zu bestimmen, d.h. zu bestimmen, wer welche dieser Daten zu welchem Zweck wie bearbeiten darf.

Es ist unbestritten, dass dieses Recht auch im Rahmen von datenschutzrechtlichen Wertentscheidungen zu berücksichtigen ist. Die Ansichten gehen allerdings auseinander bezüglich der Frage, wie das Recht auf informationelle Selbstbestimmung konkret zur Anwendung gelangen soll und welche Annahmen dabei zu treffen sind.

Hierbei ist als Regel 6 zunächst zur Kenntnis zu nehmen, dass das Recht auf informationelle Selbstbestimmung wertneutral ist, d.h. in alle «Richtungen» ausgeübt werden kann: Eine betroffene Person kann sich auf das Recht der informationellen Selbstbestimmung berufen, wenn sie *nicht* möchte, dass ihre Daten bearbeitet werden. Eine betroffene Person kann sich aber auch auf das Recht auf informationelle Selbstbestimmung berufen, wenn sie *möchte,* dass ihre Daten bearbeitet werden. Das ergibt sich zwar nicht aus dem Wortlaut von Art. 13 Abs. 2 BV, welcher nur von einem Schutz vor Missbrauch spricht, doch ergibt es sich klar aus dem Konzept der informationellen Selbstbestimmung: Der Wille einer betroffenen Person, dass ihre Daten in einer bestimmten Art und Weise bearbeitet werden dürfen, ist ebenso zu respektieren wie ihr Wille, dass dies nicht geschehen darf. Das ergibt sich wiederum aus dem System der Rechtfertigung gemäss Art. 13 Abs. 1 DSG, wonach die Einwilligung einer betroffenen Person – in den Schranken von Art. 27 ZGB und der Rechtsordnung – die Rechtswidrigkeit einer Persönlichkeitsverletzung *per se* ausschliesst. Die Interessen der betroffenen Person an einer Datenbearbeitung sind überdies im Rahmen der Interessenabwägung zu berücksichtigen.

Leider wird diese Erkenntnis in der Praxis allzu selten beachtet, weil viele das Ziel des Datenschutzes in erster Linie darin sehen, die Bearbeitung von Personendaten möglichst stark einzuschränken. Der Autor des vorliegenden Beitrags ist zwar ebenfalls der Meinung, dass eine Person gut daran tut, ihre nicht allgemein bekannten Personendaten Dritten nur sehr zurückhaltend bekanntzugeben. Doch auch er muss zur Kenntnis nehmen, dass es viele, auch stark abweichende Ansichten gibt, wie in der heutigen Zeit der Begriff der Privatsphäre zu

definieren ist und wie weit der Datenschutz die Bearbeitung von Personendaten einschränken soll. Das Internet ist ein gutes Beispiel: Es hat nicht nur das Recherchieren und sonstige Bearbeiten fremder Personendaten sehr viel einfacher gemacht; es hat auch viele Personen überhaupt erst dazu bewogen, ihre eigenen Personendaten mit zahlreichen anderen Personen zu teilen und die eigene Privatsphäre aufzugeben – ganz bewusst und ohne Zwang. Den einen ist völlig egal, wenn nebst ihren echten Freunden auch andere Personen von ihren Fotos Kenntnis nehmen können. Andere wollen sogar, dass die Öffentlichkeit von ihrem Privatleben und ihren privaten Ansichten Kenntnis nimmt, auch wenn die Öffentlichkeit sich für diese normalerweise gar nicht interessiert.

Es ist daher vermessen, die eine oder andere Ansicht als Wertmassstab zu nutzen, wenn es um das Fällen von datenschutzrechtlichen Wertentscheiden geht. Auch das Datenschutzgesetz stipuliert keine Präferenz für die eine oder andere Haltung: Keine einzige Bestimmung des Datenschutzgesetzes erfordert für die Bearbeitung von Personendaten die Zustimmung der betroffenen Person; die Zustimmung wird regelmässig nur dann relevant, wenn es darum geht, eine Persönlichkeitsverletzung zu rechtfertigen. Auch stellt das Datenschutzgesetz keine gegenüber anderen Rechtsbereichen erhöhten Anforderungen an eine gültige Einwilligung.

