



Hauke Behrendt / Wulf Loh /
Tobias Matzner / Catrin Misselhorn (Hg.)

Privatsphäre 4.0

Eine Neuverortung des Privaten
im Zeitalter der Digitalisierung



J.B. METZLER

Djeffal, C. (2019). „Privatheit 4.0“ im Spiegel von Recht und künstlicher Intelligenz. Das Recht als (Re)aktion und der status activus technicus. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Eds.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (pp. 177–197). J.B. Metzler.

https://doi.org/10.1007/978-3-476-04860-8_11



„Privatheit 4.0“ im Spiegel von Recht und künstlicher Intelligenz. Das Recht als (Re)aktion und der *status activus technicus*

Christian Djeffal

Privatheit, ihre technischen Voraussetzungen und das Recht auf Privatheit entfalten wechselseitige Wirkungen. Neue Auffassungen von Privatheit können sich u. a. politisch vermittelt auf das Recht auswirken, genauso kann das Recht die Vorstellungen von Privatheit beeinflussen. Wenn dieser Band nach einer neuen Privatheit, einer Privatheit 4.0 fragt, dann kann man auf der Suche danach auch nach Spuren suchen, die die Veränderungen der Privatheit im Recht sichtbar machen. Das veränderte Gesicht der Privatheit wird anhand des Wandels im Datenschutzrecht rekonstruiert. Dem geht dieser Beitrag nach. Er möchte anhand rechtlicher Entwicklungen verstehen, welches Bild wir uns heute von Privatheit machen. Die Gelegenheit dafür ist günstig. Denn nach langen und intensiven Verhandlungen haben sich die Europäischen Institutionen auf ein neues europäisches Datenschutzgesetz geeinigt, die Datenschutzgrundverordnung (DSGVO).¹ Sie löst eine Richtlinie aus dem Jahr 1994 ab und hat weltweit große Aufmerksamkeit erfahren. Insbesondere aus dem Vergleich der beiden Instrumente, aber auch aus Alternativen der Verhandlungen, lassen sich wichtige Bewegungen ableiten, die konzeptionelle Verschiebungen und Weiterentwicklungen aufzeigen. Die Versionierung im Konzept von „Privatheit 4.0“ insinuiert, dass es gleichgeblieben ist und dennoch wichtige Veränderungen erfahren hat.² In diesem Narrativ wird das

¹Verordnung 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG vom 27.04.2016.

²Diese Form der Versionierung wird eigentlich bei der Erstellung von Software verwandt. Bei der Zahl vor dem Punkt handelt es sich um die Hauptversionsnummer, die wesentliche Neuerungen anzeigt, die über funktionale Erweiterungen hinausgehen. Siehe dazu und zur Übertragbarkeit in die soziale Sphäre Djeffal (2016).

C. Djeffal (✉)

Munich Center for Technology in Society, Technische Universität, München, Deutschland

E-Mail: christian.djeffal@tum.de

Recht getrieben von gesellschaftlichem Wandel. Der Beitrag möchte dabei jedoch nicht verharren, sondern eine Alternative formulieren. Er wirft die Frage auf, wie Recht und Rechtswissenschaft neben der reaktiven auch eine aktive Rolle einnehmen können, in der sie Verfassung und Verfassungsvoraussetzungen progressiv gestalten. Als Weg hin zu einer solchen Aktivierung schlägt der Beitrag die Fortentwicklung der Statuslehre und das Hinzufügen eines *status activus technicus technologicusve* vor.

1 Grundrechtsinnovation als Reaktion

Jeder Grundrechtsinnovation geht regelmäßig die Innovation einer Grundrechtsverletzung voraus. Grundrechtsinnovationen sind Reaktionen auf gesellschaftliche Missstände, denen seitens des Rechts die Qualität einer Grundrechtsverletzung beigemessen wird. Grundrechtsinnovationen sind aus einer rechtsimmanenten Perspektive „signifikante Änderungen von Grundrechten“ (Hornung 2015, 173). Tatsächlich haben sowohl das Bundesverfassungsgericht als auch die Staatsrechtslehre zahlreiche Ideen zur Weiterentwicklung der Grundrechte des Grundgesetzes beigetragen. Das Gleiche gilt auf überregionaler und internationaler Ebene für Institutionen wie den europäischen Gerichtshof für Menschenrechte oder Gelehrte.³ Dennoch gehen solche signifikanten Änderungen regelmäßig auf gesellschaftliche Entwicklungen zurück. Daraus folgt, dass die eigentliche und ursprüngliche Grundrechtsinnovation in der Grundrechtsverletzung liegt, die durch eine weitere Innovation, nämlich die Wahrnehmung und Reformulierung der Entwicklung als Grundrechtsverletzung, adressiert wird. Dass diese Innovationen aus einer kontextsensitiven Perspektive als Reaktionen gesehen werden müssen, stellt weder ihren Status als Innovation in Frage, noch schmälert es den Verdienst der Innovatoren. In juristischer Hinsicht gehört einiges dazu, einen gesellschaftlichen Missstand auf den Punkt zu bringen und die Schutzwürdigkeit von Individuen überzeugend und nachvollziehbar herauszustellen. Diesen Anliegen auch politisch Gehör zu verschaffen, ist wiederum als eigene Leistung zu bewerten. Eine kontextsensitive Rechtswissenschaft kommt aber nicht umhin, den Fokus auf die notwendige Bedingung der Entstehung eines Rechts zu legen: Erst wenn Risiken oder Gefahren bestehen, kann ein Verständnis dafür entstehen, was wir als Schutzgut bezeichnen. Die Gefahr oder das Risiko muss sich nicht materialisiert haben. Je mehr Gefahr oder Risiko aber tatsächlich schon zu einem sichtbaren Missstand geführt hat, desto leichter lässt sich auch das Recht formulieren.

Dass rechtliche Innovationen Reaktionen sind, lässt sich am Recht auf Privatheit selbst ablesen. Der epochale Aufsatz „The Right to Privacy“ ist ein gutes Beispiel dafür, wie die Entwicklung des Rechts im Allgemeinen und der Grundrechte im Besonderen auf gesellschaftliche Veränderungen reagieren (Warren/Brandeis 1890). Wenn Privatheit in verschiedenen Kulturen und auch zu verschiedenen Zeiten eine Rolle spielte, so hat dieser Aufsatz in der Geschichte der Privatheit

³Für Perspektiven diesbezüglich siehe Grimm (2019).

dennoch einen besonderen Platz (Cannataci 2009). Das Werk der späteren amerikanischen Verfassungsrichter Samuel D. Warren und Louis Brandeis gilt als *locus classicus* des Rechts auf Privatheit in den Vereinigten Staaten und darüber hinaus (Glancy 1979; Bezanson 1992; Post 1991; Bratman 2002; Gajda 2018), auch wenn viele der wesentlichen Gedankengänge bereits andernorts vorweggenommen wurden.⁴ Brandeis und Warren stellten Privatheit in den Mittelpunkt ihrer Überlegungen und schufen so einen zentralen konzeptionellen Anknüpfungspunkt. Der reaktive Charakter der Argumentation wird schon in den ersten Zeilen des Beitrags offenbar, hier schreiben die Autoren:

„THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society“ (Warren/Brandeis 1890, 193).

