Souveränität, Integrität und Selbstbestimmung – Herausforderungen von Rechtskonzepten in der digitalen Transformation

Christian Rückert, Christoph Safferling, Franz Hofmann

Abstract *Der Begriff der »digitalen Souveränität« lässt sich aus einer rechtswissenschaftlichen Perspektive in die drei Unterbegriffe der Souveränität, der Integrität und der Selbstbestimmung untergliedern. Mit ihnen können die Rechtsbeziehungen zwischen Staaten, Bürger*innen sowie zwischen Staat und Bürger*innen beschrieben werden. Alle diese Konzepte stehen durch die Digitalisierung vor neuen Herausforderungen. Hinsichtlich der zwischenstaatlichen Souveränität geht es vor allem um sogenannte transnationale Datenzugriffe. Ein praktischer Anwendungsfall ist der Zugriff auf personenbezogene Daten von Bürger*innen im Ausland zu Zwecken der Strafverfolgung. In diesen Fällen, die bislang vor allem unter klassischen staatsrechtlichen Souveränitätsaspekten diskutiert wurden, sollte künftig der Blick vermehrt auf die digitale Integrität der betroffenen Bürger*innen und die entsprechenden Schutzpflichten der Staaten gerichtet werden. Aber auch die selbstbestimmte Regelung der eigenen Verhältnisse erscheint gefährdet. Das Recht hat insbesondere sicherzustellen, dass die Entscheidungsfreiheit auch in der Digitalgesellschaft gewährleistet bleibt.*

Der Datenverkehr hat durch die Weiterentwicklung der digitalen Kommunikation, durch die zunehmende Vernetzung von Alltagsgegenständen (»Internet der Dinge«) und durch die Automatisierung kommunikativer Abläufe nicht nur enorm zugenommen, sondern ist gerade durch sogenanntes »Cloud-Computing« grenzenlos geworden. Das Recht mit seinen häufig aus dem 19. Jahrhundert stammenden Vorstellungen, Konzepten und Normen, wird dabei besonders herausgefordert.

In diesem Beitrag sollen zwei Aspekte untersucht werden: Strafrecht und Privatrecht. Der bislang unscharf gebliebene Begriff der »digitalen Souveränität« wird dabei in verschiedene Teilaspekte des Konzepts aufge-

gliedert: Um klassische Souveränität im staatsrechtlichen Sinn geht es im Verhältnis von Nationalstaaten untereinander. Hier stellt sich im Bereich des grenzüberschreitenden Datenverkehrs und der Nutzung grenzüberschreitender digitaler Dienstleistungen wie Cloud-Computing die Frage, ob sich die staatliche Souveränität auch auf den digitalen Raum erstreckt, ob also im Jellinek'schen Sinne (vgl. Jellinek 1922) das Staatsgebiet auch einen digitalen Bereich umfasst. Besonders relevant wird diese Frage bei grenzüberschreitenden Dateneingriffen durch staatliche Behörden, z.B. Strafverfolgungsbehörden. Stellt eine Datenerhebung »auf« fremdem Staatsgebiet einen Eingriff in die Souveränität desjenigen Staates dar, auf dessen Staatsgebiet sich der Datenspeicher befindet?

Im Verhältnis des Staates zu (seinen) Bürger*innen geht es dagegen juristisch betrachtet nicht um die »digitale Souveränität« der Bürger*innen, sondern um deren digitale Integrität, welche ihnen durch die Grund- und Menschenrechte des Grundgesetzes, der Europäischen Grundrechtecharta und der Europäischen Menschenrechtskonvention garantiert wird. Noch weiter entfernt vom traditionellen juristischen Verständnis des Begriffs der Souveränität ist schließlich der letzte rechtliche Teilaspekt »digitaler Souveränität«: Im Verhältnis der Bürger*innen untereinander – also im Privatrecht – geht es um die Wahrung und den Ausgleich der »digitalen Selbstbestimmung« oder der »digitalen Privatautonomie« der handelnden Rechtssubjekte. Die Rechtskonzepte des Privatrechts werden hier in vielfacher Hinsicht herausgefordert: So wird allen voran die Gestaltung und Nutzung des digitalen Raums nahezu ausschließlich von großen (zumeist ausländischen) Technologiekonzernen bestimmt, welche dem*der Einzelnen nicht als Gleichgestellte, sondern als Konstrukte mit staatsähnlicher Macht gegenübertreten. Auch die schnell wachsende Bedeutung von digitalen Gütern, insbesondere Daten, spiegelt sich nicht immer hinreichend in der Ordnung des deutschen Zivilrechts wider. Namentlich die selbstbestimmte Verwertung personenbezogener Daten ist bisher nicht zufriedenstellend geklärt.

Der folgende Beitrag beleuchtet die Teilkonzepte der »digitalen Souveränität« (staatliche Souveränität über Daten im Verhältnis von Staaten untereinander, digitale Integrität der Bürger*innen gegen staatliche Dateneingriffe und digitale Selbstbestimmung/Privatautonomie im Verhältnis der Bürger*innen untereinander einschließlich gegenüber staatsähnlich agierenden Technologiekonzernen) unter zwei verschiedenen Blickwinkeln: Im Straf- und Strafverfahrensrecht wird der Blick auf mögliche Verletzungen staatlicher Souveränität und digitaler Integrität der Bürger*innen durch

grenzübergreifende Dateneingriffe gerichtet und das Verhältnis unter dem Gesichtspunkt des Grund- und Menschenrechtsschutzes neu austariert (Teil I). Das Privatrecht muss dagegen klären, wie digitale Selbstbestimmung und Privatautonomie auch unter Eindruck der Übermächtigkeit der Tech-Unternehmen funktionieren kann. Zur Illustration wird das Verhältnis von Datenschutz und Selbstbestimmung angerissen (Teil II).

Teil I: Menschenrechtsschutz und Datensouveränität im Strafprozess

Heute ist es bei strafrechtlichen Ermittlungen häufig erforderlich, Daten zu sammeln, deren physischer Speicherort (auch) im Ausland liegt. Die Datenerfassung im Ausland stellt möglicherweise einen Eingriff in die »(digitale) Souveränität« des ausländischen Staates dar und darf daher ohne die Zustimmung dieses Staates – nach klassischem Völkerrecht – nicht erfolgen. Außer in den eher seltenen Fällen des Schutzes von Staatsgeheimnissen sind staatliche Interessen bei strafrechtlichen Ermittlungen in virtuellen Speichern aber nicht unmittelbar betroffen. Die Speicher selbst sind in aller Regel auch nicht staatliches Eigentum, sondern werden von global agierenden Unternehmen (Google, Microsoft, Apple etc.) betrieben. Es geht hauptsächlich um personenbezogene Daten und damit um den Schutz der Betroffenen vor staatlicher Einmischung überhaupt. Dass diese durch eine ausländische Regierung erfolgt, ist nur ein zusätzlicher Aspekt, der an der unmittelbaren Betroffenheit des Individuums kaum etwas ändert. Damit kommt es aber auf die Qualität des Eingriffs selbst an, auf dessen Rechtsstaatlichkeit und dessen Respekt vor den Grund- und Menschenrechten der Betroffenen. Mangelt es an solchen Garantien und Schutzmaßnahmen, müssen die liberalen Staaten sicherstellen, dass sowohl ihre Bürger*innen als auch die im jeweiligen Staat lebenden Ausländer*innen vor der Ausforschung durch ausländische Regierungen geschützt sind. Bislang ist die Rechtsprechung in Deutschland eher einer völkerrechtlichen Vorstellung zugetan und differenziert danach, ob der betroffene Staat die Souveränitätsverletzung rügt. Der folgende Beitrag plädiert daher sowohl für die Ausarbeitung künftiger völkerrechtlicher Vereinbarungen (z.B. der E-Evidence-Verordnung auf Ebene der Europäischen Union auf der Grundlage des Prinzips der gegenseitigen Anerkennung) als auch für die Lösung bestimmter Rechtsfragen (z.B. betreffend die Durchsuchungsmöglichkeit externer Speichermedien in § 110 Abs. 3 StPO) für eine Verlagerung des Fokus weg von Fragen der

Souveränität (im klassischen Sinn der Staatsrechtslehre und des Völkerrechts) hin zu Fragen des Schutzes der Menschenrechte bei grenzüberschreitenden Dateneingriffen durch ausländische Staaten.

1. Die praktische Bedeutung transnationaler Dateneingriffe für das Strafverfahren

1.1 Digitale Daten als Beweismittel im Strafverfahren

In der Praxis der Strafverfolgung sind transnationale Dateneingriffe nicht nur in klassischen Cybercrime-Verfahren relevant. Daten als solche werden mehr und mehr zu einem »Standardbeweismittel« in Strafverfahren wegen ganz unterschiedlicher Delikte. Grund hierfür ist die immer stärker werdende Durchdringung aller Lebensbereiche der Bürger*innen mit digitalen Technologien. Große Teile der Berufswelt, aber auch die Verwaltung des eigenen Lebens und die Kommunikation sind weitgehend digitalisiert. Daher hinterlassen Bürger*innen – und damit auch Tatverdächtige – stetig mehr Datenspuren, die in Strafverfahren als Beweismittel oder, praktisch nochmals deutlich relevanter, als Grundlage eines Tatverdachts für weitere – ggf. realweltliche (z.B. Durchsuchungen) – Ermittlungsmaßnahmen Verwendung finden. Neben Spuren der klassischen Individualkommunikation mittels E-Mail, Messengerdiensten und Voice-over-IP-Telefonie sowie der Datenverarbeitung und -speicherung auf privaten informationstechnischen Systemen wie Smartphones, Laptops, Tablets und Smart Watches werden auch in zunehmendem Maße Gegenstände des täglichen Lebens als Geräte des »Internet of Things« (IoT) angeboten. Diese Geräte – wie z.B. Stromzähler, Kühlschränke, Automobile, Heim-Assistenzsysteme und Kaffeemaschinen – speichern und verarbeiten ebenfalls Daten und kommunizieren über das Internet mit anderen IoT-Geräten und Personen (vgl. Rückert 2020a).

1.2 Praktisch bedeutsame Arten der transnationalen Dateneingriffe

Die Datensätze, welche für deutsche Strafverfolgungsbehörden relevant sind, befinden sich dabei nicht ausschließlich auf deutschem Staatsgebiet. In vielen Fällen sind gerade Daten verfahrensrelevant, die außerhalb des deutschen Hoheitsgebiets lokalisiert sind. Als »Ort« der Daten gilt dabei nach hergebrachtem Verständnis derjenige Ort, an dem sich der Datenträger physisch befindet, auf dem die Daten gespeichert sind (vgl. Brodowski/Eisenmenger 2014). Der traditionelle und hinsichtlich staatlicher Souveränitätsansprüche unproblematische Weg, im Ausland gespeicherte Daten zu erhalten, besteht

in der Rechtshilfe. Hierbei ersucht derjenige Staat, in dem die strafrechtlichen Ermittlungen stattfinden, denjenigen Staat, auf dessen Hoheitsgebiet die Daten gespeichert sind, darum, die Daten durch seine Strafverfolgungsbehörden erheben zu lassen und diese dann an die Strafverfolgungsbehörden des ersuchenden Staates herauszugeben. Trotz Beschleunigung und Effektivierung des Rechtshilfeverfahrens durch bi- und multilaterale völkerrechtliche Abkommen (z.B. Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen mit Zusatzvertrag vom 18. April 2006) und insbesondere europarechtliche Regelungen (v.a. die Richtlinie über die Europäische Ermittlungsanordnung, RL 2014/41/EU) wird das Rechtshilfeverfahren von Strafverfolgungsbehörden insgesamt als zu langsam und ineffektiv empfunden. Dies gilt sowohl im Allgemeinen als auch im Besonderen für digitale Daten als Beweismittel, bei denen die Flüchtigkeit und Veränderlichkeit von Datensätzen eine besondere Herausforderung darstellt (vgl. Rückert 2020a). Daher fordern Strafverfolgungsbehörden seit Langem, unmittelbaren Zugriff auf Daten, welche im Ausland lokalisiert sind, zu erhalten.

Die praxisrelevanten Konstellationen der Erhebung von Daten im Ausland lassen sich dabei in drei Fallgruppen unterteilen: (1) Zunächst können öffentlich zugängliche Daten im Ausland lokalisiert sein, wenn sich der Server, über den das jeweilige allgemein zugängliche Internetangebot – z.B. Foren, Webseiten, Boards, Handelsplattformen und soziale Medien – betrieben wird, im Ausland befindet. Die von dem*der Tatverdächtigen stammenden öffentlich zugänglichen Daten wie Foreneinträge, Angebote auf Handelsplattformen oder Postings in sozialen Medien befinden sich dann auch »im« Ausland. (2) Besonders interessant für strafrechtliche Ermittlungen sind außerdem Daten von Telekommunikations- oder Telemedienanbietern wie z.B. Internetzugangsdienste, Cloud-Dienstleister, Soziale Netzwerke, Messengerdienste, Voice-over-IP-Anbieter. Diese halten Bestandsdaten (§§ 3 Nr. 6, 172 TKG und §§ 2 Abs. 2 Nr. 2, 22 Abs. 1 S. 1 TTDSG) ihrer Kunden vor, verarbeiten Verkehrs- und Nutzungsdaten (§§ 9, 12 TTDSG, § 2 Abs. 2 Nr. 3 TTDSG) und verfügen oftmals auch über Inhaltsdaten der von ihnen vermittelten Kommunikationsvorgänge oder gehosteten Inhalte. Nicht selten haben die genannten Dienstleister ihren Sitz im Ausland und betreiben auch die Serverinfrastrukturen, auf denen die relevanten Daten verarbeitet und gespeichert werden, im Ausland. (3) Schließlich können auch auf privaten, im Ausland befindlichen informationstechnischen Systemen verarbeitete Daten von Interesse für Ermittler*innen sein. In vielen Kriminalitätsbereichen –

z.B. dem Handel mit illegalen Gütern und Dienstleistungen im sogenannten Darknet, bei klassischen Cybercrime-Delikten, aber auch im Bereich der organisierten Kriminalität (vgl. Goger/Stock 2017) – befinden sich Täter*innen, Gehilf*innen oder Datenspeicher im Ausland und Täter*innengruppierungen operieren hier zunehmend grenzüberschreitend (vgl. Burchard 2018a). Besonders relevant ist dies bei denjenigen Delikten, bei denen sich die deutsche Strafgewalt – z.B. aufgrund des sogenannten Weltrechtsprinzips – auch auf Taten erstreckt, die im Ausland begangen wurden (vgl. Rückert 2020b).