Nicht einmal die Bearbeitungsgrundsätze sind nach dem Grundsatz des grösstmöglichen Schutzes der Privatsphäre ausgestaltet. Entscheidend ist vor allem, welchen Zweck der Datenbearbeiter bei der Erhebung der Daten deklariert. Im Rahmen der Zumutbarkeit und der Rechtsordnung darf ein Datenbearbeiter diesen Zweck jedoch frei festlegen. Der vielzitierte Grundsatz der Datensparsamkeit wiederum definiert sich einzig über diesen Zweck und ist damit relativ. Wer eine Internet-Plattform betreibt, deren Zweck die Veröffentlichung von privaten Fotos ist, darf auf dieser Plattform genau dies tun, vorausgesetzt den betroffenen Personen war dieser Zweck klar (und nicht unzumutbar), als sie die Fotos einstellten bzw. der Betreiber die Daten über sie erhob. Wollen die betroffenen Personen dies nicht oder nicht mehr, müssen sie widersprechen, also von sich aus tätig werden.

## 2.7 Regel 7: Stillschweigen bedeutet nicht Ablehnung

Wird einmal akzeptiert, dass das Recht auf informationelle Selbstbestimmung ein Recht ist, das in alle Richtungen geht, so stellt sich die Frage, wie es dort anzuwenden ist, wo die betroffene Person es nicht ausgeübt hat.

Das Datenschutzgesetz gibt auf diese Frage keine ausdrückliche Antwort. Es legt fest was dort gilt, wo sich eine Person gegen eine Datenbearbeitung ausgesprochen hat; in diesem Falle liegt *per se* eine Persönlichkeitsverletzung

vor[12]. Das Datenschutzgesetz sagt umgekehrt auch, dass eine Einwilligung in eine Datenbearbeitung eine damit allfällig verursachte Persönlichkeitsverletzung *per se* rechtfertigt und sie damit zulässig ist[13]. Es definiert jedoch nicht, was als Standard – oder neudeutsch als «Default» – gelten soll, wenn sich die betroffene Person weder in der einen noch der anderen Richtung dazu äussert, wie sie zu einer bestimmten Datenbearbeitung steht.

Datenschützer fordern hier wenig überraschend, dass der Standard im Schutz der Privatsphäre liegen muss: Solange die betroffene Person nichts anderes kundgibt, soll demnach davon ausgegangen werden, dass sie ihr Recht auf informationelle Selbstbestimmung einschränkend ausübt, d.h. dass ihre Personendaten *nicht* in einer bestimmten Weise bearbeitet werden dürfen. Hierzu schrieb der EDÖB im Vorwort zu seinem 17. Jahresbericht (2009/2010) unter dem Titel «Goldgräberstimmung im Internet – das Ende der Privatsphäre», dass jeder Anbieter per Gesetz verpflichtet werden müsse, jene Technologie und jene Einstellungen zu wählen, die den «grösstmöglichen Schutz der Privatsphäre» garantieren würden[14]. Und weiter: «Nutzer, die darauf verzichten wollen, können dies tun, sie müssen aber von sich aus aktiv werden und die Grundeinstellungen ihrer Accounts anpassen.»[15]

Eine solche Forderung ist nachvollziehbar, und sie erscheint auf den ersten Blick auch vernünftig und wünschenswert. Bei näherer Betrachtung ist sie jedoch zu hinterfragen.

