Freiheit in digitalen Infrastrukturen – eine Einleitung in die Thematik

Alexander Roßnagel, Michael Friedewald, Christian L. Geminn und Murat Karaboga

Freiheit als Abwehr von ungerechtfertigter Machtausübung und Schutz vor Machtmissbrauch ist Voraussetzung für individuelle Selbstentfaltung und kollektive Selbstbestimmung. Grundrechte und Demokratie sollen diese Freiheit gewährleisten. Sie sollen die Ausübung unter anderem von Meinungsfreiheit, Informationsfreiheit, Gewissensfreiheit, Wissenschaftsfreiheit und Wahlfreiheit ermöglichen und vor Diskriminierung schützen. Auch das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, die Achtung des Privat- und Familienlebens und der Schutz personenbezogener Daten sind Bedingungen von Freiheit. Wie individuelle und kollektive Freiheit gelebt werden kann, ist abhängig von den gesellschaftlichen, technischen, ökonomischen und kulturellen Bedingungen, unter denen sie ausgeübt werden soll. Diese Freiheiten sind aktuell gefährdet und müssen verteidigt werden. Damit auch die Forschung ihren Beitrag zu ihrer Erhaltung leistet, hat das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) „Freiheit" in den Mittelpunkt des Forschungsjahres 2024 gestellt.

In der modernen Welt sind für die Freiheitsausübung die gesellschaftlichen Infrastrukturen von entscheidender Bedeutung. Diese verändern sich aktuell dynamisch und damit auch die Bedingungen von Freiheit.

1. Digitale Infrastrukturen

Infrastrukturen sind netzartige sozio-technische Systeme die verlässlich einen einheitlichen Satz von Leistungen anbieten, die von Interessierten als Grundlagen des menschlichen Zusammenlebens, als Eröffnung von Handlungsmöglichkeiten und als Schutz gegenüber Lebensrisiken genutzt werden können – wie für Kommunikation, Energieversorgung, Güteraustausch, Mobilität oder Unterhaltung. Infrastrukturen sind daher Grundlagen für die Ausübung von Freiheit. Sie können aber auch durch die Abhän-

gigkeit von ihren Leistungen, durch die Machtsteigerung ihrer Anbieter und die Rigidität ihres Angebots die Freiheitsausübung einschränken oder gefährden.

Digitale Infrastrukturen sind die Basis für Digitalisierung. Sie sind Bedingungen für das Leben in der digitalen Welt. Ohne sie wären digitale Kommunikation, Informationssuche, -verbreitung und -verarbeitung, sozialer Austausch, Handel, Mobilität sowie Hardware- und Softwarenutzung nicht möglich. Vor allem die Infrastrukturnetze und -plattformen von Alphabet (Google), Apple, Meta (Facebook), Amazon und Microsoft bieten Leistungen, die derzeit Grundlagen für Freiheitsausübung in der digitalen Welt sind. Aber auch die Anbieter „alter" Infrastrukturen wie Automobilhersteller, Energieversorger, Finanzdienstleister, Gesundheitsdienstleister, Logistikunternehmen, Telekommunikationsanbieter oder Bahnbetreiber bauen digitale Infrastrukturen auf, ohne die ihre Leistungen nicht mehr genutzt werden können. Selbst der Staat errichtet neue Infrastrukturen wie Bürgerkonten, elektronische Akten, elektronische Register und elektronische Zugänge zur Verwaltung. Alle diese digitalen Infrastrukturen verändern Machtgefüge und Freiheitsspielräume.

Digitale Infrastrukturen bestimmen über den Grad der Freiheit von Individuen und Gesellschaft. Dies gilt nicht nur für ihre Betreiber. Vielmehr sind es die Infrastrukturen selbst, die durch ihre standardisierenden Effekte und ihre Plattform- und Netzwerkeffekte infrastrukturelle Macht ausüben. Da sie für ihr Funktionieren personenbezogene Daten verarbeiten müssen, können sie diese Datenverarbeitung nicht von unterschiedlichen individuellen Einwilligungen abhängig machen. Die individuelle Selbstbestimmung ist letztlich reduziert auf das grundsätzliche „Ja" oder „Nein" zum digitalen Leben. Digitale Infrastrukturen erzeugen einen eigenen virtuellen Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. In diesem hinterlässt jede Handlung Datenspuren, deren Erhebung und – letztlich weltweite – Verbreitung und Verwendung die betroffene Person nicht kontrollieren kann. Den damit verbundenen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative. Es besteht ein virtueller „Anschluss- und Benutzungszwang" für digitale Infrastrukturen, der oftmals auch mit dem Wegfall analoger Alternativen einhergeht.