Die Zugriffe auf die im Ausland belegenen Daten erfolgt in den drei gerade genannten Fallkonstellationen auf unterschiedliche Weise: (1) Auf öffentlich zugängliche Daten im Internet, z.B. in Foren und sozialen Medien, wird durch sogenannte Open Source Intelligence-Maßnahmen (OSINT) zugegriffen, zu denen sowohl einfache »Online-Streifen« als auch automatisierte Datensammlungen mittels sogenannter Crawler zählen (vgl. Kalpakis et al. 2016; Staffler/Jany 2020). (2) Der Zugriff auf Daten, die bei Telekommunikations- und Telemediendienstanbietern gespeichert sind oder von diesen verarbeitet werden, erfolgt entweder im Rahmen einer Telekommunikationsüberwachung (§ 100a StPO), durch die Abfrage von bei den Anbietern gespeicherten Daten (§§ 100g, 100j, 100k StPO) oder im Wege der Beschlagnahme (§§ 94ff. StPO; vgl. BVerfG 2009). (3) Der Zugriff auf private informationstechnische Systeme im Ausland betrifft in der Praxis vor allem sogenannte Cloud-Dienstleistungen (vgl. BVerfG 2016; Krcmar 2016). Auf diese Daten wird entweder im Wege einer elektronischen Durchsicht nach § 110 Abs. 3 StPO (vgl. Wicker 2013a) oder mittels einer Online-Durchsuchung unter Nutzung von Spähprogrammen (vgl. Grözinger 2019) zugegriffen.

2. Die bisherige – souveränitätsgeprägte – Debatte um strafprozessuale transnationale Dateneingriffe

Die bisher – und bisweilen recht intensiv – geführte Debatte über die Zulässigkeit von strafprozessualen Zugriffen auf Daten im Ausland dreht sich bislang um die staatliche Souveränität über Daten, die auf staatlichem Hoheitsgebiet gespeichert wurden. Das grundlegende Argumentationsmuster lautet dabei, dass Daten auf staatlichem Hoheitsgebiet der Souveränität des jeweiligen Staates unterfallen und Zugriffe von ausländischen Staaten daher eine Verletzung der staatlichen Souveränität mit sich brächten. Im Übrigen spaltet sich die Diskussion danach auf, ob es sich um den Zugriff auf öffentlich zugängliche Daten, auf Daten bei Telekommunikations- und Te-

lemediendienstanbietern oder auf private informationstechnische Systeme, insbesondere Cloud-Speicher, handelt.

2.1 Der Anknüpfungspunkt: staatliche Souveränität über Daten?

Dreh- und Angelpunkt der bisherigen Debatte ist damit die Grundannahme, dass Daten, die auf einem Datenträger gespeichert sind, der sich physisch im Hoheitsgebiet eines Staates befindet, der Hoheitsgewalt des jeweiligen Staates unterfallen. Diese Annahme wird zwar in zahlreichen Publikationen zum Problemkreis gemacht, aber nur selten hinterfragt oder ausführlich begründet (ausführliche Auseinandersetzung dagegen bei Burchard 2018a, 2018b). Dass jedenfalls die Rechtspolitik davon ausgeht, dass die Nationalstaaten ihre Herrschaftsgewalt auch über Daten ausüben, zeigt allein schon die Existenz von völkerrechtlichen Abkommen und – innerhalb von Europa – expliziten Regelungen der EU (z.B. Art. 29, 32 Cybercrime Convention, Art. 26ff., 30f. Richtlinie 2014/41/EU). Auch in deutschen (vgl. BVerfG 2018) und internationalen Strafverfahren (vgl. Jansen 2018) wurde das Problem der Souveränitätsverletzung bei grenzüberschreitenden Datenerhebungen thematisiert, und in der strafprozessualen Literatur wird die Problematik bislang ausschließlich unter dem Stichwort der Souveränitätsverletzungen diskutiert (statt vieler: Brodowski 2021; Hauschild 2014; Bruns 2019). Dass diese Grundannahme sowohl technisch-faktisch als auch normativ-juristisch nicht widerspruchsfrei durchhaltbar ist, soll später noch ausführlich gezeigt werden (s. Abschnitt 3.1). Durch die Fokussierung auf die Souveränität der Nationalstaaten über Datenbestände »auf« ihrem Hoheitsgebiet wird jedenfalls auch die Debatte um die Legitimierung von strafprozessualen Zugriffen auf diese Datenbestände über Ländergrenzen hinweg ausschließlich auf Grundlage der möglichen Souveränitätsverletzungen geführt.

2.2 Öffentlich zugängliche Daten: die Cybercrime Convention

Für die Erhebung öffentlich zugänglicher Daten existiert bereits eine Regelung in der sogenannten Cybercrime Convention, welche neben den Mitgliedstaaten des Europarates auch von zahlreichen weiteren Ländern wie z.B. den USA, vielen lateinamerikanischen Ländern, Japan, Kanada und Israel unterzeichnet wurde. Dort ist in Art. 32 lit. a geregelt, dass ein Vertragsstaat ohne Zustimmung oder Genehmigung eines anderen Vertragsstaats »auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen [darf], gleichviel, wo sich die Daten geographisch befinden« (Council of Europe 2001: 19). Ob aus dieser Regelung nun geschlossen werden kann, dass die

Vertragsstaaten im Umkehrschluss davon ausgehen, dass auch ein Zugriff auf öffentlich zugängliche Daten – ohne eine entsprechende Vereinbarung – eine Souveränitätsverletzung darstellt, ist unklar. Möglich wäre auch die umgekehrte Interpretation, dass es sich um eine deklaratorische Regelung handelt und der Zugriff auf öffentlich verfügbare Daten die Datensouveränität nie tangiert (so wohl die derzeit herrschende Meinung, vgl. Bruns 2019 mit weiteren Nachweisen). In der Praxis der deutschen Gerichte hat jedenfalls die Erhebung öffentlich zugänglicher Daten unter Aspekten der Souveränitätsverletzung noch keine Rolle gespielt (soweit ersichtlich). Dagegen dürfte es – angesichts der Verbreitung von Online-Streifen und anderen OSINT-Maßnahmen – naheliegen, dass es sehr häufig zu entsprechenden Erhebungen kommt.

2.3 Zugriff auf Daten bei Telekommunikations- und Telemediendienstanbietern

Für die Erhebung von Daten bei Telekommunikations- und Telemediendienstanbietern existiert auf europäischer Ebene noch keine Regel für den Direktzugriff. Bisher wird hier vor allem auf die Europäische Ermittlungsanordnung zurückgegriffen, welche grundsätzlich von allen Mitgliedstaaten anzuerkennen und zu vollstrecken ist (vgl. Art. 1 Abs. 2, Art. 9ff. Richtlinie 2014/41/EU). Auch die Telekommunikationsüberwachung im europäischen Ausland ist so möglich (s. Art. 30f. Richtlinie 2014/41/EU). Gerade für volatile Daten von Telekommunikations- und Telemediendienstanbietern erlangt auch die Möglichkeit des Erlasses von Eilmaßnahmen nach Art. 32 der Richtlinie große Bedeutung. Hier muss die zur Vollstreckung berufene Behörde des ausländischen Staates innerhalb von 24 Stunden über entsprechende Maßnahmen entscheiden (s. Art. 32 Abs. 2 Richtlinie 2014/41/EU).

Da ein grenzüberschreitender Direktzugriff der Strafverfolgungsbehörden dabei auf die Kooperation der Anbieter angewiesen ist und diese von ausländischen Strafverfolgungsbehörden nicht unmittelbar (nur mittelbar über das Rechtshilfeverfahren) zur Mithilfe verpflichtet werden können, findet die Debatte in diesem Bereich weniger anhand tatsächlicher Fälle in Rechtsprechung und Literatur, sondern vor allem auf rechtspolitischer Ebene statt.

Der Fall »Microsoft Ireland«

Insbesondere in der internationalen Debatte prominent ist der Fall »Microsoft Ireland«. In diesem Fall verlangte das FBI von Microsoft die Herausgabe von E-Mail-Daten. Microsoft verweigerte die Herausgabe mit der Begründung, die fraglichen E-Mails wären auf Datenträgern in Irland und damit außerhalb des US-Hoheitsgebietes gespeichert. Der Beschluss zur Herausgabe könne nicht auf diese im Ausland gespeicherten E-Mails erstreckt werden. Außerdem würde eine Herausgabe die in Irland geltenden Datenschutzgesetze verletzen (vgl. Jansen 2018).

CLOUD-Act, E-Evidence-VO und zweites Zusatzprotokoll zur Cybercrime Convention

Nicht zuletzt der beschriebene Fall »Microsoft Ireland« führte dazu, dass in den USA mittlerweile der sogenannte CLOUD-Act erlassen wurde. Dieser gewährt US-amerikanischen Strafverfolgungsbehörden ausdrücklich Zugriff auf die Daten von in den USA ansässigen Unternehmen auch dann, wenn diese Daten auf Datenträgern im Ausland gespeichert sind (vgl. Rath/Spies 2018). In der Europäischen Union wird seit längerer Zeit über die sogenannte E-Evidence-VO verhandelt, die europäischen Strafverfolgungsbehörden Direktzugriff auf die Daten von Telekommunikations- und Telemediendienstanbietern verschaffen soll, auch wenn die Daten im (aus Sicht der jeweiligen Strafverfolgungsbehörde) europäischen Ausland gespeichert sind (vgl. Hamel 2020). Im Zuge dessen wird auch mit den USA über ein ergänzendes völkerrechtliches Abkommen verhandelt, das den US-amerikanischen und europäischen Strafverfolgungsbehörden wechselseitigen Direktzugriff ermöglichen soll (vgl. Moechel 2021). Schließlich soll auch die bereits oben genannte Cybercrime Convention um ein zweites Zusatzprotokoll ergänzt werden. Dieses Protokoll, das Ende 2021 vom Komitee der Minister*innen der beteiligten Staaten verabschiedet und im Mai 2022 unterschriftsreif wurde, enthält u.a. Regelungen zum Direktzugriff auf Daten von sogenannten Domain Name Services (v.a. IP-Adressen von Webseiten und weitere Informationen über Webseitenbetreiber) und auf Bestandsdaten von Telekommunikations- und Telemediendiensten (s. Art. 6 und 7 des zweiten Zusatzprotokolls). Die Verhandlungen über derartige Regulierungen und Abkommen zeigen einmal mehr, dass die einzelnen Nationalstaaten die Souveränität über auf ihrem Hoheitsgebiet gespeicherte Daten prinzipiell einfordern und diese zum Gegenstand von Verhandlungen mit anderen Staaten machen. In der Debatte über beide Regelungen (CLOUD-Act und E-Evidence-VO) sowie das flankie-

rende völkerrechtliche Abkommen zwischen den EU-Mitgliedstaaten und den USA wird von der Literatur indes zu Recht kritisiert, dass der Schutz der personenbezogenen Daten der betroffenen Bürger*innen und damit der Schutz der digitalen Grund- und Menschenrechte zu wenig thematisiert und problematisiert werde (vgl. von Galen 2020).

2.4 Zugriff auf private informationstechnische Systeme

Für transnationale Zugriffe auf private informationstechnische Systeme – vor allem im Wege der elektronischen Durchsicht nach § 110 Abs. 3 StPO – existiert nur eine sehr begrenzte Regelung in der Cybercrime Convention. Nach Art. 32 lit. b der Konvention ist für den Zugriff auf solche Daten die freiwillige und rechtmäßige Einwilligung derjenigen Person erforderlich, die berechtigt ist, die Daten abzurufen und weiterzugeben. Diese Regelung ist damit auf Fälle beschränkt, in denen der*die Berechtigte die Daten freiwillig an die Ermittlungsbehörden herausgibt. Im Umkehrschluss ergibt sich, dass – zumindest von den Unterzeichnerstaaten der Konvention – der Zugriff ohne diese Zustimmung des*der Berechtigten auf Daten im Ausland, sowohl per elektronischer Durchsicht als auch per Online-Durchsuchung, einen Eingriff in die Souveränität des ausländischen Staates darstellt.

Strafprozessuale Zulässigkeit des Zugriffs auf Daten, die (möglicherweise) im Ausland liegen

Über die strafprozessuale Zulässigkeit für transnationale Zugriffe auf Daten in privaten informationstechnischen Systemen herrscht daher Streit, welcher sich bislang vor allem um die Souveränitätsverletzung und ihre Folgen dreht. Klar ist zunächst, dass weder § 110 Abs. 3 StPO noch § 100b StPO den Zugriff auch auf im Ausland lagernde Datenbestände explizit erlaubt. Dies wäre auch gar nicht möglich bzw. eine entsprechende Erlaubnis – unter Annahme einer fremden Datensouveränität – im Verhältnis zum betroffenen ausländischen Staat nach allgemeinen Regeln des Völkerrechts unwirksam (vgl. Brodowski 2021).

Gestritten wird jedoch darüber, ob ein etwaiger Souveränitätsverstoß überhaupt – und wenn ja, unter welchen Umständen – Einfluss auf die Rechtmäßigkeit einer Maßnahme nach Maßstäben der deutschen Strafprozessordnung hat. Teilweise wird hier vertreten, dass die Maßnahme rechtmäßig ist, solange die Ermittlungshandlung im Inland stattfindet (vgl. Wicker 2013a). Die Gegenauffassung geht jedoch davon aus, dass in jedem

Zugriff auf ausländische Daten – unabhängig davon, ob der Zugriff bewusst (also in Kenntnis der ausländischen Belegenheit der zu erhebenden Daten) oder unbewusst erfolge – eine Souveränitätsverletzung liege, die zur Rechtswidrigkeit der Maßnahme auch nach deutschem Strafprozessrecht führe (vgl. Brodowski 2021). Schließlich wird teilweise danach differenziert, ob die Strafverfolgungsbehörden positiv wissen (vgl. Köhler 2021), dass sich die Daten im Ausland befinden (dann rechtswidrig) oder nicht (dann rechtmäßig).