Zunächst handelt es sich um Forderungen *de lege ferenda*. Das heutige Datenschutzgesetz sieht diese Präferenz des grösstmöglichen Schutzes der Privatsphäre nicht vor. Es bürdet es wie gezeigt der betroffenen Person auf, sich gegen eine zu weit gehende Bearbeitung ihrer Personendaten zu wehren, d.h. ihr zu widersprechen. Dieses «Opt-out»-Konzept wiederspiegelt sich im Zweckbindungsgrundsatz von Art. 4 Abs. 3 DSG und ebenso im Grundsatz der Erkennbarkeit nach Art. 4 Abs. 4 DSG. Entscheidend ist somit, ob die betroffene Person die zur Diskussion stehende Datenbearbeitung erkennen konnte, denn nur dann kann sie ihr bei Bedarf auch widersprechen. Tut sie dies jedoch nicht, ist lediglich in extremen Situationen durch den Verhältnismässigkeitsgrundsatz nach Art. 4 Abs. 2 DSG sichergestellt, dass der Schutz der Privatsphäre nicht zu sehr ausgehöhlt wird. Das geschieht allerdings weder über das im Verhältnismässigkeitsgrundsatz enthaltene Erfordernis der Datensparsamkeit noch über die Anforderung, wonach nur geeignete Daten bearbeitet werden dürfen,

**12** Art. 12 Abs. 2 Bst. b DSG.
**13** Art. 13 Abs. 1 DSG.
**14** http://www.edoeb.admin.ch/dokumentation/00445/00509/01615/01617/index.html?lang=de.
**15** Ebd.

da beide keine absolute Schranke der Datenbearbeitung definieren, sondern ihrerseits vom Zweck der Datenbearbeitung abhängig sind. Es ist vielmehr der dritte Aspekt des Verhältnismässigkeitsgrundsatzes, die Verhältnismässigkeit im engeren Sinn, welche im Einzelfall dazu führen kann, dass eine aus der Perspektive der betroffenen Person (objektiv) zu weit gehende Datenbearbeitung zur Persönlichkeitsverletzung wird. In der Praxis wird dieser Punkt jedoch eher selten erreicht; es braucht somit viel, bis eine Datenbearbeitung für eine davon betroffene Person als unzumutbar erachtet werden muss.

Die Forderung des grösstmöglichen Datenschutzes als «Standard» erweist sich auch in der Umsetzung als problematisch. Die immer wieder ins Feld geführten Social-Media-Plattformen im Internet sind ein Beispiel: Was wäre hier der «grösstmögliche» Schutz der Privatsphäre? Er läge darin, sich gar nicht anzumelden. Wenn aber der Zweck einer Plattform darin besteht, dass deren Benutzer ihre Privatsphäre in einem bestimmten Umfang aufgeben und auch anerkannt wird, dass jedermann gerade *wegen* der informationellen Selbstbestimmung das Recht haben sollte, dies zu tun, worin kann dann der geforderte «grösstmögliche Schutz der Privatsphäre» bestehen? Besteht er darin, dem Benutzer mehrere Optionen anzubieten, in welchem Umfang er seine Privatsphäre aufgeben möchte? Und wenn ja, wo ist die Grenze in Bezug auf diese einzelnen Optionen zu ziehen und wieviele Optionen muss er haben? Welchen Aufwand hat der Anbieter diesbezüglich zu betreiben? Diese Fragen zeigen bereits, dass die Forderung des grösstmöglichen Datenschutzes letztlich ein Allgemeinplatz ist. Entscheidend kann nur sein, ob den Benutzern der Social-Media-Plattformen vorgängig hinreichend klar gemacht wurde, wie ihre Daten bearbeitet werden. Ist dies geschehen, haben sie nicht widersprochen, oder haben sie durch Übermittlung ihrer Daten sogar eingewilligt, ist jedenfalls dem informationellen Selbstbestimmungsrecht Genüge getan. Es liegt dann an jeder Person selbst, darüber zu entscheiden, wie sie sich verhalten will. Dazu gehört auch der Entscheid darüber, ob sie sich für das Schicksal und damit den Schutz ihrer Daten überhaupt interessiert. Bei vielen betroffenen Personen dürfte schon Letzteres nicht der Fall sein.