Diesen Aufschlag greifen die Autoren in ihrer Argumentation auf und argumentieren mit neuen Entwicklungen jenseits des Rechts, die Ursache für eine Reaktion und Weiterentwicklung des Rechts sind. Sie nehmen ausdrücklich Bezug auf Innovationen und neue Geschäftsmodelle, insbesondere die Sofortfotographie und die Druckpresse und das dadurch ermöglichte neue Zeitungsgewerbe, insbesondere den Sensationsjournalismus (ebenda, 195). Sie versuchen nachzuvollziehen, welche Wirkungen diese neuen Entwicklungen auf Individuen haben und stellen dabei eine große Belastung fest. Daraus leiten sie die Notwendigkeit ab, das Recht weiterzuentwickeln und bauen dazu auf Analogien zum Eigentum auf. Dieses hat im Recht der Vereinigten Staaten sowohl eine grundrechtliche als auch eine deliktsrechtliche Dimension. Dadurch gelingt es ihnen, den Boden für eine Analogie zu schaffen, die sowohl die grundrechtliche Bedeutung der Privatheit betont, als auch konkrete Ansprüche zur Durchsetzung der Rechte bereithält. Dieser innovative Ansatz steht also an der Quelle des Rechts auf Privatheit. Was Privatheit bedeutet, wurde im Recht verdichtet, als diese Ideen Eingang in die Rechtsprechung fanden und beginnend mit dem Land Hessen auch in Gesetzen ausformuliert wurden. Jede gesetzliche Fixierung und jede Erneuerung ändern das Antlitz der Privatheit. Daher soll im Folgenden argumentiert werden, dass geänderte Konzept der Privatheit rechtlich zu rekonstruieren.

2 Juristische Rekonstruktion

Es gibt viele Indikatoren, die auf neue Formen und Versionen von Privatheit hinweisen können. Dazu zählen etwa Untersuchung der (sich ändernden) Einstellung der Bevölkerung und empirische Recherchen über neue oder bessere

⁴Siehe etwa die Analyse von Glancy (1979), 2. Weitere Nachweise Glancy (1979), Fn. 2.

Erkenntnismöglichkeiten über Individuen auf der Grundlage von technischen Innovationen⁵. Will man aber herausfinden, ob sich eine neue Form von Privatheit in grundsätzlich akzeptierter Form generell verfestigt hat, kann man dies gut am Stand der Entwicklung des Rechts ablesen. Denn die Rechtsentwicklung wird durch demokratische Verfahren vorangetrieben, die einen Konsens repräsentieren. Ferner sind Rechtssätze transparent und allgemein zugänglich. Das Recht selbst beantwortet allerdings nur in den seltensten Fällen die Frage, ob wir vor einer neuen Stufe der Entwicklung stehen. Dazu bedarf es einer systematischen Untersuchung, die das geltende Recht so rekonstruiert, dass Änderungen und Entwicklungen nachvollzogen werden können. Bei der Rekonstruktion der Datenschutzgrundverordnung spielen grundlegende Änderungen eine große Rolle, denn sie sind die stärksten Indizien dafür, wie sich Privatheit ändert. Diese grundlegenden Neuerungen sollen hier Novationen genannt werden. Genauso wichtig wie das Neue ist aber auch das, was im Laufe der Jahre stabil geblieben ist. Denn nur unter Kenntnis der Kontinuitäten kann man abschätzen, wie statisch bzw. dynamisch die Entwicklungen verlaufen sind. Zwischen Novationen und Kontinuitäten liegen rechtliche Evolutionen, also graduelle Verschiebungen, die weder völlig neu, noch gänzlich ursprünglich sind.⁶ Entlang dieser Kategorien sollen wesentliche Strukturentscheidungen der Datenschutzgrundverordnung vorgestellt und diskutiert werden.

2.1 Novationen

2.1.1 Marktortprinzip

Eine wesentliche Novation in Art. 3 DSGVO liegt darin, dass das europäische Datenschutzrecht seinen Einfluss viel stärker als zuvor auch auf Auslands Sachverhalte erstreckt. Datenverarbeitende Stellen, die keine Niederlassung in Europa haben, werden dem europäischen Recht unterworfen.⁷ Das bezeichnen Beobachter*Innen als „eine der wichtigsten Neuerungen“ (Albrecht/Jotzo 2017, 67) oder sogar „eines der wichtigsten politischen Signale, das der Gesetzgeber mit der DS-GVO aussendet“ (Schantz 2016, 1842).⁸ Der territoriale Anwendungsbereich eines Gesetzes betrifft seine örtliche Reichweite. Kann ein deutsches

⁵Hierunter fallen etwa die neuen Möglichkeiten der Verhaltensbeeinflussung bei Wahlen, siehe Bodó/Helberger/Vreese (2017); Djeffal (2019, 260–262).

⁶Unter den Vorzeichen von Evolution und Revolution wird die Datenschutzgrundverordnung diskutiert von Kühling/Martini (2016).

⁷Wer im Anwendungsbereich der DSGVO ist aber keine Niederlassung in Europa hat, muss gemäß Art. 27 DSGVO zudem einen Vertreter in den betreffenden Mitgliedsstaaten benennen, der sowohl für Betroffene wie auch für Aufsichtsbehörden Ansprechpartner ist.

⁸Als „größten Pluspunkt“ bezeichnet es auch Dammann (2016), 309. Kritisch gegenüber dem innovativen Gehalt ist Gömann (2017).

Strafgesetz auch im Ausland gelten? Diese Fragen tauchen im Datenschutz besonders dann auf, wenn die datenverarbeitende Stelle und das Datensubjekt aus unterschiedlichen Rechtsordnungen stammen. Nach dem alten europäischen Recht auf Grundlage der Datenschutzrichtlinie galt hierbei, dass datenverarbeitende Stellen grundsätzlich nur unter das europäische Datenschutzregime fallen, wenn sie in Europa niedergelassen sind.⁹ Die Datenschutzgrundverordnung bleibt bei diesem Grundsatz, versieht ihn jedoch mit zwei Ausnahmen. Die DSGVO ist nach Art. 3 Abs. 2 a) anwendbar, „wenn die Datenverarbeitung im Zusammenhang damit steht ... betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten“. Sie ist nach Art. 3 Abs. 2 b) DSGVO auch anwendbar, wenn es darum geht, „das Verhalten betroffener Personen zu beobachten“. Erwägungsgründe 23 und 24 der Datenschutzgrundverordnung hilft bei der Auslegung der beiden Ausnahmen. Bei den Waren und Dienstleistungen kommt es darauf an, ob die datenverarbeitende Stelle das Angebot „offensichtlich beabsichtigt“. Die bloße Abrufbarkeit im Internet reicht nicht aus. Die Entscheidung kann nur aufgrund von deutlicheren Indizien vorgenommen werden wie etwa die Sprache des Angebots oder die Währung bei einer Transaktion. Diese Ausnahme erfasst also Anbieter, die zielgerichtet geschäftliche Aktivitäten im Hoheitsgebiet der EU entfalten wollen. Die andere Ausnahme betrifft nur das Verhalten von Personen in der Union und bezieht sich insbesondere auf Techniken der Erstellung von Persönlichkeitsprofilen, die Entscheidungsgrundlagen bilden und die die Analyse und Vorhersage von „persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten“ ermöglichen. Während die erste Ausnahme sich besonders auf kommerzielle Tätigkeiten erstreckt – wobei es nicht auf eine Gegenleistung in Geld ankommt – erfasst die zweite Ausnahme sowohl kommerzielle als auch hoheitliche Verhaltensbeobachtungen.

Worauf reagiert das Recht mit dieser Formulierung? Erwägungsgrund 23 liefert eine Antwort auf diese Frage: „Damit einer natürlichen Person der gemäß dieser Verordnung gewährleistete Schutz nicht vorenthalten wird, sollte die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter dieser Verordnung unterliegen.“ Der Erwägungsgrund stellt klar, dass es hier um eine Effektivierung des Schutzes der Datenschutzgrundverordnung geht. Diese Anknüpfung an europäischen Datensubjekten wird auch als Markttortprinzip bezeichnet. In Gesetzeskommentaren wird zur Erklärung insbesondere darauf hingewiesen, dass zuvor große Unternehmen nicht unter die Regeln des Datenschutzes fielen, wenn sie keine Niederlassung in der Europäischen Union hatten (Weichert 2018). Aus der Sicht der europäischen Rechtsordnung konnte es also zu Schutzlücken kommen. Denn Bürger mussten sich bei etwaigen Verstößen nach dem Recht des Staates richten, in dem die Behörden

⁹Einzigste Ausnahme nach der Richtlinie war, dass die datenverarbeitende Stelle auf Mittel im Hoheitsgebiet zurückgreift, die im Hoheitsgebiet gelegen sind.

niedergelassen sind und sich auch an die entsprechenden Behörden wenden. Aus der Sicht der Datenschutzgrundverordnung bedeutet die Ausweitung der territorialen Anwendbarkeit eine Steigerung der praktischen Wirksamkeit. Dies ist im Europarecht auch in der Auslegung ein geläufiges Argument, für das die französische Wendung *effet utile* steht.