Rechtsfolge: Beweisverwertungsverbot nur bei Rüge des betroffenen Staates

Die Frage, ob aus einer rechtswidrigen Beweisgewinnung wegen Verletzung der Souveränität eines ausländischen Staates ein Beweisverwertungsverbot entspringt, richtet sich nach deutschem Strafprozessrecht und somit in der Praxis nach der Abwägungslehre der Rechtsprechung (vgl. Hauschild 2014). Hiernach ist ein Beweisverwertungsverbot bei rechtswidriger Beweisgewinnung die Ausnahme, welche nur vorliegt, wenn eine Abwägung zwischen den (grundrechtlich geschützten) Interessen des*der Beschuldigten und dem staatlichen Strafanspruch ergibt, dass die Interessen des*der Beschuldigten im jeweiligen Einzelfall überwiegen (vgl. BGH 2007). Dies soll nach herrschender Meinung in den Fällen der Souveränitätsverletzung grundsätzlich nur der Fall sein, wenn der ausländische Staat der Verwertung der erlangten Beweismittel widerspricht (vgl. Bär 2011). Auch hier zeigt sich also die »Souveränitätszentrierung« der bisherigen Debatte um transnationale Dateneingriffe, wenn primär auf die Interessen des ausländischen Staates und nicht auf diejenigen des*der betroffenen Grundrechtsträger*in abgestellt wird.

3. Plädoyer für eine Verschiebung der Debatte weg von Souveränitätsüberlegungen hin zu einem Fokus auf Grund- und Menschenrechtsschutz

Nach unserer Auffassung erscheint die Fokussierung der Debatte um strafprozessuale transnationale Dateneingriffe auf Souveränitätsaspekte als verfehlt. Notwendig ist eine Verschiebung des Diskurses hin zu Fragen des Schutzes der digitalen Integrität der von der Datenerhebung betroffenen Menschen durch die Grund- und Menschenrechte. Es sprechen bereits grundlegende Erwägungen gegen eine Anwendung der traditionellen Vorstellungen und Konzepte staatlicher Souveränität auf Daten. Außerdem übersieht eine souveränitätsfokussierte Debatte, dass die eigentlich von der jeweiligen transnatio-

nalen Ermittlungsmaßnahme Betroffenen nicht die Nationalstaaten, sondern die betroffenen Bürger*innen sind. Bei der Erhebung und Verwertung personenbezogener Daten durch ausländische Strafverfolgungsbehörden sind nicht unmittelbar staatliche Interessen bedroht, sondern – sofern es nicht hinreichende Schutzkonzepte hierfür gibt – die grund- und menschenrechtlich geschützten Positionen und Interessen derjenigen, die vom ausländischen Staat ausgeforscht werden. Gerade im Hinblick auf das Konzept der gegenseitigen Anerkennung, wie es z.B. der E-Evidence-VO der EU zugrunde liegt, und die zunehmende Kooperation auch mit Staaten, deren Verständnis von Rechtsstaatlichkeit sich nicht mit demjenigen hierzulande deckt, besteht hier eine ernstzunehmende Bedrohungslage.

3.1 Grundlegende Bedenken gegen die Anwendung des traditionellen juristischen Souveränitätskonzepts auf digitale Daten und deren Speicherung/Übertragung

Bereits die Grundannahme, dass Nationalstaaten überhaupt Souveränität »über« Daten ausüben können, ist gewichtigen Bedenken ausgesetzt (s. hierzu auch den Beitrag von Fritzsche 2022 in diesem Band, dort insbesondere Kap. 3.). So hat die technische Entwicklung dazu geführt, dass es bereits schwierig ist, den »Ort« von Daten zu bestimmen. Zwar kann zu einem bestimmten Zeitpunkt theoretisch (praktisch ist hierfür ein uneingeschränkter physischer Zugriff auf den Datenträger notwendig) der genaue Belegenheitsort der Bits und Bytes bestimmt werden, welche die Daten physisch repräsentieren. Allerdings ist dies nur möglich, wenn die Ermittlungsbehörden zu diesem Zeitpunkt physischen Zugang zum Datenträger haben, auf dem die Bits und Bytes gespeichert sind. Für die hier beschriebenen, praktisch relevanten Konstellationen des grenzüberschreitenden Datenzugriffs ist dies dagegen technisch nur schwierig, in manchen Konstellationen gar nicht möglich (vgl. Bruns 2019). In diesen Konstellationen des »Fernzugriffs« ist zu berücksichtigen, dass viele Dienstleister, insbesondere im Bereich des Cloud-Computings, die Daten ihrer Kundinnen und Kunden nicht mehr zwingend an einem festen Ort speichern. Sowohl partielle Speicherung von Daten eines »Datensatzes« (z.B. eines Cloud-Speichers oder eines E-Mail-Kontos) auf verschiedenen Servern, die in verschiedenen Ländern stehen können, als auch der »Umzug« von Daten in zeitlichen Intervallen und teilweise über Ländergrenzen hinweg sind aus wirtschaftlichen Gründen nicht unüblich. Viele Dienstleister legen nicht offen, wo sie die Daten ihrer Kundinnen und Kunden speichern (vgl. Bruns 2019). Diese Vorgänge machen die exakte »Lokalisierung« von Daten bei

Fernzugriffen derart komplex, dass es in der Praxis kaum möglich erscheint, im entscheidenden Moment des Zugriffs eine Verletzung der Souveränität durch den Zugriff »auf« fremdem Hoheitsgebiet auszuschließen oder positiv festzustellen (vgl. Wicker 2013b).

Diese Überlegungen führen auch zu einem normativen Argument gegen die Anwendung traditioneller Souveränitätskonzepte auf Daten: Der Idee der Souveränität liegt der Gedanke der ausschließlichen Herrschaft oder Entscheidungsgewalt zugrunde (vgl. Bergmann 2014; s. zur Dekonstruktion des Konzepts der »absoluten« Souveränität die Einleitung dieses Bandes von Glasze/Odzuck/Staples 2022, dort insbesondere Kap. 3.). Der eigentliche Wert von Daten liegt nicht in den Bits und Bytes, denen ein physischer Standort (theoretisch, s.o.) zugewiesen werden kann, sondern in den Informationen, welche die Daten enthalten. In zunehmendem Maße und gerade bei Cloud-Lösungen existieren jedoch von Datensätzen mehrere Kopien (sog. Back-ups) an verschiedenen Speicherorten (nicht nur bei dem*der Nutzer*in selbst, also auf dessen*deren lokalen Speichergeräten, sondern auch bei den Cloud-Dienstleistern, um Datenverlust vorzubeugen). Damit lässt sich jedoch der exakte Ort der wertentscheidenden Information eigentlich gar nicht bestimmen, was das Konzept der Souveränität über Daten (eigentlich über die Information in den Daten) grundsätzlich infrage stellt. Dem zugrunde liegt das Problem, dass Souveränität bislang nur anhand von dinglichen Bezugsgegenständen gedacht wurde (s. hierzu auch mit historischen Bezügen Fritzsche 2022): Staatsvolk und Staatsgebiet (inklusive aller dinglichen Gegenstände, die sich auf dem Staatsgebiet befinden bzw. im Falle von Menschen aufhalten). Die Information bzw. das Wissen, um das es bei Souveränität über Daten eigentlich geht (s.o.), ist jedoch gerade nicht dinglich. Denkbar wäre es allenfalls, das Souveränitätskonzept an Rechten bezüglich der Information/des Wissens anzuknüpfen, wie wir das von Immaterialgüterrechten u.Ä. kennen (s. hierzu noch Teil II). Dabei geht es dann aber um die Frage, welche natürliche oder juristische Person das Recht hat, die Information (ausschließlich) zu kennen/zu nutzen und über ihre Verbreitung zu entscheiden. Dieses Recht steht jedoch in unserer Eigentums- und Rechtsordnung (s. dazu ebenfalls noch Teil II) – mit Ausnahme von Staatsgeheimnissen (vgl. Safferling/Rückert 2020) – gerade nicht dem Staat, sondern den einzelnen Grundrechtsträger*innen zu. Damit ist beim Schutz dieser Rechte nicht die »digitale Souveränität« des Staates, sondern die digitale Integrität des Individuums betroffen. Und deren Schutz ist Sache der Grund- und Menschenrechte.

3.2 Garantie der digitalen Integrität durch Grund- und Menschenrechte (Überblick)

Die digitale Integrität der Bürger*innen wird mittlerweile sowohl auf deutscher als auch auf europäischer Ebene durch Grund- und Menschenrechte geschützt. Die Grund- und Menschenrechte der Europäischen Menschenrechtskonvention (EMRK) und der Grundrechtecharta der EU (GRC) setzen dabei im Bereich strafprozessualer Dateneingriffe den Mindeststandard, konkrete Vorgaben für Schaffung und Anwendung der Dateneingriffsbefugnisse der Strafprozessordnung machen dagegen die »digitalen« Grundrechte des Grundgesetzes.

Das Schutzkonzept des Grundgesetzes

Im deutschen Grundgesetz ruht der umfassende Schutz der digitalen Integrität der Bürger*innen vornehmlich auf drei Säulen. Die Integrität der Telekommunikationsinfrastruktur und die Vertraulichkeit der Kommunikationsinhalte und -umstände werden umfassend durch das Telekommunikationsgeheimnis in Art. 10 Abs. 1 Var. 3 GG geschützt (vgl. BVerfG 2008 [120]). Der Schutzbereich ist dabei am Akt der Telekommunikation orientiert und schützt inhaltsunabhängig jede Form der elektronischen und digitalen Fernkommunikation (z.B. klassische Sprachtelefonie, E-Mails, Messengerdienste, Voice-over-IP-Telefonie etc.), es handelt sich mithin um einen Schutz der Systeme der Fernkommunikation (vgl. ebd.). Ebenfalls systemorientiert ist der Schutz der informationstechnischen Systeme selbst ausgestaltet: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht 2008 aus dem Allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hergeleitet hat, schützt sowohl die von Bürger*innen genutzten Systeme – inklusive vernetzter Systeme wie Cloud-Speicher (vgl. BVerfG 2016 [141]) – vor dem Zugriff des Staates (systembezogener Integritätsschutz) als auch die auf solchen Systemen verarbeiteten Daten vor einer Erhebung und Kenntnisnahme (systembezogener Vertraulichkeitsschutz; vgl. BVerfG 2008 [120]). Schließlich gewährt das Recht auf informationelle Selbstbestimmung – ebenfalls aus dem Allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hergeleitet (vgl. BVerfG 1983 [65]) einen – systemunabhängigen – inhaltsorientierten Schutz aller personenbezogenen Daten (datenbezogener Vertraulichkeitsschutz).

Das Schutzkonzept von EMRK und GRC

Auf europäischer Ebene wird der grund- und menschenrechtliche Datenschutz von EMRK und GRC abweichend von der Konzeption des Grundgesetzes ausgestaltet. In der EMRK findet sich mit Art. 8 lediglich eine Vorschrift zum Schutz des Privatlebens. Diese umfasst dabei neben dem Recht auf informationelle Selbstbestimmung auch das Recht auf Vertraulichkeit der individuellen Kommunikation (vgl. EGMR 2015). In der GRC schützt Art. 7 ausdrücklich die Kommunikation, wobei hierbei ebenfalls nur die Individualkommunikation (wie z.B. Sprachtelefonie, E-Mails) und nicht die Massenkommunikation (z.B. Rundfunk) gemeint ist. Ebenfalls von Art. 7 GRC umfasst ist der Schutz des Privatlebens, welcher auch die informationelle Selbstbestimmung umfasst (vgl. EuGH 2014). Hierbei kommt es zu Schutzbereichsüberschneidungen mit dem spezielleren Art. 8 GRC, in dem explizit ein Grundrecht auf Schutz der personenbezogenen Daten geregelt ist. Erfasst wird dabei jede Art der Datenverarbeitung – von der Erhebung über die Auswertung bis hin zu der Speicherung und Übermittlung von Daten (vgl. Jarass 2021). Ein spezielles Grund- oder Menschenrecht zum Schutz von informationstechnischen Systemen gibt es dagegen auf europäischer Ebene bislang nicht.

Verhältnis von Grundgesetz zu EMRK und GRC im Bereich strafprozessualer Dateneingriffe

Das Verhältnis zwischen dem digitalen Grundrechtsschutz auf nationaler Ebene und dem digitalen Grund- und Menschenrechtsschutz auf europäischer Ebene lässt sich für den Bereich strafprozessualer Dateneingriffe vereinfacht wie folgt beschreiben: Während EMRK und GRC verbindliche Mindeststandards vorgeben, ist primärer Prüfungsmaßstab für deutsche Eingriffsbefugnisse weiterhin das Grundgesetz. Der Grund hierfür liegt in der aktuellen Rechtsprechung des Bundesverfassungsgerichts in den Entscheidungen »Recht auf Vergessen I + II« und »Europäischer Haftbefehl III«. Ausgangspunkt ist, dass durch die Datenschutzrichtlinie 2016/680/EU nunmehr sämtliche Datenverarbeitungen durch Strafverfolgungsbehörden innerhalb der EU den Mindeststandards der Richtlinie entsprechen müssen. Nach den sehr extensiven Kriterien der Rechtsprechung des Europäischen Gerichtshofs zur Frage, wann es sich um eine »Durchführung von Unionsrecht« i.S.v. Art. 51 Abs. 1 GRC (Voraussetzung zur Anwendung der Grundrechte der Charta) durch die Mitgliedstaaten handelt (vgl. Safferling 2014), ist demnach

nunmehr (wohl) jede Datenverarbeitung durch Strafverfolgungsbehörden eine »Durchführung von Unionsrecht« (vgl. Safferling/Rückert 2021). Da auch die Menschenrechte der EMRK über die »Brücken« des Art. 6 Abs. 3 EUV und Art. 52 Abs. 3 GRC zumindest faktisch als Grundrechte in der EU gelten, ist hier auch die EMRK anwendbar und steht nicht nur – wie sonst bei der Rechtsanwendung in Deutschland – im Rang eines einfachen Bundesgesetzes, sondern ranggleich mit den Grundrechten der GRC und damit über der deutschen Strafprozessordnung (vgl. Rückert 2020a). Allerdings wendet das BVerfG auch bei der Durchführung von Unionsrecht weiterhin primär die Grundrechte des Grundgesetzes an, wenn die europäischen Rechtsvorgaben dem deutschen Gesetzgeber einen echten Umsetzungsspielraum belassen und der deutsche Grundrechtsschutz dem Schutz aus GRC und EMRK mindestens gleichkommt (vgl. BVerfG 2020a, 2020b, 2021). Die allermeisten Vorgaben der Richtlinie 2016/680/EU – und vor allem diejenigen, die für alle Datenverarbeitungsvorgänge gelten – sind nur Mindestvorgaben, häufig lediglich sehr abstrakter Natur (z.B. Datenverarbeitung nach »Treu und Glauben«) und in aller Regel durch den nationalen Gesetzgeber ausfüllungsbedürftig. Dementsprechend kommt GRC und EMRK in diesem Bereich »nur« die Funktion zu, verbindliche Mindestvorgaben für den Schutz vor strafprozessualen Dateneingriffen zu machen (vgl. Safferling/Rückert 2021; Rückert 2020a).