Die großen digitalen Infrastrukturen sind global und durchdringen überall auf der Welt in intensiver Weise das digitale Leben. Ihre Marktanteile sind monopolartig und ihre Anbieter haben den mit Abstand höchsten Marktwert aller Unternehmen weltweit. Für diese ungeheure ökonomische

Macht gibt es vor allem zwei Gründe: Zum einen sind ihre Angebote für das digitale Leben hilfreich und verführerisch und zum anderen sind sie „umsonst". Die Abhängigkeit von ihnen ist hoch und nimmt weiter zu. Diese ökonomischen Erfolge erzielen sie vor allem durch die Verarbeitung der Daten ihrer Nutzenden. Mit deren Hilfe erstellen sie Personenprofile, beuten die Subjektivität der Betroffenen aus, verkaufen ihre Aufmerksamkeit, steuern ihre Informationen und beeinflussen ihr Denken. Mit ihrer Informationsmacht versuchen sie, ihr Verhalten zu beeinflussen oder gar zu steuern – bisher noch insbesondere für Konsumwahl und Kundenbindung, potenziell aber auch für andere Verhaltensformen wie z. B. Wahlentscheidungen. Politisches Micro-Targeting könnte auf der Grundlage der Personenprofile leicht zur Manipulation demokratischer Wahlen verwendet werden. Zahlreiche weitere Techniken der Verhaltensmanipulation wie z. B. Dark Patterns oder Nudging stehen zur Verfügung. Die personalisierten Dienstleistungen der Infrastrukturen werden über den gesamten Tagesverlauf hinweg in die individuellen Handlungsabläufe integriert und unmerklich Teil des Verhaltens und Handelns. Die gleichen Infrastrukturen, die Freiheit und Demokratie unterstützen können, entwickeln sich zu ihren Gefährdern.

Der ungeheure Reichtum, den die Anbieter der großen digitalen Infrastrukturen innerhalb kurzer Zeit erringen konnten, ermöglicht ihnen, ihre Macht immer weiter auszubauen. Ihnen gelang es innerhalb ihrer Infrastrukturen alle wesentlichen Bausteine zu integrieren – von Hardware über Rechenzentren, Cloud-Systemen, APIs und Software bis hin zu Plattformen, Suchmaschinen, Anwendungssystemen und Forschungszentren. Sie binden mit interessanten Projekten und konkurrenzlosen Gehältern junge Talente. Sie kaufen Start-ups und mögliche Konkurrenten auf und werden dadurch auch führend in neu entstehenden digitalen Infrastrukturen. Sie steuern damit die technologische Entwicklung, bestimmen, was sich durchsetzt, und verhindern Entwicklungen, die nicht zu ihren Interessen passen.

Die Anbieter digitaler Infrastrukturen beherrschen auch die Entwicklung der neuesten Infrastruktur: Große Sprachmodelle als Kern generativer Systeme Künstlicher Intelligenz. Sie verfügen über die erforderlichen finanziellen Ressourcen und enormen Rechenkapazitäten sowie über die notwendigen Cloud-Infrastrukturen. Durch die von ihnen betriebenen Infrastrukturen können sie auf ungeheure Datenschätze zurückgreifen, über die sie allein verfügen, und sind damit hinsichtlich ihrer KI-Trainingsmöglichkeiten konkurrenzlos. Andere Entwickler sind gezwungen, auf ihren KI-Infrastrukturen aufzusetzen und sich darauf zu beschränken, diese auf

die spezifischen Bedürfnisse bestimmter Anwendungsbereiche wie etwa Medizin, Verwaltung oder Wissenschaft anzupassen. Die Entwicklung zu Künstlicher Intelligenz verstärkt daher ihre infrastrukturelle Macht zusätzlich.