Das Bild der neuen Privatheit ist eines, das nicht davor zurückschreckt, die eigenen Standards auf der ganzen Welt durchzusetzen, unabhängig davon, ob die datenverarbeitenden Stellen in der Europäischen Union niedergelassen sind. Datenverarbeitende Stellen müssen gegebenenfalls verschiedene Rechtsordnungen gleichzeitig berücksichtigen. Im Hinblick auf die territoriale Anwendbarkeit des Rechts verschiebt sich die Perspektive. Jedenfalls im Bereich gezielter kommerzieller Aktivitäten und Beobachtungen hat das Datenschutzrecht einen neuen Ort. Das Datensubjekt rückt in den Mittelpunkt, die datenverarbeitenden Stellen haben alle Orte zu berücksichtigen, auf die sich ihr Verhalten auswirkt. Gleichzeitig wirken bestimmte Vorstellungen der Privatheit damit viel stärker über ihr Hoheitsgebiet hinaus.

2.1.2 Datenübertragbarkeit

Art. 20 DSGVO gewährt das Recht auf Datenübertragbarkeit. Auch diese Regelung gehört zu den genuinen Neuerungen der Datenschutzgrundverordnung im Vergleich zur bisherigen Rechtslage (Kühling/Martini 2016, 450; Jülicher/Röttgen/Schönfeld 2016). In der Zielvorstellung können Nutzer frei von einem Dienst zum anderen wechseln und ihre Daten einfach mitnehmen (Paal 2018, Rn. 4–6). Wer einer datenverarbeitenden Stelle Daten zur Verfügung gestellt hat, hat das Recht, diese Daten zu erhalten, sie weiterzugeben und auch die Weitergabe von einer datenverarbeitenden Stelle an die nächste zu veranlassen. Das Recht auf Datenübertragbarkeit ist ein Novum, das das Potenzial hat, auch den Blick auf das Konzept der Privatheit zu variieren. Die Datenschutzgrundverordnung erlaubt nicht mehr nur, eine Einwilligung zu widerrufen und die Löschung der Daten zu verlangen. Sie macht Daten für Einzelne disponibel. Man könnte das durchaus so deuten, als würden Daten hier in gewisser Weise mit körperlichen Gegenständen gleichgestellt (Jülicher/Röttgen/Schönfeld 2016, 361).

Dieses Recht auf Datenübertragbarkeit tauchte zum ersten Mal im Eckpunktepapier auf, in dem die Kommission ihr Gesamtkonzept für eine Reform des Datenschutzes erläuterte (so Dix 2019, 2). Die Kommission nahm sich vor, „die Rechte des von der Verarbeitung Betroffenen zu erweitern, in dem die „Datenübertragbarkeit“ sichergestellt wird, also das Recht des Einzelnen, seine Daten (z. B. Fotos oder Freundeverzeichnisse) auf einer Anwendung oder einem Dienst zurückzuholen und die zurückgeholten Daten auf eine andere Anwendung oder einen anderen Dienst zu übertragen, sofern dies technisch möglich ist, ohne von dem für die Verarbeitung Verantwortlichen daran gehindert zu werden.“ (Mitteilung der Europäischen Kommission, Gesamtkonzept für den Datenschutz in der Europäischen Union, Brüssel, den 04.11.2010, KOM(2010), 609, Fn. 2.) Diese Formulierung ist interessant, weil sie auf die Rechtfertigung der Kommission verweist. Die Kommission führt nämlich an, dass sich Nutzer über soziale Online-Netzwerke

beschwert haben, weil sie ihre Daten dort nicht zurückbekommen haben (ebenda, 8). Damit bezog sich die Kommission in ihrer Rechtfertigung im Wesentlichen auf die Möglichkeit der Datensubjekte, ihre Daten zu beherrschen und von Anbietern wieder herauszuverlangen. In seiner Stellungnahme zur Mitteilung der Kommission unterstützte das Parlament diesen Vorschlag, fügte jedoch weitere mögliche Rechtfertigungsgründe hinzu. Das angedachte Recht auf Datenübertragbarkeit soll dazu dienen, „... das reibungslose Funktionieren sowohl des Binnenmarktes als auch des Internet und seiner charakteristischen Offenheit und Interkonnektivität zu erleichtern“ (Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union 2011/2025(INI) Rn. 16, Fn. 2). Neben den individuellen Datenschutz treten hier also noch allgemeine wirtschaftliche Überlegungen sowie Fragen der Internet Governance auf.

Diese Vielfalt an Gründen spiegelt sich in der juristischen Literatur wider. Hier werden dem Recht auf Datenübertragbarkeit aber insbesondere verbraucherschützende und wettbewerbspolitische Absichten unterstellt. Dabei wird besonders darauf abgestellt, dass Datenübertragbarkeit den Wettbewerb zwischen verschiedenen Diensten ermöglicht, weil sogenannte „Lock-In Effekte“ vermieden werden (Art. 29 Gruppe 2016, 5). Eine fehlende Datenübertragbarkeit kann Konsumenten nämlich an einen Dienst binden, wenn der Wechsel dadurch umständlich oder sogar unmöglich gemacht wird. Aus diesen Gründen wird diskutiert, ob diese Norm vorwiegend noch mit Fragen der Privatheit in Zusammenhang steht (Kamann/Braun 2018, Rn. 3; Herbst 2018, Rn. 4).

2.2 Evolutionen: Automatisierte Entscheidungen im Einzelfall

Automatisierte Entscheidungssysteme¹⁰ rücken immer mehr in den Fokus der juristischen öffentlichen Aufmerksamkeit. Während einfache Entscheidungssysteme wie Verkehrsampeln bereits zur „unsichtbaren“ Infrastruktur unseres alltäglichen Lebens geworden sind, kommt es durch technologische Trends wie Big Data und künstliche Intelligenz zu immer mehr Anwendungsfällen. Die neuen Möglichkeiten basieren auf gestiegenen Rechenleistungen und Speicherkapazitäten, aber auch auf Verbesserungen der Systeme selbst. Daher spielte auch bei den Verhandlungen zur Datenschutzgrundverordnung das Thema automatisierte Entscheidungen eine wichtige Rolle. Das Ergebnis der Beratungen ist eher als Evolution und nicht als Revolution zu bezeichnen.¹¹ Der neue Art. 22 DSGVO folgt in wesentlichen Strukturentscheidungen der Vorgängervorschrift des Art. 15 DSRL, allerdings ergeben sich an verschiedenen Stellen wichtige Veränderungen. Die Grundstruktur beider Regelungen ist ein grundsätzliches Verbot automatisierter

¹⁰Im Englischen „automated decision mechanisms“ (ADM) genannt.

¹¹Beide Vorschriften sind zur besseren Vergleichbarkeit im Anhang abgedruckt.

Einzelentscheidungen, auf das sich der Einzelne berufen kann. Von diesem Verbot werden dann bestimmte Ausnahmen gemacht. Liegen diese Ausnahmen vor, sind die automatisierten Entscheidungen rechtmäßig.

Beide Regelungen verbieten grundsätzlich, dass Menschen automatisierten Einzelentscheidungen unterworfen sind. Nach dem alten Recht galt das jedoch nur für eine Entscheidung, die „aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht“ (Martini 2018, Rn. 14). Dieser Zusatz findet sich nicht mehr in Art. 22 DSGVO. Nach dem Wortlaut kommt es also nicht darauf an, ob die automatisierte Entscheidung auf der Bewertung einzelner Aspekte der Person beruht.¹² Alle automatisierten Entscheidungen gegenüber Einzelnen fallen jetzt in den Anwendungsbereich der Vorschrift. Das bedeutet, dass der Anwendungsbereich der Vorschrift grundsätzlich größer ist. Er betrifft nicht mehr nur Systeme, die Aspekte einer Person bewerten wollen. Damit dehnt die Vorschrift ihren Zweck über den Schutz der Privatheit hinaus auf alle Fälle aus, in denen Individuen von automatisierten Entscheidungen im Einzelfall adressiert werden.