3.3 Bedrohung der Garantie des Schutzes durch Grund- und Menschenrechte durch strafprozessuale transnationale Dateneingriffe

Aus einer grund- und menschenrechtlichen Perspektive macht es für die Betroffenen wenig Unterschied, ob die Dateneingriffe von demjenigen Nationalstaat, in dem sie leben, oder einem fremden Nationalstaat ausgehen. Ein Unterschied ergibt sich zwar grundsätzlich hinsichtlich der konkreten (nachteiligen) Rechtsfolgen für die Betroffenen: Die Gefahr eines strafrechtlichen Ermittlungsverfahrens und die Verhängung von Freiheits- oder Geldstrafen als typische Folgen strafprozessualer Ermittlungen stellen sich zwar auf den ersten Blick nur bei Dateneingriffen des Heimatstaates. Nicht aus dem Blick geraten darf aber, dass vor dem Hintergrund von Auslieferungsersuchen (s. §§ 3 Abs. 1, 78ff. IRG für die EU), internationalen Haftbefehlen (s. §§ 17ff., 21ff. IRG) oder der Zugriffsmöglichkeit bei Ein- oder Durchreise in den zugreifenden Staat heute auch die Strafverfolgung im ausländischen Staat ein reales Risiko darstellt (vgl. Safferling 2021). Überdies findet nicht selten eine Durchmischung strafverfolgender und geheimdienstlicher Interessen und Tätigkeiten

bei der Ausforschung im Ausland lebender Staatsbürger*innen statt. Eine besondere Bedeutung kommt hier der Ausforschung von Exilant*innen, Dissident*innen und Asylsuchenden zu (vgl. Safferling/Rückert 2020).

Für innerstaatliche strafprozessuale Dateneingriffe enthalten die Eingriffsbefugnisse der deutschen Strafprozessordnung dabei zahlreiche Eingriffsschwellen und Schutzmechanismen – wie z.B. Straftatenkataloge, Anforderungen an den Grad des Tatverdachts, Subsidiaritätsklauseln, Beschränkungen hinsichtlich des Adressat*innenkreises, Richter*innenvorbehalte, Benachrichtigungs- und Mitteilungspflichten –, welche das Bundesverfassungsgericht aus den einschlägigen Grundrechten des Grundgesetzes herleitet (vgl. Bode 2012; Schwabenbauer 2013; Hauck 2014; Tanneberger 2014, jeweils mit weiteren Nachweisen aus der Rechtsprechung des Bundesverfassungsgerichts). Für Zugriffe deutscher Strafverfolgungsbehörden auf Daten im Ausland ist außerdem vor Kurzem vom Bundesverfassungsgericht klargestellt worden, dass die deutsche Staatsgewalt und damit ebenso die deutschen Strafverfolgungsbehörden auch bei Handeln im Ausland an die Grundrechte des deutschen Grundgesetzes gebunden sind (vgl. BVerfG 2020c; Schmahl 2020). Umgekehrt ergeben sich aus den »digitalen« Grundrechten auch Schutzpflichten für den Staat zugunsten der Grundrechtsträger*innen (auch zugunsten von Asylsuchenden, Exilant*innen, Dissident*innen usw., vgl. Safferling/Rückert 2020) gegen Eingriffe von fremden Staaten in deren Grundrechte (vgl. Durner 2021). Dieser Schutz der digitalen Integrität erlangt gerade dann besondere Bedeutung, wenn es sich bei den zugreifenden ausländischen Staaten um solche handelt, deren Rechtsstaatlichkeitsniveau rechtlich oder faktisch nicht mit demjenigen Deutschlands zu vergleichen ist.

4. Conclusio: Verschiebung der Debatte weg von Souveränitätsüberlegungen hin zur Garantie von Grund- und Menschenrechten auch bei transnationalen Dateneingriffen

Wir haben gezeigt, dass grundlegende Bedenken gegen eine Übertragung des traditionellen Konzepts der staatlichen Souveränität – wie sie vom derzeitigen juristischen Diskurs weitgehend ohne Problembewusstsein vorgenommen wird – auf Datenbestände »auf« dem Hoheitsgebiet eines Staates sprechen. Gleichzeitig sind die digitalen Grund- und Menschenrechte der von Dateneingriffen betroffenen Grundrechtsträger*innen bei transnationalen Dateneingriffen in ähnlichem Maße bedroht wie bei innerstaatlichen strafprozessualen Ermittlungen. Nicht zuletzt aufgrund der extraterritorialen

Geltung der deutschen Grundrechte und der aus den Grund- und Menschenrechten erwachsenden Schutzpflichten des Staates gegenüber seinen Bürger*innen, aber auch Asylsuchenden, Exilant*innen und Dissident*innen aus anderen Staaten, ist daher eine Neufokussierung des Diskurses weg von einer klassischen Souveränitätsdebatte hin zu einem Diskurs über die notwendigen Mechanismen und Regelungen nötig, um den Schutz der digitalen Grund- und Menschenrechte auch bei transnationalen strafprozessualen Dateneingriffen zu garantieren.

4.1 Rechtspolitische Erwägungen zur E-Evidence-VO und zu den Verhandlungen mit Drittstaaten (CLOUD-Act, Zweites Zusatzprotokoll zur Cybercrime Convention)

Für die rechtspolitische Debatte um Regelungen für den Direktzugriff von nationalen Strafverfolgungsbehörden auf Datenbestände von Telekommunikations- und Telemedienprovidern – wie beispielsweise die E-Evidence-VO der EU, dem zweiten Zusatzprotokoll zur Cybercrime Convention oder die Verhandlungen über ein die VO ergänzendes völkerrechtliches Abkommen mit den USA – bedeutet dies folgendes:

Derartige Regelungen und Übereinkommen sollten ausschließlich mit solchen Staaten getroffen werden, die ein vergleichbares grund- und menschenrechtliches sowie rechtsstaatliches Niveau aufweisen, wie dies in Deutschland der Fall ist. Dabei ist nicht nur die Lage »auf dem Papier« zu betrachten, sondern welche Rolle die Grund- und Menschenrechte in der Praxis der Strafverfolgung im jeweiligen Land spielen. So sind beispielsweise durchaus Zweifel angebracht, ob Polen oder Ungarn derzeit tatsächlich ein vergleichbares Schutzniveau aufweisen (vgl. Oberlandesgericht Karlsruhe 2020; Diel-Gligor 2021). Außerdem müssen die aus den Grundrechten fließenden Eingriffsschwellen und Schutzmechanismen auch bei transnationalen Dateneingriffen Geltung beanspruchen. Zur Gewährleistung der Einhaltung dieser Mechanismen ist weiterhin die Gewährleistung von effektiven Rechtsschutzmöglichkeiten notwendig. Bei heimlichen Maßnahmen muss daher auch eine nachträgliche Benachrichtigung – wie z.B. in § 101 StPO – der Betroffenen gewährleistet sein, damit diese Rechtsschutz in Anspruch nehmen können. Zur Gewährleistung der Beachtung rechtsstaatlicher Grundsätze und zur Wahrung der Grund- und Menschenrechte des*der Betroffenen ist schließlich eine Informationspflicht zugunsten der nationalen Datenschutzbehörden zu erwägen.

4.2 Maßstab für die Rechtmäßigkeit von strafprozessualen transnationalen Dateneingriffen (inklusive Beweisverwertungsverbote)

Bei der Frage des Durchschlagens einer etwaigen Völkerrechtswidrigkeit auf die Rechtmäßigkeit nach deutschem Strafverfahrensrecht sollte intensiv diskutiert werden, ob bei einem transnationalen Dateneingriff überhaupt eine Souveränitätsverletzung vorliegt (s. Argumente oben) und – falls ja – ob diese einen Einfluss auf die Rechtmäßigkeit nach deutschem Strafverfahrensrecht hat. Es ließe sich hier auch gut vertreten, dass aufgrund der Unterschiedlichkeit der beteiligten Subjekte und Verhältnisse im Völkerrecht (Staat – Staat) und im Strafverfahrensrecht (Staat – Bürger*in) ein Durchschlagen zu verneinen ist. Für die Rechtmäßigkeit bei transnationalen Datenzugriffen im Verhältnis ausländischer Staat – Bürger*in muss vielmehr entscheidend sein, dass die Grund- und Menschenrechte der betroffenen Bürger*innen gewährleistet sind. Im Falle Deutschlands bedeutet dies, dass die Vorgaben, Eingriffsschwellen und Schutzmechanismen aus den oben beschriebenen digitalen Grundrechten des Grundgesetzes und den Grund- und Menschenrechten der EMRK und der GRC beachtet werden.

Teil II: »Digitale Souveränität« und Privatrecht

1. Digitalgesellschaft als Herausforderung für die Privatrechtsgesellschaft

1.1 Privatrechtsgesellschaft

Das Privatrecht beschäftigt sich mit den rechtlichen Beziehungen der Privatrechtssubjekte untereinander. Anders als im öffentlichen Recht geht es – wie in der Einleitung schon aufgezeigt – nicht um das Verhältnis des Staates zu seinen Bürger*innen oder gar um das Verhältnis souveräner Staaten untereinander, sondern um die Rechtsverhältnisse zwischen den einzelnen gleichgeordneten Mitgliedern der Gemeinschaft (vgl. Brox/Walker 2020: § 1 Rn. 10). Das Privatrecht basiert auf den Ideen individueller Freiheit und Selbstbestimmung (vgl. näher Grigoleit 2008; Riesenhuber 2009: 4ff.). Freie, rechtlich gleiche Bürger*innen gestalten in der Privatrechtsgesellschaft (vgl. Böhm 1966: 75) ihre Beziehungen untereinander nach Maßgabe ihrer individuellen Vorstellungen ohne staatliche Bevormundung eigenverantwortlich aus. Interessengegensätze

werden durch Verhandlungen ausgeglichen. Das Privatrecht vertraut darauf, dass der*die Einzelne selbst am besten weiß, wie er*sie seine*ihre Verhältnisse zu Dritten regeln möchte. Dezentralen Lösungen wird der Vorzug vor zentraler Steuerung eingeräumt. Zugleich liegt dem Privatrecht die Einsicht zugrunde, dass Individuen in der Lage sind, die Konsequenzen ihres Handelns selbst einzuschätzen. Selbst in ihrer Rolle als Verbraucher*innen werden Private als verantwortlich handelnde Personen verstanden. Es besteht das Leitbild eines*einer durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbraucher*in (vgl. Bornkamm/Feddersen 2021: § 5 Rn. 1.76; s. auch Erwägungsgrund 18 RL 2005/29/EG [UGP-RL]).

Rechtlich wird dies über die Privatautonomie abgesichert (zur Privatautonomie vgl. Flume 1975: § 1; Petersen 2011; Brehm 2008: § 5 Rn. 82ff.). Der*die Einzelne kann im Grundsatz seine*ihre Rechtsbeziehungen zu anderen durch Rechtsgeschäft (Verträge) frei gestalten (vgl. Köhler 2017: § 5 Rn. 1). Es gilt die Vertragsfreiheit mit den Kerninhalten Abschlussfreiheit (das Ob eines Vertragsschlusses liegt grundsätzlich in den Händen der Privatrechtssubjekte genauso wie die Wahl des*der Vertragspartner*in), Inhaltsfreiheit (der Inhalt des Rechtsgeschäfts kann im Ausgangspunkt frei ausgehandelt werden) und Formfreiheit (im Grundsatz ist rechtsgeschäftliches Handeln formfrei) (vgl. Brox/Walker 2020: § 2 Rn. 5; Medicus/Lorenz 2015: § 9 Rn. 61ff.). Durch zwei übereinstimmende Willenserklärungen gestalten die Parteien ihre Verhältnisse zueinander frei aus (»Konsensprinzip«; vgl. Brehm 2008: § 1 Rn. 5, § 5 Rn. 84; s. § 311 Abs. 1 BGB). Die Parteien müssen sich an ihren Erklärungen festhalten lassen (*pacta sunt servanda*, s. § 145 BGB). Die Gestaltung der Rechtsverhältnisse durch die*den Einzelne*n nach ihrem*seinem Willen ist ein Teil der allgemeinen Handlungsfreiheit (s. Art. 2 I GG) und damit verfassungsrechtlich abgesichert (vgl. BVerfG 1994; Medicus/Lorenz 2015: § 9 Rn. 66f.).

Private Eigentumsrechte unterstützen dieses System dezentralen Wirtschaftens (»Eigentumsfreiheit«; vgl. Köhler 2017: § 3 Rn. 8; zur Verknüpfung mit dem Souveränitätsbegriff Schuppert 2019: 242f.). Eigentumsrechte an Sachen in Form von Ausschließlichkeitsrechten (s. § 903 BGB als »Prototyp«; zur Struktur von Ausschließlichkeitsrechten Hofmann 2020a: 9 u. 12ff.) gewähren nicht nur einen Raum zur Verwirklichung individueller Freiheit, sondern sorgen dafür, dass über die Güterverteilung dezentral durch Verträge entschieden werden muss. Zugleich bestehen Anreize, in den Erhalt abnutzbarer Güter zu investieren. Eigentumsrechte an immateriellen Gütern (Patentrechte, Urheberrechte etc.) schaffen nicht nur Anreize zur Schöpfung unkörperli-

cher Gegenstände, sondern sie sind auch Grundlage für deren Verwertung, beispielsweise durch die Kulturindustrie. Im Übrigen werden durch die Zuweisung derartiger Ausschließlichkeitsrechte (zudem existieren Rechte zum Schutz der Persönlichkeit) die Freiheitssphären untereinander abgegrenzt. Resultieren Schäden aus Eingriffen in derartige Rechte Dritter, besteht eine Verpflichtung zum Schadensersatz, regelmäßig aber nur unter der Voraussetzung der Verletzung einer Verhaltenspflicht (»Verkehrspflicht«). Per se gefährliche Tätigkeiten sind mitunter im Grundsatz erlaubt, verpflichten aber verschuldensunabhängig zum Schadensersatz im Falle der Verletzung Rechter Dritter (Gefährungshaftung). Anderweitige Ausgestaltungen durch Verträge sind im Grundsatz aber möglich.