2. Normativer Rahmen

Die Europäische Union hat neue Regelungen erlassen, um Gefahren durch die globalen digitalen Infrastrukturen einzuschränken und deren Macht zu begrenzen. Vor allem das Gesetz über digitale Dienste, das Gesetz über digitale Märkte, die Verordnung über künstliche Intelligenz (KI-VO) und die Datenschutz-Grundverordnung (DSGVO) enthalten Regelungen, um die Freiheit des Individuums zu schützen, die Voraussetzungen eines funktionierenden Marktes zu erhalten und demokratisch festgelegte Regeln des Zusammenlebens durchzusetzen. Sie sollen unter anderem informationelle Selbstbestimmung gewährleisten, vor Diskriminierung schützen und menschenzentrierte Gestaltung in der Entwicklung von Künstlicher Intelligenz erreichen. Aufsichtsbehörden sollen die Einhaltung dieser Ziele sicherstellen. Sie haben daher die Befugnis, bestimmte Verhaltensweisen anzuordnen und Sanktionen in spürbarer Höhe zu verhängen.

Den Anbietern digitaler Infrastrukturen helfen jedoch spezifische Schwachstellen der Unionsgesetze. So adressiert die DSGVO nur Verantwortliche und knüpft an den einzelnen Datenverarbeitungsvorgängen an, regelt aber nicht die freiheitsbeschränkenden Wirkungen großer digitaler Infrastrukturen. Ebenso enthält die KI-VO Gestaltungsanforderungen an KI-Systeme und nimmt damit primär Künstliche Intelligenz in Form von einzelnen Produkten in den Blick. Sie adressiert jedoch die infrastrukturelle Perspektive allenfalls indirekt, beispielsweise in Bezug auf Risikobewertungen und Folgenabschätzungen. Ob die Regelungen der Europäischen Union insgesamt genügen werden, um die verfolgten Ziele zu erreichen, muss sich erst noch erweisen. Sie sind jedenfalls sinnvolle erste Schritte zur Freiheitssicherung und Machtbegrenzung.

Die Anbieter digitaler Infrastrukturen agieren jedoch weltweit. Sie ignorieren daher vielfach die demokratisch getroffenen Entscheidungen zur regionalen Regulierung von Infrastrukturen – auch in Europa oder Deutschland. Sie legen ihrem Handeln eigene Regeln zugrunde, die den europäischen oder nationalen Regelungen oft widersprechen. Sie wollen ihre eigene globale Rechtsordnung – verkleidet als Vertragsbedingungen für die

Nutzung ihrer Infrastrukturen – weltweit durchsetzen. Ihre infrastrukturelle Macht erschwert die Durchsetzung des normativen, freiheitssichernden rechtlichen Rahmens in Europa erheblich.

Diese Hindernisse werden neuerdings noch dadurch verstärkt, dass die Anbieter digitaler Infrastrukturen (wenn auch fragile) Symbiosen mit der politischen Macht in den USA eingehen. Die amtierende US-Regierung betrachtet die Anwendung von geltendem Unionsrecht als gezielte Benachteiligung von US-Anbietern und droht mit wirtschaftlichen Vergeltungsmaßnahmen.

3. Folgen für Freiheit und Selbstbestimmung

Was kann Freiheit und Selbstbestimmung unter diesen neuen und sich verändernden Bedingungen bedeuten? Jede Infrastruktur ist mit bestimmten Technologien und Praktiken verbunden und durch ihre sozio-technische infrastrukturelle Form in besonderem Maße handlungsnormierend. Infrastrukturen eröffnen oder verschließen Handlungsmöglichkeiten und steuern Wissen, Werte und Ressourcen.

Eine wichtige Forschungsfrage für die Auswirkungen von digitalen Infrastrukturen ist, wie sich die komplexen Interaktionen zwischen sozialen Systemen und technischen Infrastrukturen entwickeln. Diese Interaktionen sind entscheidend für die Gestaltung und Nutzung von Technologien, die sowohl Chancen als auch Herausforderungen mit sich bringen. Wie aber beeinflussen technologisch geprägte Praktiken unterschiedliche Werte, die Vielfalt und Ambivalenz von Privatheitsansprüchen und die divergierende individuelle Vulnerabilität verschiedener Nutzergruppen?

Die Wirkung der Datenverarbeitung in digitalen Infrastrukturen hängt auch davon ab, wie die betroffenen Personen die auf sie bezogenen Datenverarbeitungen für sich deuten und erklären. Wann empfinden sie diese Einflüsse für ihre Freiheit als positiv oder negativ? Je nach Erwartung und Empfinden können die objektiven Wirkungen dateninvasiver Technologien einen relativen Freiheitsgewinn oder eine schmerzende Freiheitsverletzung bedeuten.