Genau dies scheint auch der Grund dafür zu sein, dass Datenschützer heute Forderungen nach einem Standard des «grösstmöglichen» Schutzes der Privatsphäre aufstellen. Es ist die Annahme, dass die breite Masse der Bevölkerung mit dem Konzept des Datenschutzes, welches auf Eigenverantwortung der betroffenen Personen setzt, nicht oder nicht mehr zurechtkommt. Nach der hier vertretenen Ansicht ist eine solche Annahme wie dargelegt in dieser Allgemeinheit unzutreffend. Sie verkennt, dass mangelndes Interesse am Schutz der Privatsphäre und mangelnde Eigeninitiative keineswegs in mangelnder Eigenverantwortung begründet sein müssen.

Trotzdem erliegt der Gesetzgeber gerade im Bereich des Datenschutzes immer wieder der falschen Versuchung, die betroffenen Personen zu ihrem «Glück» zu zwingen. Ein Beispiel ist die Verschärfung der Regeln betreffend des Einsatzes von «Cookies» im Internet. Diese Technik erlaubt es Betreibern von Websites, Besucher ihrer Website wiederzuerkennen. Sie können dies, indem sie beim ersten Besuch dem Internet-Browser des Benutzers zum Beispiel einen Identifikationscode (ein «Cookie») übermitteln. Je nach Privacy-Einstellung des Browsers des Benutzers wird dieser den Code der Website auf dem Computer des Benutzers speichern und beim nächsten Besuch der Website ihr wieder mitteilen. Auf diese (oder ähnliche) Weise wird eine Re-Identifikation ermöglicht. Der Benutzer kann es also selbst steuern, ob er wiedererkannt wird oder nicht. Die Technik wird heute für statistische Auswertungen, für Profile von Benutzern und für die Speicherung von Benutzernamen und anderen Daten benutzt. Etliche Online-Shops würden ohne Cookies nicht mehr richtig funktionieren. Cookies können aber auch benutzt werden, um die Bewegungen von Benutzern über mehrere Websites hinweg zu verfolgen. Schon seit etlichen Jahren gilt daher in der EU und in der Schweiz die Pflicht, den Benutzer über solche «Cookies» zu informieren, in der Schweiz jedenfalls soweit es sich um Personendaten handelt[16]. Es muss auch informiert werden, wie sich das Tracking durch «Cookies» abstellen lässt. Diese Information erfolgt regelmässig im Rahmen der Datenschutzerklärungen, wie sie sich heute auf den meisten kommerziellen Websites finden. Dem Europäischen Parlament hat diese «opt-out»-Regelung jedoch nicht genügt. Es hat vor kurzem die betreffende Richtlinie dahingehend angepasst, dass inskünftig grundsätzlich die Zustimmung des betroffenen Benutzers erforderlich wird, bevor ein Cookie gesetzt werden darf[17]. Wie dies im Einzelnen zu geschehen hat und welche Ausnahmen gelten sollten[18], ist zwar noch nicht ganz klar, da diverse EU-Mitgliedsstaaten die betreffende Richtlinie trotz abgelaufener Frist noch nicht umgesetzt haben. Es ist jedoch absehbar, dass Internet-Benutzer zwar in Zukunft noch mehr Bestätigungen anklicken oder Warnungen zur Kenntnis nehmen müssen, bevor sie ein Angebot im Internet nutzen können[19]. Genauso absehbar ist auch, dass die meisten Internet-Benutzer diese Bestätigungen oder Warnungen ebenso rasch und ohne nähere

**16** Art. 45c FMG; für die EU siehe Art. 5 Abs. 3 der EU Richtlinie 2002/58/EG.

**17** EU Richtlinie 2009/136/EG vom November 2009, mit welcher auch Art. 5 Abs. 3 der EU Richtlinie 2002/58/EG angepasst wurde.

**18** Z.B. bei Cookies für virtuelle Einkaufswagen und vorübergehenden Cookies («Session-Cookies»).

**19** Vgl. jedoch die Empfehlung 16/2011 (WP188) der Artikel-29-Datenschutzgruppe vom 8. Dezember 2011 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf).