Für die Durchsetzung seiner Rechte ist das Privatrechtssubjekt ebenfalls selbst zuständig. Auch wenn der*die Einzelne hierbei auf staatliche Hilfe angewiesen ist, hängt die Rechtsdurchsetzung von seiner*ihrer Initiative ab. Statt kollektiver Rechtsdurchsetzung liegt es grundsätzlich in der Hand des*der Gläubiger*in, seinen*ihren Anspruch selbst zu verwirklichen (vgl. Zech 2012: 66; Brehm 2008: § 20 Rn. 608). Das subjektive Recht ist einer der zentralen Begriffe des Privatrechts (vgl. von Tuhr 1957: § 1 I, S. 53). Subjektive Rechte als dem*der Einzelnen von der Rechtsordnung verliehene Willensmacht zur Durchsetzung seiner*ihrer Interessen (vgl. Raiser 1961) vermitteln individuelle Freiheit (vgl. Brox/Walker 2020: § 28 Rn. 12).

Die Rechtswirklichkeit steht diesen Idealvorstellungen vielfach entgegen. Faktisch treten sich Private regelmäßig nicht als »Gleiche unter Gleichen« gegenüber, sondern es bestehen gravierende Verhandlungsungleichgewichte – beispielsweise durch Informationsasymmetrien oder unterschiedliche Marktmacht (s. etwa zu den unterschiedlichen Machtverhältnissen in der Arbeitswelt den Beitrag von Sauer/Staples/Steinbach 2022 in diesem Band). Vor allem auf faktische Hindernisse für selbstbestimmtes Handeln reagiert das Privatrecht mit einer Vielzahl von Instrumenten (zu den »Grenzen der Privatautonomie« vgl. Paulus/Zenker 2001). Ziel ist es dabei zuallererst, die Voraussetzungen für selbstbestimmtes Handeln zu schaffen (vgl. Grigoleit 2008: 56ff.).

Dies kann beispielsweise dadurch abgesichert werden, dass bestimmte Normen als zwingend ausgestaltet sind (vgl. Köhler 2017: § 3 Rn. 23). Ein Abweichen durch Rechtsgeschäft ist nicht möglich. In diesem Sinne stehen die Mängelgewährleistungsrechte beim Verbrauchsgüterkauf gemäß § 476 BGB nicht zur Disposition der Parteien. Auch im Falle vorformulierter, im Massenverkehr einseitig gestellter allgemeiner Geschäftsbedingungen (AGB), also wiederum dort, wo real kein Verhandlungsgleichgewicht besteht, greift

das Recht ein (vgl. Köhler 2017: § 16 Rn. 1ff.): Überraschende Klauseln werden gemäß § 305c BGB von vornherein nicht Vertragsbestandteil. Die Klauseln müssen zudem einer »Inhaltskontrolle« standhalten. Selbst wenn der Gesetzgeber die Unangemessenheit einer bestimmten Abrede nicht über abstrakte Verbote (s. z.B. § 138 BGB) oder konkrete Kontrollvorschriften (s. §§ 308f. BGB) für nichtig erklärt, kann die Generalklausel aus § 307 Abs. 1 S. 1 BGB, wonach Bestimmungen in allgemeinen Geschäftsbedingungen unwirksam sind, wenn sie den*die Vertragspartner*in des*der Verwender*in entgegen den Geboten von Treu und Glauben unangemessen benachteiligen, Abhilfe schaffen. Formvorschriften, z.B. das Schriftformerfordernis oder gar die notarielle Beurkundung, erweisen sich als Warnungen vor überstürztem Handeln (vgl. Köhler 2017: § 12 Rn. 7). Während Widerrufsrechte den*die Verbraucher*in vor Entscheidungen schützen u.a. wenn diese*r situationsspezifisch zu einem unüberlegten Geschäftsabschluss gedrängt worden ist (s. § 312b BGB; vgl. Wendehorst 2019: § 312b Rn. 2), sollen diverse Informationspflichten (z.B. § 5a UWG; § 312d BGB) insbesondere Informationsasymmetrien ausgleichen und die Voraussetzung für selbstbestimmtes Handeln schaffen (vgl. Wendehorst 2019: § 312d Rn. 1f.; Alexander 2019: § 9 Rn. 572).

Mehr und mehr ist das Privatrecht schließlich für unerwünschte Ungleichbehandlungen (»Diskriminierung«) sensibilisiert. Bei Massengeschäften des täglichen Lebens (s. § 19 AGG), vor allem aber im Arbeitsrecht ist das allgemeine Gleichbehandlungsgesetz (AGG) zu beachten. Des Weiteren werden unfaire Geschäftspraktiken durch das Lauterkeitsrecht (UWG) in Schach gehalten. Das Kartellrecht versucht dafür zu sorgen, dass überhaupt Wettbewerb besteht. Bekämpft werden der Missbrauch einer marktbeherrschenden Stellung (s. Art. 102 AEUV) und wettbewerbsbeschränkende Vereinbarungen (s. Art. 101 AEUV). Eigentumsrechte unterliegen einer Vielzahl von »Schranken«, wodurch der Rechtskreis des*der Eigentümer*in, Urheber*in oder Patentinhaber*in zugunsten von Dritt- und Allgemeininteressen beschränkt wird (exemplarisch zum Urheberrecht vgl. Geiger 2004). Ferner müssen die Grundrechte auch im Privatrecht beachtet werden (»mittelbare Drittwirkung«; vgl. allgemein Brox/Walker 2020: § 2 Rn. 9ff.; zum Gleichheitssatz vgl. BVerfG 2018). In diesem Sinne lässt sich beispielsweise im Urheberrecht eine »Konstitutionalisierung« beobachten, wonach die private Eigentumsordnung ganz maßgeblich aus den europäischen Grundrechten heraus entwickelt wird (vgl. Leistner/Roder 2016). Nicht zuletzt darf die »Steuerungswirkung« des Privatrechts nicht unterschätzt oder gar übersehen werden (vgl. grundlegend Hellgardt 2016). Regulatorische Ziele werden vielfach über

das Privatrecht, beispielsweise mittels des Haftungsrechts über Pflichten zur Schadensvermeidung (indirekt statuiert durch die andernfalls drohende Haftung auf Schadenersatz), verwirklicht (zu »autonomen Systemen« vgl. Wagner 2017). Die regulatorische Überformung des Privatrechts (nicht nur im Verbraucherschutzrecht, sondern auch im Wirtschaftsrecht) wird auch als »Veröffentlichrechtlichung« bezeichnet.

1.2 Digitalgesellschaft

Die Digitalisierung fordert dieses Privatrechtsverständnis in vielfacher Hinsicht heraus. Auch wenn nicht oft genug betont werden kann, dass sich die Grundideen des Privatrechts seit jeher in einem Spannungsverhältnis zur Rechtswirklichkeit bewegen, lassen sich die mit der Digitalisierung einhergehenden Veränderungen nicht als bloße weitere graduelle Verschiebung abtun. Es sind hier gravierende Entwicklungen zu beobachten. Vier übergreifende Gefährdungen seien dabei besonders hervorgehoben.

Erstens wird die Prämisse des Privatrechts, wonach die Bürger*innen ihre Verhältnisse selbstbestimmt und eigenverantwortlich mit Dritten aushandeln, fundamental erschüttert. Die marktmächtigen Akteure der Digitalwirtschaft setzen die Bedingungen der Digitalgesellschaft, sodass für »Verhandlungen« regelmäßig kein Raum bleibt. Die Vertragsfreiheit besteht allem Anschein nach häufig nur noch auf dem Papier. Die Rechtsordnung einschließlich der Möglichkeiten der Rechtsdurchsetzung (»Meldeprotokolle« einschlägiger Internetdienste) erscheint mehr und mehr privatisiert. Die entpersonalisierten Strukturen der Plattformökonomie erschweren es dem*der Verbraucher*in vielfach, im Falle von Streitigkeiten (individuell) Abhilfe zu bekommen (vgl. Hofmann 2020c). All dies ist zwar nicht grundsätzlich neu, wird aber wie gesagt über die digitalen Möglichkeiten, allen voran die dadurch bedingte Plattformökonomie (zur Plattformökonomie aus Sicht des Privatrechts vgl. etwa Grünberger 2017; Tonner 2017; Busch 2019; Schweitzer 2019a; Busch/Dannemann/Schulte-Nölke 2020) mit wenigen marktmächtigen internationalen Internetkonzernen wie Amazon oder Google, erheblich verstärkt.

In der Plattformökonomie wirken sich zudem Rechtsbeziehungen Dritter verstärkt auf das traditionelle Zweipersonenverhältnis zwischen Gläubiger*in und Schuldner*in aus. Ein Anbieter von Musik wird im Verhältnis zu dem*der Endnutzer*in die Klauseln, die er mit den Inhaber*innen der Rechte an der Musik akzeptieren musste, an die Nutzer*innen weitergeben. Kurzum, statt Zweipersonenverhältnissen spielen »Netzwerke« eine zentrale Rolle (vgl. Grünberger 2018: 290ff.). Oder mit Grünberger: Der »Individualvertrags-

Fixierung« der klassischen Rechtsdogmatik werde es nicht gelingen, die Verbraucher*innenerwartungen in Netzwerken abzubilden (ebd.: 291). Dazu ein Beispiel: Über die Portabilitätsverordnung hat der europäische Gesetzgeber in diesem Sinne ein Konzept zur grenzüberschreitenden Portabilität von Online-Inhaltediensten eingeführt (zur Datenportabilität nach Art. 20 DSGVO vgl. Kühling/Martini 2016: 450), indem sichergestellt wird, dass die Abonnent*innen von portablen Online-Inhaltediensten, die in ihrem Wohnsitzmitgliedstaat rechtmäßig bereitgestellt werden, während eines vorübergehenden Aufenthalts in einem anderen Mitgliedstaat als ihrem Wohnsitzmitgliedstaat auf diese Dienste zugreifen und sie nutzen können (s. Art. 1 Portabilitäts-VO). Der Regulierungsbedarf folgte vor allem aus dem urheberrechtlichen Territorialitätsprinzip, das in den jeweiligen Vertragsbeziehungen wie angedeutet abgebildet wurde.

Zweitens wird wesentliche Infrastruktur (z.B. Suchmaschinen) ebenfalls von privater Seite zur Verfügung gestellt. Private Akteure gleichen nicht nur vermehrt staatlichen Akteuren, sondern übernehmen auch verstärkt deren Aufgaben. Dies gilt nicht zuletzt für die Durchsetzung subjektiver Rechte im Internet (»Privatisierung der Rechtsdurchsetzung«, vgl. Hofmann 2019: 1223). Der*die Einzelne muss auch tatsächlich die Möglichkeit haben, seine*ihre Individualrechte gegenüber marktmächtigen Privaten zu verwirklichen. Praktisch konnte dies schon daran scheitern, dass die Plattform nicht »greifbar« war. Um eine sichere Zustellung zu gewährleisten, sah sich der Gesetzgeber daher veranlasst, gemäß § 5 Netzwerkdurchsetzungsgesetz (NetzDG) einen »Zustellungsbevollmächtigten« zu verlangen (s. BR-Drs. 315/17: 25). Gefahr droht aber auch von einer überschießenden Durchsetzung: Während allen voran bei Persönlichkeitsrechtsverletzungen *(»hate speech«)* im virtuellen Raum gravierende Rechtsdurchsetzungsdefizite zu beklagen sind, könnte mit Blick auf bestimmte Wirtschaftsrechte das Gegenteil zu befürchten sein. Über technische Möglichkeiten (»Upload-Filter«; zu Filtertechnologien vgl. Raue/Steinebach 2020; zum UrhDaG vgl. Hofmann 2021) wird die Vision von hundertprozentiger Rechtsdurchsetzung plötzlich zur greifbaren Realität. Dass Recht aber auch einmal nicht durchgesetzt wird, ist von der Rechtsordnung eingepreist. Der fein austarierte Interessenausgleich kann so aus den Fugen geraten (vgl. Hofmann 2020d). In jedem Fall muss der Staat um seine Hoheitsansprüche kämpfen. Bestimmt er die Regeln der Plattformökonomie oder werden diese letztlich über die Nutzungsbedingungen der einschlägigen Plattformen von privater Seite unwiderruflich gesetzt (vgl. Schweitzer 2019a: 4ff.)? Der staatliche Regelungsanspruch (»Souveränität«) wird durch das uni-

verselle Internet infrage gestellt (vgl. aber EuGH 2019: Rn. 48). Die Freiheit der Bürger*innen wird weniger durch den Staat als durch marktmächtige Private gefährdet. Deutlich wird dies beispielsweise im Falle der Sperrung von Facebook-Konten oder der Zugangsbedingungen für kleine Händler*innen zur Verkaufsplattform Amazon.

Drittens besteht die Gefahr einer schleichenden Entmündigung. Hier spielen nicht nur Informationsasymmetrien eine Rolle, sondern zunehmende Personalisierung (bspw. zur Preispersonalisierung vgl. Hofmann/Freiling 2020). Der*die gläserne Bürger*in ist Unternehmer*innen mitunter besser bekannt, als diese*r sich selbst kennt. Durch Präferenzmanipulationen kann selbstbestimmtes Handeln weiter untergraben werden (vgl. Wagner/Eidenmüller 2019: 234ff.). Während das Bild des*der rational handelnden Verbraucher*in auch in der analogen Welt durch die Verhaltensökonomik schon erschüttert wurde (Überblick vgl. bei Englerth/Towfigh 2010: § 7), haben die digitalen Möglichkeiten die Gefahr der »Ausnutzung von Verhaltensanomalien« freilich nochmals auf eine neue Stufe gehoben (Wagner/Eidenmüller 2019: 230ff.). Die »Filterblase« lässt grüßen.

Viertens wird auch die Eigentumsordnung herausgefordert. Physische Gegenstände verlieren gegenüber unkörperlichen Gegenständen an Bedeutung. »Smarte« Produkte schöpfen ihren Wert weniger aus der Hard- als aus der Software. Über die Möglichkeiten digitaler Vernetzung kann der Hersteller aber auch über die gesamte Lebenszeit des Produkts dasselbe kontrollieren. Über diese Fernkontrolle können Gebrauchsbeschränkungen, z.B. zur Absicherung nachgelagerter Produktmärkte (etwa für Kaffeekapseln), technisch abgesichert werden. Aber auch das Softwareurheberrecht muss sicherstellen, dass Lock-in-Effekte nicht verstärkt werden. So könnten hier weitergehende Möglichkeiten zum *reverse engineering* erforderlich sein (s. derzeit nur § 69e UrhG; vgl. Wiebe 1992).

