Smarte Resilienz

Wie Europas Werte in der Digitalisierung gestärkt werden können

BertelsmannStiftung

Smarte Resilienz

Wie Europas Werte in der Digitalisierung gestärkt werden können

Dr. Annegret Bendiek und Prof. Dr. Jürgen Neyer

Impressum
© Juli 2020
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Verantwortlich
Falk Steiner, Bertelsmann Stiftung

Autoren
Dr. Annegret Bendiek und Prof. Dr. Jürgen Neyer

Lektorat
Rudolf Jan Gajdacz, team 4media&event, München

DOI 10.11586/2020019 https://doi.org/10.11586/2020019

Inhalt

1 Vorwort

Europa steht digital unter Druck. Chinas autoritäres Modell und die Marktmacht der USA gelten als Wettbewerbsvorteile im digitalen Wandel. Ein oft gehörter Vorschlag: Europa muss seinen eigenen, einen dritten Weg gehen, der dem Gemeinwohl eine höhere Priorität als in den USA, zugleich aber ein hohes Maß an individueller Freiheit wahrt – anders als in China. Innovation und Ethik sollten auf diesem europäischen Weg miteinander vereinbar und so ein Alleinstellungsmerkmal werden. Nicht wirtschaftliche Zweckbündnisse, sondern das Wertebündnis müssten nun im Vordergrund stehen, um im digitalen Wandel zu bestehen.

Doch welche Werte genau machen eigentlich Europa in digitalen Zeiten aus? Die Antwort auf diese Frage schlägt sich unmittelbar in der Gestaltung unserer Gesellschaft nieder: Wenn digitale Technologien zunehmend den praktischen Rahmen für die Ausübung (oder die Versagung!) von Grundrechten und -freiheiten bilden, stellt dies die Politik vor völlig neue Herausforderungen – und Werteabwägungen. Das Primat der Politik drückt sich in westlich geprägten Gesellschaften im Recht aus – doch was ist das appellierende und oft – wenn überhaupt – erst im Nachgang durchsetzbare Recht in einer Zeit, in der die realen Regeln über das technologische Jetzt gesetzt werden? Was, wenn diese Technologien dabei unter dem Einfluss von Wertemodellen stehen, die mit unseren europäischen Vorstellungen inkompatibel scheinen?

Es gibt viele gute Gründe für die Beschäftigung mit der Frage, wessen Regeln in der Digitalisierung gelten und wer diese Regeln wie setzen und durchsetzen kann. Doch je mehr in Europa Thesen zur eigenen Souveränität und Handlungsfähigkeit, zur Durchsetzung eigener Werte aufgestellt werden, desto drängender wird die besagte Frage: Welche Werte sind dies eigentlich? Sind die europäischen Werte jene, welche in der Charta der Grundrechte der Europäischen Union niedergeschrieben und in den vergangenen Jahren schrittweise vom Europäischen Gerichtshof mit Leben gefüllt worden sind? Sind sie ein Destillat der Europäischen Menschenrechtskonvention? Oder sind sie der (kleinste) gemeinsame Nenner gelebter Praxis in allen EU-Mitgliedstaaten? Sind die europäischen Werte eine Konstante der Digitalisierung oder unterliegen sie vielleicht ihrerseits durch die Digitalisierung rapiden Veränderungen in Wesenskern und praktischer Ausprägung?

Wer international für Europas Werte streiten möchte, kommt um Antworten auf diese Fragen nicht umhin. Sie zu finden, ist alles andere als trivial. Nur wer die Faktoren versteht, die die eigenen Werte in der Digitalisierung beeinflussen, kann auch die Einflüsse externer Wertesysteme verstehen, die mittelbar durch Technologienutzung in unseren europäischen Kontext hineinwirken.

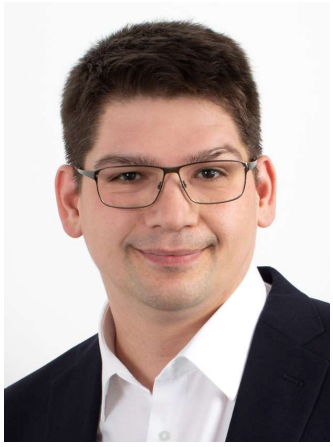
Um möglichen Antworten näher zu kommen, haben wir mit Dr. Annegret Bendiek und Prof. Dr. Jürgen Neyer zwei ausgewiesene Spezialisten um ihre Expertise gebeten. Ihr Konzept der „Smarten Resilienz“ ist ein vielversprechender Ansatz zur Verortung der europäischen Werte in der Digitalisierung. Es arbeitet ihre Herausforderungen, Einflussfaktoren sowie Lösungsansätze klar heraus und bietet den vielbeschworenen Europäischen Werten so einen Interpretations- und Handlungsrahmen, aus dem sich klare politische Schlussfolgerungen ableiten lassen.

Wenn Europa digitalpolitisch handlungsfähiger werden möchte, sind solche konkreten Antworten und Zielsetzungen dringend nötig. Europas Digitalpolitik darf nicht länger von unterschiedlichen nationalen, sektoralen und reaktiven Versatzstücken geprägt werden. Ein erfolgversprechender Europäischer Weg braucht ein konsistentes Gesamtkonzept, dessen Maßnahmen gezielt auf die Stärkung Europäischer Werte einzahlen.

Diese Expertise ist als Teil der einjährigen Exploration Digitalpolitik Gestalten – Towards a Fair Digital Society? entstanden, mit der die Bertelsmann Stiftung seit Sommer 2019 wesentliche Stellschrauben für eine teilhabeförderliche Digitalpolitik in Europa identifiziert hat. In der gleichen Reihe erschienen sind zwei weitere Analysen über Digitale Governance (Wagner und Ferro 2020) und über Europäische Digitalstrategien im Vergleich (Joschua Helmer 2020).

Um den Diskurs und die Debatte über die Ergebnisse dieser Expertise zu erleichtern, veröffentlichen wir sie unter einer freien Lizenz (CC BY-SA 4.0 DE). Wir bedanken uns bei Dr. Annegret Bendiek und Prof. Dr. Jürgen Neyer für die vertrauensvoll produktive Zusammenarbeit; zusammen mit den beiden Autoren würden wir uns über Resonanz und natürlich auch konstruktive Kritik an dieser Publikation sehr freuen.

Falk Steiner
Senior Expert Digitalpolitik
Bertelsmann Stiftung



Ralph Müller-Eiselt
Director Programm Megatrends
Bertelsmann Stiftung

2 Zusammenfassung

Die europäische Werteordnung ist Gegenstand dynamischer Veränderungen. Ein wesentlicher Faktor dieser Veränderung ist der technologische Wandel. Neue Technologien und deren Durchsetzung bringen nicht nur vorherrschende gesellschaftliche Problemverständnisse zum Ausdruck. Unter dem Einfluss der digitalen Transformation, der Einführung und Durchsetzung künstlicher Intelligenzen und allgegenwärtiger Algorithmen, einem sich rasant verändernden Kommunikationsverhalten und grundlegend neuen gesellschaftlichen und politischen Handlungsmöglichkeiten verändert sich auch unsere europäische Werteordnung.

Dieser Veränderungsprozess führt oftmals zu der Befürchtung, dass das europäische Gesellschaftsmodell in einer tiefen Krise sei. Dass wir am Beginn einer neuen Zeit stünden, in der unsere Freiheit von künstlichen Intelligenzen bedroht wird und wir uns aus Bequemlichkeit in unser Schicksal ergeben; dass unser Sinn für gesellschaftliche Verantwortung vor einer umfassenden “Krise des Allgemeinen”[1] kapituliere; dass der Wert der Nachhaltigkeit in Zeiten disruptiver Veränderungen keine Bedeutung mehr haben könnte und dass wir uns vor dem Hintergrund kaum noch zuordenbarer Sicherheitsgefahren in eine digitale Festung Europa zurückziehen müssten.

Im Gegensatz zu diesen Befürchtungen verwenden wir in dieser Expertise zur Beschreibung europäischen Wertewandels den Begriff der „smarten Resilienz“. Sie lässt sich als eine Form der Widerstandsfähigkeit verstehen, die auf die technologische Herausforderung des digitalen Wandels nicht mit dem bloßen Versuch der Bewahrung oder Wiederherstellung eines bereits vergangenen Zustands reagiert, sondern Lernfähigkeit und Adaption beinhaltet.

Die europäische Werteordnung gibt nicht den Wert der Freiheit auf, sondern reinterpretiert ihn als Eröffnung neuer Gestaltungsspielräume; das Verständnis von *Freiheit in Europa individualisiert sich* zunehmend. Der Wert der Verantwortung geht nicht in einer generellen “Krise des Allgemeinen“[2] auf, sondern drückt sich in neuen Formen gesellschaftspolitischen Engagements aus, die es so zu analogen Zeiten noch gar nicht gegeben hat; auch *Verantwortung wird zunehmend als ein individuell zu interpretierender Wert verstanden*. Nachhaltigkeit hat als Wert heute eine zentrale Bedeutung erhalten, auch wenn seine Praxis noch immer höchst defizitär ist; *Nachhaltigkeit gewinnt in der digitalen Transformation neue Relevanz als progressiver Gestaltungsbegriff.* Auch die Idee von Sicherheit löst sich nicht auf, sondern verändert sich; mit der digitalen Transformation hat der *Begriff der Sicherheit eine neue Bedeutung als Schutz von Infrastrukturen* erhalten. Insgesamt verschiebt sich das politische Verhältnis zwischen den vier Werten der Freiheit, Verantwortung, Nachhaltigkeit und Sicherheit im digitalen Wandel *zugunsten der Sicherheit*.

Der in dieser Expertise beschriebene Wandel europäischer Werte in der digitalen Transformation beschreibt keine tief greifende Krise der europäischen Werteordnung, sondern seine konstruktive Adaption. Die europäische Werteordnung der offenen Gesellschaft ist smart resilient. Ihre Resilienz stellt sie dort unter Beweis, wo sie den Kern ihrer Werte bewahrt. Sie ist smart, wo sie anpassungsfähig ist, ohne beliebig zu werden; wo sie innovativ ist, ohne Bewährtes über Bord zu werfen; und wo sie wertbewusst ist, ohne konservativ zu erstarren.