Gedanken abgeben bzw. wegklicken werden, wie sie dies schon mit anderen, ähnlichen Warnungen oder Nutzungsbedingungen tun, mit denen sie im Internet dauernd konfrontiert werden und die sie nie lesen. Ausser technischem Mehraufwand und zusätzlichen Aufträgen für Datenschutzberater wird das EU-Parlament mit seiner Gesetzesverschärfung nach der hier vertretenen Ansicht somit nichts erreichen.

Wird der Datenschutz im Bereich der Cookies tatsächlich als unzureichend erachtet, wäre es ehrlicher und vernünftiger gewesen, darauf hinzuwirken, dass die Benutzer sich der Möglichkeiten zur Abwehr von Datenerhebungen über Cookies besser bewusst werden. Denn mit den in heutigen Browsern verfügbaren Privacy-Funktionen lässt sich eine Überwachung durch Cookies ohne Weiteres verhindern oder einschränken – der Benutzer muss diese Funktionen bloss in Anspruch nehmen. Zwar hat diese Vorgehensweise den Schönheitsfehler, dass sie bei der betroffenen Person und nicht beim Datenbearbeiter als Verursacher des Problems ansetzt. Der Schutz der betroffenen Person wäre abermals davon abhängig, dass diese Person diesen Schutz tatsächlich sucht. Aber diese Vorgehensweise wäre wesentlich wirksamer als die Alibiübung der gesetzlichen Zustimmungserfordernisse. Sie würde zudem dem Grundsatz der informationellen Selbstbestimmung entsprechen.

Was gilt also, wenn sich eine betroffene Person weder für noch gegen eine bestimmte Datenbearbeitung ausgesprochen hat? Die eingangs gestellte Frage lässt sich nach dem Gesagten klar beantworten: Ist die betroffene Person über eine Datenbearbeitung hinreichend ins Bilde gesetzt worden und konnte sie dieser in zumutbarer Weise widersprechen, so ist ihr informationelles Selbstbestimmungsrecht respektiert und damit ein wesentliches Grundanliegen des Datenschutzes erfüllt worden. Im Rahmen der Gewichtung der Datenschutzinteressen der betroffenen Personen hat dies – als Regel 7 – auch der Rechtsanwender zu beachten, selbst wenn er persönlich der Ansicht sein sollte, die betroffenen Personen hätten der Datenbearbeitung im eigenen Interesse besser widersprechen sollen. Ebensowenig kann aus dem Schweigen betroffener Personen geschlossen werden, dass sie eine möglichst einschränkende Datenbearbeitung wünschen. Dafür fehlt es nicht nur an einer Grundlage im heutigen Datenschutzgesetz. Es würde auch das informationelle Selbstbestimmungsrecht verletzen, das, wie im Rahmen von Regel 6 gezeigt, gerade *keine* Präferenz für oder gegen mehr Privatsphäre vorsieht, sondern den Entscheid ganz der Eigenverantwortung der betroffenen Personen überlässt – einschliesslich dem Entscheid, die Eigenverantwortung wahrzunehmen oder eben nicht. Daher ist im Datenschutzgesetz grundsätzlich auch keine Zustimmung erforderlich, bevor eine Privatperson Personendaten über eine andere Person bearbeiten darf. Die Zustimmung ist lediglich eine von mehreren Möglichkeiten der Rechtfertigung.

Diese Rechtslage lässt sich zwar auf dem Weg der Gesetzgebung ändern, wie dies in der EU im Fall der Cookies geschehen ist (und dort wohl auch in anderen Bereichen geschehen wird). Es sollte vor einem solchen Schritt jedoch bedacht werden, dass eine entsprechende Anpassung nebst dem damit verbundenen Systemwechsel im Ergebnis auch eine gewisse datenschutzrechtliche Bevormundung der betroffenen Personen zur Folge hätte: Der Gesetzgeber würde nicht mehr darauf vertrauen wollen, dass sich die betroffenen Personen selbst bei hinreichender Information und Möglichkeit eines Widerspruchs selbst wehren würden, wenn sie mit einer Datenbearbeitung nicht mehr einverstanden wären. In der Praxis dürfte ein solches Ausbleiben an Widerspruch gegenüber bestimmten Formen der Datenbearbeitung jedoch meist entweder darin begründet sein, dass die betroffenen Personen mit der fraglichen Datenbearbeitung einverstanden oder aber am Schicksal ihrer Daten schlichtweg nicht interessiert sind. In beiden Fällen dürfte sich eine Gesetzesanpassung nur schwer mit dem Grundsatz der informationellen Selbstbestimmung unter einen Hut bringen lassen.

