

**Suzanne Dvořák
Prof. Dr. Raoul Stocker
Florian Gasche**

Alps Forum 2021

Law and Economics of Data Science

Law and Economics Foundation St. Gallen

Tagungsband

Editions Weblaw, Bern 2022

GENIE OUT OF THE BOTTLE?

*lic. iur. David Rosenthal*⁴

Partner VISCHER AG, Lehrbeauftragter der Universität Basel
und Eidg. Technischen Hochschule Zürich



1. POLARISIERUNG IM DATENSCHUTZ- RECHTLICHEN DISKURS

Datenschutz bewegt die Gemüter, und zwar immer stärker. Verantwortlich dafür, so scheint es, ist die immer stärker um sich greifende Kommerzialisierung von Personendaten. Von “Datenkraken” und “Datenstaubsaugern” ist die Rede, oder vom “Ausspionieren” von Benutzern durch irgendwelche datenhungrige Unternehmen. Wenig erstaunlich, dass im Zuge der voranschreitender Digitalisierung das Weltbild im Datenschutz heute von “Gut” und “Böse” geprägt wird. So sind Begrifflichkeiten wie GAFAM⁵, Tracking, Cloud, Cookies, Big Data, KI und USA⁶ zu Inbegriffen einer “böartigen” Entwicklung verkommen, der es Einhalt zu gebieten gilt. Ihnen gegenübergestellt werden “gutartig” konnotierte Konzepte wie Transparenz, informationelle Selbstbestimmung, Datensparsamkeit, Einwilligung und Europa⁷. Ausfluss dieser dichotomen Auffassung, sind Regulierungsbemühungen wie etwa auf europäischer Ebene die Datenschutzgrundverordnung (DSGVO) oder die ePrivacy-Richtlinie, die derzeit in eine Verordnung überführt werden soll.

Datenschutzbehörden in ganz Europa nutzen wiederum die Gunst der Stunde und die Aktualität des Themas um die nach ihrer Ansicht nötigen Zeichen zu setzen und überbieten sich gegenseitig mit Sanktionen in mehrstelliger Millionenhöhe. So verhängte die irische Datenschutzbehörde 2021 gegenüber WhatsApp eine Strafe von über

⁴ Vielen Dank an Florian Gasche (studentischer Mitarbeiter bei der Law and Economics Foundation St. Gallen) für die Mitwirkung an der Ausarbeitung dieses Textes.

⁵ GAFAM als Sammelbegriff für Google, Amazon, Facebook, Apple und Microsoft.

⁶ Im datenschutzrechtlichen Kontext zu verstehen.

⁷ Im datenschutzrechtlichen Kontext zu verstehen.

EUR 225 Mio., weil sie nach Ansicht der Behörde die Datenschutzerklärung der Firma in einzelnen Punkten nicht den Vorgaben der DSGVO entsprach. Zum Vergleich: Strafen in solcher Höhe mussten in anderen Fällen Pharmaunternehmen dafür bezahlen, dass sie mit ihren Arzneimitteln Patienten in die Abhängigkeit getrieben haben. Doch haben wir es hier wirklich mit vergleichbar schwerem Unrecht zu tun?

Das Beispiel ist kein Einzelfall und macht deutlich, wie den Datenschutzbehörden in der EU inzwischen jede Verhältnismässigkeit abhanden gekommen ist. Alles noch schlimmer gemacht hat im Juli 2020 der Schrems II-Entscheid des Europäischen Gerichtshofs. Dieser befasste sich mit dem internationalen Transfer von Personendaten aus dem EWR, kritisierte die Möglichkeiten der Überwachung durch US-Nachrichtendienste und wird von einer Reihe von EU-Datenschutzbehörden heute dazu benutzt, jegliche Datenübermittlungen an US-Provider kurzerhand zu verbieten. Das ist zwar rechtlich unhaltbar und weltfremd, wird aber eisern postuliert. Der Flurschaden ist entsprechend gross und die Situation in der Praxis ziemlich verfahren. Wichtige Forschungsprojekte müssen zum Beispiel eingestellt werden, weil Daten nicht mehr in Länder wie die USA transferiert werden können, Anwender von Cloud-Lösungen sind völlig verunsichert, ob sie die bereits im Einsatz befindlichen Lösungen weiterhin noch einsetzen können und es werden Unsummen für Rechtsgutachten ausgegeben, ohne, dass ein Nutzen für die betroffenen Personen ersichtlich ist. Da sind die zahlreichen Cookie-Banner, über die sich mittlerweile selbst die Datenschützer öffentlich ärgern, noch ein harmloses Problem.