Eine Begrenzung findet sich allerdings in neuen oder erweiterten Ausnahmebestimmungen. So kann jetzt nach Abs. 2 c) eine Einwilligung dazu führen, dass die automatisierte Einzelentscheidung rechtmäßig ist. Nach der alten Rechtslage konnten die Eingehung oder Erfüllung von Verträgen eine Erlaubnis nur dann rechtfertigen, wenn dabei dem Ersuchen einer Person entsprochen wurde. Nur wenn also bei der Entscheidung das herauskam, was die betroffene Person wollte, war die Entscheidung rechtmäßig (Martini 2018, Rn. 14). Diese Einschränkung entfällt. Beide Ausnahmen können in vielen Fällen greifen. Eine ausdrückliche Einwilligung lässt sich insbesondere in allgemeinen Geschäfts- oder Benutzungsbedingungen leicht vereinbaren, sodass über diesen Weg eine Vielzahl von automatisierten Entscheidungssystemen gerechtfertigt werden kann. Auch die Erforderlichkeit für die Eingehung oder Erfüllung von Verträgen betrifft ein potenziell sehr großes Spektrum von Sachverhalten. Die Alternative einer Erlaubnis durch Rechtsvorschriften kann in ganz unterschiedlichen Kontexten genutzt werden. Vor dem Hintergrund dieser weitreichenden Ausnahmen sind die allgemeinen Gestaltungsvorgaben für die Systeme besonders bedeutend.

Auch wenn ein System unter einen der Ausnahmetatbestände fällt, müssen bestimmte Gestaltungsvoraussetzungen erfüllt sein. Auch diese Gestaltungsvoraussetzungen wurden durch das Recht geändert. Verpflichtend sind „angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren“. Im alten Recht war an dieser Stelle nur von „berechtigten Interessen“ der betroffenen Person die Rede. Die Weiterentwicklung dieser Formulierung, die auch an vielen anderen Stellen der Datenschutzgrundverordnung zu finden ist, spiegelt rhetorisch wider, was sich

¹²Das wird allerdings von einigen Rechtsgelehrten bestritten, die den Zusatz wieder in die Vorschrift hineinlesen.

auch an der Substanz des Art. 22 DSGVO zeigen lässt: Fragen des Datenschutzes sind geeignet, Menschen in ganz grundsätzlicher Art und Weise zu betreffen. Die Formulierung „Rechte und Freiheiten“ eröffnet eine allgemeine grundrechtliche Dimension, die weiter und tiefer geht als die „berechtigten Interessen“, die durch das Wort „sowie“ ohnehin nachrangig betrachtet werden. Im Rahmen der Datenschutzrichtlinie fokussierte sich die Betrachtung auf eine Abwägung der Interessen an der Datenverarbeitung, die meistens die Privatheit der betroffenen Person gegen die Gründe der Datenverarbeitung hielt. Schon die Beispiele aus Erwägungsgrund 71, nämlich „die automatische Ablehnung eines Online-Kreditantrags“ und „Online-Einstellungsverfahren“, zeigen, dass neben dem Schutz der Privatheit auch noch ganz andere Rechte und Freiheiten berührt sein können. Dies betrifft die Berufsfreiheit, die Meinungsfreiheit oder das Recht auf Gleichheit. Das neue Recht beschränkt sich nun nicht auf Erlaubnis oder Verbot, sondern verschiebt die tatsächliche Lösung auf die Gestaltungsebene, wobei die Grundrechte als Anforderungen gelten. Auch hier wird die Latte höher gelegt als noch zuvor. Während die Datenschutzrichtlinie nur beispielhaft die Möglichkeit erwähnt, den eigenen Standpunkt darzulegen, definiert die Datenschutzgrundverordnung gleich eine Reihe von Mindestanforderungen. Sie verlangt „mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung“.

Wenn man den Stand der Privatheit aus diesen Änderungen ableiten will, fallen verschiedene Dinge ins Auge. Ein wichtiger Aspekt ist die Gestaltungsdimension des Rechts, die auch in der Pflicht zum Datenschutz durch Technikgestaltung (privacy by design) in Art. 25 gestärkt wird. Das Recht hat im Hinblick auf die Technik nicht mehr nur die Funktion der Begrenzung von Technik oder aber der Motivation zum Technikeinsatz, es greift tief in Gestaltungsprozesse ein und gibt Gestaltungsziele vor (Djeffal 2018, 503 ff.; 2017, 811–815). Hier verwächst die Privatheit also mit der Technik. Andererseits verweben sich auch andere Grundrechte mit den Rechten auf Privatheit und Datenschutz.¹³ Gerade bei automatisierten Entscheidungen können andere Schutzgüter im Vordergrund stehen, die keinen direkten Bezug zur Privatheit haben. Das kann sogar so weit gehen, dass es der grundrechtskonformen Gestaltung der Privatheit abträglich ist, etwa wenn aus besonderen Gründen Transparenz gefordert ist. Im Datenschutzrecht wird das Recht auf Privatheit zunehmend mit anderen Rechten abgewogen und auch verwoben. Das hat auch zur Folge, dass der Anwendungsbereich der Regelungen wächst. Es geht dann nicht mehr nur um den Schutz der Privatheit, sondern um umfassende Regelungen von automatisierten Systemen. Die Rechtsentwicklung auf diesem Gebiet ist sicher noch nicht abgeschlossen und es könnte gut sein, dass

¹³Während man im deutschen Verfassungsrecht von informationeller Selbstbestimmung spricht, spricht der europäische Grundrechtsschutz in Art. 7 vom Recht auf die Achtung des Privat- und Familienlebens bzw. in Art. 8 vom Recht auf den Schutz personenbezogener Daten.

das Recht automatisierter Entscheidungen oder automatisierter Systeme sich noch stärker verselbstständigt. Für den Moment lässt sich jedenfalls ein Wachstum der Anwendungsbereiche beobachten, gekoppelt mit einem Verwachsen mit der Technik und anderen Rechten und Freiheiten.

2.3 Kontinuität: Grundsätzliches Verbot mit Ausnahmen

Zur Rekonstruktion einer neuen Version der Privatheit ist aber nicht nur die Erfassung evolutionärer und revolutionärer Änderungen, sondern auch der Kontinuitäten des Rechts erforderlich. Manchmal treten durch Änderungen Aspekte noch deutlicher hervor, die gleichgeblieben sind. Privatheit 4.0 ist immer noch Privatheit. Es kann auch sein, dass rechtliche Institutionen gerade im Wandel noch wichtiger werden und noch deutlicher als Aspekt der Privatheit erscheinen. Hier soll eine zentrale Regelungsstruktur des Datenschutzrechts diskutiert werden, nämlich des generellen Verbots mit bestimmten Erlaubnistatbeständen.