## 2.8 Regel 8: Nur offenkundige Spielregeln wirken wirklich

Die vorangehenden Ausführungen über das Recht auf informationelle Selbstbestimmung führen noch zu einer weiteren Erkenntnis: Ob der «gefühlte» Datenschutz eingehalten wird, hängt selten genug von der Schwere eines Eingriffs in die Persönlichkeit ab, sondern oft davon, ob dieser Eingriff nach vorgängig klar kommunizierten und allseits akzeptierten Spielregeln stattfindet.

Vergleichen wir zum Beispiel TV-Formate wie «Big Brother» oder das «Dschungelcamp» mit der Datenbearbeitung wie sie heute viele Anbieter von Online-Dienstleistungen im Internet vornehmen: Im ersteren Fall lassen sich Personen während Wochen in eine Wohnung oder an einen anderen Ort sperren und sich Tag und Nacht von Kameras und TV-Publikum beobachten. Es ist heute anerkannt, dass diese Eingriffe in die Privatsphäre zulässig sind, da es sich um mündige Personen handelt, die einer solchen medialen Beobachtung aus freien Stücken und in Kenntnis der Umstände zugestimmt haben. Die Datenbearbeitung der Online-Dienstleister im Internet geht in aller Regel weniger weit: Zwar bearbeiten auch sie viele Daten über ihre Kunden und ermöglichen diesen über ihre Community-Plattformen oft auch, private Daten über sich mit ihren «Freunden» oder kurzerhand jedermann zu teilen. Die Benutzer können aber nüchtern betrachtet sehr viel differenzierter kontrollieren, welche Daten über sie bearbeitet werden, und die Datenbearbeitung geht insgesamt auch weniger weit als in den genannten TV-Formaten. Trotzdem wird das datenschutz-

rechtliche «Unbehagen» im Falle der Datenbearbeitung im Internet regelmässig grösser sein als bezüglich jener im Fernsehen.

Dieses Bauchgefühl hat verschiedene Ursachen. Eine davon ist das Verständnis der Öffentlichkeit darüber, wie Daten einer Person in einer bestimmten Situation bearbeitet werden: Im Falle von «Big Brother» & Co. wissen nicht nur die betroffenen Personen, worum es geht. Es ist dies jedermann von Anfang an klar. Wer sich als Teilnehmer (oder Zuschauer) darauf einlässt, ist selbst schuld, möchte man sagen. Anders verhält es sich bei vielen Internet-Anbietern: Es ist häufig nicht auf den ersten Blick ersichtlich, was mit den Daten der Benutzer geschieht. Zwar wird fast jeder Anbieter belegen können, dass er darüber irgendwo in einer Ecke seiner Website oder vergraben in einem Wust von Kleingedrucktem in verklausulierter Form informiert hat. Bei nachträglichen Anpassungen werden Anbieter zudem regelmässig zeigen können, dass sie die geänderten Bestimmungen den Benutzern zur Bestätigung vorgelegt haben und diese auch «abgenickt» wurden. Im Einzelfall mag dies sogar den Anforderungen der Transparenzgrundsätze gemäss Art. 4 Abs. 3 und 4 DSG oder den Voraussetzungen einer gültigen Einwilligung nach Art. 4 Abs. 5 DSG genügen. Die betreffende Information und Einwilligung werden in solchen Fällen trotzdem regelmässig als Alibiübung empfunden werden.