2. WAS HEUTE SCHIEF LÄUFT

Was läuft hier schief? Das Problem ist vielschichtig. Neue Phänomene schaffen *erstens* einen Leidensdruck, mit dessen Regulierung der Gesetzgeber und die Behörden nach wie vor überfordert sind. Das Ergebnis sind Regeln aus dem Elfenbeinturm, wie etwa die Informationspflicht gemäss DSGVO: Sie führt zu seitenlangen Datenschutzerklärungen, die keiner der betroffenen Personen lesen will, aber nach der Vorstellung des Gesetzgebers für deren Schutz unabdingbar und von zentraler Bedeutung sind. Ebenso wird auf Allerheilmittel gesetzt, die keine sind, wie beispielsweise das Instrument der Einwilligung, welches die Verantwortung für den Datenschutz an die betroffene Person

abschiebt, aber aufgrund der Widerrufbarkeit einer Einwilligung in vielen Fällen für die Praxis untauglich ist. Zu den vermeintlichen Allerheilmitteln gehören auch mit der DSGVO eingeführte bürokratische Dokumentationspflichten oder die bereits erwähnten “aufzehrenden” Sanktionen. Mitunter prägt auch Planlosigkeit der Datenschutzbehörden das Bild, wie die praxisfremden Forderungen der Datenschutzbehörden im Nachgang zum Schrems II-Entscheid deutlich machen – sie sind es nämlich, die für jede Datenübermittlung in die USA ein Rechtsgutachten verlangen.

Zweitens wird Datenschutz immer mehr als Klassenkampf verstanden. Es dominieren auch seitens des Gesetzgebers und der Behörden häufig Emotionen statt sachlicher Diskussion; auch die Sachkenntnis fehlt über weite Strecken. Den extremen Bussen liegen wiederum extreme Gesetzesauslegungen zugrunde, die ein natürliches Gegengewicht zur empfundenen oder tatsächlichen Übermacht der grossen Online-Konzerne bilden sollen.

Drittens dient die Gesetzgebung und die Auslegung der Gesetze durch die Datenschutzbehörden zunehmend dem Zweck, ein Zeichen zu setzen. Ergebnis sind unerfüllbare Regelungen, die gut klingen und der Politik die Aussage erlauben, gegen Datenmissbräuche der Online-Konzerne “etwas getan” zu haben, aber mit zahlreichen “*unintended consequences*” verbunden sind, welche die restliche Wirtschaft tragen muss. Würden Datenschutzerklärungen beispielsweise wirklich so verfasst, wie die Datenschutzbehörden es in ihren Papieren fordern, wären sie noch um ein Vielfaches länger (und teurer) als sie es heute schon sind. Gewonnen wäre damit für den Datenschutz nichts.

Nichtsdestotrotz: “*the genie is out of the bottle*” und verlangt nach Regulierung. Wichtig wird es sein, dass diese sinnvoll und wirksam ausgestaltet wird. Nachfolgend soll übersichtsartig aufgezeigt werden, wieso ein Regulierungsbedarf der Datenwirtschaft überhaupt besteht, welche Probleme der aktuellen Regulierung inhärent sind und welche Handlungsempfehlungen sich daraus ableiten lassen.

3. **REGULIERUNGSBEDARF DER DATENWIRTSCHAFT**

Bevor über die Ausgestaltung von Regulierung diskutiert werden kann, ist der grundsätzliche *Regulierungsbedarf* zu klären. Wieso stellt die Datenwirtschaft ein für den Regulator notwendig zu regelndes Sachgebiet dar? Mit personenbezogenen Daten kann Geld verdient werden; die Bearbeitung von Daten kann negative Folgen für das Daten-subjekt selbst haben; es herrscht teilweise keine vollständige Transparenz darüber, wie Daten verwendet werden; und es bestehen z.T. keine effektiven Einflussmöglichkeiten für die betroffene Person – das Datensubjekt – auf die Bearbeitung der eigenen Daten. Doch sind dies tatsächlich problematische Gegebenheiten oder fühlt es sich nur so an? Wäre ein solcher Unterschied überhaupt relevant, um die Regulierung rechtfertigen zu können? Immerhin kann es Sinn und Zweck einer solchen sein, dass wir uns gut fühlen, weil uns die Regulierung und die Behörden den Eindruck erwecken, dass sie uns vor Missbrauch schützen.