[1] Reckwitz 2017.
[2] ebd.

Smarte Resilienz

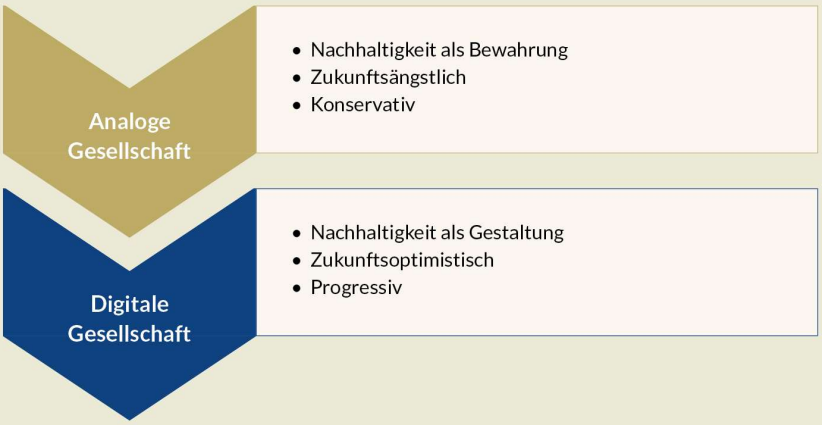
Der Begriff der Resilienz kommt ursprünglich aus der Sozialpsychologie und beschreibt die Fähigkeit von Menschen, mit widrigen Rahmenbedingungen umgehen und sich von Beeinträchtigungen erholen zu können. Er hat in den letzten Jahren verstärkte Anwendung in der Informatik sowie der Analyse technischer und politischer Systeme gefunden. Gerade offene Gesellschaften sind allerdings strukturell dynamisch und lernorientiert. Sie lassen sich mit einem Status-quo-ante-orientierten Begriff weder empirisch erfassen noch angemessen normativ reflektieren. Um diesem dynamischen Umstand moderner Gesellschaften angemessen Rechnung zu tragen, ist es daher hilfreich, von smarter Resilienz zu sprechen. Smartness bezeichnet die Fähigkeit eines Akteurs oder Systems, sich auf veränderte Rahmenbedingungen einzustellen und neue Handlungsmöglichkeiten auszubilden, ohne dabei die eigene Identität zu verlieren.

Smarte Resilienz ist eine regulative Idee im Kant'schen Sinn: Sie beschreibt in idealisierter Weise die Reaktion der offenen Gesellschaft auf die digitale Transformation. Smarte Resilienz bringt die Gleichzeitigkeit von Tradition und Innovation zum Ausdruck: Resilienz steht für Wertegebundenheit und Bewahrung der europäischen Tradition von Humanismus und Aufklärung. Smart steht für Anpassungsfähigkeit an veränderte technologische Rahmenbedingungen. In der Kombination beider Elemente baut der Begriff auf empirisch beobachtbaren Phänomenen auf und interpretiert sie als Momente eines größeren Prozesses. Gleichzeitig ist der Begriff normativ gehaltvoll: Er bietet eine Idee des richtigen Umgehens mit der digitalen Transformation an und kann damit als Angebot an die Politik verstanden werden. Smarte Resilienz kombiniert Wertegebundenheit ohne starres Beharren auf dem Gestrigen, Innovation ohne Missachtung bewahrenswerter Traditionen und Adaptivität ohne normative Beliebigkeit.

Verantwortung in der digitalen Gesellschaft

Quelle: eigene Darstellung | BertelsmannStiftung

Nachhaltigkeit in der digitalen Gesellschaft



Quelle: eigene Darstellung | BertelsmannStiftung

Sicherheit in der digitalen Gesellschaft

Quelle: eigene Darstellung | BertelsmannStiftung

3 Executive Summary

European values constitute a system that is subject to ongoing change. Technological change is a major factor in this change. New technologies and their usage are, on the one hand, an expression of dominant approaches to problems in society. At the same time, our European values are also shaped by developments such as digital transformation, the introduction and implementation of artificial intelligence and ubiquitous algorithms, rapidly changing behavior in communication and fundamentally new opportunities for social and political activity.

This process of change often results in fears that the European social model is facing a profound crisis. Many express the fear that we are entering a new age dominated by an artificial intelligence to which we have – out of complacency – surrendered our fate and which threatens our freedom. Others fear that our sense of social responsibility has capitulated to what Andreas Reckwitz has referred to as a "crisis of the universal," that the value of sustainability may no longer prove meaningful in an era of disruptive change and that, given the prevalence of diffuse security threats, we will be forced to retreat behind the walls of a digital European fortress.

In contrast to such fears, we use the term "smart resilience" in this expert opinion paper to describe the changes underway in European values. This can be understood as a form of resilience that responds to the technological challenge of digital transformation not with an attempt to maintain or restore a *status quo ante* but involves instead the ability to learn and adapt to change.

Within this context, our European value system does not abandon the principle of freedom. Instead, it reinterprets freedom as that which expands opportunities for shaping the world around us as the concept of *freedom in Europe is increasingly an individualized concept*. The principle of responsibility does not simply dissipate amid the crisis of the universal. It is expressed rather in new forms of sociopolitical commitment that were not present in the analog era, because *responsibility is also increasingly understood as a principle subject to individual interpretation*. Sustainability continues to be a crucially relevant principle, despite our failure to apply it in practice. *Sustainability is gaining new relevance in digital transformation as a progressive concept.* Even the concept of security is not eclipsed but has simply changed. With digital transformation, *the concept of security has acquired a new significance that involves the protection of infrastructures*. Overall, in the context of digital transformation, efforts to balance these four principles in policymaking are giving way to an emphasis on the principle of security.

The transformation of European values through digital transformation that is described in this expert opinion paper points to the constructive adaptation of these values – not to a profound crisis of the European value system itself. The European values of an open society are smart in their resilience. They demonstrate their resilience by perserving the core of their principles. They are smart where they adapt without proving arbitrary, where they are innovative without throwing overboard that which is tried and tested, and where they are value-conscious without being conservative.

Smart resilience

With its origins in the field of social psychology, the term resilience describes a person's ability to cope with adverse conditions and to "bounce back" from such adversity. In recent years, the term has found growing use in information science and the analysis of technical and political systems. And yet since open societies in particular are learning-oriented and subject to structural change, a concept anchored in the *status quo ante* will permit neither an empirical account of such societies nor an adequate normative consideration of what they entail. In order to take appropriate account of the dynamic condition of modern societies, it is therefore helpful to speak of smart resilience. Smartness refers to the ability of an actor or system to adapt to changing conditions and to develop new options for action without losing its own identity.

Smart resilience is a regulative idea in the Kantian sense. It describes in terms of an ideal an open society's response to digital transformation. Smart resilience expresses the simultaneity of tradition and innovation. Resilience refers to the adherence to values and the preservation of the European tradition of humanism and enlightenment. Smart refers to adaptability to changing technological conditions. Combining both elements, the term builds on empirically observable phenomena and interprets them as specific moments in a larger ongoing process. At the same time, the term carries normative weight: By providing an idea as to how to deal with digital transformation, it offers policymakers a tenable way forward. The concept of smart resilience expresses a commitment to values without dogged insistence on yesterday's standards, the merit of innovation without disregard for the traditions worth holding on to, and an adaptability without normative arbitrariness.

4 Was sind Werte und wozu braucht man sie?

Die intensive wissenschaftliche Befassung mit Veränderungen der europäischen Werteordnung ist längst überfällig. Bisherige Studien zur digitalen Transformation befassen sich ausführlich mit ihren politischen, ökonomischen, sozialen und kulturellen Aspekten und vernachlässigen die Frage, inwiefern hiervon auch Fragen unseres Verständnisses gültiger Werte berührt werden. Werte sind im gesellschaftlichen Diskurs entstehende abstrakte Orientierungsmarken für die Suche nach Antworten auf die Frage nach dem Richtigen. Sie definieren die Ziele gesellschaftlich erwünschten sozialen Handeln und legen die Basis für die politische und rechtliche Ordnung. Werte sind die Basis des Grundgesetzes und der Grundrechtecharta sowie der Ausgangspunkt für die europäischen Verträge. Sie stellen damit als internationale Rechtordnung wichtige Grundlagen für konkrete Rechtsakte und individuelle Entscheidungen dar. Gesellschaftliche Werte sind dabei gleichzeitig kontinuierlichem Wandel unterworfen. Als „regulative Fiktionen“ stellen sie keine objektiven Fakten dar, sondern sind das Produkt gesellschaftlicher Aushandlungsprozesse und individueller Präferenzen.[3] Sie sind damit notwendig plural, relativ und immer umstritten.

Zentrale analytische Begriffe

Digitalisierung ist die numerische Abbildung von Informationen und Prozessen in Wirtschaft, Politik, Recht und Gesellschaft und damit die Grundlage jeder computerbasierten und algorithmengestützten Gestaltung sozialer Realität.

Werte sind in der Gesellschaft verankerte Festlegungen über wünschenswerte Zustände. Sie sind wesentliche Bezugspunkte für formelle und informelle gesellschaftliche Regeln (Recht und Ethik).

Smarte Resilienz bezeichnet die Fähigkeit eines Systems, mit internen und externen Herausforderungen adaptiv umgehen und seine Funktionsfähigkeit durch eine Kombination von eigener Anpassung und Umweltgestaltung aufrecht halten zu können.