Dies führt zu Regel 8: Geht es um den «gefühlten» Datenschutz, so spielt die rein rechtliche Betrachtungsweise – sprich: die Einhaltung der Bearbeitungsgrundsätze und etwaige Rechtfertigungen – oft eine untergeordnete Rolle. Das gilt auch für die Frage, wie stark in die Persönlichkeit der betroffenen Personen eingegriffen wurde. Entscheidend ist stattdessen, ob die Spielregeln für den «durchschnittlichen Betrachter» von Anfang an augenscheinlich waren und kein Raum für Missverständnisse bestand. Dies ist dann der Fall, wenn das Zielpublikum zum Schluss kommt, dass sich jeder, der sich darauf eingelassen hatte, selbst «an der Nase nehmen» muss, wenn später mit seinen Daten das geschehen ist, was vorhersehbar war. Mit anderen Worten: Niemand sieht den Datenschutz als verletzt bei einer Person, die ihr Privatleben in einer Fernsehsendung in aller Öffentlichkeit ausbreitet, auch wenn sie selbst sich im Einzelfall über die Konsequenzen möglicherweise keinerlei Gedanken gemacht hat. Wer jedoch als Internet-Dienstleister einerseits so tut, als wäre ihm der Datenschutz wichtig, sich aber andererseits in den Datenschutzbestimmungen jedes Recht zur Bearbeitung der Daten seiner Kunden einräumen lässt, muss sich trotz tadelloser Privacy-Compliance über einen schlechten Ruf in Sachen Datenschutz nicht wundern. Trotzdem leitet noch immer fast jede Firma ihre Datenschutzerklärung mit den Worten ein, der Schutz der Privatsphäre und der Daten ihrer Kunden sei ihr ein sehr grosses Anliegen, verhält sich beim «gefühlten» Datenschutz aber genau andersrum.

Der Rechtsanwender darf und sollte sich diesem «gefühlten» Datenschutz in seinen Wertentscheiden durchaus beeinflussen lassen, jedenfalls wenn es darum geht, die soziale Akzeptanz einer Datenbearbeitung zu beurteilen. Es handelt sich dabei um einen durchaus objektiven Parameter datenschutzrechtlicher Wertentscheidungen, der letztlich ebenfalls im Recht auf informationelle Selbstbestimmung gründet. Er rückt jedoch die Eigenverantwortung der betroffenen Person, sich über das Schicksal der sie betreffenden Daten zu informieren, in den Hintergrund und fragt stattdessen danach, inwiefern das Publikum über eine bestimmte Datenbearbeitung *tatsächlich* im Bilde ist. Dies zu erreichen, erfordert vom Datenbearbeiter freilich mehr an Kommunikationsleistung als das Bereitstellen einer Datenschutzerklärung. Rechtlich mag dazu zwar keine Verpflichtung bestehen. Entspricht eine Datenbearbeitung in den Augen des Publikums jedoch erst einmal den Anforderungen des «gefühlten» Datenschutzes, wird dies normalerweise zur sozialen Akzeptanz dieser Datenbearbeitung führen und damit auch die Rechtfertigung etwaiger Persönlichkeitsverletzungen im Einzelfall entsprechend erleichtern oder sogar erfordern.

## 2.9 Regel 9: Es kommt (nicht) auf die Anzahl Betroffener an

So entscheidend die öffentliche Wahrnehmung der Offenlegung einer Datenbearbeitung und ihrer Spielregeln für das dadurch verursachte Bauchgefühl ist, so gewichtig ist auch ein zweiter Aspekt: Die Anzahl der betroffenen Personen.

Das Prinzip ist einfach: Je mehr Personen von einer Datenbearbeitung tatsächlich oder potenziell betroffen sind, desto gravierender wird ihr Eingriff in der Öffentlichkeit wahrgenommen. Auch dies ist ein Grund, warum in den vorstehend erwähnten Beispielen «Big Brother» & Co. als datenschutzrechtlich weniger heikel empfunden werden als die Datenbearbeitung eines Internet-Anbieters, selbst wenn beide offen deklarieren was sie tun: Im ersteren Fall sind ein Dutzend Personen betroffen, im letzteren Fall mitunter Millionen.