Das eigentliche Problem, welches wir mit den Entwicklungen – und Auswüchsen – der Datenwirtschaft haben ist die *Emotionalität*, die *Komplexität* und die *Vielschichtigkeit* dieser Entwicklungen. So setzen gewisse Unternehmen im Rahmen von Bewerbungsverfahren heute beispielsweise automatisierte Einzelentscheide auf maschineller Basis ein, um die schlechtesten Bewerber für eine offene Arbeitsstelle auszusortieren. Mit anderen Worten schaut sich ein Computer und nicht mehr ein Mensch ihre Dossiers an. Muss ein Bewerber dies akzeptieren? Nein, sagt das Datenschutzrecht, denn es regelt solche Fälle sogenannter automatisierter Einzelentscheide. In wichtigen Fragen hat jeder von uns den Anspruch darauf, von einem Menschen beurteilt zu werden, nicht “nur” von einem Computer – übrigens auch im revidierten Schweizer Datenschutzgesetz. Doch ist diese Regelung wirklich richtig? Wir wissen heute, dass menschliche Entscheide wesentlich stärker vom Zufall geprägt sind und qualitativ oft schlechter als solche durch einen gut trainierten Computer. Die Frage wurde im Gesetzgebungsprozess jedenfalls in der Schweiz nie diskutiert. Geht es also in Wirklich nicht um die Qualität der Entscheide, sondern um etwas ganz anderes, wie zum Beispiel die Menschenwürde oder letztendlich schlicht um die diffuse Angst vor der Maschine? Beides kann, wie gesagt, ein legitimer Grund für eine gesetzliche Regelung sein. Problematisch ist freilich,

dass sich der Gesetzgeber im Bereich des Datenschutzes viele dieser Überlegungen gar nicht macht.

Vor diesem Hintergrund stellt sich die Frage, wie das *vermeintliche* Problem gelöst werden kann, welches aus dem Spannungsfeld der Datenwirtschaft und unserer sachlichen und emotionalen Reaktion auf diese hervorgeht.

Regulierungsansätze gibt es mittlerweile zahlreiche. Sie reichen von neuen Konzepten, wie Eigentumsrechte an Daten, über neuartige technischen Lösungen bis hin zur Einschränkung der weiteren Entwicklungsmöglichkeiten. Auch klassische Methoden wie Bürokratie (negativ formuliert) bzw. Governance (positiv formuliert) und natürlich scharfe Sanktionen werden gerne postuliert.

In der Diskussion um den besten Regulierungsansatz im Datenschutz häufig übersehen wird allerdings die Tatsache, dass die (rechtliche) Regulierung regelmässig spät kommt, um nicht zu sagen zu spät. Sie ist im Datenschutz jeweils eine Reaktion auf einen wachsenden Leidensdruck, der durch eine neue gesellschaftliche, staatliche oder wirtschaftliche datenbezogene Anwendung ausgelöst wird. Er führt regelmässig zu einer faktischen Regulierung durch den Markt⁸, die in der Regel deutlich vor dem Wirksamwerden einer rechtlichen Regulierung zu wirken beginnt und dem Leidensdruck entgegenwirkt. Sie setzt also verzögert ein, ist jedoch langlebig. Der Leidensdruck ist zu diesem Zeitpunkt oft bereits am Sinken und Gewöhnung setzt ein. In dieser Phase sinkt das Problemempfinden bezüglich dieser Anwendung allmählich auf ein Minimum. Abbildung 1 hält diesen Verlauf bildlich fest.

⁸ Wie beispielsweise Selbstregulierung, Ablehnung durch Konsumenten, öffentlicher Druck, Druck durch datenschutzfreundliche Wettbewerber.

Der Weg zur gesellschaftlichen Akzeptanz

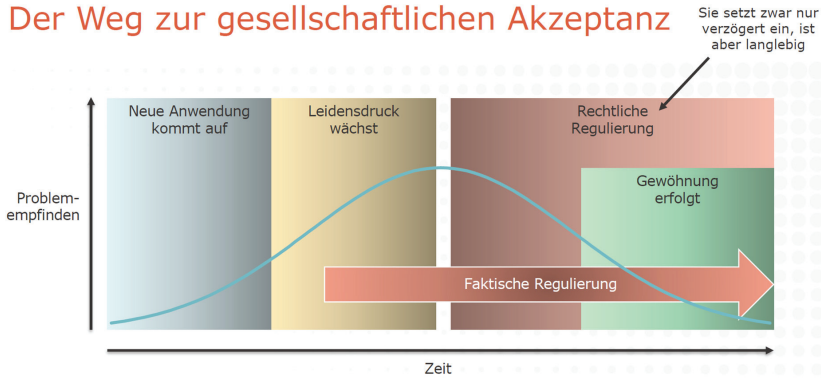


Abbildung 1: Der Weg zur gesellschaftlichen Akzeptanz von neuen Anwendungen

4. HANDLUNGSEMPFEHLUNGEN

Was aber braucht es vor diesem Hintergrund im Datenschutz an konkreter Regulierung? Zunächst ist zur Kenntnis zu nehmen, die datenschutzkonforme Ausgestaltung einer Datenbearbeitung ist wichtiger als deren Dokumentation und formale Vorgaben. Es ist daher angezeigt, die Regulierung auf den *materiellen* Datenschutz zu fokussieren. Der formelle Datenschutz genießt in der aktuellen Regulierung zu viel Aufmerksamkeit; sowohl die Einführung der DSGVO als auch die Revision des Datenschutzgesetzes in der Schweiz baute praktisch ausschliesslich den formellen Datenschutz aus.