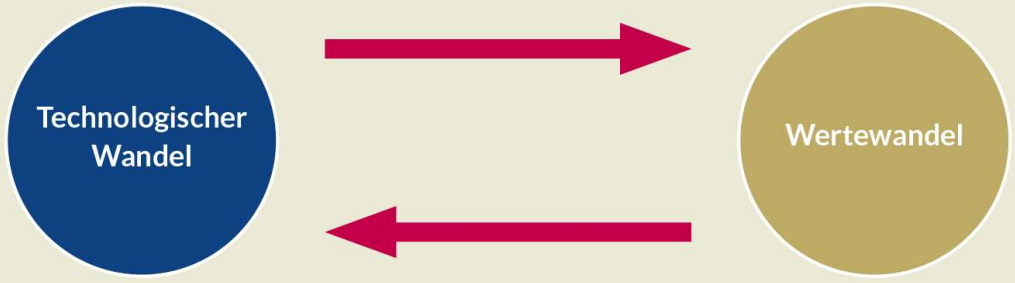
Ein oftmals übersehener Einflussfaktor gesellschaftlichen Wertewandels ist der technologische Wandel. Technologie verändert gesellschaftliche Realität und individuelle Präferenzen. Was wir wollen, hängt auch davon ab, was wir als möglich betrachten und welche Handlungen für uns realisierbar sind. Diese eigenständige Wirkungsmächtigkeit lässt sich quer durch die Technologiegeschichte verfolgen. Bereits der Buchdruck beabsichtigte zwar nur eine ökonomischere Vervielfältigung von Schriften, ermöglichte gleichzeitig aber auch den breiten Zugang der damaligen Gesellschaft zum humanistischen Gedankengut. Er war eine wichtige Bedingung für die Möglichkeit der Reformation, den späteren Prozess der Aufklärung und damit letztlich die Durchsetzung bürgerlicher Vergesellschaftung. Genauso hat die Dampfmaschine ursprünglich zwar nur die Effizienzsteigerung der Arbeit beabsichtigt, letztlich aber den Menschen die Möglichkeit eröffnet, in kürzerer Zeit mehr Güter zu produzieren, Distanzen zu überwinden, Freizeit zu genießen und sich politisch zu engagieren. Technologien haben schon immer vorherrschende gesellschaftliche Praktiken und damit auch Werteordnungen beeinflusst.

Gleiches gilt heute für digitale Technologien. Datenbanken, Algorithmen und die allgegenwärtige Verfügbarkeit von Informationen greifen in die Rahmung unseres Alltags ein und werden Bestandteil des erfahrenen Möglichkeitsraumes sozialen Handelns. Sie werden zu einer „Bedingung der Gegenwartsgesellschaft“[4]. Die Allgegenwart von Kameras an öffentlichen Plätzen, in Bahnhöfen und U-Bahnen wird heute kaum noch als staatlicher bzw. privatwirtschaftlicher Übergriff in individuelle Freiheiten interpretiert, sondern als Notwendigkeit für den Erhalt der öffentlichen Ordnung hingenommen. Viele Menschen gewöhnen sich daran, überwacht und kontrolliert zu werden und das hiermit einhergehende Gefühl von Sicherheit dann zu vermissen, wenn sie außerhalb der Reichweite von Kameras, Auditing, Zertifizierung und Gütesiegeln sind. Ganz ähnlich beginnt der ursprüngliche Widerstand gegen flexible Formen der plattformbasierten Arbeit („Gig Economy“) einer generellen Akzeptanz Platz zu machen, dass

[3] Sommer 2016.
[4] Häußling 2019: 331.

gewerkschaftlich abgesicherte und auf unbefristete Dauer angelegte Arbeitsverhältnisse nur noch ein Modell neben anderen sind.[5] Zum Ausdruck kommt hier, dass Technologie nicht nur von gesellschaftlichen Werten geprägt ist, sondern auch umgekehrt auf diese einwirkt.

ABBILDUNG 1 **Ko-Konstituierung von Technologie und Normen**



Quelle: Jasanoff 2004, eigene Darstellung | BertelsmannStiftung

Der Prozess der Ko-Konstituierung von Technologie und Werten verändert unsere Rezeption von Informationen und damit auch unsere Wahrnehmung von „gewünschter" Realität (Abbildung 1). Wir erschließen uns die Welt zunehmend über Datenbanken und die hier vorhandenen Inhalte. Was sich im Netz oder unseren spezialisierten Datenbanken nicht finden lässt, das gibt es auch nicht. Es verschwindet sozusagen von unserem kognitiven Radar. Im Ergebnis überlagert die Onlinewelt die Offlinewelt so sehr, dass wir letztere oftmals nur noch dort wahrnehmen, wo sie digital abgebildet ist. Online- und Offlinewelt verzahnen sich damit nicht nur, sondern lassen sich in ihrer Kombination als eine geschichtete Konstruktion von Realität verstehen, in der die Abbildung wichtiger für unsere Wahrnehmung von Realität zu werden droht als die Realität selbst. Hier entsteht ein wesentliches Moment des viel zitierten Unbehagens an der Kultur.

Ko-Konstituierung

„Ko-Konstituierung" bezeichnet einen Prozess der wechselseitigen Beeinflussung von technologischen Entwicklungen und der Veränderung von Werten. Werte geben einen Rahmen für technologische Entwicklungen vor und werden selbst wieder von diesen geprägt.

Digitale Modellierungen von Realität erhalten normative Kraft. Sie bilden nicht nur ab, sondern schaffen gleichzeitig auch eine Behauptung „normalen" Handelns. Die Digitalisierung befördert die Durchsetzung einer gesellschaftlichen Rationalität, die auf den Prinzipien von Kalkulation, Effizienz und Objektivität aufgebaut ist. Wir fangen an, uns an ein Bewegen in der Gesellschaft zu gewöhnen, das Beschleunigung und Präzision einen immer höheren Stellenwert einräumt und das die Räume von Redundanz, Entspannung und damit auch Erholung auszudünnen droht. So wie die ubiquitäre Verfügbarkeit der Uhrzeit ab dem 15. Jahrhundert die Rationalisierung und Disziplinierung von Arbeit ermöglichte, so fängt auch heute das technisch Mögliche an, normative Kraft zu entwickeln. Die Digitalisierung ist ein schleichender Prozess der Ökonomisierung von Privatheit. Wir arbeiten nicht mehr nur, während wir im Büro sind, sondern gewöhnen uns daran, 24/7 auch mit unserem privaten Datensatz online verfügbar

[5] Degner und Kocher 2018: 247–265.

zu sein. Die im Zuge der Industrialisierung eingezogenen Abgrenzungen von Arbeit und Privatleben verschwimmen. Viele Geschäftsmodelle basieren auf einer rationalen Professionalisierung des Privaten. Der letzte Blick am Abend und der erste am Morgen gehören dem Handy.

Die Digitalisierung ist ein umfassender Prozess der Umgestaltung sozialer Realität, der Verdichtung und Beschleunigung von Interaktion und der Neuausrichtung normativer Erwartungen.[6] Das, was wir für richtig halten, ist nicht nur das Produkt sozialer Präferenzen und etablierter Denktraditionen, sondern entzieht sich der individuellen Intuition und wird von technologischer Innovation (mit)produziert. Diese Veränderungsprozesse, in denen das Mögliche zum Erwarteten und das Erwartete zum Eingeforderten wird, haben gravierende Konsequenzen für unsere Werteordnung. Sich dieser Veränderung Rechenschaft abzulegen bedeutet gleichzeitig, sich der Grundlagen unserer Gesellschaft und damit unseres Zusammenlebens zu vergewissern.

4.1 Europa im digitalen Umbruch

Die gesellschaftspolitische Analyse dieser Prozesse ist in eine intensive Debatte über die Konsequenzen der digitalen Transformation eingebettet. Auf der einen Seite gibt es ein breites Lager von Stimmen, die den Untergang des demokratisch-rechtsstaatlichen Modells gesellschaftlicher Integration und das Entstehen einer „Übermacht im Netz“[7] diagnostizieren. Die Zukunft würde von einem neuen „Zeitalter des Überwachungskapitalismus“[8] und dem „Ende der Demokratie“[9] geprägt. Die moderne Welt stünde vor einem „Ende der Zukunft“[10] und dem Beginn eines neuen Mittelalters.[11] Es lasse sich ein „Angriff der Algorithmen“[12] und das Entstehen einer „smarten Diktatur“[13] beschreiben, die einen „Angriff auf unsere Freiheit“[14] führt, „alles weiß“[15] und eine „Welt ohne Geist“ zurücklässt.[16] Für Bürger:innen[17] gelte es, in dieser apokalyptischen Welt den „Cyberwar“[18] zu überleben, ein Minimum an Autonomie zu bewahren[19] und im besten Fall aus dem „Datengefängnis“[20] auszubrechen.[21] Spekuliert wird über die Entstehung eines Oligopols von Megakonzernen und Datenmilliardären, die von Robotern geschaffenen Reichtum ernten.[22] Für positive Visionen jenseits eines „digitalen Nihilismus“[23] bleibt hier kein Platz. Der Ausbreitung künstlicher Intelligenz wird die Fähigkeit zugeschrieben, zu einer technologischen Singularität zu führen, in der die maschinelle Intelligenz die kognitiven Fähigkeiten eines erwachsenen Menschen übertrifft. Sie lerne zunehmend, ehrgeizige intellektuelle Aufgaben, wie das Erkennen komplexer Muster, das Synthetisieren von Informationen und das Ziehen von Schlussfolgerungen, auszuführen und damit eine Vielzahl von Arbeitsplätzen überflüssig zu machen. Technische Innovationen, wie die Blockchain, Kryptowährungen wie Libra oder Bitcoin, und immer ausgefeiltere virtuelle Realitäten ermöglichten es Unternehmen, Regierungsbehörden zu entkommen, Unternehmensgewinne in Offshorehäfen zu hinterlegen, in Niedrigsteuerländer zu verschieben und demokratische Vorschriften zu umgehen.

---

[6] Grundlegend hierzu: Jasanoff 2004.
[7] Brodnig 2019; Bostrom 2016.
[8] Zuboff 2018.
[9] Hofstetter 2016a.
[10] Bridle 2019.
[11] ebd.
[12] O´Neil 2017.
[13] Welzer 2016.
[14] ebd.
[15] Hofstetter 2016b.
[16] Foer 2018.
[17] Aus Gründen der Einfachheit und besseren Lesbarkeit verwendet diese Publikation vorwiegend die männliche Sprachform. Es sind jedoch jeweils beide Geschlechter gemeint.
[18] Kurz und Rieger 2018.
[19] Morgenroth 2016.
[20] Lobe 2019.
[21] Burkhardt 2018.
[22] Xiang 2018.
[23] Lovink 2019.

