

# Datenschutz und Einschüchterung

Das Selbstverständnis von Datenschutzbehörden, die Grundrechte der Bürger zu schützen, unterscheidet sich stark von der Wahrnehmung vieler, die im Datenschutz vor allem ein Risiko für gesellschaftliches Handeln sehen. Das hat Gründe.

*Ein Gastbeitrag von Dr. Paul Klimpel.*

## Von einem Abwehrrecht gegen den Staat zu einer Eingriffbefugnis für den Staat

In dem für die Entwicklung des Datenschutzes grundlegenden „[Volkszählungsurteil](#)“ formulierte das Bundesverfassungsgericht:

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] 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.“

Heute geht eine Atmosphäre ständiger Bedrohung ausgerechnet von den Behörden aus, die in Folge dieses Urteils erst entstanden sind – den Datenschutzbehörden. War der Datenschutz zunächst als Abwehrrecht des Bürgers gegen den Staat gedacht, dient er inzwischen der Ermächtigung staatlicher Interventionen gegen den Bürger. Spätestens seit der DSGVO ist der Datenschutz allgegenwärtig – und damit die Angst, gegen die für Laien schwer verständlichen und häufig unklaren und in ihrer Bedeutung umstrittenen Vorschriften zu verstoßen.

Diese Angst ist durchaus begründet, schließlich sind die Datenschutzbehörden mit weitreichenden Befugnissen ausgestattet. Sie dürfen Bußgelder verhängen, Kontrollen auch in den Räumen des „Datenverarbeiters“ durchführen und Computer stilllegen.

## Drohungen

Doch mehr noch als reale Risiken, datenschutzrechtliche Vorschriften zu verletzen, lässt die Rhetorik der Drohung sowie die Veröffentlichung von rechtlich umstrittenen Positionen der Datenschutzbehörden eine lähmende Atmosphäre der Einschüchterung und der Angst entstehen.

Der „Vater der DSGVO“, Jan Philipp Albrecht drohte in einem Spiegel-Interview im Februar 2018: „[Pardon wird nicht gegeben!](#)“ Diese Formulierung ist nicht neu, Kaiser Wilhelm II nutzte sie in seiner berühmten „[Hunnenrede](#)“ am 27. Juli 1900 anlässlich der Entsendung von Soldaten im Rahmen einer Strafexpedition der Kolonialmächte gegen China. Selbst wenn es kein bewusstes Zitat war, zeigt doch die Übereinstimmung in der Wortwahl den martialischen Charakter der Drohung. Albrecht führte aus, das neue Recht könne zu schmerzhaften Sanktionen führen. Seine Drohung richtete sich insbesondere gegen europäische Unternehmen, während er im selben Interview Facebook für die Einführung neuer Datenschutzeinstellungen lobte.

Datenschutzbehörden sind im Tonfall meist weniger martialisch, doch auch ihr Verhalten wird vielfach als bedrohlich wahrgenommen. Ich will hier einige Beispiele nennen, die eine Atmosphäre der Einschüchterung entstehen lassen und verstärken.

Als im Frühjahr 2020 die Schulen vor der Herausforderung standen, Distanzunterricht aufzubauen, reagierten Datenschutzbehörden mit Drohungen. Der Thüringer Datenschutzbeauftragte Lutz Haase [drohte Lehrern direkt mit Bußgeldern](#) von 1.000€, wenn sie unzulässige Kommunikationsdienste oder Software nutzen. Auch in Hamburg gab es Presseberichte, wonach die Landesdatenschutzbehörde den Schulen die Nutzung von „Skype“ und anderen amerikanischen Diensten verboten hätte. Auf die folgende öffentliche Empörung reagierte der Hamburger Datenschutzbeauftragte Prof. Casper mit einer [Erklärung](#), es habe weder ein Skype-Verbot noch eine Untersagung des Unterrichts via Skype oder eines anderen Messenger-Dienstes gegeben. Allerdings habe einer seiner Mitarbeiter einer Schule die Haltung der Datenschutzbehörde wie auch der Datenschutzbehörden anderer Bundesländer erläutert, nachder die Nutzung solcher kommerzieller Kommunikationsplattformen für schulische Zwecke unter datenschutzrechtlichen Aspekten kritisch zu sehen sei. Wie aber soll sich ein Lehrer oder eine Schuldirektorin verhalten, wenn ihm eine Behörde sagt, bestimmte Kommunikationsplattformen seien datenschutzrechtlich kritisch?

In autoritären Staaten ist es eine häufige Praxis des Repressionsapparats, Handlungen nicht direkt zu verbieten, sondern nur unspezifisch vor möglichen „Folgen“ zu warnen.

Auch wenn es den Datenschutzbehörden nicht um Repression geht, so wirken ihre öffentlichen Bedenken über die Zulässigkeit bestimmter Kommunikationstechniken, gepaart mit der Ungewissheit über die Folgen einer Nutzung, einschüchternd. Und zwar stärker noch als ein klares Verbot, das man gerichtlich überprüfen lassen kann.