Darf dies bezüglich der datenschutzrechtlichen Beurteilung jedoch tatsächlich einen Unterschied ausmachen? Die Antwort darauf ist ein klares Nein. Eine hohe Zahl betroffener Personen mag zwar ein besonderes öffentliches Interesse *an* einer Beurteilung der betreffenden Datenbearbeitung rechtfertigen. Eine grössere Zahl (potenziell) betroffener Personen ist nach Art. 29 Abs. 1 DSG auch eine der Voraussetzungen dafür, dass der EDÖB einen Sachverhalt näher untersuchen und eine Empfehlung aussprechen kann.

In der Sache selbst muss jedoch differenziert werden. Hier darf sich der Rechtsanwender nicht durch die öffentliche Meinung oder hohe Zahl an potenziell betroffenen Personen irreführen lassen. Das ist Regel 9: Eine Persönlichkeitsverletzung wirkt nicht deshalb schwerer oder weniger schwer, weil sie

zahlreichen Personen widerfährt. Zehn leichte Verletzungen ergeben nicht automatisch eine schwere. Die Persönlichkeit ist ein Rechtsgut des Individuums, nicht des Kollektivs. Der Datenschutz soll nur dieses Individuum schützen. Daher ist auch eine Persönlichkeitsverletzung immer aus seiner Sicht zu beurteilen. Dies ist insbesondere im Rahmen der Gewichtung des Datenschutzinteresses einer betroffenen Person gegen die jeweilige Datenbearbeitung zu beachten. Die Anzahl der (ebenfalls) betroffenen Personen darf dabei keine Rolle spielen.

Bezüglich der davon zu trennenden Frage, welches kumulierte private oder öffentliche Interesse für und gegen die Durchführung dieser Datenbearbeitung besteht, ist die Anzahl betroffener Personen mitunter relevant. Das kann etwa dort der Fall sein, wo das Interesse an der Datenbearbeitung letztlich darin besteht, dass Daten einer möglichst grossen oder bestimmten Zahl von Personen bearbeitet werden können. Kommt es dabei zu Persönlichkeitsverletzungen, wird nicht nur deren Schwere im Einzelfall beurteilt werden müssen. Es wird auch darauf ankommen, wieviele Personen in ihrer Persönlichkeit verletzt worden sind. Allerdings sind auch in diesem Fall nicht die absoluten Zahlen entscheidend: Wer bei der Bearbeitung von zehn Datensätzen fünf Fehler macht, verletzt die Persönlichkeit der betroffenen Personen im Schnitt häufiger als derjenige, der 100 Datensätze bearbeitet und «nur» zehn Fehler macht. Letzterer wird seine Datenbearbeitung eher rechtfertigen können als ersterer Datenbearbeiter, auch wenn Letzterer insgesamt mehr Personen verletzt. Entscheidend ist das Verhältnis.

## 3. Fazit

Neun verschiedene Regeln für etwas mehr Objektivität in datenschutzrechtlichen Wertentscheiden sind in diesem Beitrag diskutiert worden. Gemeinsam ist allen neun Regeln, dass sie verdeutlichen, dass der Schlüssel zu mehr Objektivität in datenschutzrechtlichen Wertentscheiden letztlich in der schon zu Beginn dieses Beitrags aufgeworfenen Frage liegt: Welchem Zweck dient der Datenschutz? Eine abschliessende Antwort geben die neun Regeln nicht; sie erheben auch keinen Anspruch auf Vollständigkeit. Sie machen allerdings deutlich, dass Datenschutz nicht Selbstzweck sein darf. Sie zeigen auch, dass selbst erfahrene Rechtsanwender in diesem Bereich gut daran tun, ihr Bauchgefühl von Zeit zu Zeit kritisch zu hinterfragen, bevor sie ihm den nächsten datenschutzrechtlichen Wertentscheid anvertrauen. So rasch es sich einstellen kann, so leicht lässt es sich auch beeinflussen. Darüber sollten sich die Rechtsanwender wenigstens bewusst sein.