Es ist zwar zweifellos richtig, dass die Digitalisierung bereits heute eine tief greifende Veränderung unserer Gesellschaft bewirkt hat. Keinesfalls ausgemacht ist es allerdings, dass der Alarmismus der aktuellen gesellschaftspolitischen Literatur angemessen ist, um die Reichweite technologischer Veränderungen und ihrer Auswirkungen angemessen zu beschreiben. Die Digitalisierung birgt nicht nur neue Risiken für die Demokratie, sondern trägt auch ein großes Versprechen im Hinblick auf neue Freiheiten und Möglichkeiten der Selbstentfaltung.[24] Individuell bestimmte Arbeitsverhältnisse, raumübergreifende soziale Beziehungen sowie neue Formen des geteilten Eigentums und der Gemeinschaftsbildung werden möglich. Über das Netz organisieren sich politische Willensbildung und politischer Aktivismus. Hier entstehen Formen der kooperativen Kollektivgutproduktion, die noch vor wenigen Jahren undenkbar gewesen wären. Nationale Grenzen und kognitive Begrenztheiten verlieren im Bildungswesen, in der Informationsgewinnung und in der Prägung individueller Lebensstile für viele Menschen immer mehr an Bedeutung.

Über die mittel- und längerfristigen Konsequenzen der Digitalisierung lässt sich daher heute nur spekulieren. Sicher ist allerdings, dass die alte analoge Welt und ihre Werte an Relevanz verlieren. In dieser großen Umbruchsituation drängt sich eine Reihe von grundlegenden Fragen auf, die von zentraler Bedeutung für das europäische Vergesellschaftungsmodells sind: Welchen Stellenwert kann die Freiheit in einer zukünftigen Welt noch haben, in der private Unternehmen und staatliche Autoritäten ausgeprägte Fähigkeiten zur Erfassung, Kontrolle und Steuerung individuellen Handelns haben? Wie werden wir individuell und gesamtgesellschaftlich Verantwortung wahrnehmen, wenn Bürger:innen sich immer stärker als User:innen verstehen? Welchen Stellenwert kann der Wert der Nachhaltigkeit in einer Welt der Disruptionen haben? Und sollten wir dem Wert der Sicherheit eine gleichrangige Bedeutung neben der Freiheit, der Verantwortung und der Nachhaltigkeit beimessen, wenn die Verunsicherung über die Resilienz kritischer Infrastrukturen und die Wahrnehmung ihrer Gefährdung zunimmt? Welche Konsequenzen wird die künstliche Intelligenz für unsere Arbeitsverhältnisse, für unsere Kultur und damit letztlich für unsere ganze Art des Zusammenlebens haben?

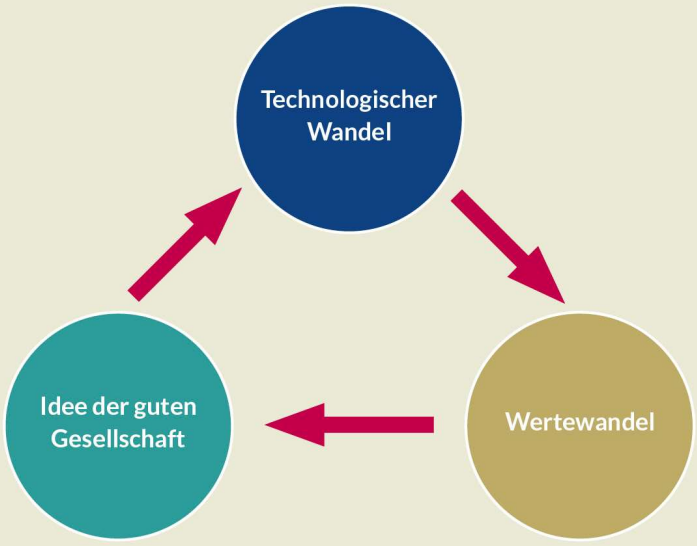
4.2 Werte in Zeiten von Wandel und die Aufgabe Europas

Vor dem Hintergrund dieser Verunsicherungen drängt sich die Frage nach dem normativen Fundament des europäischen Gesellschaftsmodells auf. Welche kodifizierten und nichtkodifizierten Grundwerte sind für die Gestaltung des digitalen europäischen Raumes besonders relevant und wie verändern sich diese unter dem Einfluss der Digitalisierung? Und welchen Einfluss haben hierbei der globale Kontext und die Konkurrenz mit China und den USA?

In Zeiten schnellen technologischen Wandels sind diese Fragen von hoher Bedeutung. Als normative Grundlage unseres Zusammenlebens und als Basis unseres Gesellschaftsmodells verändern sie sich heute vielleicht so schnell und so tief greifend wie seit der industriellen Revolution nicht mehr. Die umfassenden Disruptionen, die mit der Digitalisierung einhergehen, werfen die Frage nach der Gültigkeit und Anpassungsbedürftigkeit unserer Werte und damit auch unseres Gesellschaftsmodells auf. Können wir die Ideen der Freiheit und der Verantwortung weiterhin als Grundlagen unserer Gesellschaftsordnung behandeln, wenn gleichzeitig künstliche Intelligenzen und Algorithmen immer detaillierter in unsere konkreten Lebensabläufe eingreifen und unsere Realitätswahrnehmungen zunehmend von digitalen Datenbanken vorstrukturiert werden? Wie verhalten sich der technologische Wandel, der Wandel gesellschaftlicher Werte und normativ begründete Ideen von der guten Gesellschaft zueinander? Die Frage nach den europäischen Werten im digitalen Raum ist damit auch die Frage nach der Gesellschaft, in der wir leben wollen (Abbildung 2).

[24] So z. B. Shirkey 2010.

ABBILDUNG 2 **Technologie, Werte und die Idee der guten Gesellschaft im Wandel**



Quelle: eigene Darstellung | BertelsmannStiftung

Diese Fragen lassen sich weder in den europäischen Mitgliedstaaten noch auf der internationalen Ebene Erfolg versprechend behandeln. Der europäische Nationalstaat ist aufgrund seiner Einbindung in den Binnenmarkt zu sehr an europäischen Vorgaben ausgerichtet, um inhaltlich autonom agieren zu können. Auf der internationalen Ebene ist die Formulierung eines gesellschaftsübergreifenden Werteverständnisses noch schwieriger. Die USA verfolgen ein Gesellschafts- und Marktmodell, das hochgradig individualistisch ausgerichtet ist und wenig Sensibilität für die wohlfahrtsstaatlichen Traditionen Europas aufweist. Mit China wären normative Einigungsprozesse noch schwieriger. Die hohe gesellschaftliche Bereitschaft, staatliche Überwachungsinstrumente zu tolerieren, sich auf digitale soziale Bewertungssysteme (Social Scoring) einzulassen und der Idee einer harmonischen gesamtgesellschaftlichen Entwicklung Vorrang vor der individuellen Freiheit einzuräumen, zeigt deutlich die Grenzen möglicher normativer Übereinstimmung.

Die Frage nach der Universalität europäischer Werte und ihrer Gültigkeit in anderen Kulturen ist daher alles andere als eine rein philosophische Frage. Sie verweist auf die Notwendigkeit einer europäischen normativen Selbstvergewisserung. Die Europäische Union stellt sich dieser Herausforderung der Etablierung einer spezifisch europäischen digitalen Gesellschaft bereits seit einigen Jahren. Der Europarat[25] und der Europäische Rat[26] befassen sich intensiv mit den Herausforderungen der digitalen Transformation für die europäische Werteordnung. Die Europäische Kommission[27] hat eine Expertengruppe mit der Aufgabe eingesetzt, ethische Leitlinien für eine „vertrauenswürdige KI“[28] zu entwickeln. Der im April 2019 veröffentlichte Abschlussbericht der Gruppe betont die Notwendigkeit, die Autonomie des Menschen zu wahren, Schäden für die Menschen zu vermeiden und die Grundsätze der Fairness und Verständlichkeit zu berücksichtigen.[29] Ebenso fordert der Europäische Rat die Einführung einer „Folgenabschätzung für Menschenrechte“ für KI-Systeme. KI-Systeme sollten verständlich und einfach zu

[25] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (verabschiedet vom Ministerkomitee am 13.2.2019 auf der 1337 Sitzung der abgeordneten Minister). Mehr zu finden unter: https://www.coe.int/en/web/artificial-intelligence.
[26] Council of Europe 2019.
[27] European Commission 2018.
[28] Europäische Kommission 2019 https://ec.europa.eu/germany/news/ki20190408_de
[29] European Commission 2019.

deaktivieren sein.[30] Der Europarat fordert außerdem, dass den technologiebedingten Machtverschiebungen in der Gesellschaft und dem Verhältnis von Staat und Gesellschaft besondere Aufmerksamkeit geschenkt wird.[31]

Deutlich zum Ausdruck kommt in diesen Dokumenten, dass Europa heute weit mehr ist als ein Markt. Es umfasst ein System miteinander verknüpfter Gesellschaften, die trotz aller Unterschiedlichkeiten im Detail auf einem übergreifenden Wertekonsens aufbauen. Dieser bringt sich in der Grundrechtecharta, den gelebten Verfassungspraktiken der Mitgliedstaaten und einer übergreifenden Kultur von Freiheit, Verantwortung, Nachhaltigkeit und Sicherheit zum Ausdruck. Diese vier Werte stehen für eine spezifisch europäische Idee von Gesellschaft, die auf einer Balance von individueller Freiheit und kollektiver Verantwortung aufbaut, die nachhaltiges Wirtschaften als hohes Ziel ansieht und die der öffentlichen Sicherheit eine wichtige Rolle beimisst. Die europäische Werteordnung weist intern hohe Varianzen und regional sehr spezifische Ausprägungen auf. Finnland und Sizilien sind sicherlich nicht identisch. Die übergreifenden Gemeinsamkeiten erscheinen gleichwohl doch recht deutlich, wenn die europäische Werteordnung der sehr viel individualistischer geprägten US-amerikanischen und der sehr viel kollektivistischer geprägten chinesischen Werteordnung gegenübergestellt wird.