Die Datenschutzgrundverordnung statuiert in Art. 6 ein grundsätzliches Verbot und beschreibt verschiedene Ausnahmen.¹⁴ Eine solche Regelungstechnik verbietet ein bestimmtes Verhalten nicht um es ganz zu verhindern oder auszuschließen, sondern um eine Rechtfertigung nach bestimmten Tatbeständen zu erzwingen. Vor jeder Verarbeitung personenbezogener Daten muss sich die datenverarbeitende Stelle fragen, ob und wie das gerechtfertigt werden kann. Dies ist nur der Fall, wenn bestimmte gesetzliche Voraussetzungen vorliegen. Als Rechtfertigung nach Art. 6 kommen etwa die Einwilligung der betroffenen Person (a), die Erfüllung eines Vertrages (b), oder die Wahrung einer öffentlichen Aufgabe (e) in Betracht. Datenverarbeitungen sind also nur möglich, wenn eine Ausnahme in Art. 6 einschlägig ist. Ein solches Verbot mit bestimmten Ausnahmen setzt die handelnden Akteure – hier die datenverarbeitenden Stellen – unter einen besonderen Zwang, weil er jede datenverarbeitende Tätigkeit an sich schon untersagt. Der Gesetzgeber begnügt sich nicht damit, gewisse Anforderungen an das Verhalten zu stellen, die datenverarbeitende Stellen erfüllen müssen. Vielmehr statuiert er einen grundsätzlichen Rechtfertigungszwang, der sich juristisch etwa darin ausdrückt, dass die datenverarbeitende Stelle die Beweislast für ihr Verhalten trägt. Wer Daten verarbeitet, steht bildlich gesprochen zuerst mit beiden Beinen in der Illegalität und muss bewusst und nachweisbar auf die Seite des Rechts übertreten. Vermittelt über

¹⁴Umfassend auch zur grundrechtlichen Fundierung der Vorschrift Roßnagel (2019). In seinem Beitrag weist dieser darauf hin, dass die Regelungstechnik rechtsdogmatisch weder als Verbotsprinzip noch als Verbot mit Erlaubnisvorbehalt zu qualifizieren ist. Für den Zusammenhang dieses Beitrags ist entscheidend, dass das in Art. 6 Abs. 1 generell enthaltene Verbot eine spezifische Regelungstechnik darstellt, die bestimmte rechtliche Folgen nach sich zieht, z. B. bei der Beweislast. Daneben sind auch andere Regelungstechniken denkbar, die dem grundrechtlichen Gesetzesvorbehalt ebenfalls entsprechen könnten.

diesen Rechtfertigungszwang führt diese Regelungstechnik zu einer starken Verrechtlichung. Die Qualifizierung als verbotenes Verhalten macht rechtliche Erwägungen zum zentralen Punkt für jede Entscheidung über weitere Handlungen. Als Alternative gilt ein sogenannter risikobasierter Ansatz, der stärker zwischen den verschiedenen Verarbeitungsvorgängen unterscheidet und Abstufungen hinsichtlich der Regulierung einzieht (Article 29 Data Protection Working Party 2014).

In Deutschland wurde bereits vor der Einführung der Datenschutzgrundverordnung über ein grundsätzliches Verbot gestritten (Bull 2013; Weichert 2013; Kramer 2013). Dieser Streit flammte auch bei den Diskussionen rund um die Datenschutzgrundverordnung wieder auf (Buchner 2016, 157). Es war denkbar, dass der europäische Gesetzgeber von diesem Regelungsansatz abweicht und stärker auf einen risikobasierten Ansatz umschwenkt. Dies ist nicht geschehen. Durch die unterlassene Änderung bleibt es bei den oben herausgearbeiteten Effekten, nämlich eines erhöhten Rechtfertigungszwangs und einer Verrechtlichung. Eine solche strikte Gebundenheit ist in der Verwaltung in Bezug auf den Bürger die Regel. Diese wird nun aber durch das Verbot auf alle Akteure ausgedehnt. Im Anwendungsbereich werden Fragen der Privatheit damit zu einem großen Maße rechtlich determiniert. Das ist eine bemerkenswerte Kontinuität, die zu einer starken Verrechtlichung der Privatheit durch das Datenschutzrecht führt. Denn prinzipiell muss jede einzelne Entscheidung des Datenschutzes rechtlich nachvollziehbar sein. Damit wird Privatheit rechtlich geregelt. Institutionen, wie die datenschutzrechtliche Einwilligung, führen zwar dazu, dass Akteure frei über den Datenschutz disponieren können. Dazu zählt auch der sogenannte risikobasierte Ansatz, der an vielen Stellen der Datenschutzgrundverordnung verlangt, dass datenverarbeitende Stellen selbst mit den Gegebenheiten der konkreten Situation umgehen.¹⁵ All das gilt aber wiederum nur innerhalb der Grenzen, die das Datenschutzrecht den Einwilligungen und den risikobasierten rechtlichen Institutionen zieht. Diese Regulierungstechnik führt also im Ergebnis dazu, dass eine zunehmende Datafizierung auch zu einer zunehmenden Verrechtlichung führt.

2.4 Privatheit 4.0 als Reaktion

Das Vorhergehende zeigt, dass sich aus der Datenschutzgrundverordnung verschiedene Aspekte ableiten lassen, die auf eine neue Privatheit schließen lassen. Aus den neuen Jurisdiktionsregeln in Art. 3 DSGVO lässt sich ableiten, dass der

¹⁵Dazu gehören etwa die Rechenschaftspflicht in Art. 6 Abs. 1, die Nachweispflicht gemäß Art. 24 und die Pflicht zur Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO. Siehe zum Grundsatz der Verantwortlichkeit Heberlein (2018).

Einzelne stärker in den Mittelpunkt rückt. Das Recht auf Datenübertragbarkeit stärkt die Verfügungsmacht des Einzelnen, verbindet Privatheitserwägungen allerdings mit dem Wettbewerbsrecht und dem Verbraucherschutz. Die neue Regel zu automatisierten Entscheidungen im Einzelfall schützt ebenfalls nicht mehr nur das Recht auf Privatheit, sondern bezieht auch andere Grundrechte und Freiheiten in den Schutzbereich mit ein. Dies wirkt sich auch auf die konkreten Gestaltungsanforderungen aus. So wird Privatheit zunehmend mit anderen verfassungsrechtlichen Gütern verwoben. Stabil bleibt die Datenschutzgrundverordnung in Bezug auf das grundsätzliche Verbot der Datenverarbeitung, das durch verschiedene Ausnahmetatbestände gerechtfertigt werden kann. Damit wird die Idee der Verrechtlichung der Privatheit aufrechterhalten.

3 Präliminarien einer Grundrechtsinnovation als Aktion

3.1 Grundrechte und Zukunft

Was wäre aber, wenn das Recht die Entwicklungen nicht nachzeichnet, sondern vorzeichnet? Dann geht es darum, wie besonders im „wechselseitigen Werden“ (Kloepfer 2002) von Grundrechten und Technik Grundrechtsinnovationen möglich sind. Die Gesetzgebung leitet nach reiflicher Überlegung aus der Vergangenheit die Zukunft ab.¹⁶ Gerade im Angesicht emergenter Technologien ist diese Arbeit des Gesetzgebers eine Sisyphosaufgabe, weil sich technologische Möglichkeiten fortlaufend verändern. So urteilte auch der Berichterstatter des Europäischen Parlaments zur Datenschutzreform, dass die Datenschutzgrundverordnung aufgrund neuer Technologien wie künstlicher Intelligenz, dem Internet der Dinge und Robotik eigentlich bereits überholt war, bevor sie in Kraft trat (Albrecht 2016, 98). Zwar hat insbesondere das Technikrecht einige Mechanismen der Beschleunigung entwickelt, wie etwa das sogenannte Komitologieverfahren im Rahmen der Gesetzgebung der Europäischen Union. Diese können allerdings das Grundproblem nicht lösen, dass das Recht grundsätzlich reagiert. Das gilt besonders für das Verhältnis von Recht und Technik. Hier steht am Anfang meist eine technologische Innovation, darauf folgt ihre soziotechnische Operationalisierung, dann das Verständnis der Konsequenzen für die Gesellschaft. Erst im Anschluss daran werden rechtliche Folgen definiert. Auf jeder dieser vier Stufen findet eine Innovation statt, so auch auf der rechtlichen. Allerdings kann man sich schwerlich der Einsicht verschließen, dass die rechtlichen Innovationen in diesem Bereich reaktiv

¹⁶Husserl (1955) bezieht die Zeitlichkeit der Gesetzgebung auf die Zukunft, jedoch schließt auch dieser Zukunftsbezug nicht aus, dass die Gesetzgebung v. a. aus der Vergangenheit lernt.

sind. Während Verfassungsgerichte auf nationaler und europäischer Ebene hier meist eine entscheidende Rolle spielen, sind die Änderungen von der Rechtswissenschaft vorbereitet worden.¹⁷ Hieraus ergibt sich die Frage, ob neben dieser reaktiven Schöpfung neuer Rechte auch eine aktive Innovation möglich ist. Um diese Diskussion anzustoßen, soll hier der Versuch unternommen werden, eine solche aktive Innovation rechtswissenschaftlich zu begründen und am Beispiel von Privatheit und künstlicher Intelligenz auszuprobieren.