Um in digitalen Infrastrukturen Freiheit und Grundrechte ausüben zu können, sind je nach Situation unterschiedliche individuelle und unternehmerische Kompetenzen und Motive sowie familiäre, wirtschaftliche, aber auch politisch-institutionelle und technische Verwirklichungsbedingungen

erforderlich. Eine wichtige Forschungsfrage ist daher, wie Selbstbestimmung und Handlungsfähigkeit von Individuen sichergestellt werden kann.

Für die Auswirkungen auf Freiheit sind auch die Strategien bedeutsam, die betroffene Personen zum Schutz ihrer Selbstbestimmung in digitalen Infrastrukturen verfolgen können. Entscheidend dafür dürfte sein, wie Regulierung, Technologie, Nutzererwartungen und Interaktivität aufeinander abgestimmt sind. Nutzerzentrierte Datenschutzinitiativen können dabei hilfreich und wirksam sein, indem sie virtuelle Belästigungen verhindern sowie die Transparenz von Datenverarbeitungsprozessen erhöhen und dadurch Entscheidungsspielräume deutlich und nutzbar machen. Hierzu erscheint es unerlässlich, die Auswirkungen der algorithmischen Informationsverarbeitung und der damit verbundenen Datenschutzfragen zu verstehen.

4. Teilhabe an Infrastrukturen

Aufgrund der selbstverantworteten Abhängigkeit wird die Nutzung der digitalen Infrastrukturen zu den Bedingungen ihrer Anbieter von vielen als Zwang erlebt. In solchen Situationen könnte die Teilhabefunktion der Grundrechte an Bedeutung gewinnen. Grundrechte bieten nicht nur Abwehrrechte gegen staatliche Einschränkungen der Freiheit oder Schutz der Freiheit gegen Übergriffe mächtiger Privater, sondern fordern auch die Teilhabe an den Voraussetzungen modernen Miteinanderlebens. Gerade mit Blick auf die globalen digitalen Infrastrukturen ist zu diskutieren, ob die Rechtsprechung des Bundesverfassungsgerichts zur Geltung der Grundrechte für übliche Infrastrukturanbieter auch auf die Anbieter der globalen digitalen Infrastrukturen anzuwenden ist.

Die Betreiber von digitalen Infrastrukturen nehmen Aufgaben der Daseinsvorsorge in der digitalen Gesellschaft wahr. Sie sind daher mit den Betreibern der Straßen, des Bahnverkehrs, des Briefverkehrs, der Wasserver- und -entsorgung, der Abfallentsorgung oder der Energieversorgung in der analogen Welt vergleichbar. Ohne ihre Leistungen wäre das gesellschaftliche Zusammenleben in Frage gestellt und die Ausübung von Grundrechten gefährdet. Infrastrukturbetreiber haben daher, unabhängig davon, ob sie privatrechtlich oder öffentlich-rechtlich verfasst sind, eine gesteigerte gesellschaftliche Verantwortung und unterliegen in besonderem Maße staatlicher Aufsicht. Sie haben auch die Grundrechte der von ihnen Abhängigen in besonderer Weise zu achten und zu schützen.

Dies gilt in verstärkter Weise, wenn die Infrastrukturbetreiber durch autoritative Setzung eine eigene Rechtsordnung in Form von „Gemeinschaftsregeln" erstellen, die staatlichen Rechtsregeln, die durch demokratische Prozesse zustande kommen, Konkurrenz machen. Im Zweifelsfall müssen das staatliche Recht und erst recht die Grundrechte der EU-Grundrechtecharta und des Grundgesetzes diesen „Gemeinschaftsregeln" vorgehen. Soweit Grundrechte betroffen sind, muss die Ausgestaltung und der Betrieb der Infrastrukturen stärker an diesen als an ökonomischen Konzernzielen ausgerichtet sein.

Daher sind mit der Rechtsprechung des Bundesverfassungsgerichts die öffentliche Verantwortung von Infrastrukturbetreibern und ihre verstärkte Grundrechtsbindung auch gegenüber privaten Infrastrukturbetreibern zu betonen. Auch wenn diese sich grundsätzlich auf Berufs- und Eigentumsfreiheit berufen können, muss gelten: Je abhängiger die Gesellschaft von ihren Infrastrukturleistungen ist und je tiefgreifender ihre Leistungserbringung die Verwirklichung von Grundrechten, insbesondere der informationellen Selbstbestimmung und der gesellschaftlichen Kommunikation, beeinflusst, desto eher unterliegen sie einer bis hin zu staatsgleichen Grundrechtsbindung.