Ferner stehen vor allem immaterielle Güter, namentlich Daten, im Fokus der Zuweisung: Wem »gehören« die Daten? Mit Blick auf Daten, dem zentralen Rohstoff der Digitalgesellschaft (das Bild passt im Grunde genommen nicht, da mit Rohstoffen vor allem physische und damit verbrauchbare, also rivale Güter gemeint sind), wird nicht nur diskutiert, wem diese zuzuweisen sind (vgl. Zech 2015a, 2015b), sondern vor allem, wie Zugang zu Daten sichergestellt werden kann (vgl. Louven 2018; Schweitzer 2019b). Schließlich drohen überkommene Ausschließlichkeitsrechte zweckentfremdet zu werden. Allen voran das Urheberrecht findet sich plötzlich in der Rolle, maßgeblich Fragen der digitalen Infrastruktur (z.B. Verbreitung von öffentlichen WLAN wegen ur-

heberrechtlicher Haftungsregelungen) zu determinieren (vgl. Hofmann 2017). Dies ist nur ein weiteres Beispiel, wie vor allem das Urheberrecht die sozialen Bedürfnisse der Digitalgesellschaft konterkarieren kann (vgl. Grünberger 2018: 261ff.).

Diese Liste ist nicht abschließend (zu denken ist beispielsweise auch an die vom Kartellrecht zu bewältigende Gefahr, dass Marktmechanismen durch wenige marktbeherrschende Plattformen ausgehebelt werden; zu dieser Herausforderung für das Kartellrecht vgl. insbesondere Podszun 2020), zeigt aber bereits deutlich, dass sich das Privatrecht seiner Rolle in der Digitalgesellschaft vergewissern muss. Oder in den Worten des Titels dieses Bandes: Schafft es das Privatrecht, »digitale Souveränität« im Verhältnis der Bürger*innen untereinander zu gewährleisten? Reaktionen sind unabdingbar.

2. Privatrechtliche Reaktionsmöglichkeiten

Was ist zu tun? Wie erwähnt ist es eine der zentralen Aufgaben des Privatrechts, die Voraussetzungen für selbstbestimmtes Handeln zu gewährleisten. Es bedarf eines Ordnungsrahmens, der freie Entscheidungen ermöglicht. Unter dem Eindruck der fortschreitenden Digitalisierung mit ihren Gefahren für die Privatrechtsgesellschaft findet sich auch in der Privatrechtswissenschaft eine breite Debatte zu möglichen Reaktionsmöglichkeiten (vgl. z.B. Körber 2016; Wagner/Eidenmüller 2019: 220; Paal/Kumkar 2021).

2.1 Transparenz und Opt-out-Regelungen

Diskutiert werden dabei beispielsweise Möglichkeiten des Abbaus von Informationsasymmetrien über Informationspflichten. Spezielle Transparenzvorgaben erscheinen vielen als das Regulierungsinstrument der Stunde (vgl. kritisch Wagner/Eidenmüller 2019: 239ff. sowie mit Blick auf Preisregulierung Hofmann 2016: 1080f.). Hinter dem Schlagwort »Algorithmentransparenz« stehen in diesem Sinne neue Regelungen wie Art. 7 Abs. 4a der Richtlinie über unlautere Geschäftspraktiken (s. RL 2005/29/EG; zur Neuregelung durch die RL 2019 [EU] 2161):

> »Wenn Verbrauchern die Möglichkeit geboten wird, mithilfe eines Stichworts, einer Wortgruppe oder einer anderen Eingabe nach Produkten zu suchen, die von verschiedenen Gewerbetreibenden oder von Verbrauchern angeboten werden, gelten, unabhängig davon, wo Rechtsgeschäfte letztendlich abgeschlossen werden, allgemeine Informationen, die die

> Hauptparameter für die Festlegung des Rankings der dem Verbraucher im Ergebnis der Suche vorgeschlagenen Produkte, sowie die relative Gewichtung dieser Parameter im Vergleich zu anderen Parametern, betreffen und die in einem bestimmten Bereich der Online-Benutzeroberfläche zur Verfügung gestellt werden, der von der Seite, auf der die Suchergebnisse angezeigt werden, unmittelbar und leicht zugänglich ist, als wesentlich.«

Über »wesentliche« Informationen hat der*die Unternehmer*in zu informieren; andernfalls begeht er*sie einen Wettbewerbsverstoß (s. §§ 8, 3, 5a UWG).

Transparenz allein wird jedoch vielfach als unzureichend empfunden. Namentlich Wagner und Eidenmüller sprechen sich daher für eine weitergehende Regulierung aus: Verbraucher*innen sollten vielmehr vermittels von »Opt-out-Rechten« in die Lage versetzt werden, namentlich personalisierte Preise abzulehnen und stattdessen ein »Angebot zum Marktpreis« zu erhalten. Es bedürfe eines Rechts, Preispersonalisierung abzuwählen (vgl. Wagner/Eidenmüller 2019: 228ff.). Um Präferenzmanipulationen vorzubeugen, sollten Verbraucher*innen allgemein eine Wahlmöglichkeit haben, zwischen »einer personalisierten und einer nichtpersonalisierten virtuellen Welt«, »zwischen einer ›Welt der Kontrolle‹, die auf der Basis vergangener Entscheidungen kuratiert wurde, und einer ›Welt der Spontaneität‹, die Präferenzen des Durchschnitts der Nutzer*innen widerspiegelt oder andere Selektionskriterien verwendet« (Wagner/Eidenmüller 2019: 242). Es müssten dafür anonyme Online-Einkaufsmöglichkeiten ohne Persönlichkeitsprofil zur Verfügung stehen (vgl. ebd.: 246). Digitale Anonymität sei zu gewährleisten (vgl. ebd.: 242). Nicht zuletzt sollten Verbraucher*innen das Recht haben, unter Einfluss von Verkaufsalgorithmen getätigte Transaktionen, die in einem Zustand besonderer Verletzlichkeit getätigt wurden, zu widerrufen (vgl. ebd.: 233f.). Größere Bedeutung kann dabei nicht zuletzt dem Trend zu *law by design* kommen. Plattformen könnten in diesem Sinne schon von vornherein zu einer bestimmten verbraucher*innenfreundlichen, verhaltensökonomischen Erkenntnis berücksichtigenden Gestaltung der Benutzeroberflächen verpflichtet werden.

2.2 Datenschutz und Selbstbestimmung

Ein weiterer, zentraler Aspekt der Debatte um »digitale Souveränität« im Privatrecht liegt im Datenschutzrecht (»Datensouveränität der Nutzer*innen«; vgl. Krüger 2016: 191). Das Verhältnis von Datenschutz und Selbstbestimmung soll im Folgenden exemplarisch etwas näher beleuchtet werden.

Um die »digitale Souveränität« zu stärken, wird in der Literatur die »Anerkennung eines Dateneigentums der Bürger an ihren Informationsdaten« vorgeschlagen (Fezer 2017). Ein »Immaterialgüterrecht sui generis an den Informationen« soll »eine zivilgesellschaftliche Gestaltungskompetenz der Bürger« begründen, »an der Architektur der digitalen Räume zur Organisation der Geschäftsmodelle einer kommerziellen Vermarktung der Informationsdaten mitzuwirken« (Fezer 2017). Schon heute erkennt das Datenschutzrecht freilich die »Hoheit« über die eigenen Daten an, wenn auch nicht im Sinne einer »eigentumsartigen« Zuweisung (vgl. BVerfG 1984). Das Datenschutzrecht als Abwehrrecht (Hofmann 2020a: 15ff.) ermöglicht es aber dem*der Einzelnen, sich gegen unbefugte Datenverarbeitungen zu wehren. Ohne gesetzlichen Erlaubnistatbestand zur Datenverarbeitung (s. insbesondere Art. 6 Abs. 1 lit. f DSGVO) bedarf es insbesondere einer »Einwilligung« des*der Betroffenen (s. Art. 6 Abs. 1 lit. a DSGVO). »Einwilligung« bedeutet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (s. Art. 4 Nr. 11 DSGVO). Namentlich auch bei vorformulierten Einwilligungserklärungen kommt es darauf an, dass diese in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden (s. Art. 7 Abs. 2 DSGVO mit Erwägungsgrund 42 DSGVO). Die Erklärung darf nicht in allgemeinen Geschäftsbedingungen »versteckt« werden (vgl. Wendehorst/von Westphalen 2016). Neben der Einwilligung wird vielfach der Erlaubnistatbestand aus Art. 6 Abs. 1 lit. b DSGVO vorliegen, wonach die Datenverarbeitung rechtmäßig ist, soweit sie zur Erfüllung eines Vertrags erforderlich ist. Hier muss das Datenschutzrecht aufpassen, dass ausufernde Leistungsbeschreibungen nicht mehr oder weniger zu einer praktischen Umgehung der restriktiv formulierten Erlaubnistatbestände führen (vgl. ebd.: 3746f.).

Praktisch erweist sich vor allem das Erfordernis der Einwilligung allerdings als schwaches Schwert. Dies liegt nicht nur an der nach wie vor unbefriedigenden Durchsetzung des Datenschutzrechts insgesamt, sondern auch daran, dass Einwilligungen freigiebig erteilt werden. Dies liegt aber weniger an Bürger*innen, die den Anforderungen der Digitalgesellschaft nicht gewachsen sind, sondern an den faktischen Gegebenheiten. Die Vorbedingungen für selbstbestimmtes Handeln (insbesondere: Kenntnis des einschlägigen Sachverhalts, freie Entscheidungsmöglichkeit im Lichte alternativer, gleich-

wertiger Entscheidungsoptionen) sind im digitalen Umfeld häufig nicht gegeben. Die datenschutzrechtliche Einwilligung soll nach verbreiteter Ansicht angesichts von Lock-in-Effekten und komplexen Nutzungsbedingungen »für sich genommen kaum noch ein Garant für die Datensouveränität des Einzelnen« sein (Krüger 2016). Einwilligungserklärungen decken in der Tat praktisch nicht nur eine Vielzahl von Datenverarbeitungssituationen ab, sondern entziehen sich auch dem Einfluss des*der Datenschutzberechtigten (Betroffenem). Auch wenn der europäische Gesetzgeber die »Informiertheit« zur Voraussetzung der Einwilligung erhebt und sich die Einwilligung auf jede einzelne angedachte Verarbeitung zu beziehen hat (»Zweckbindungsgrundsatz«; s. auch Erwägungsgrund 32 und 39 DSGVO; vgl. Veil 2018: 3339f.), lehrt die Rechtspraxis, dass die Steuerungskraft des Rechts hier faktisch massiv beschränkt ist (vgl. Specht 2017a: 1042 u. 1046; Hofmann/Freiling 2020: 335).

Um die*den Einzelne*n zu stärken, wird vorgeschlagen, auf Visualisierung zu setzen (s. auch Art. 12 Abs. 7 DSGVO). Ein »selbstbestimmter, bewussterer Umgang mit personenbezogenen Daten« werde nur dann erfolgen, wenn es endlich gelingen würde, »dem Betroffenen vor Augen zu führen, in welche Datenverarbeitungen er einwilligt und welche Rechte ihm zur Verfügung stehen« (Specht 2017a: 1042). Symbole, die ergänzend zu vertraglichen Klauseln eingesetzt werden sollten, könnten ein geeignetes Mittel darstellen, der fehlenden Kenntnisnahme von Datenschutzerklärungen entgegenzuwirken (vgl. Krüger 2016: 191). Auch Zertifizierungssysteme wären, so Stimmen in der Literatur, ein Schritt zur Stärkung der Betroffenen (vgl. ebd.).

Dessen ungeachtet erweist sich der faktische Zwang zur Einwilligung als Problem. Will der*die Nutzer*in einen bestimmten Dienst nutzen, kommt er*sie häufig nicht umhin, entweder der (überschießenden) Verarbeitung seiner*ihrer Daten zuzustimmen oder das Angebot nicht nutzen zu können. Dem versucht zwar Art. 7 Abs. 4 DSGVO entgegenzuwirken. Demnach ist bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob u.a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Es scheint aber vor allem geboten, dass der*die Nutzer*in ohne Mühe differenzierte Einwilligungen erteilen kann. Ihm*ihr sollte es ohne Weiteres möglich sein, bestimmten Verarbeitungen zuzustimmen, anderen nicht. Statt der Möglichkeit, einen Haken unter die Datenschutzerklärung zu setzen, wäre dem*der Betrof-

fenen gedient, wenn er*sie mit mehreren Haken seine*ihre Zustimmung maßgeschneidert geben könnte (vgl. Krüger 2016: 191).

Noch nicht ausgeschöpft erscheinen auch die Möglichkeiten der Klauselkontrolle (zurückhaltend BGH 2008). Intransparenten (s. 307 Abs. 1 S. 2 BGB; s. auch Art. 7 Abs. 2 DSGVO; vgl. Ernst 2017: 113, 2010: 297158; von Westphalen 2017) oder nicht interessengerechten datenschutzrechtlichen Klauseln (s. § 307 Abs. 1 S. 1 BGB) könnte die Wirksamkeit versagt werden. Es ist kein Grund ersichtlich, warum vorformulierte Einwilligungserklärungen nicht oder nur eingeschränkt kontrollfähige Vertragsbedingungen sein sollten (vgl. so auch Krüger 2016: 191f.; soweit die Datenschutzerklärung informativen Charakter hat, s. z.B. Art. 13, 14 DSGVO, scheidet eine AGB-Kontrolle aus, vgl. Wendehorst/von Westphalen 2016: 3748). Es muss möglich sein, die Klausel auch über die Vorgaben des Datenschutzrechts hinaus zu kontrollieren (vgl. aber BGH 2012: Rn. 16, alleiniger Prüfungsmaßstab sollen die Vorschriften des Datenschutzrechts sein; ggf. können auch Vorschriften des UWG zur Unwirksamkeit einer Klausel führen, vgl. BGH 2008). In diesem Sinne verweist Erwägungsgrund 42 DSGVO unter Hinweis auf die Klauselrichtlinie (Richtlinie 93/13/EWG) darauf, dass Klauseln nicht »missbräuchlich« sein dürften (vgl. auch Wendehorst/von Westphalen 2016: 3749).