Das "Giesskannen"-Prinzip mit starren Regelungen soll im Datenschutzrecht keine Anwendung finden. Vielmehr bedarf es einen risiko- und prinzipienbasierten Datenschutz. Wie dies auch in anderen Rechtsgebieten der Fall ist, empfiehlt sich auch im Datenschutzrecht die Kombination aus Grundsätzen und Interessenabwägung. Die DSGVO geht jedoch beispielsweise in die gegensätzliche Richtung.

Weiter ist es zentral, dass die behördliche Aufsicht nur dort wirkt, wo es sich auch lohnt. Dies bedeutet, dass die Aufsichtsbehörden von unnützen Aufgaben wie etwa dem Abarbeiten von Pflichtmeldungen über alltägliche Verletzungen der Datensicherheit entlastet werden sollten. Stattdessen sollten sie sich ihre Fälle selbst aussuchen

können, wie das unter dem bisherigen Schweizer Datenschutzgesetz der Fall war und sich als höchst wirksam erwies. Sie sollten mehr Mittel erhalten, denn eine Aufsicht mit mehr Ressourcen und Sachkunde kann für den Datenschutz wesentlich mehr bewirken als schärfere Gesetze. Zudem sollen die Aufsichtsbehörden aus vernünftigen Schiedsrichtern bestehen, anstelle ideologischer Interessensvertreter. Abschliessend braucht es im Bereich der Sanktionen ein vernünftiges Augenmass. Das Bussenregime, wie es heute gelebt wird, hilft in der Sache nicht weiter.

5. SCHLUSSFOLGERUNGEN

“The genie is out of the bottle” und es stehen weitere Flaschen bereits bereit. Dennoch ist es wichtig zu betonen, dass nicht die Datenwirtschaft per se als “böse” zu bezeichnen ist, sondern deren ungewollte Exzesse. Der gefühlte Datenschutz ist ebenso wichtig wie der echte und eine effektive Regulierung ist erforderlich, damit ein gefühltes Gleichgewicht zwischen den verschiedenen Kräften sichergestellt werden kann. Hierzu bedarf es einer starken, fokussierten aber auch fairen Aufsicht. Denn aufzehrende Bussen und ein Überfluss an Regelungen zielen an der Sache vorbei und schütten das Kind mit dem Bade aus.

Schlussendlich soll hier jedoch auch erwähnt sein, dass manches, was wir heute als Bedrohung sehen, in einigen Jahren gesellschaftlich akzeptiert oder gar erwünscht sein wird. Dies hat uns die Vergangenheit gelehrt. Nehmen wir nur “Google Street View” als Beispiel, das einst als Instrument fast des Teufels auch in der Schweiz von den Datenschutzbehörden bitter bekämpft wurde – der Autor dieser Zeilen war beteiligt – und heute als völlig normal, akzeptiert und unproblematisch gilt. So gesehen ist es durchaus ein Vorteil, dass die Schweiz (auch) in der Datenschutzregulierung wesentlich langsamer ist als die Europäische Union. So konnten wir in der Revision des Datenschutzgesetzes bereits aus den Fehlern der DSGVO lernen.

INHALTSVERZEICHNIS

Digital Sovereignty and Data Transparency – Thoughts from an Interdisciplinary Perspective	1
<i>Bernhard Waltl</i>	
Genie out of the Bottle?	3
<i>David Rosenthal</i>	
Data Assets – Können Daten bilanziert werden?	11
<i>Angelica M. Schwarz</i>	
Data Science im Recht	23
<i>Philip Hanke</i>	
Artificial Intelligence – Spotlight on Risks, Regulation and Liability	35
<i>Lisa Bechtold</i>	
“Gibt es noch EINE freie Meinung?”	43
<i>Johann Justus Vasel</i>	
Commodifying data without embodiment: insight from mindfulness practices as a game changer	51
<i>Valérie M. Saintot</i>	
Influencer Marketing	67
<i>Dana Sindermann</i>	
Data Driven Impact	73
<i>Christin ter Braak-Forstinger</i>	
Nachhaltigkeit und Footprint – Grundsätzliches und Praxisorientiertes über die ordnende Kraft von Daten	79
<i>Felix R. Ehrat</i>	

A Call to Think in Moonshots and Invest in AI Ecosystems	89
<i>Adrian Locher</i>	
Forschungsprojekt "FoodCoach"	95
<i>Simon Mayer</i>	
The Digital Services Act Package: Eine Law and Economics Analyse	97
<i>Giulia Canova</i>	
Plattformen und (Daten-)Monopole: Braucht es neue Instrumente im Kartellrecht?	111
<i>Fabio Anceschi/Florian Gasche</i>	