[30] Council of Europe 2019.

[31] „(P)articular attention should be paid to the significant power that technological advancement confers to those – be they public entities or private actors – who may use such algorithmic tools without adequate democratic oversight or control", Erklärung des Ministerkomitees über die manipulativen Fähigkeiten algorithmischer Prozesse (verabschiedet vom Ministerkomitee am 13.2.2019 auf der 1337 Sitzung der abgeordneten Minister).

5 Die Werte des digitalen Europas

Der zentrale analytische Begriff für die Beschreibung des europäischen Wertewandels lautet „smarte Resilienz“. Hierunter ist die Fähigkeit des europäischen Gesellschaftsmodells zu verstehen, mit internen und externen Herausforderungen adaptiv umgehen und seine Funktionsfähigkeit durch eine Kombination von eigener Anpassung und bewusster Umweltgestaltung aufrechthalten zu können. Smart zu sein bedeutet in diesem Kontext: anpassungsfähig zu sein, ohne beliebig zu werden; innovativ zu sein, ohne bewährte Werte über Bord zu werfen; und wertbewusst zu sein, ohne konservativ zu erstarren. Diese Herausforderung stellt sich für die EU in den vier großen Wertekontexten von Freiheit, Verantwortung, Nachhaltigkeit und Sicherheit. Alle vier Kontexte sind von zentraler Bedeutung für die Stabilität unserer freiheitlich-demokratischen Ordnung:

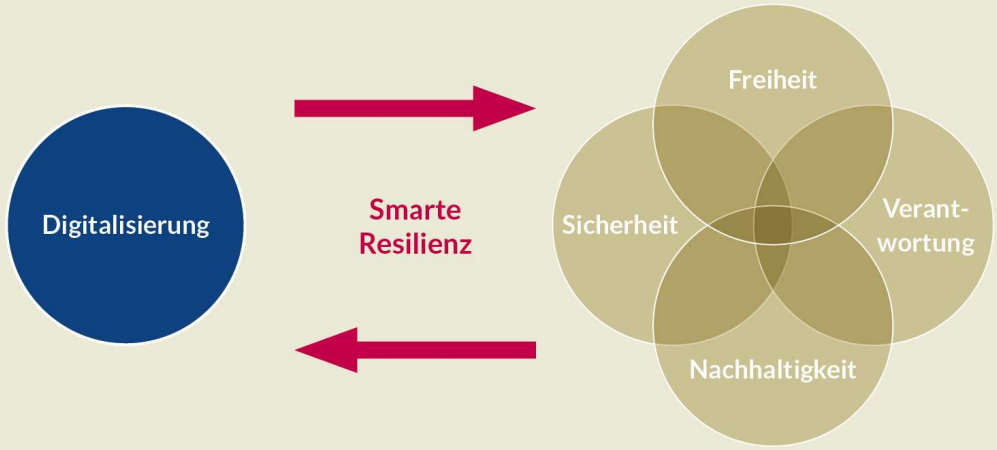
1. *Freiheit* beschreibt die Möglichkeit freier individueller und kollektiver Selbstverwirklichung und sowohl eine positive als auch eine negative Dimension.

2. *Verantwortung* bezieht sich auf die Bereitschaft, eigene Freiheiten für die Gemeinschaft zurückzustellen, und kann sich in Form sozialer Einbindung, ökonomischer Unterstützung und politischer Rücksichtnahme ausdrücken.

3. *Nachhaltigkeit* bedeutet eine wertebasierte Form der Ressourcennutzung, die die Entfaltungsmöglichkeiten zukünftiger Generationen berücksichtigt. Sie ist nicht lediglich konservativ ausgerichtet, sondern beinhaltet eine reflektierte Gestaltung von Realität mit dem Ziel der Eröffnung neuer Entwicklungschancen.

4. *Sicherheit* meint eine Risiken abwägende ungestörte Selbstbestimmung, die durch polizeiliche, militärische und ökonomische Komponenten gewährleistet wird.

ABBILDUNG 3 **Verknüpfung Wertekontext mit Digitalisierung**



Quelle: eigene Darstellung | BertelsmannStiftung

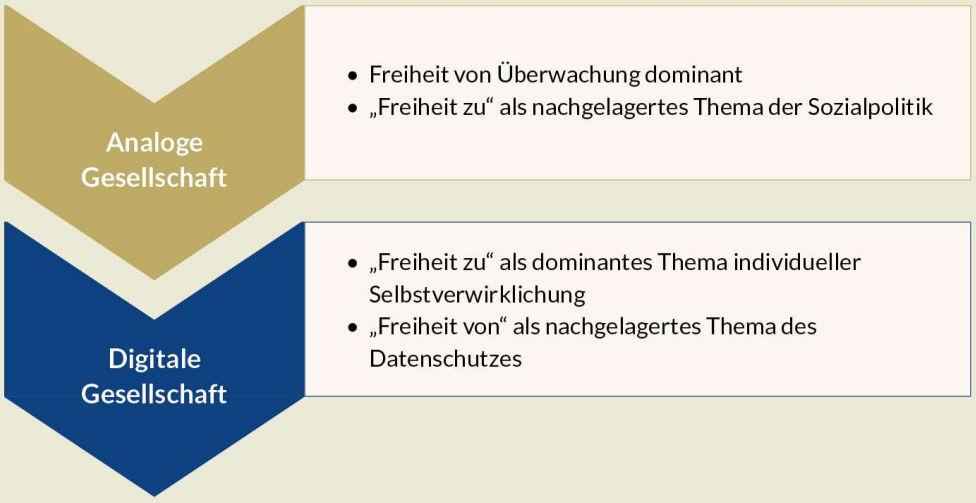
Alle vier Werte sind eng mit dem Begriff der Resilienz verknüpft (Abbildung 3). Die europäische Werteordnung verändert sich in einem dynamischen Prozess der Auseinandersetzung zwischen gesellschaftlichen, politisch-regulatorischen und technologischen Beharrungskräften einerseits und der Emergenz neuer Praktiken, Rechtsakte und technologischen Standards andererseits. Auf allen drei Ebenen gibt es sowohl innovative Prozesse als auch Versuche der Bewahrung. In der Auseinandersetzung zwischen diesen gegenläufigen Kräften entwickelt sich die europäische Werteordnung. Die Rekonstruktion dieses Prozesses wirft ein deutliches Bild auf die „smartness“ einer offenen europäischen Gesellschaft, die ihre Werte grundsätzlich aufrechterhält, ohne sich ihrer gleichzeitigen Adaption und Anpassung an die neuen technologischen Rahmenbedingungen zu verweigern.

5.1 Von der negativen zur positiven Freiheit

Europas Weg aus dem Mittelalter war wesentlich mit der Einräumung von Freiheitsrechten verbunden. In England wurde mit der Magna Charta der erste große Schritt auf diesem Weg gegangen. Auf dem Kontinent war es die revolutionäre These Luthers, dass der Mensch in der Lage sei, seinen Glauben eigenverantwortlich und ohne kirchliche Vermittler auszuüben, die seine Befreiung von kirchlichen Autoritäten einleitete und letztlich zum Prozess der Aufklärung führte. In den großen Verfassungsdokumenten der amerikanischen Bill of Rights, in der französischen Erklärung der Menschen- und Bürgerrechte und den aufklärerischen Schriften von Immanuel Kant, Jean-Jacques Rousseau und vielen anderen fanden diese Prozesse einen weiteren Höhepunkt. Die Freiheit des Einzelnen und die feste Überzeugung, dass das Individuum als vernunftbegabt und selbstbestimmt zu denken ist und unveräußerliche Abwehrrechte gegenüber illegitimen staatlichen oder privaten Übergriffen hat, sollte künftig die Grundlage jeder demokratischen politischen Ordnung in Europa sein. Auch die europäische Integration ist ohne die Idee der Freiheit nicht zu denken. Ihr konzeptionelles Kernstück sind die vier Grundfreiheiten für Waren, Dienstleistungen, Kapital und Personen sowie die Grundrechtecharta.

Auch in der digitalisierten Gesellschaft hat der Wert der Freiheit eine zentrale Rolle. Er strukturiert weite Teile der Debatte über Privatheit und Datenverfügbarkeit, Überwachung und Kontrolle sowie der neuen Möglichkeiten individueller Informiertheit und Kommunikation. Unser heutiges Verständnis von Freiheit hat sich unter dem Einfluss der Digitalisierung gleichwohl weitreichend verändert. Mit Isaiah Berlin lässt sich zwischen der sogenannten negativen Freiheit, die sich auf das Freisein von äußeren und inneren Zwängen bezieht (Freiheit *von*), und der positiven Freiheit, die sich auf unsere Möglichkeiten bezieht, Dinge aktiv zu tun (Freiheit *zu*), unterscheiden (Abbildung 4). Negative Freiheit bezieht sich auf einen Zustand, in dem keine von anderen Menschen ausgehenden Zwänge ein Verhalten erschweren oder verhindern. Positive Freiheit ist hingegen ein Zustand, in dem Menschen miteinander gemeinsam Gesellschaft gestalten können.

ABBILDUNG 4 **Freiheit in der digitalen Gesellschaft**



Quelle: eigene Darstellung | BertelsmannStiftung

5.1.1 Positive Freiheit als dominante Freiheitsinterpretation

Die digitalen Dienstleistungen des Internet haben das gesellschaftlich konsumierbare Ausmaß positiver Freiheit fundamental verändert. Im Vergleich mit den individuellen Kommunikations-, Informations- und Konsummöglichkeiten des 20. Jahrhunderts stellt der heutige digitale Raum eine Vielzahl neuer Möglichkeiten der Selbstentfaltung dar. In Abhängigkeit von der jeweiligen sozialen Bezugsgruppe sind wir auf Instagram, Facebook, Snapchat, WhatsApp oder Twitter unterwegs und organisieren hierüber einen großen Teil unserer privaten oder professionellen Kontakte. Universitäre Seminare werden über Moodle oder andere digitale Lernplattformen angeboten, von

pigeonhole unterstützt und mit Formen des Blended Learning online organisiert. Einkäufe werden über Zalando, Amazon oder andere Anbieter erledigt und nicht mehr Gewünschtes wird über Ebay, Kleiderkreisel oder Foren der Organisation von Nachbarschaft wieder weitergegeben.