3.2 Aktive Grundrechtsinnovation: *status activus processualis*

Wie kann man eine nicht-reaktive Grundrechtsinnovation denken? Notwendigerweise darf eine solche nicht auf die Umwelt reagieren, vielmehr muss die Innovation dazu geeignet sein, ihre Umwelt aktiv in einer Weise zu gestalten, dass auf dieser Basis ein zuvor nicht mögliches Verständnis der Grundrechte Wirklichkeit werden kann. Hier werden Recht und Umwelt gleichzeitig entwickelt. Durch eine enge Interaktion mit emergenten Technologien wird der normative Möglichkeitsraum¹⁸ erweitert, sodass neue grundrechtliche Zielgehalte definiert werden können, ohne dass es zuvor eine Bedrohung dieser Gehalte gibt. So könnte also eine neue Facette des allgemeinen Persönlichkeitsrechts entdeckt werden, ohne dass eine Gefahr oder ein Risiko Auslöser waren. Eine solche schöpfende Verquickung von Recht und Technik ist die höchste Stufe der normativen Integration beider Bereiche. Die unterste Stufe ist die verfassungsverträgliche Technikgestaltung. Hier werden Verfassungsziele so in den technischen Entwicklungsprozess integriert, dass sie Berücksichtigung finden, sodass sich das Endprodukt im Rahmen der verfassungsmäßigen Ordnung hält.¹⁹ Im Hinblick auf das Recht auf informationelle Selbstbestimmung beschreibt Art. 25 der Datenschutzgrundverordnung eine Pflicht zur datenschutzkonformen Technikgestaltung (Domingo-Ferrer u. a. 2014). Einen Schritt weiter geht hier die verfassungsinduzierte Technikentwicklung. Diese setzt der Technik Zielvorgaben jenseits des Stands von Wissenschaft und Technik. Es werden also Ziele gesetzt, die im Moment noch außerhalb des Bereichs des Möglichen liegen.²⁰ Ein solches Instrumentarium sind etwa Technologieklauseln in Menschenrechtsverträgen. Hier werden Staaten zur progressiven Entwicklung von Technologien verpflichtet, um bestimmten menschenrechtlichen

¹⁷Siehe zu diesem Themenkomplex Grimm (2019).

¹⁸Und mithin der Gefahr der Unternormativität zu begegnen, siehe dazu Möllers (2015), 452.

¹⁹Siehe grundlegend Roßnagel (1989, 2008).

²⁰Im Kontext von Innovationen beschreibt dies Hoffmann-Riem (2016).

Zielvorstellungen zu entsprechen. So verpflichtet Art. 4 g des UN Behindertenrechtsübereinkommens die Vertragsstaaten, „Forschung und Entwicklung für neue Technologien, die für Menschen mit Behinderungen geeignet sind, einschließlich Informations- und Kommunikationstechnologien, Mobilitätshilfen, Geräten und unterstützenden Technologien, zu betreiben oder zu fördern sowie ihre Verfügbarkeit und Nutzung zu fördern und dabei Technologien zu erschwinglichen Kosten den Vorrang zu geben“. Hier folgt direkt aus den Menschenrechten eine Pflicht nicht nur zur konformen Entwicklung, sondern auch zur Innovation menschenrechtsfreundlicher Technologien. Ein integratives Werden von Verfassung und Technologie geht noch weiter. Während bei der verfassungsinduzierten Technikentwicklung die Verfassung einen konkreten Gehalt hat, die Technologie aber als kontingent und entwicklungsfähig betrachtet wird, sind sowohl Technologie als auch das Verfassungsrecht im Rahmen eines integrativen Werdens im Wandel. Dieser Wandel ist dann nicht pathologisch motiviert, sondern offen. Auch strebt er nicht einem bestimmten festen Sinn- oder Kerngehalt an, sondern imaginiert und entwickelt rechtliche Gehalte weiter. Neue anspruchsvollere Verfassungsgehalte werden gemeinsam mit ihren Voraussetzungen erfunden und gedacht (Abb. 1).

Was die Verfassung und insbesondere die Grundrechte hier zu leisten vermögen, lässt sich schwer in die überlieferten Kategorien der Grundrechtsfunktionen und der grundrechtlichen Statuslehre einfügen. Nach der Statuslehre Jellineks unterscheidet man den *status activus*, der politische Beteiligungsrechte verleiht, vom *status negativus* der Freiheitsrechte und dem *status positivus* der

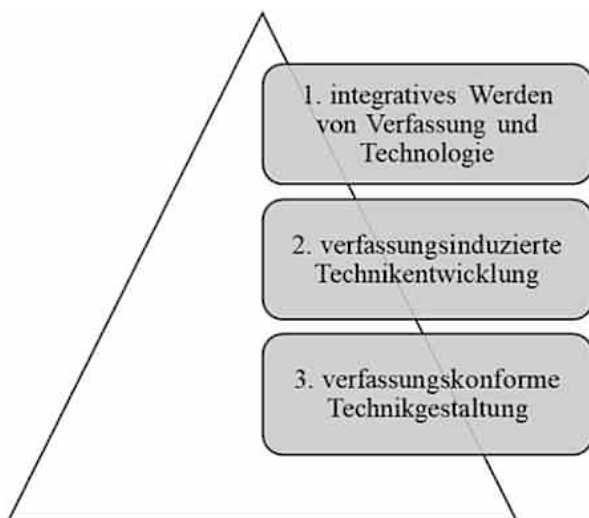


Abb. 1 Verfassung und Technik

Leistungsrechte.²¹ Genauso wie der von Häberle entwickelte *status activus processualis* die verfahrensmäßigen Voraussetzungen der Grundrechtsverwirklichung in den Blick nimmt (Häberle 1973, 51, 82 ff.), kann man in Zeiten einer zunehmenden Technisierung durch emergente Technologien an einen *status activus technicus* denken. Dieser nimmt die Grundrechtsvoraussetzungen der Technik in den Blick und trägt zu ihrer Gestaltung bei. Gerade in Phasen technischer Entwicklung ermöglicht er aber eine Dynamik auch grundrechtlicher Selbstbestimmung. Welches Gestaltungspotenzial dem zugrunde liegt, soll hier am Beispiel der künstlichen Intelligenz gezeigt werden.

3.3 Die vielen Pfade der künstlichen Intelligenz

Ein technologischer Trend, dessen Auswirkungen auf die Gesellschaft gerade intensiv auch in den Rechtswissenschaften diskutiert wird (Hoffmann-Riem 2017; Wischmeyer 2018), ist die künstliche Intelligenz (KI). Dabei handelt es sich nicht um eine einzelne Technologie, sondern ein Bündel von Technologien (Gasser/Budish/Ashar 2018), das eine Forschungsfrage beantwortet, die man wie folgt fassen könnte: können technische Systeme komplexe Probleme selbstständig lösen?²² So versammeln sich unter dem Banner der künstlichen Intelligenz Technologien, die in verschiedensten Graden von der Auswertung großer Datensätze abhängig sind. Manche Mechanismen des maschinellen Lernens sind etwa zum Training der Bildererkennung darauf angewiesen, dass sie mit Millionen von Datensätzen trainiert werden. Demgegenüber können sogenannte „general adversarial networks“ bestimmte Aufgaben lernen, indem zwei Systeme sich gegenseitig trainieren (Goodfellow/Bengio/Courville 2016). Unter Verwendung der gängigen Schlagwörter kann man also sagen, dass künstliche Intelligenz sowohl auf „Big Data“ als auch auf „Small Data“ beruhen kann. Schon auf der Ebene der Grundlagenforschung gibt es viele Entscheidungen, die sich unmittelbar auf Fragen der Verwendung personenbezogener Daten auswirken. Wie stark hier Innovationsprozesse beeinflusst werden können, zeigt nicht zuletzt die Förderung einiger Durchbrüche zum automatisierten Fahren, die nach Beschluss des US-Amerikanischen Parlaments in Wettbewerben der Forschungsförderungsinstitution des US-Verteidigungsministeriums (DARPA) öffentlich in Wettbewerben ausgelobt wurden und die tatsächlich zu Durchbrüchen auf diesen Gebieten führten.