### **Überhöhte Bußgelder**

Zu einer Atmosphäre der Einschüchterung trägt auch bei, dass Datenschutzbehörden völlig überhöhte Bußgelder verhängen. Jüngstes Beispiel ist ein Bußgeld von 9,55 Millionen Euro, das der Bundesbeauftragte für Datenschutz und Informationssicherheit (BfDI) gegen den Telekommunikationsdienstleister 1&1 Telekom GmbH Anfang Dezember 2019 verhängt hatte. Um den beanstandeten Datenschutzverstoß soll es nicht gehen, dieser wurde vom [Landgericht Bonn bestätigt](#). Doch hat das Gericht das Bußgeld auf 900.000€ herabgesetzt. Wenn Behörden Bußgelder verhängen, die mehr als zehnfach über dem liegen, was angemessen ist, dann ist dies keine bloße Randunschärfe in der Ermessensausübung, sondern Ausdruck eines repressiven Selbstverständnisses. Während sich die 1&1 Telekom GmbH als große Firma gegen solche Repressionen wehren konnte, wäre ein Bußgeld, das zehnfach über dem Angemessenen liegt, für kleinere Firmen, Vereine, zivilgesellschaftliche Institutionen oder Privatleute eine existenzielle Bedrohung.

### **Keine Pressefreiheit bei Kinderfotos?**

Auch nüchterne Papiere der Datenschutzbehörden enthalten rechtlich falsche Aussagen, die grundrechtseinschränkende Wirkungen entfalten. So schreibt die Berliner Datenschutzbeauftragte im [Jahresbericht 2019](#) auf Seite 89, es sei „unabhängig von der Frage, ob berechnigte Interessen des Verantwortlichen in Bezug auf die Anfertigung und Veröffentlichung von Fotoaufnahmen bestehen, davon auszugehen, dass die Interessen der betroffenen Personen von vornherein überwiegen, wenn es sich hierbei um Kinder handelt. Solche Aufnahmen lassen sich insoweit ausnahmslos (sic) nur auf Einwilligungen stützen.“

Danach wäre also beispielsweise unzulässig, Pressefotos einer „Fridays for Future“-Demonstration zu machen. Dies aber wäre mit dem Grundrecht auf Presse- und Meinungsfreiheit unvereinbar. Die Aussage ist in dieser Absolutheit verfassungswidrig und geht ungeachtet vieler ungeklärter Rechtsfragen in Zusammenhang mit Fotografie weit über das hinaus, was unter Juristinnen und Juristen herrschende Meinung ist. Doch drängt die Datenschutzbehörde durch solche Formulierung die Grenzen des Erlaubten immer weiter zurück.

### **Keine Fotos öffentlicher Veranstaltungen?**

Inzwischen wurde sogar gerichtlich durch das [OVG Lüneburg bestätigt](#), dass Datenschutzbehörden Bußgelder gegen das Publizieren von Fotos politisch relevanter öffentlicher Veranstaltungen verhängen dürfen. Eine SPD-Ortsgruppe hatte Fotos eines Ortstermins unter freiem Himmel im Internet veröffentlicht. Doch das Bestreben, kommunalpolitische Entscheidungsprozesse aus den Hinterzimmern heraus für jeden sichtbar auf die offene Straße zu verlagern, durfte nicht öffentlich dokumentiert werden. Sowohl die Kommunikationsfreiheiten als auch die besondere Bedeutung von politischen Parteien für die politische Willensbildung mussten zurücktreten vor einem absolut gesetzten Datenschutz, nach dem selbst die Fotos gesellschaftlich relevanter, öffentlicher Veranstaltungen nicht veröffentlicht werden dürfen.

### **Auswirkungen auf das öffentliche Leben**

Löst man sich ein wenig von dem Pathos, mit dem jetzige Regelungen im politischen und juristischen Diskurs zum Garanten der Grundfreiheiten erklärt werden, kann man die Augen nicht davor verschließen, dass das Datenschutzrecht eine Atmosphäre der Angst geschaffen hat, die das gesellschaftliche Leben zu lähmen droht. Lehrkräfte, Kindergärtner, Pastoren, Altenheimmitarbeiter, Feuerwehrleute, Jugendgruppenleiter, Parteifunktionäre, Vereinsvorstände, kurz, alle die in sozialen Kommunikationsverhältnissen stehen, befürchten, gegen Datenschutzvorschriften zu verstoßen und damit ins Visier der Datenschutzbehörden geraten zu können.

Die Warnung vor „datenschutzrechtlichen Risiken“ lässt gerade bei zivilgesellschaftlichen Organisationen und kleinen Unternehmen viele sinnvolle Aktivitäten im Keim ersticken. Und dafür ist unerheblich, ob durch diese Aktivitäten tatsächlich gegen Datenschutzvorschriften verstoßen würde oder nicht.