Digitale Technologien erlauben ebenfalls neue Formen der intelligenten und ressourcenschonenden Energieversorgung (Smart Grids), der Optimierung von Verkehrsflüssen und der Erhöhung subjektiver Sicherheitswahrnehmungen etwa durch die Installation von Kameras im öffentlichen Raum. Crowdsourcing hat neue Wege der Finanzierung von politischen Anliegen und neuen Unternehmungen eröffnet und erlaubt eine dezentrale und gesellschaftsbasierte Unterstützung von Anliegen, die vorher oftmals an den formalen Hürden der Erteilung von Bankkrediten scheiterten. Digitale Technologien eröffnen neue Möglichkeitsräume positiver Freiheiten, indem sie soziale Koordinationsleistungen erlauben, die in analogen Zeiten noch kaum denkbar waren.

5.1.2 Toleranz für weniger negative Freiheit

Die Selbstverständlichkeit, mit der wir die neuen Möglichkeiten des digitalen Raumes für die Entfaltung positiver Freiheit nutzen, steht in offenem Gegensatz zu der erhöhten gesellschaftlichen Bereitschaft, Einschränkungen negativer Freiheit hinzunehmen. Die Schärfe dieser Differenz wird bei einem Vergleich zwischen der 1987 durchgeführten ersten Volkszählung in Deutschland mit der heutigen gesellschaftlichen Bereitschaft zur Preisgabe persönlicher Daten in den sozialen Medien offensichtlich. Die Ankündigung der Volkszählung 1981 führte innerhalb weniger Wochen zur Gründung von Hunderten von Bürgerinitiativen und breiten Boykottaufrufen. Befürchtet wurden der „Gläserne Bürger“, die schleichende Einführung eines Überwachungsstaates und ein stärkerer Datenaustausch von Polizei und Geheimdiensten. Die damals erfassten Daten muten im Vergleich zu der Tiefe der Informationen, die die meisten Menschen heute bereitwillig im Netz über sich zur Verfügung stellen, vergleichsweise harmlos an. Weder wurden private Kontakte und Freundschaften noch Freizeitaktivitäten, politische oder religiöse Orientierungen oder gar sexuelle Vorlieben abgefragt. Die Daten wurden zudem nur anonymisiert erhoben und nur von staatlichen Stellen ausgewertet. Sie waren weder Gegenstand der Erfassung von Bilderkennungssoftware, Google oder anderer Analyseinstrumente.

Hier hat sich über die Zeit ein Gewöhnungseffekt eingeschlichen, der das Mögliche in das Erwartete transformiert hat. Viele Nutzer:innen von sozialen Medien sind heute ohne größeres Zögern bereit, ihre persönlichen Profile auf kommerziellen Webseiten einzustellen. Die Datenschutzgrundverordnung (DSGVO) zieht hier zwar insofern ein gewisses Schutzniveau für Bürger:innen ein, das Unternehmen darauf verpflichtet, eine Reihe von Grundsätzen, wie die Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit, zu respektieren. Sie kann gleichzeitig aber wenig an der generellen öffentlichen Akzeptanz gegenüber einem Geschäftsmodell ändern, das Informationsdienstleistungen im Austausch gegen das Recht zur Auswertung und Verwendung persönlicher Daten anbietet. Das Gleiche gilt für Kurznachrichten, E-Mails und Sprachnachrichten. Wir senden sie über Server, die außerhalb Europas stehen und damit keine Garantie aufweisen, nicht von der National Security Agency (NSA) oder anderen Nachrichtendiensten gelesen und ausgewertet zu werden. Die allermeisten Nutzer:innen von kommerziellen Webseiten akzeptieren faktisch und ohne größeres Zögern, dass Cookies auf ihren Endgeräten hinterlegt und automatische Nutzerprofile erstellt werden. Datenskandale wie jüngst bei Cambridge Analytica führen kaum zu verändertem Nutzerverhalten, sondern zumeist zu kurzfristiger Empörung gepaart mit langfristigem Schulterzucken.

Die gestiegene gesellschaftliche Bereitschaft, private Daten preiszugeben, dürfte eng mit den expansiven Datenerhebungs- und Verwendungspraktiken von sowohl autoritären als auch demokratischen Staaten zu tun haben. Mit den Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden wurde 2013 deutlich, dass selbst so freiheitliche und die Menschenrechte betonende Staaten wie die Vereinigten Staaten und das Vereinigte Königreich seit spätestens 2007 in großem Umfang die Telekommunikation und insbesondere das Internet global und verdachtsunabhängig überwachen. Rechnernetze wurden von den beiden Regierungen großräumig mit Schadsoftware infiziert, unterseeisch verlegte Glasfaserkabel und Internetknotenpunkte systematisch angezapft und massenweise Telefongespräche abgehört und gespeichert. Und selbst die infolge der auf Snowdens Material basierenden Enthüllungen neu geregelte strategische Fernmeldeüberwachung der Bundesrepublik ist weiterhin

Gegenstand verfassungsrechtlicher Überprüfung. Es war spätestens jetzt offensichtlich, dass der Schutz der Privatsphäre nicht nur von autoritären Staaten wie China oder Russland missachtet wurde, sondern dass selbst demokratische Regierungen im Dienst der Sicherheit grundlegende Freiheitsrechte missachteten und selbst innerhalb der Europäischen Union die gemeinsamen Rechte aller EU-Bürger keineswegs respektiert wurden. Alle diese Enthüllungen haben zwar zu großer Empörung und Medienberichterstattung geführt. Sie haben gleichzeitig aber auch einen Gewöhnungseffekt bewirkt, der mit zu der heute sehr viel größeren Bereitschaft beigetragen haben dürfte, private und staatliche Überwachung zuzulassen.

Ein weiterer Grund für die gestiegene Bereitschaft zur Akzeptanz reduzierter negativer Freiheit dürfte in den technologischen Schwierigkeiten begründet liegen, Datensicherheit und informationelle Selbstbestimmung unter den Bedingungen digitaler Vernetzung überhaupt aufrechtzuerhalten. Die Vielzahl von Datenspuren, die wir heute bewusst oder unbewusst und aktiv oder passiv hinterlassen, ermöglicht ganz neue Formen des Profiling und der Identifizierung einzelner Nutzer:innen. Jedes Mal, wenn wir im Netz unterwegs sind, mit Google Maps unseren Weg finden oder ein Bahnticket kaufen, wenn wir an Videokameras vorbeigehen, zum Arzt gehen und unsere Chipkarte einlesen lassen, hinterlassen wir Datenspuren. Wenn diese unterschiedlichen Datensätze und Informationsquellen miteinander kombiniert werden, dann lassen sich selbst weitgehend anonymisierte Daten häufig Personen eindeutig zuordnen.

Mit der breiten Einführung von künstlicher Intelligenz und vernetzten Geräten (Internet of Things, IoT) könnte dieser Prozess zur Durchsetzung einer Technologie führen, die detaillierte Muster vergangenen Handelns zu erkennen und Prognosen über zukünftiges Handeln zu erstellen erlaubt. Bei hinreichend breiter Datengrundlage lassen sich möglicherweise zukünftig sowohl (wahrscheinliche) kollektive als auch individuelle Handlungen prognostizieren. Manche Autor:innen befürchten hier gar die Entstehung von Kontrollgesellschaften im Sinne von „ultra-schnellen Kontrollformen mit freiheitlichem Aussehen“[32]. Alle derartigen Befürchtungen gehören heute allerdings noch in das Reich der Spekulation. Sie sind letztlich nur dann plausibel, wenn die offene Gesellschaft keine Mechanismen entwickeln sollte, um diesen Gefahren zu begegnen.

5.2 Neue Verantwortung im digitalen Raum

Die Idee der Freiheit hat sich historisch in Europa in enger Auseinandersetzung mit dem Begriff der Verantwortung entwickelt. Die Freiheiten, die die Magna Charta dem englischen Adel einräumte, dienten nicht seiner Verselbstständigung, sondern zielten auf eine verantwortungsvolle Ausübung des Lehnsrechts ab. Die protestantische Freiheit war ebenfalls nicht anarchisch gemeint, sondern kombiniert mit einer Verantwortung gegenüber Gott. In der französischen Revolution firmierte der Begriff des *volonté générale* zentral und damit die Verpflichtung des Einzelnen auf die Befolgung dessen, was als gut und richtig für die ganze Gesellschaft verstanden werden konnte. Die Einbettung der Freiheit in die Verantwortung findet sich heute in so vielen unterschiedlichen Ideen wie der progressiven Besteuerung, der Rücksichtnahme auf Schwächere in der Gesellschaft, der Mülltrennung, dem freiwilligen sozialen Jahr und – zumindest in manchen Mitgliedstaaten – der Wehrpflicht. Auch in der EU treten die Marktfreiheiten in Verbindung mit den Strukturfonds und der hier angelegten Idee einer Verantwortung aller dafür auf, dass die wirtschaftlich schwächeren Mitgliedstaaten in die Lage versetzt werden, am gemeinsamen Binnenmarkt erfolgreich teilzunehmen.

In der digitalisierten Gesellschaft ist der Begriff der Verantwortung ebenfalls zentral. Er steht für kollektives Handeln in netzbasierten Gemeinschaften, für digitalen Aktivismus und für eine Vielzahl neuer Formen gemeinschaftsorientierten Handelns (Abbildung 5). Die Digitalisierung wird dabei zuerst einmal häufig in Zusammenhang mit einer rückläufigen Bereitschaft gebracht, Verantwortung für gesellschaftliche Belange zu übernehmen. Manuel Castells zufolge kommt es in der Netzwerkgesellschaft zu einer zunehmenden Spannung zwischen einem territorialen

[32] Deleuze 1993: 255.