²¹Diese Unterscheidung geht zurück auf Jellinek (1892), 89 ff.

²²So die Arbeitsdefinition in Mainzer (2016), 3.

Aus der Offenheit der oben formulierten Forschungsfrage ergibt sich, dass auch die Zwecke, zu welchen die Systeme verwendet werden können, grundsätzlich offen sind. Man spricht von einer Querschnittstechnologie (general purpose technology). Es hängt von Entscheidungen auf verschiedenen Ebenen und nicht zuletzt vom soziotechnischen Kontext ab, welchen sozialen und ethischen Zwecken künstliche Intelligenz dient. Das lässt sich nicht zuletzt an neueren Anwendungen im Bereich des Datenschutzes zeigen. Hier treten Systeme der künstlichen Intelligenz als neue Gefahren für Privatheit, Datenschutz und informationelle Selbstbestimmung auf. So wird aktuell an verschiedenen Stellen um das Thema der Bilderkennung gestritten. Das betrifft beispielsweise die Gesichtserkennung an öffentlichen Orten zum Auffinden von gesuchten Personen (Kurpujuweit 2017), die systematische Kennzeichenerfassung zum Durchsetzen von Diesel-Fahrverboten oder das Erkennen sozialer Situationen wie etwa Diebstahl oder Körperverletzungen.²³ Demgegenüber kann künstliche Intelligenz zu Zwecken der Förderung der Privatheit eingesetzt werden, etwa zur datenschutzfreundlichen Technikgestaltung oder zur Durchsetzung der Präferenzen von Individuen. Ein Beispiel in diesem Bereich ist die Möglichkeit der Anonymisierung von Videoaufnahmen, sodass Parkraumüberwachungssysteme durch das Unkenntlichmachen von Gesichtern und Kennzeichen nicht mehr auf personenbezogene Daten zugreifen können. Ein anderes Beispiel betrifft den Einsatz von Chatbots zur Durchsetzung von Präferenzen einzelner Nutzer. Ein solches Konzept verfolgt etwa der Chatbot Chommy, der Datenschutzpräferenzen bei Nutzern abfragt und diese anschließend bei Internetdiensten umsetzen soll.

Diese Beispiele zeigen, dass das Recht über die Regelung der Zulässigkeit einzelner Systeme in seiner Funktion als Instrument der vorausschauenden Technikgestaltung sowohl auf der Ebene der Innovation als auch auf der Ebene der soziotechnischen Ausgestaltung zahlreiche Möglichkeiten offeriert. Diese Möglichkeiten können wahrgenommen werden, um das bisherige Verständnis von Privatheit in Technik fließen zu lassen. Genauso können aber neue und auch imaginierte Potenziale dazu dienen, unsere Vorstellung von Privatheit weiterzuentwickeln. Das setzt allerdings eine konzeptionelle und gelebte Nähe von Verfassungsrecht und Technikentwicklung voraus, die sehr voraussetzungsreich ist. Dabei darf man auch nicht vergessen, dass auch ohne eine solche Partizipation auf verfassungsrechtlicher Ebene zahlreiche Ideen und Haltungen implizit in die Technikentwicklung einfließen. Die Öffnung von Innovation und Forschung in dem Bereich würde diese hingegen an demokratisch konsentierten Grundwerten

²³Ein solches System wird gerade etwa für die Stadt Mannheim unter dem Projektnamen Mannheim 2.0 entwickelt.

ausrichten. Im Zuge dieser Auseinandersetzung würde die verfassungsrechtliche Debatte wiederum selbst Impulse aufnehmen. In diesem Wechselspiel könnte die Vorstellung von Privatheit in einer Art und Weise weiterentwickelt werden, die nicht bloß auf technische Entwicklungen reagiert, sondern sowohl die Technik als auch sich selbst weiterdenkt.

4 Epilog

Die Analyse der Datenschutzgrundverordnung zeigt also, dass das Recht kontinuierlich auf verschiedene technische und soziale Neuerungen reagiert. Dabei reagiert es durch Novationen und evolutionäre Weiterentwicklungen, aber auch durch das Beharren auf bestimmten Strukturmerkmalen. Eine strukturelle Analyse einer umfassenden Reform wie der Datenschutzgrundverordnung kann auch zeigen, wie sich Privatheit im Spiegel des Rechts als konsentrierte Ordnung der Privatheit entwickelt hat. Dies lässt das Recht allerdings reaktiv erscheinen, denn es vollzieht gesellschaftliche Änderungsprozesse nach. Gerade im Bereich von Forschung und Innovation kann das Verfassungsrecht eine Gestaltungsfunktion übernehmen, die zu einer aktiven Gestaltung von Recht und Technik führt. Im Angesicht von emergenten Technologien wie etwa künstlicher Intelligenz und der beschleunigten Veränderung von Technik und Gesellschaft werden diese Potenziale zur aktiven Gestaltung der Verfassungsvoraussetzungen gut sichtbar. Im Rahmen dieses Beitrags sollte diese aktive Seite des Verfassungsrechts anhand der grundrechtlichen Statuslehre gefasst und im Begriff des *status activus technicus technologicusve* in Anlehnung an den *status activus processualis* konzentriert werden. Ob und wie eine solche aktive Gestaltung der Privatheit und anderer verfassungsrechtlicher Güter gelingen kann, hängt von der Debatte in allen beteiligten wissenschaftlichen Disziplinen und darüber hinaus ab. So gesehen sind die Möglichkeiten der aktiven Gestaltung von Recht und Technik genauso groß und offen wie unser aller Zukunft.

Appendix

Vergleich der Vorschriften

Datenschutzrichtlinie Art. 15 Automatisierte Einzelentscheidung	Datenschutzgrundverordnung Art. 22 Automatisierte Entscheidung im Einzelfall einschließlich Profiling
<p>(1) Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.</p> <p>(2) Die Mitgliedstaaten sehen unbeschadet der sonstigen Bestimmungen dieser Richtlinie vor, daß eine Person einer Entscheidung nach Absatz 1 unterworfen werden kann, sofern diese</p> <p>a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags ergeht und dem Ersuchen der betroffenen Person auf Abschluß oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen - garantiert wird oder</p> <p>b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.</p>	<p>(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.</p> <p>(2) Absatz 1 gilt nicht, wenn die Entscheidung</p> <p>a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,</p> <p>b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder</p> <p>c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.</p> <p>(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.</p> <p>(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.</p>