Die reale Sorge einer Vorstandsvorsitzenden eines gewöhnlichen Vereins, dass personenbezogene Daten der Mitglieder von sinistren Geheimdiensten missbraucht werden, ist gering. Ihre Angst vor Datenschutzbehörden dürfte groß sein. Denn sie können Bußgelder verhängen, weil Fehler in der Mitgliederverwaltung gemacht wurden oder weil sich auf der Homepage des Vereins keine oder eine fehlerhafte Datenschutzerklärung befindet. Angesichts der Komplexität und Unbestimmtheit des Datenschutzrechts gibt es wohl keinen Verein, dem nicht datenschutzrechtliche Verstöße vorgeworfen werden könnten.

Die „chilling effects“ – die entmutigende, abschreckende Wirkung des Datenschutzrechts – trifft strukturell gerade die Zivilgesellschaft sowie kleine und mittlere Unternehmen, während internationale Konzerne in der Lage sind, mit den datenschutzrechtlichen Vorgaben umzugehen und die rechtlichen Möglichkeiten bis zur Grenze des Zulässigen auszunutzen. Dies ist insofern tragisch, als dass die Zähmung der Übermacht internationaler Datenkonzerne ein mit der DSGVO verfolgtes Ziel war.

## **Struktur des Datenschutzes**

Die lähmende Sorge, sich datenschutzrechtlich angreifbar zu machen, ist auch keine Randerscheinung, sondern ist in der Struktur des Datenschutzrechts angelegt. Diese wird oft als [„Verbot mit Erlaubnisvorbehalt“](#) beschrieben. Es kann dahinstehen, ob diese Kategorisierung rechtsdogmatisch zutreffend ist. Denn das grundsätzliche „Verbot“ der „Verarbeitung personenbezogener Daten“ ist klar und auch leicht verstehbar, während die Umstände, unter denen diese doch erlaubt ist, weit weniger offensichtlich, in ihren Grenzen auch unter Experten umstritten und für Laien kaum zu begreifen sind. So herrscht beispielsweise auch unter den Landesdatenschutzbeauftragten keine Einigkeit darüber, ob so alltägliche Handlungen wie die [Nutzung von MS Office 365](#) datenschutzrechtlich zulässig sind.

Öffentliches Leben ist schlechterdings nicht denkbar, ohne dass dabei auch personenbezogene Daten genutzt werden. Damit aber schwebt der Datenschutz wie ein Damoklesschwert über dem öffentlichen Leben. Generell ausgenommen vom grundsätzlichen Verbot ist lediglich der kleine Bereich des rein persönlichen oder familiären Gebrauchs, Art. 2 Abs 2c DSGVO. Aber es ist nicht Aufgabe des Rechts, einen Rückzug ins Private, ein neues Biedermeier zu befördern und gesellschaftliches Leben zu behindern.

## **Datenschutzbehörden sind staatliche Stellen**

Dazu kommt, dass es wohl keinen anderen Bereich gibt, wo die Schwelle für staatliche Intervention so niedrig ist wie im Datenschutzrecht. Für eine Intervention durch Datenschutzbehörden reicht die Nutzung eines personenbezogenen Datums aus – und es gibt kaum etwas, was nicht mit der Nutzung von personenbezogenen Daten zusammenhängt.

Datenschutzbehörden sind – genau wie Polizei, Geheimdienste oder das Ordnungsamt – Behörden, also mit hoheitlichen Mitteln ausgestattete Institutionen. Sie sind ein Arm des Leviathan. Zwar hat der Rechtsstaat den Leviathan gefesselt, doch ausgerechnet bei Datenschutzbehörden sind diese Fesseln gelockert: Sie unterliegen keinerlei Weisungen. Zwar kann ihr Handeln gerichtlich überprüft werden, doch werden Schwächere, etwa kleinere Unternehmen oder Vereine, oft gar nicht die Mittel haben, langwierige rechtliche Überprüfung durchzustehen.

Ihre Sorgen sind real.

## **Die neue Einschüchterung**

In diesem Sinne möchte ich das oben genannte Zitat des Bundesverfassungsgerichts umformulieren:

Wer unsicher ist, ob sein Umgang mit Personendaten, auch der unbewusste, belanglose oder alltägliche, gegen ein schwer überschaubares Geflecht an Vorschriften verstößt, darunter auch rein formale Vorgaben, wird versuchen, den Umgang mit personenbezogenen Daten in sozialen Kommunikationszusammenhängen zu vermeiden. Dies beeinträchtigt nicht nur die individuellen Entfaltungschancen des Einzelnen, sondern auch das Gemeinwohl, weil soziale Interaktion, öffentliche Meinungsäußerung, Vereinigungsfreiheit und Selbstbestimmung elementare Funktionsbedingungen eines auf der Mitwirkung seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens sind.

In diesem Sinne hat sich der Datenschutz aufgrund seiner einschüchternden Wirkung zu einer ernststen Gefährdung der freiheitlichen Ordnung entwickelt – und zwar ganz unabhängig davon, wie bestimmte Einzelfälle zu bewerten sind.



Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung 4.0 International Lizenz](https://creativecommons.org/licenses/by/4.0/).