„Raum der Orte“ und einem funktionalen „Raum der Ströme“[33]. Die gut ausgebildete Elite der Programmierer:innen, Manager:innen und sonstigen „Symbolanalytiker“[34] vernetze sich global und entwickle wirtschaftliche, soziale und kulturelle Praktiken, die sich immer weiter von dem politisch bestimmten und ökonomisch und sozial marginalisierten Raum der Orte entferne. Diejenigen, die in der Lage seien, die neue Welt der grenzenlosen Kommunikation im Raum der Flüsse zu meistern, schafften neue Bindungen der Zugehörigkeit und reduzieren frühere nationale Loyalitäten. Viele andere würden in einem zunehmend entkoppelten „Raum der Orte“ zurückgelassen.

ABBILDUNG 5 **Verantwortung in der digitalen Gesellschaft**

Quelle: eigene Darstellung

BertelsmannStiftung

5.2.1 Krise der Verantwortung

Neuere soziologische Analysen wie jüngst von Andreas Reckwitz greifen diese Diagnosen auf und beschreiben eine generelle „Krise des Allgemeinen“[35]. Der Einzelne würde sich zunehmend als egozentrischer Performer in einem Wettbewerb um Aufmerksamkeit präsentieren und habe nur noch wenig Bereitschaft zur Übernahme von sozialer Verantwortung. Alte Klassen- und Gruppenidentitäten verlören mit dem Untergang des Industriekapitalismus an Prägekraft. An ihre Stelle träte ein neues Vergesellschaftungsmodell, das sich um sogenannte „Neo-Communities“"[36] oder „Communities of Practice“[37] organisiere. Felix Stalder beschreibt einen „vernetzten Individualismus“, wonach „… Menschen in westlichen Gesellschaften […] ihre Identität immer weniger über die Familie, den Arbeitsplatz oder andere stabile Kollektive definieren, sondern zunehmend über ihre persönlichen sozialen Netzwerke, also über die gemeinschaftlichen Formationen, in denen sie als Einzelne aktiv sind und in denen sie als singuläre Personen wahrgenommen werden“.[38] Diese neuen sozialen Gruppen weisen im Vergleich zur ehemaligen nationalstaatlichen Gesellschaft des Industriezeitalters einen sehr viel geringeren Verpflichtungsgrad gegenüber der nationalen Gemeinschaft auf. Es sind keine „Erinnerungs-, Erfahrungs- und Traditionsgemeinschaften“[39] mehr und auch keine tief ins kollektive Bewusstsein implantierten „imagined communities“[40]. Die neuen

[33] Castells 1996: 476.
[34] Reich 1991.
[35] Reckwitz 2017.
[36] a. a. O.: 261.
[37] Stalder 2016: 135.
[38] a. a. O.: 144.
[39] Kielmannsegg 2003: 49–84.
[40] Anderson 1983.

partikularen Vergesellschaftungsformen sind vielmehr funktional ausgerichtet und üben nur so lange Verbindlichkeit für ihre Teilnehmer:innen („User:innen“) aus, wie sie vom Einzelnen anerkannt werden.

Die Idee einer von der digitalen Vernetzung beförderten Krise des Allgemeinen wird ebenfalls in den beiden verwandten Begriffen der Filterblase und der Echokammer aufgegriffen. Eli Pariser und Cass Sunstein zufolge bricht der einst allumfassende öffentliche Raum in eine Vielzahl paralleler Echokammern auf, in denen jeder Einzelne sich nur noch solche Diskurspartner:innen aussucht, die das Gleiche denken, die gleichen Vorlieben haben und die gleichen Interessen verfolgen. Der Prozess des öffentlichen Vernunftgebrauches, der ehemals die Vielzahl der unterschiedlichen Meinungen in der Demokratie immer wieder aufs Neue zusammenfügte und „Solidarität unter Fremden“[41] schuf, degeneriere zu einer Vielzahl paralleler Diskursuniversen. Die Bewohner:innen dieser partikularen Universen überzeugten sich nicht mehr von abweichenden Meinungen, sondern bestätigten nur noch ihre Vorurteile. Sie lebten in „Filterblasen“,[42] in denen alles Abweichende und Irritierende ausgefiltert werde. Gemeinschaft entstehe hier nur noch unter Gleichen, ohne dass das Abweichende und Andere mitintegriert würde.[43] In der Konsequenz, so die Befürchtung, bröckle der kommunikative Kitt gesamtgesellschaftlicher Verständigung und dünne sich die Identifikation von Bürger:innen mit der Gesellschaft insgesamt aus. Aus der ehemaligen nationalen Gemeinschaft werde so eine „dissonante Öffentlichkeit“[44] ohne übergreifende Verständigungsfähigkeit.

Einen offensichtlichen regulativen Ausdruck findet diese Reduktion gemeinschaftlicher Ausrichtung in den Politiken der EU. Obwohl es heute immer deutlicher wird, dass die digitale Transformation den Wettbewerbsdruck und die individuellen Anforderungsprofile an gut bezahlte Arbeitsplätze erhöht, gibt es kaum europäische Regelungen, die sich dieses Problems annehmen. Das McKinsey Global Institute schätzt, dass in der näheren Zukunft ungefähr ein Drittel der Aktivitäten für etwa sechzig Prozent der Arbeitsplätze vollständig automatisiert werden kann.[45] KI ermögliche massive Rationalisierungspotenziale in einfachen und routiniert auszuübenden Tätigkeiten. Eine große Anzahl von Personen, die in automatisierbaren Jobs arbeiten, wie z. B. Verwaltungsassistent:innen, Kundendienstmitarbeiter:innen, Buchhalter:innen, Fahrer:innen, Telemarketer:innen, Fastfood-Köchinnen und Köche und Rechtsassistent:innen sowie Elektriker:innen/Mechaniker:innen könnten schon bald überflüssig werden. Autonom fahrende Autos, rein digitale Banken und vollautomatisierte Convenience-Stores sind bereits heute Realität.

Aus der Geschichte der Entwicklung disruptiver Technologien wissen wir gleichwohl, dass technologisch induzierte Rationalisierungseffekte sich mittelfristig nur dann zum Nutzen der breiten Bevölkerung auswirken, wenn diese frühzeitig von entsprechenden Bildungs- und Umschulungsprogrammen begleitet werden.[46] Wenn derartige Maßnahmen unterlassen werden, dann intensivieren sich soziale Fragmentierungsprozesse hingegen mit der Wahrscheinlichkeit zunehmender gesellschaftlicher Gegenreaktionen. Deutlich wird hier, dass die Regulierung des technologischen Fortschritts sich nicht auf Fragen der Sicherheit, Freiheit und ethischen Verantwortung beschränken darf, sondern immer auch ihre sozialen Implikationen mitdenken muss. Ethische Richtlinien sind daher zwar eine notwendige, allerdings keine hinreichende Bedingung für eine angemessene Auskleidung des Spannungsverhältnisses von Freiheit, Verantwortung, Nachhaltigkeit und Sicherheit im Sinne einer Stabilisierung der wohlfahrtstaatlichen Errungenschaften Europas.

5.2.2 Neue Verantwortungsformen

Der hier zum Ausdruck kommende Pessimismus über die Fähigkeit der digitalisierten Gesellschaft, Verantwortung und Gemeinschaftsbewusstsein zu generieren und das nötige Korrektiv zur Freiheit zu betonen, ist nicht unbestritten. Gerade die digitalaffine junge Generation zeichnet sich durch ein hohes Maß an politischem Aktivismus sowohl on- als auch offline aus. Der aktuellen Shell-Jugendstudie zufolge hält es mehr als ein Drittel aller Jugendlichen heute für wichtig, sich politisch zu engagieren; ein Wert, der höher ist als jemals zuvor in den letzten fast zwanzig

[41] Brunkhorst 1997.
[42] Pariser 2012.
[43] Min 2010: 22–35; Norris 2010; Selwyn 2004: 341–362.
[44] Knüpfer, Pfetsch und Heft 2020.
[45] Vgl. auch Bughin et al. 2017.
[46] Frey 2019.

Jahren. Der Protest gegen die Überwachungspraktiken der USA und ihrer europäischen Partner im Zuge der Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden, der Kampf gegen die Einführung von Upload-Filtern und für ein freies Internet bringen regelmäßig Millionen junger Menschen auf die Straße. Die Proteste gegen die Urheberrechtsrichtlinie haben in mehr als 80 Städten in ganz Europa Kundgebungen ausgelöst.[47] Die Bewegung „Fridays for Future“ hat am 15. Mai 2019 weltweit mehr als 1,7 Millionen Demonstrant:innen auf die Straße gebracht. In Deutschland erhielt ein politischer Videoclip des 27-Jährigen Rezo mit dem Titel „Zerstört die CDU“ mehr als 15 Millionen Klicks innerhalb von weniger als zwei Wochen.

Hier entwickelt sich eine neue Form des politischen Aktivismus an der Schnittstelle zwischen analoger und digitaler Welt. Viele analoge politische Praktiken werden durch Onlineaktivitäten überhaupt erst angeregt. Menschen, die nie für etwas gekämpft hätten, können eine geeignete Onlinecommunity finden und so offline soziale Veränderungen und Solidarität fördern. Spezielle Plattformen für den lokalen Gebrauch wie Ozeanhousing oder Nebenan können die lokalen Beziehungen stärken. Eine ganz ähnliche Logik ist in der Teilhabe an der Entwicklung von Open-Source-Software sowie Projekten wie der Wikipedia oder Open Data am Gange. Stalder sieht hier das Potenzial für „eine radikale Erneuerung der Demokratie“[48]. Kommunikationsintensive und horizontale Prozesse ließen sich mit den digitalen Technologien sehr viel effektiver organisieren als noch zuvor. Die ehemals an Koordinierungskosten scheiternde politische Organisation von Betroffenen werde zu einer konkreten Möglichkeit.