Für die Adressaten von Grundrechten gilt somit: Je größer die gesellschaftliche Macht, desto stärker muss die Bindung an Grundrechte sein. Für die Freiheit spielt es keine Rolle, wer sie gefährdet. Angesichts der zunehmenden Machtkonzentration erwächst für Demokratie und Rechtsstaat daher im Schutz der Freiheit die wohl wichtigste Aufgabe der Zukunft.

5. Digitale Souveränität

Aufgrund der hohen Abhängigkeit von digitalen Infrastrukturen aus den USA wird zunehmend die Forderung nach digitaler Souveränität Europas erhoben. Eine häufig angewandte Definition versteht unter digitaler Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können". Nicht nur eine konkurrenzfähige und selbstbestimmte wirtschaftliche Entwicklung setzt mehr digitale Souveränität voraus. Vielmehr werden durch sie auch die Bedingungen, individuelle und kollektive Freiheit auszuüben und europäische Werte in der digitalen Welt durchsetzen zu können, verbessert.

Forschungsthemen betreffen die Frage, mit Hilfe welcher nationalen und internationalen Mechanismen oder Rechtsinstrumente die Europäische Union oder ihre Mitgliedstaaten versuchen sollten, das Angebot von digitalen Infrastrukturen zu regulieren. Ansatzpunkte hierzu könnten das Wettbewerbsrecht, das Datenschutzrecht, das Produktrecht, das Vergaberecht oder der Grundrechtsschutz sein.

Für das Cloud Computing sind öffentliche Verwaltungen verpflichtet, strategisch souveräne Clouds zu fordern und zu nutzen. Angesichts der Übermacht der zumeist nicht-europäischen Hyperscaler und der Abhängigkeit von ihnen wird Souveränität im Cloud Computing schon angenommen, wenn eine ausreichende Wechselmöglichkeit, Gestaltungsfähigkeit und Einflussmöglichkeiten auf die Cloudanbieter bestehen. Open Source gilt als hilfreich, aber nicht als ausreichend.

Im Hinblick auf die Informationssuche könnte ein durch die Europäische Union geförderter offener Webindex als Basis für neue, unabhängige Suchmaschinen dienen und Innovationen im Bereich der Künstlichen Intelligenz fördern und so den monopolisierten Markt diversifizieren und Pluralität fördern. Ein solcher Index bringt nicht nur technische, sondern auch rechtliche und gesellschaftliche Herausforderungen mit sich, deren Berücksichtigung für eine erfolgreiche Umsetzung entscheidend ist.

Eng mit der digitalen Souveränität gegenüber Big Tech aus den USA ist die geopolitische Position Europas zu sehen, die zwischen den konkurrierenden US-amerikanischen und chinesischen Modellen digitaler Governance verortet werden kann. Während die USA einen Laissez-faire-Ansatz verfolgen und China auf staatliche Kontrolle und Überwachung setzt, strebt die Europäische Union einen eigenständigen „Dritten Weg" mit einem umfassenden regulatorischen Rahmen an, der Menschenrechte, Demokratie und Nachhaltigkeit betont. Durch die Umsetzung der DSGVO und weiterer Digitalrechtsakte, die digitale Infrastrukturen betreffen, will die Europäische Union globale Standards setzen und ihren Einfluss mittels des „Brüssel-Effekts" ausweiten. Die entscheidende Frage hierfür wird sein, ob das europäische Modell als Referenz für digitale Souveränität in den entscheidenden Schwellenländern angesehen wird.

6. Gestaltung von digitalen Infrastrukturen

Der beste Schutz von Freiheit und Demokratie kann erreicht werden, wenn es gelingt, digitale Infrastrukturen so zu entwickeln und zu gestalten,

dass durch sie Freiheit und Selbstbestimmung gestärkt und unerwünschte Entwicklungen vermieden werden. Hierfür ist es notwendig, sich interdisziplinär mit den Gestaltungsherausforderungen und -möglichkeiten digitaler Infrastrukturen auseinanderzusetzten. Diskutiert werden müssen technische, ökonomische, soziale, politische, rechtliche, kulturelle und pädagogische Ansätze, um den Schutz der Privatsphäre und der informationellen Selbstbestimmung unter den Bedingungen digitaler Infrastrukturen weiterzuentwickeln. Dabei sind normative, institutionelle und instrumentelle Konzepte eines freiheitsfördernden Datenumgangs im Kontext digitaler Infrastrukturen zu erörtern. Welche Gestaltungsmöglichkeiten bestehen oder entwickelt werden können, ist die zentrale Frage der meisten Beiträge dieses Bandes.