Während der*die Verbraucher*in in der Lage sein muss, freiwillige, informierte Entscheidungen zu treffen (Information und Transparenz als »Grundpfeiler der Datensouveränität«; vgl. Krüger 2016: 192), begrenzt das Datenschutzrecht die Souveränität des*der Einzelnen aber auch aus einer anderen Richtung. Es stellt sich die Frage, ob das Datenschutzrecht nicht dem*der Betroffenen das Recht nimmt, eigenverantwortlich über seine*ihre Daten zu verfügen, also beispielsweise, vereinfacht gesagt, mit Daten zu bezahlen. Art. 7 Abs. 4 DSGVO (»Kopplungsverbot«) könnte sich insoweit als Hürde erweisen (vgl. Krohm/Müller-Peltzer 2017; Hacker 2019; Dix 2017). Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss demnach dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob u.a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Mit unterschiedlichen Begründungen wird versucht, dem Geschäftsmodell »Daten gegen Leistung« über eine mehr oder weniger restriktive Auslegung des Art. 7 Abs. 4 DSGVO nicht von vornherein das Wasser abzugraben (vgl. Übersicht bei Kumkar 2020: 328ff.). Es wird darauf hingewiesen, dass es weder mit Art. 8 EU-Grundrechtecharta noch mit dem europäischen Verbrau-

cher*innenleitbild vereinbar wäre, »dem Einzelnen prinzipiell die Fähigkeit abzusprechen, auf Grundlage einer überlegten Entscheidung seine Daten zum Gegenstand eines Austauschverhältnisses zu machen« (Kumkar 2020: 330). Darauf aufbauend wird gefordert, dass über die grundsätzlich freie Widerruflichkeit der Einwilligung (s. Art. 7 Abs. 3 S. 1 DSGVO) disponiert werden können müsse (vgl. Sattler 2017: 1041ff.; zu einem »Datenschuldrecht« vgl. Schmidt-Kessel 2017; vgl. Specht 2017a, 2017b). Einem kategorischen Ausschluss von bindenden Vereinbarungen über personenbezogene Daten wird nach dieser Sichtweise eine Absage erteilt (vgl. Sattler 2017: 1045).

Gemeinsames Schlussfazit: Herausforderungen für die Rechtskonzepte der Souveränität, Integrität und Privatautonomie durch die Digitalisierung

Wir haben gezeigt, dass die klassischen rechtswissenschaftlichen Konzepte der Souveränität, Integrität und Privatautonomie in den Zeiten der Digitalisierung neu herausgefordert werden. Grenzen verschwimmen und eine direkte Übertragung dieser Rechtskonstruktionen aus einer »analogen« Zeit scheitert oftmals an den neuen Gegebenheiten der digitalen Welt. Nicht nur staatliche Souveränität, sondern auch die »individuelle Souveränität« als Basis des Privatrechts wird durch die fortschreitende Digitalisierung herausgefordert. Auf den Punkt gebracht: Privatrechtliche Grundprinzipien werden im Digitalen radikal hinterfragt.

In einer ersten Perspektive wurde gesehen, dass die faktische Grenzenlosigkeit des Internets und damit des weltweiten Datenverkehrs und der entsprechenden Zugriffsmöglichkeiten ein striktes Anknüpfen der Souveränität über »Daten« an deren physischen Speicherort anachronistisch erscheinen lässt. Ein Belegenheitsort der in den Daten enthaltenen Informationen ist technisch-faktisch heute oftmals kaum mehr festzulegen. Mit Ausnahme des – vom Volumen her betrachtet – sehr kleinen Bereichs der Staatsgeheimnisse ist auch das Interesse an der »Herrschaft« über die Informationen und Daten bzw. an der Aufrechterhaltung der digitalen Integrität der Daten kein genuin staatliches, sondern ein solches des einzelnen betroffenen Rechtssubjekts. Künftig kommt es daher weniger auf Fragen der staats- und völkerrechtlichen Souveränität im digitalen Raum, sondern vielmehr auf den grund- und menschenrechtlich verbürgten Schutz der digitalen Integrität der Rechtssubjekte gegenüber inner- und außerstaatlichen Zugriffen auf Daten

und Informationen an. Wir plädieren daher sowohl für rechtspolitische Debatten als auch für den Diskurs um die Auslegung von Rechtsnormen für eine Verschiebung der Perspektive weg von klassischem staatsrechtlichem Souveränitätsdenken hin zur Fokussierung der Gewährleistung und des Ausbaus des grund- und menschenrechtlichen Schutzes der digitalen Integrität der Rechtssubjekte.

Während in einer zweiten Perspektive die weitere Erschütterung privatrechtlicher Grundkonzepte im digitalen Raum anhand verschiedener Stichpunkte zu illustrieren versucht wurde, bleibt am Ende festzuhalten: Die Reaktion des Privatrechts muss dabei eine genuin privatrechtliche sein (marktermöglichender statt marktkompensierender Regulierung). Es gilt auch weiterhin einen Rahmen zu schaffen, in dem individuelle Freiheit größtmöglich verwirklicht werden kann (vgl. Podszun 2020: F 102). Allen voran ist es nicht die Aufgabe des Rechts, sich im Sinne einer Zentralsteuerung selbst an die Stelle der privaten Akteure zu setzen: Statt beispielsweise die Bestimmung von Vertragsinhalten selbst in die Hand zu nehmen, ist es stattdessen die Aufgabe des Privatrechts, dafür zu sorgen, dass ein fairer Rahmen für Vertragsverhandlungen besteht (vgl. Hofmann 2019: 1224, 2020b: 667).

Literaturverzeichnis

Teil I

Bär, Wolfgang (2011): »Transnationaler Zugriff auf Computerdaten«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 6 (2), S. 53–59.

Bergmann, Jan (2014): »Stichwort: Souveränität«, in: Jan Bergmann (Hg.), Handlexikon der Europäischen Union, Baden-Baden: Nomos.

BGH – Bundesgerichtshof (2007): »5 StR 546/06«, in: NJW – Neue Juristische Wochenschrift 60 (31), S. 2269–2274.

Bode, Thomas A. (2012): Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin/Heidelberg: Springer.

Brodowski, Dominik (2021): »§ 110«, in: Georg Borges/Marc Hilber (Hg.), Beck'scher Online-Kommentar IT-Recht, München: C.H. Beck, S. Rn. 12.

Brodowski, Dominik/Eisenmenger, Florian (2014): »Der Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden. Zur sachlichen und zeitlichen Reichweite der ›kleinen Online-Durchsuchung‹ nach § 110 Abs. 3 StPO«, in: ZD – Zeitschrift für Datenschutz 4 (3), S. 119–126.

Bruns, Michael (2019): »§ 110«, in: Rolf Hannich (Hg.), Karlsruher Kommentar zur Strafprozessordnung, München: C.H. Beck, S. Rn. 8a.

Burchard, Christoph (2018a): »Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit – Teil 1«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 13 (6), S. 190–203.

Burchard, Christoph (2018b): »Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 13 (7–8), S. 249–267.

BVerfG – Bundesverfassungsgericht (1983) (65): »1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83«, in: BVerfGE, S. 1–71.

BVerfG – Bundesverfassungsgericht (2008) (120): »1 BvR 370/07, 1 BvR 595/07«, in: BVerfGE, S. 274–350.

BVerfG – Bundesverfassungsgericht (2009): »2 BvR 902/06«, in: NJW – Neue Juristische Wochenschrift 62 (34), S. 2431–2439.

BVerfG – Bundesverfassungsgericht (2016) (141): »1 BvR 966/09, 1 BvR 1140/09«, in: BVerfGE, S. 220–378.

BVerfG – Bundesverfassungsgericht (2016): »1 BvR 966, 1140/09«, in: NJW – Neue Juristische Wochenschrift 69 (25), S. 1781–1814.

BVerfG – Bundesverfassungsgericht (2018): »2 BvR 1405/17,2 BvR 1780/17«, in: BeckRS, S. 14189.

BVerfG – Bundesverfassungsgericht (2020a): »1 BvR 16/13«, in: NJW – Neue Juristische Wochenschrift 73 (5), S. 300–314.

BVerfG – Bundesverfassungsgericht (2020b): »1 BvR 276/17«, in: NJW – Neue Juristische Wochenschrift 73 (5), S. 314–328.

BVerfG – Bundesverfassungsgericht (2020c): »1 BvR 2835/17«, in: NJW – Neue Juristische Wochenschrift 73 (31), S. 2235–2269.

BVerfG – Bundesverfassungsgericht (2021): »2 BvR 1845/18, 2 BvR 2100/18«, in: NJW – Neue Juristische Wochenschrift 74 (21), S. 1518–1526.

Council of Europe (2001): Übereinkommen über Computerkriminalität vom 23.11.2001 (= Sammlung Europäischer Verträge Nr. 185). Online unter: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, abgerufen am 19.07.2022.

Diel-Gligor, Katharina (2021): »Sicherungsinstrumente für die Rechtsstaatlichkeit in der EU«, in: ZRP – Zeitschrift für Rechtspolitik 54 (2), S. 63–66.

Durner, Wolfgang (2021): »Art. 10«, in: Roman Herzog/Rupert Scholz/Matthias Herdegen/Hans Klein (Hg.), Dürig/Herzog/Scholz Grundgesetz Kommentar Band I, München: C.H. Beck, S. Rn. 141ff.

EGMR – Europäischer Gerichtshof für Menschenrechte (2015): »Zakharov gg. Russland 47143/06«, in: NLMR – Newsletter Menschenrechte 24 (6), S. 509–516.

EuGH – Europäischer Gerichtshof (2014): »C-293/12, C-594/12«, in: NJW – Neue Juristische Wochenschrift 67 (30), S. 2169–2173.

Fritzsche, Albrecht (2022): »Konturenbildung im Gestaltungsraum der digitalen Transformation – eine Reflexion der Debatte über ›digitale Souveränität‹ aus betriebswirtschaftlicher Sicht«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 229–245.

Galen, Margarete von (2020): »Kritische Anmerkungen zur E-Evidence-Verordnung«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 127–138.

Glasze, Georg/Odzuck, Eva/Staples, Ronald (2022): »Einleitung: Digitalisierung als Herausforderung – ›Souveränität‹ als Antwort? Konzeptionelle Hintergründe der Forderungen nach ›digitaler Souveränität‹«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 7–28.

Goger, Thomas/Stock, Jürgen (2017): »Cybercrime – Herausforderung für die internationale Zusammenarbeit«, in: ZRP – Zeitschrift für Rechtspolitik 47 (1), S. 10–14.

Grözinger, Andreas (2019): »Heimliche Zugriffe auf die Cloud – Befugnis zur Plünderung eines unermesslichen Datenschatzes«, in: StV – Strafverteidiger 39 (6), S. 406–412.

Hamel, Patricia (2020): »Schnellerer grenzüberschreitender Zugriff auf elektronische Beweismittel: Die E-evidence Vorschläge der Europäischen Kommission«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 103–126.

Hauck, Pierre (2014): Heimliche Strafverfolgung und Schutz der Privatheit: Eine vergleichende und interdisziplinäre Analyse des deutschen und englischen Rechts unter Berücksichtigung der Strafverfolgung in der Europäischen Union und im Völkerstrafrecht, Tübingen: Mohr Siebeck.

Hauschild, Jörn (2014): »§ 110«, in: Christoph Knauer/Hans Kudlich/Hartmut Schneider (Hg.), Münchener Kommentar zur StPO, Band 1: §§1-150, München: C.H. Beck, S. Rn. 18f.

Jansen, Marek (2018): »Microsofts ›Search Warrant‹ Case – oder die Zukunft der europäischen Datensouveränität«, in: ZD – Zeitschrift für Datenschutz 9 (4), S. 149–150.

Jarass, Hans D. (2021): »Art. 8 GrCh«, in: Hans D. Jarass (Hg.), Charta der Grundrechte der Europäischen Union, München: C.H. Beck, S. Rn. 9.

Jellinek, Georg (1922): Allgemeine Staatslehre, Berlin: Springer.

Kalpakis, George/Tsikrika, Theodora/Cunningham, Neil/Iliou, Christos/Vrochidis, Stefanos/Middleton, Jonathan/Kompatsiaris, Ioannis (2016): »OSINT and the Dark Web«, in: Babak Akhgar/P. Saskia Bayerl/Fraser Sampson (Hg.), Open Source Intelligence Investigation, Cham: Springer, S. 111–132.

Köhler, Marcus (2021): »§ 110«, in: Lutz Meyer-Goßner/Bertram Schmitt (Hg.), Strafprozessordnung mit GVG und Nebengesetzen, München: C.H. Beck, S. Rn. 7b.

Krcmar, Helmut (2016): »§ 1 Technische Grundlagen des Cloud Computings«, in: Georg Borges/Geert Meents (Hg.), Rechtshandbuch Cloud Computing, München: C.H. Beck, S. 1–17.

Moechel, Erich (2021): Verhandlungen EU-USA zur Cloud-Überwachung gestartet. FM4 ORF, Issue vom 06.05.2021. Online unter: https://fm4.orf.at/stories/3014416/, abgerufen am 16.07.2022.

Oberlandesgericht Karlsruhe (2020): »Ausl 301 AR 156/19«, in: BeckRS, S. 1720.

Rath, Michael/Spies, Axel (2018): »CLOUD Act: Selbst für Wolken gibt es Grenzen«, in: CCZ – Corporate Compliance Zeitschrift 11 (5), S. 229–230.

Rückert, Christian (2020a): »Herausforderungen der Digitalisierung für das Strafverfahren«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 9–38.

Rückert, Christian (2020b): »§ 21 Strafanwendungsrecht«, in: Philipp Maume/Lena Maute/Mathias Fromberger (Hg.), Rechtshandbuch Kryptowerte, München: C.H. Beck, S. 537–546.

Safferling, Christoph (2014): »Der EuGH, die Grundrechtecharta und nationales Recht: Die Fälle Åkerberg Fransson und Melloni«, in: NStZ – Neue Zeitschrift für Strafrecht 34 (10), S. 545–551.

Safferling, Christoph (2021): »Entführung durch ausländischen Geheimdienst auf deutschem Boden«, in: JR – Juristische Rundschau 93 (7), S. 306–331.

Safferling, Christoph/Rückert, Christian (2020): »Schutz von Dissidenten und Abwehr von Cyberspionage – die neue Bedeutung des § 99 StGB«, in: ZStW – Zeitschrift für die gesamte Strafrechtswissenschaft 132 (2), S. 367–369.