Literatur

- Albrecht, Jan P.: Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. In: *Computer und Recht* 32/2 (2016), 88–98.
- Albrecht, Jan P./Jotzo, Florian: *Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse*. Baden-Baden 2017.
- Article 29 Data Protection Working Party: Statement on the role of a risk-based approach in data protection legal frameworks (2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.
- Art. 29 Gruppe: Leitlinien zum Recht auf Datenübertragbarkeit (2016). https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP242de_Art_29-Gruppe_Datenubertragbarkeit.pdf.
- Bezanson, Randall P.: The Right to Privacy Revisited: Privacy, News, and Social Change, 1890–1990. In: *California Law Review* 80 (1992), 1133–1175.
- Bodó, Balázs/Helberger, Natali/Vreese, Claes H. de: Political micro-targeting: a Manchurian candidate or just a dark horse? In: *Internet Policy Review (IPR)* (2017).
- Bratman, Ben: Brandeis and Warren’s the Right to Privacy and the Birth of the Right to Privacy. In: *Tennessee Law Review* 69 (2002), 623–651.
- Buchner, Benedikt: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. In: *Datenschutz und Datensicherheit - DuD* 40/3 (2016), 155–161.
- Bull, Hans Peter: *Netzpolitik Freiheit und Rechtsschutz im Internet*. Baden-Baden 2013.
- Cannataci, Joseph: Privacy, Technology Law and Religions across Cultures. In: *Journal of Information, Law & Technology (JILT)* 1 (2009), 1–22.
- Dammann, Ulrich: Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt Schwächen und überraschende Innovationen. In: *Zeitschrift für Datenschutz* 6/7 (2016), 307–314.
- Dix, Alexander: 20. In: Spiros Simitis/Gerrit Hornung/Indra Spiecker Döhmman (Hg.): *Datenschutzrecht. DSGVO mit BDSG*. Baden-Baden 2019.
- Djeflal, Christian: Das Internet der Dinge und die öffentliche Verwaltung. Auf dem Weg zum automatisierten Smart Government? In: *Deutsches Verwaltungsblatt* (2017), 808–816.
- Djeflal, Christian: xGovernment n.0 oder von der Informatisierung der Begriffe (2016), www.juwiss.de/90-2016 (05.12.2018).
- Djeflal, Christian: AI, Democracy, and the Law. In: Andreas Sudmann (Hg.): *The Democratization of Artificial Intelligence. Net Politics in the Era of Learning Algorithms*. Bielefeld 2019, 255–284.
- Djeflal, Christian: Normative Leitlinien Für Künstliche Intelligenz in Regierung und Verwaltung. In: Resa Mohabbat Kar/Basanta Thapa/Peter Parycek (Hg.): *»(Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft«*. Berlin 2018, 493–515.
- Domingo-Ferrer, Josep/Hansen, Marit/Hoepman, Jaap-Henk/Le Métayer, Daniel/Tirtea, Rodica/Schiffner, Stefan/Danezis, George: *Privacy and data protection by design from policy to engineering*. Heraklion 2014.
- Gajda, Amy: Privacy, Press, and the Right to Be Forgotten in the United States. In: *Washington Law Review* 93 (2018), 201–264.
- Gasser, Urs/Budish, Ryan/Ashar, Amar: Module on Setting the Stage for AI Governance. Interfaces, Infrastructures, and Institutions for Policymakers and Regulators. In: *Artificial Intelligence (AI) for Development Series* (2018).
- Glancy, Dorothy J.: Invention of the Right to Privacy, The. In: *Arizona Law Review* 21 (1979).
- Gömann, Merlin: The new territorial scope of EU data protection law. Deconstructing a revolutionary achievement. In: *Common market law review* 54/2 (2017), 567–590.
- Goodfellow, Ian/Bengio, Yoshua/Courville, Aaron: *Deep Learning*. Michigan 2016.
- Grimm, Dieter (Hg.): *Vorbereiter – Nachbereiter? Der Beitrag der Staatsrechtslehre zu den großen Innovationen der Verfassungsrechtsprechung im Grundrechtsbereich*. Tübingen 2019.

- Häberle, Peter: Grundrechte im Leistungsstaat. In: *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer* 31 (1973), 43.
- Heberlein, Horst: Art. 5. In: Eugen Ehmann/Martin Selmayr (Hg.): *DS-GVO. Datenschutzgrundverordnung Kommentar*. München ²2018.
- Herbst, Tobias: Art. 20. In: Jürgen Kühling/Benedikt Buchner/Matthias Bäcker (Hg.): *Datenschutz-Grundverordnung BDSG. Kommentar*. München ²2018.
- Hoffmann-Riem, Wolfgang: *Innovation und Recht Recht und Innovation*. Tübingen 2016.
- Hoffmann-Riem, Wolfgang: Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht. In: *AöR (Archiv des öffentlichen Rechts)* 142/1 (2017), 1–42.
- Hornung, Gerrit: *Grundrechtsinnovationen*. Tübingen 2015.
- Husserl, Gerhart: Recht und Zeit. In: Ders.: *Recht und Zeit. Fünf rechtsphilosophische Essays*. Frankfurt a.M. 1955, 7–66.
- Jellinek, Georg: *System der subjektiven öffentlichen Rechte*. Freiburg 1892.
- Jülicher, Tim/Röttgen, Charlotte/Schönfeld, Max v.: Das Recht auf Datenübertragbarkeit. Ein datenschutzrechtliches Novum. In: *Zeitschrift für Datenschutz* 6/8 (2016), 358–362.
- Kamann, Hans-Georg/Braun, Martin. In: Eugen Ehmann/Martin Selmayr (Hg.): *DS-GVO. Datenschutzgrundverordnung Kommentar*. München ²2018, 428–443.
- Kloepfer, Michael: *Technik und Recht im wechselseitigen Werden. Kommunikationsrecht in der Technikgeschichte*. Berlin 2002.
- Kramer, Philipp: Verbot mit Erlaubnisvorbehalt zeitgemäß? In: *Datenschutz und Datensicherheit - DuD* 37/6 (2013), 380–382.
- Kühling, Jürgen/Martini, Mario: Die Datenschutz-Grundverordnung. Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? In: *Europäische Zeitschrift für Wirtschaftsrecht* 27/12 (2016), 448–454.
- Kurpjuweit, Klaus: Bahn testet intelligente Videoüberwachung am Südkreuz (2017), <http://www.tagesspiegel.de/berlin/berliner-bahnhof-bahn-testet-intelligente-videoueberwachung-am-sue-dkreuz/19413266.html> (12.06.2017).
- Mainzer, Klaus: *Künstliche Intelligenz Wann übernehmen die Maschinen?* Berlin/Heidelberg 2016.
- Martini, Mario: Art. 22. In: Boris Paal/Daniel Pauly (Hg.): *[Duplikat] Datenschutz Grundverordnung: DS-GVO*. München ²2018.
- Möllers, Christoph: *Die Möglichkeit der Normen. Über eine Praxis jenseits von Moralität und Kausalität*. Berlin 2015.
- Paal, Boris: Art. 20. In: Boris Paal/Daniel Pauly (Hg.): *[Duplikat] Datenschutz Grundverordnung: DS-GVO*. München ²2018.
- Post, Robert C.: Rereading Warren and Brandeis: Privacy, Property, and Appropriation Symposium: The Right to Privacy One Hundred Years Later. In: *Case Western Reserve Law Review* 41 (1991), 467–680.
- Roßnagel, Alexander: Technik und Recht. wer beeinflusst wen? In: Ders.: *Freiheit im Griff. Informationsgesellschaft und Grundgesetz*. Stuttgart 1989, 9–20.
- Roßnagel, Alexander: Rechtswissenschaftliche Gestaltung von Informationstechnik. In: Harald F.O.v. Korfflesch (Hg.): *Wissen, Vernetzung, Virtualisierung. Liber amicorum zum 65. Geburtstag von Udo Winand*. Lohmar 2008, 381–390.
- Roßnagel, Alexander: Kein “Verbotsprinzip” und kein “Verbot mit Erlaubnisvorbehalt” im Datenschutzrecht. Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff. In: *Neue juristische Wochenschrift* 72/1/2 (2019), 1–5.
- Schantz, Peter: Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. In: *Neue Juristische Wochenschrift* (2016), 1841–1847.
- Warren, Samuel D./Brandeis, Louis D.: The Right to Privacy. In: *HLR (Harvard Law Review)* 4/5 (1890), 193.

- Weichert, Thilo: Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz? Zugleich Besprechung von “Bull Hans Peter Netzpolitik: Freiheit und Rechtsschutz im Internet 2013 154 Seiten“. In: *DuD* 37/4 (2013), 246–249.
- Weichert, Thilo: Art. 3. In: Jürgen Kühling/Benedikt Buchner/Matthias Bäcker (Hg.): *Datenschutz-Grundverordnung BDSG. Kommentar*. München ²2018, 319–358.
- Wischmeyer, Thomas: Regulierung intelligenter Systeme. In: *AöR (Archiv des öffentlichen Rechts)* 143/1 (2018), 1–66.