Zu untersuchen ist, welche relevanten technischen Funktionen adäquate Ergänzungen zur DSGVO darstellen. So ist zum Beispiel zu fragen, inwiefern *Privacy Enhancing Technologies* (PETs) zum Instrument einer globalen Regulierung werden können. Es wäre hilfreich, wenn Wege gefunden werden könnten, wie sie einsetzbar sind, um Selbstbestimmung gegenüber digitalen Infrastrukturen zu sichern. Hierfür wäre erforderlich, geeignet die Voraussetzungen und Rahmenbedingungen für ihre Umsetzung zu finden.

In der Realität werden digitale Infrastrukturen nicht nach grundrechtlichen Erwägungen gestaltet. Vielmehr werden sie nach technischen Anforderungen konstruiert oder entsprechend ökonomischen Zielsetzungen entwickelt. Sicherheits- oder Datenschutzaspekte werden erfahrungsgemäß nachträglich und nachrangig berücksichtigt. Ein späteres Aufsatteln oder Nachrüsten von Eigenschaften oder Funktionen, die Sicherheit und Datenschutz befördern, ist jedoch nicht immer einfach und jedenfalls schwieriger und teurer, als wenn sie von Anfang an berücksichtigt werden, manchmal ist es sogar unmöglich. Wichtig sind daher Untersuchungen, wie der Prozess der Entwicklung von digitalen Infrastrukturen so verändert werden kann, dass diese Aspekte von Anfang an in die Gestaltung einfließen.

7. Transformation der rechtlichen Infrastruktur

Auch der rechtliche Rahmen als Steuerungs- und Gestaltungsmittel für Infrastrukturen ist selbst Teil einer normativen Infrastruktur. Sie wird nicht nur durch Gesetzgebung, Rechtsprechung und Aufsichtsbehörden gezielt weiterentwickelt, sondern verändert sich auch durch die milliardenfachen alltäglichen gesellschaftlichen Praktiken, die sich in der Nutzung digitaler

Infrastrukturen ungezielt ausbilden. Abstrakte Rechtsregeln, die auf praktische Fälle angewendet werden müssen, nehmen in ihrer Konkretisierung auf den praktischen Fall dessen Eigenschaften und Umstände in den Entscheidungssatz mit auf. Dadurch ändert sich allmählich die Bedeutung eines Rechtssatzes über die Zeit mit der Veränderung der gesellschaftlichen Praxis.

Dies ist zum Beispiel deutlich nachzuvollziehen in der normativen Veränderung des Verhältnisses von Sicherheit und Freiheit. Die zunehmende Abhängigkeit von digitalen Infrastrukturen und die steigende Wahrscheinlichkeit von Ausfällen, Anschlägen und Manipulationen sowie das wachsende Schadenspotenzial lassen auch Vorsorge gegen und Bekämpfung von Risiken dringender erscheinen. Solche Entwicklungen verschieben allmählich die Balance zwischen der Nutzung von Technologie zur Förderung individueller Freiheiten und dem Schutz vor Missbrauch und Verletzungen der Privatsphäre.

Sollen solche – oft unbemerkten und ungezielten – Veränderungen des rechtlichen Rahmens vermieden werden, erfordert dies immer wieder eine gezielte und bewusste Transformation der rechtlichen Infrastruktur. Diese kann nicht darin bestehen, einen relevanten Wert zu ignorieren, sondern erfordert eine rechtliche Gestaltung des technischen Entwicklungsprozesses. Zu untersuchen ist, wie effektive Regulierung gestaltet werden kann, um sowohl die Sicherheit als auch die Selbstbestimmung der Nutzer zu stärken und die gesellschaftlichen und rechtlichen Rahmenbedingungen zu verbessern. Dies gelingt nur, wenn Recht auch die Umstände der riskanten gesellschaftlichen Entwicklung in den Blick nimmt. Erforderlich ist daher, die Design- und Entwicklungsprozesse der digitalen Infrastrukturen in den Blick zu nehmen und von Anfang an freiheitsverträgliche und demokratiefördernde Gestaltung einzufordern und durch Prozessgestaltung zu ermöglichen und sicherzustellen.