Safferling, Christoph/Rückert, Christian (2021): »Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?«, in: NJW – Neue Juristische Wochenschrift 74 (5), S. 287–292.

Schmahl, Stefanie (2020): »Grundrechtsbindung der deutschen Staatsgewalt im Ausland«, in: NJW – Neue Juristische Wochenschrift 73 (31), S. 2221–2224.

Schwabenbauer, Thomas (2013): Heimliche Grundrechtseingriffe: Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen: Mohr Siebeck.

Staffler, Lukas/Jany, Oliver (2020): »Künstliche Intelligenz und Strafrechtspflege – eine Orientierung«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 15 (4), S. 164–177.

Tanneberger, Steffen (2014): Die Sicherheitsverfassung: Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts; zugleich ein Beitrag zu einer induktiven Methodenlehre, Tübingen: Mohr Siebeck.

Wicker, Magda (2013a): »Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden«, in: MMR – Multimedia und Recht 16 (12), S. 765–769.

Wicker, Magda (2013b): »Ermittlungsmöglichkeiten in der Cloud«, in: Jürgen Taeger (Hg.), DSRI-Tagungsband, Oldenburg: OlWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht, S. 981–1001.

Teil II

Alexander, Christian (2019): Wettbewerbsrecht, Köln: Carl Heymanns.

BGH – Bundesgerichtshof (2008): »Urt. v. 16.7.2008 – VIII ZR 348/06«, in: NJW – Neue Juristische Wochenschrift 61 (42), S. 3055.

BGH – Bundesgerichtshof (2012): »Urt. v. 11.11.2009 – VIII ZR 12/08«, in: NJW – Neue Juristische Wochenschrift 65 (12), S. 864.

Böhm, Franz (1966): »Privatrechtsgesellschaft und Marktwirtschaft«, in: Ordo – Jahrbuch für die Ordnung von Wirtschaft und Gesellschaft 17, S. 75–151.

Bornkamm, Joachim/Feddersen, Jörn (2021): »§ 5 Irreführende geschäftliche Handlungen«, in: Helmut Köhler/Joachim Bornkamm/Jörn Feddersen (Hg.), Gesetz gegen den unlauteren Wettbewerb: UWG, München: C.H. Beck, S. 750–1074.

Brehm, Wolfgang (2008): Allgemeiner Teil des BGB, Stuttgart: Boorberg.

Brox, Hans/Walker, Wolf-Dietrich (2020): Allgemeiner Teil des BGB, München: Vahlen.

Busch, Christoph (2019): »Mehr Fairness und Transparenz in der Plattformökonomie?«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (8), S. 788–796.

Busch, Christoph/Dannemann, Gerhard/Schulte-Nölke, Hans (2020): »Bausteine für ein europäisches Recht der Plattformökonomie«, in: MMR – Multimedia und Recht 23 (10), S. 667–675.

BVerfG – Bundesverfassungsgericht (1984): »Urt. v. 15.12.1983 – 1 BvR209/83«, in: NJW – Neue Juristische Wochenschrift 37 (8), S. 419.

BVerfG – Bundesverfassungsgericht (1994): »Beschl. v. 19.10.1993 – 1 BvR 567/89«, in: NJW – Neue Juristische Wochenschrift 47 (1), S. 36.

BVerfG – Bundesverfassungsgericht (2018): »Beschl. v. 11.4.2018 – 1 BvR 3080/09«, in: NJW – Neue Juristische Wochenschrift 71 (23), S. 1667 – Stadionverbot.

Deutscher Bundestag (2009): Bundestag-Drucksache 17/315 vom 18.12.2009. Online unter: https://dserver.bundestag.de/brd/2017/0315-17.pdf, abgerufen am 19.07.2022.

Dix, Alexander (2017): »Daten als Bezahlung – zum Verhältnis zwischen Zivilrecht und Datenschutzrecht«, in: ZEuP – Zeitschrift für europäisches Privatrecht 25 (1), S. 1–5.

Englerth, Markus/Towfigh, Emanuel V. (2010): »§ 8 – Verhaltensökonomik«, in: Emanuel V. Towfigh/Niels Petersen (Hg.), Ökonomische Methoden im Recht. Eine Einführung für Juristen, Tübingen: Mohr Siebeck, S. 237–276.

Ernst, Stefan (2010): BGH: Ausgestaltung von Kundenbindungssystemen – Happy Digits. LMK, Kommentierte BGH-Rechtsprechung, Lindenmaier-Möhring (Fachdienst Zivilrecht), 297158.

Ernst, Stefan (2017): »Die Einwilligung nach der Datenschutzgrundverordnung«, in: ZD – Zeitschrift für Datenschutz 7 (3), S. 110–113.

EuGH – Europäischer Gerichtshof (2019): »Urt. v. 3.10.2019 – C-18/18 – Eva Glawischnig-Piesczek/Facebook Ireland Ltd.«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (11), S. 1208.

Fezer, Karl-Heinz (2017): »Dateneigentum der Bürger«, in: ZD – Zeitschrift für Datenschutz 7 (3), S. 99–104.

Flume, Werner (1975): Allgemeiner Teil des Bürgerlichen Rechts. Zweiter Band: Das Rechtsgeschäft, Berlin/Heidelberg: Springer.

Geiger, Christoph (2004): »Der urheberrechtliche Interessenausgleich in der Informationsgesellschaft. Zur Rechtsnatur der Beschränkungen des Urheberrechts«, in: GRUR Int. – Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (10), S. 815–820.

Grigoleit, Hans Christoph (2008): »Anforderungen des Privatrechts an die Rechtstheorie«, in: Matthias Jestaedt/Oliver Lepsius (Hg.), Rechtswissenschaftstheorie, Tübingen: Mohr Siebeck, S. 51–78.

Grünberger, Michael (2017): »Internetplattformen – Aktuelle Herausforderungen der digitalen Ökonomie an das Urheber- und Medienrecht«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 61 (2), S. 89–92.

Grünberger, Michael (2018): »Verträge über digitale Güter«, in: AcP – Archiv für die civilistische Praxis 218, S. 213–296.

Hacker, Philipp (2019): »Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DSGVO und allgemeinem Vertragsrecht«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 5 (2), S. 148–197.

Hellgardt, Alexander (2016): Regulierung und Privatrecht: Staatliche Verhaltenssteuerung mittels Privatrecht und ihre Bedeutung für Rechtswissenschaft, Gesetzgebung und Rechtsanwendung, Tübingen: Mohr Siebeck.

Hofmann, Franz (2016): »Der maßgeschneiderte Preis. Dynamische und individuelle Preise aus lauterkeitsrechtlicher Sicht«, in: WRP – Wettbewerb in Recht und Praxis 13 (9), S. 1074–1081.

Hofmann, Franz (2017): »Das Allgemeininteresse an der Verfügbarkeit von Internet im Spannungsverhältnis zum Schutz von Urheberrecht«, in: GPR – Zeitschrift für das Privatrecht der Europäischen Union 14 (4), S. 176–182.

Hofmann, Franz (2019): Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (12), S. 1219–1229.

Hofmann, Franz (2020a): »›Absolute Rechte‹ an Daten – immaterialgüterrechtliche Perspektive«, in: Tereza Pertot (Hg.), Rechte an Daten, Tübingen: Mohr Siebeck, S. 9–33.

Hofmann, Franz (2020b): »Plattformregulierung im Lichte des Unionsrechts«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 64 (10), S. 665–670.

Hofmann, Franz (2020c): »Einseitige und übereinstimmende Erledigungserklärungen vor unzuständigem Gericht«, in: NJW – Neue Juristische Wochenschrift 73 (16), S. 1117–1119.

Hofmann, Franz (2020d): »Standpunkt: Recht auf ›Unrecht‹«, in: NJW-Aktuell – Neue Juristische Wochenschrift Aktuell (36), S. 15.

Hofmann, Franz (2021): »Das neue Urheberrechts-Diensteanbieter-Gesetz«, in: NJW – Neue Juristische Wochenschrift 74 (27), S. 1905–1910.

Hofmann, Franz/Freiling, Felix (2020): »Personalisierte Preise und das Datenschutzrecht«, in: ZD – Zeitschrift für Datenschutz 10 (7), S. 331–335.

Köhler, Helmut (2017): BGB. Allgemeiner Teil, München: C.H. Beck.

Körber, Torsten (2016): »›Ist Wissen Marktmacht?‹ Überlegungen zum Verhältnis von Datenschutz, ›Datenmacht‹ und Kartellrecht – Teil 1«, in: NZKart – Neue Zeitschrift für Kartellrecht 4 (7), S. 303–309.

Krohm, Niclas/Müller-Peltzer, Philipp (2017): »Auswirkungen des Koppelungsverbots auf die Praxistauglichkeit der Einwilligung«, in: ZD – Zeitschrift für Datenschutz 7 (12), S. 551–555.

Krüger, Philipp-L. (2016): »Datensouveränität und Digitalisierung«, in: ZRP – Zeitschrift für Rechtspolitik 49 (7), S. 190–192.

Kühling, Jürgen/Martini, Mario (2016): »Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?«, in: EuZW – Europäische Zeitschrift für Wirtschaftsrecht 27 (12), S. 448–453.

Kumkar, Lea K. (2020): »Herausforderungen eines Gewährleistungsrechts im digitalen Zeitalter«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 6 (3), S. 306–333.

Leistner, Matthias/Roder, Verena (2016): »Die Rechtsprechung des EuGH zum Unionsurheberrecht aus methodischer Sicht – zugleich ein Beitrag zur Fortentwicklung des europäischen Privatrechts im Mehrebenensystem«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 2 (2), S. 129–172.

Louven, Sebastian (2018): »Datenmacht und Zugang zu Daten«, in: NZKart – Neue Zeitschrift für Kartellrecht 6 (5), S. 217–222.

Medicus, Dieter/Lorenz, Stephan (2015): Schuldrecht I. Allgemeiner Teil, München: C.H. Beck.

Paal, Boris P./Kumkar, Lea K. (2021): »Wettbewerbsschutz in der Digitalwirtschaft«, in: NJW – Neue Juristische Wochenschrift 74 (12), S. 809–815.

Paulus, Christoph G./Zenker, Wolfgang (2001): »Grenzen der Privatautonomie«, in: JUS – Juristische Schulung 41 (1), S. 1–8.

Petersen, Jens (2011): »Die Privatautonomie und ihre Grenzen«, in: JURA – Juristische Ausbildung 33 (3), S. 184–186.

Podszun, Rupprecht (2020): Gutachten Teil F zum 73. Deutschen Juristentag. Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen?, München: C.H. Beck.

Raiser, Ludwig (1961): »Der Stand der Lehre vom subjektiven Recht im Deutschen Zivilrecht«, in: JZ – Juristen Zeitung 16, S. 465–473.

Raue, Benjamin/Steinebach, Martin (2020): »Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 64 (5), S. 355–364.

Riesenhuber, Karl (2009): »§ 1 Privatrechtsgesellschaft: Leistungsfähigkeit und Wirkkraft im deutschen und Europäischen Recht. Entwicklung, Stand und Verfassung des Privatrechts«, in: Karl Riesenhuber (Hg.), Privatrechtsgesellschaft. Entwicklung, Stand und Verfassung des Privatrechts, Tübingen: Mohr Siebeck, S. 1–32.

Sattler, Andreas (2017): »Personenbezogene Daten als Leistungsgegenstand«, in: JZ – Juristen Zeitung 72 (21), S. 1036–1046.

Sauer, Stefan/Staples, Ronald/Steinbach, Vincent (2022): »Der relationale Charakter von ›digitaler Souveränität‹. Zum Umgang mit dem ›Autonomie/Heteronomie‹-Dilemma in sich transformierenden Arbeitswelten«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 287–315.

Schmidt-Kessel, Martin (2017): »Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 3 (1), S. 84–108.

Schuppert, Gunnar (2019): Eigentum neu denken. Ein Rechtsinstitut zwischen Wandel und Resilienz, Baden-Baden: Nomos.

Schweitzer, Heike (2019a): »Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische ›Plattform-Regulierung‹«, in: ZEuP – Zeitschrift für Europäisches Privatrecht 27 (1), S. 1–12.

Schweitzer, Heike (2019b): »Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (6), S. 569–580.

Specht, Louisa (2017a): »Das Verhältnis möglicher Datenrechte zum Datenschutzrecht«, in: GRUR Int. – Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (12), S. 1040–1047.

Specht, Louisa (2017b): »Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?«, in: JZ – Juristen Zeitung 72 (15–16), S. 763–770.

Tonner, Klaus (2017): »Verbraucherschutz in der Plattform-Ökonomie«, in: VuR – Verbraucher und Recht 32 (5), S. 161–162.

Tuhr, Andreas von (1957): Der Allgemeine Teil des Deutschen Bürgerlichen Rechts. Erster Band: Allgemeine Lehren und Personenrecht, Berlin: Duncker & Humblot.

Veil, Winfried (2018): »Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis«, in: NJW – Neue Juristische Wochenschrift 71 (46), S. 3337–3343.

Wagner, Gerhard (2017): »Produkthaftung für autonome Systeme«, in: AcP – Archiv für die civilistische Praxis 217 (6), S. 707–765.

Wagner, Gerhard/Eidenmüller, Horst (2019): »In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 5 (2), S. 220–246.

Wendehorst, Christiane (2019): »§§ 312–312k«, in: Franz J. Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg (Hg.), Münchener Kommentar zum BGB, Band 3: Schuldrecht – Allgemeiner Teil II, München: C.H. Beck, S. 156–317.

Wendehorst, Christiane/Westphalen, Friedrich von (2016): »Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht«, NJW – Neue Juristische Wochenschrift 69 (52), S. 3745–3749.

Westphalen, Friedrich von (2017): »Nutzungsbedingungen von Facebook – Kollision mit europäischem und deutschem AGB-Recht«, in: VuR – Verbraucher und Recht 32 (9), S. 323–331.

Wiebe, Andreas (1992): »Reverse Engineering und Geheimnisschutz von Computerprogrammen«, in: CR – Computer und Recht 8 (3), S. 134–141.

Zech, Herbert (2012): Information als Schutzgegenstand, Tübingen: Mohr Siebeck.

Zech, Herbert (2015a): »›Industrie 4.0‹ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 117 (12), S. 1151–1159.

Zech, Herbert (2015b): »Daten als Wirtschaftsgut – Überlegungen zu einem ›Recht des Datenerzeugers‹«, in: CR – Computer und Recht 31 (3), S. 137–146.