Die Digitalisierung ermöglicht ebenfalls eine neue Hinwendung zu Europa. Bürger:innen aus ganz Europa treffen sich heute bei #Europe, #EUelections, #GDPR und Hunderten von anderen Kommunikationsknoten auf Twitter. Sie können individuelle Portfolios von Nachrichten gestalten, kommentieren, mit anderen online diskutieren und damit zu aktiven Prosument:innen für Nachrichten und Debatten werden. YouTube, Twitter, Facebook und viele Onlineoutlets von Offlinezeitungen fügen sich zu einem europäischen öffentlichen Raum zusammen.

Digitale Räume fordern gleichzeitig national verfasste Demokratien heraus. Sie werden meist von oligopolistischen Unternehmen betrieben, wenden nicht offenbarte Algorithmen an und profitieren von der Nutzung privater Daten. Social Bots, Microtargeting und andere Techniken der verzerrenden Beeinflussung von Öffentlichkeit sind relevante Phänomene. Teilnehmer:innen, denen es an der Fähigkeit mangelt, ihre Positionen laut zu formulieren, werden zudem meist ignoriert.[49] Die neuen öffentlichen Räume sind weder macht- noch herrschaftsfrei, sondern bilden in vielen Bereichen die gleichen Verzerrungen ab, die aus der Offlinewelt bekannt sind oder verstärken diese sogar.

Die Digitalisierung der Gesellschaft ist nur sehr verkürzt als eine Verringerung von Verantwortungsübernahme in der Gesellschaft zu verstehen.[50] Sie erlaubt so sehr den Rückzug in private Welten der Selbstbezüglichkeit und des Narzissmus wie die Entwicklung aktiver Prosument:innen in einer zunehmend offenen Gesellschaft.[51] Die grundlegende Erfahrung, andere, auch Fremde, als potenzielle Kooperationspartner:innen zu behandeln, trägt in der digitalisierten Gesellschaft dazu bei, eine über bloße Marktbeziehungen und die Selbstdarstellung hinausgehende neue Qualität sozialer Bindungen zu ermöglichen.[52]

5.3 Nachhaltige Digitalisierung

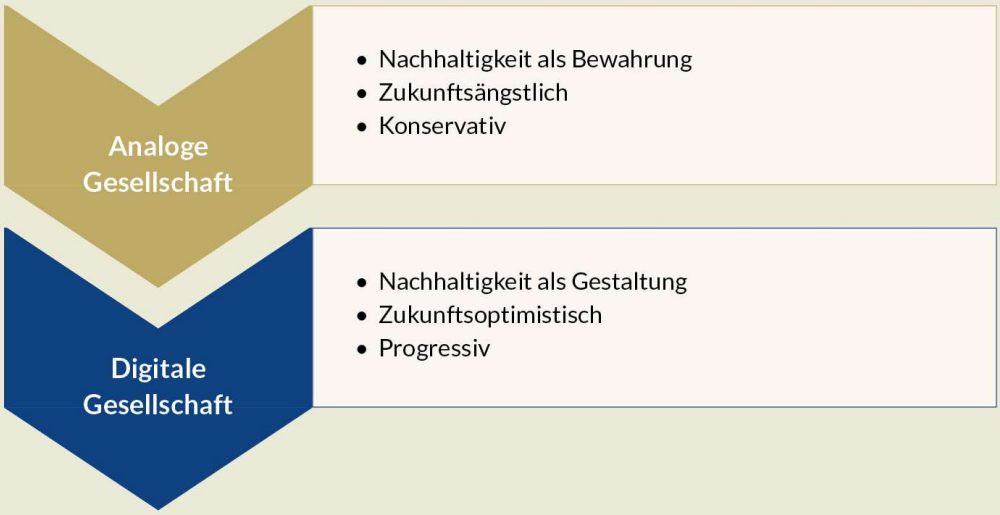
Der Wert der Nachhaltigkeit ist in den letzten Dekaden zu einem Zentralbegriff der modernen Gesellschaft geworden. Mit dem Brundtland-Bericht der Vereinten Nationen wurde 1987 festgehalten, dass jede gegenwärtige Entwicklung die Entfaltungsmöglichkeiten zukünftiger Generationen nicht über Gebühr einschränken dürfe.[53] Die

[47] Biselli 2019.
[48] Stalder 2016: 205.
[49] Blank 2017: 679–697.
[50] Alloway et al. 2014: 150–158.
[51] Siehe auch a. a. O.; Sherman, Michikyan und Greenfield 2013; Vossen und Valkenburg 2016: 118–124.
[52] Benkler 2006: 466–467.
[53] https://www.nachhaltigkeit.info/artikel/brundtland_report_563.html (Download 14.11.2019); https://www.spektrum.de/lexikon/geographie/brundtland-bericht/1267 (Download 14.11.2019).

UN-Konferenz für Umwelt und Entwicklung fügte dem 1992 in Rio de Janeiro die Erkenntnis hinzu, dass ein globaler Umweltschutz nur möglich sei, wenn auch ökonomische und soziale Aspekte berücksichtigt werden. Die EU übernahm im Vertrag von Amsterdam 1997 diese Idee und machte sie damit zu einer normativen Grundlage der weiteren europäischen Integration. Kommissionspräsidentin Ursula von der Leyen erklärte Ende 2019 die Sustainable Development Goals, die Nachhaltigkeitsziele der Vereinten Nationen, zum Leitprinzip ihrer Amtsführung.

Die Digitalisierung hat das vorherrschende Verständnis von Nachhaltigkeit stark beeinflusst. Es ist in den letzten Jahren deutlich geworden, dass das rasante Tempo der technologischen Veränderung jede rein konservative Interpretation verbietet. Nachhaltige Digitalisierung muss entsprechend als ein Auftrag zur wertbezogenen Gestaltung von technologisch induzierten Veränderungsprozessen begriffen werden.

ABBILDUNG 6 **Nachhaltigkeit in der digitalen Gesellschaft**



Quelle: eigene Darstellung | BertelsmannStiftung

5.3.1 Ambivalenzen der Digitalisierung

Es muss von einem grundlegend ambivalenten Verhältnis zwischen Digitalisierung und Nachhaltigkeit ausgegangen werden. Die Digitalisierung kann sowohl zu einem nachhaltigeren Lebensstil als auch zu einer höheren Umweltbelastung und einer Vergrößerung der sozialen Ungleichheit führen. Ein deutliches Beispiel hierfür ist Carsharing. Die Digitalisierung erlaubt zwar einen leichteren Verzicht auf eigene PKWs und erscheint insofern ressourcenschonend durch höhere Auslastung. Gleichzeitig kann die hierdurch gestiegene Attraktivität des Individualverkehrs auch zu einer Verlagerung von Verkehrsströmen weg von der Schiene und hin zu einer weiter intensivierten Straßennutzung führen.

Ambivalenzen finden sich auch in der Landwirtschaft. GPS-gesteuerte Traktoren können mithilfe von Korrektursignalen zentimetergenau geführt werden. Verlässliche Informationen über das Wetter und landwirtschaftliche Nutzflächen sparen ebenfalls Ressourcen. Durch das sogenannte Tiermonitoring kann die Tiergesundheit besser überwacht und mithilfe von Drohnen, die mit einer Infrarot- und Farbkamera ausgestattet sind und über spezielle Software verfügen, können bei der Grasernte Wildtiere besser geschützt werden. Gleichzeitig geht mit allen diesen Schritten die Notwendigkeit einer optimierten digitalen Infrastruktur[54] und eine immer umfassendere Kontrolle des natürlichen Raumes einher. Der erhöhte Energiebedarf und die ausnutzbaren Skaleneffekte der Digitalisierung

[54] Bundesministerium für Ernährung und Landwirtschaft 2018.

dürften zu einer weiteren Industrialisierung der Landwirtschaft und einer Konzentration auf eine begrenzte Zahl von Landwirtschaftsunternehmern führen. Mit Nachhaltigkeit im konservativen Sinn lässt sich das kaum vereinbaren.

Eine der großen Herausforderungen für eine nachhaltige Digitalisierung stellt die Anhäufung von Elektroschrott und deren unsachgemäße Entsorgung dar. Allein in Deutschland werden jährlich durchschnittlich 1,03 Millionen Tonnen Elektroschrott nicht erfasst und dementsprechend nicht richtig entsorgt.[55] Westlicher Elektroschrott landet häufig auf Müllhalden in Afrika, wo Menschen unter unwürdigen Bedingungen und unter Einsatz ihrer Gesundheit versuchen, diesen zu verwerten. Ein wesentlicher Grund für die große Menge an anfallendem Elektroschrott findet sich darin, dass neue Software immer datenintensiver wird und nach entsprechend leistungsfähiger neuer Hardware verlangt.[56] Bei der Herstellung von digitalen Geräten werden große Mengen seltener Ressourcen verwendet. In einem durchschnittlichen Smartphone sind beispielsweise 5 Gramm Kobalt, 22 Gramm Aluminium und 15 Gramm Kupfer enthalten. Hochgerechnet auf die in den letzten zehn Jahren verkauften sieben Milliarden Smartphones ergibt dies eine Masse von 38.000 Tonnen Kobalt, 157.000 Tonnen Aluminium und 107.000 Tonnen Kupfer. 25 Prozent des weltweit gewonnen Silbers werden derzeit in Elektroprodukten verbaut.[57]

Ein weiteres zentrales Problem ist der enorme Stromverbrauch. Allein für die Herstellung von sieben Milliarden Smartphones werden ca. 250 Terrawattstunden (TWh) benötigt. Dies entspricht der jährlichen Stromnachfrage von Schweden oder Polen.[58] Der Stromverbrauch von Informations- und Kommunikationstechnologien (IKT) kann bis zum Jahr 2030 auf 30 bis 50 Prozent der weltweiten Stromversorgung ansteigen. Momentan liegt dieser Wert schon bei rund zehn Prozent. Wenn das Internet ein Land wäre, dann wäre es das Land mit dem sechsthöchsten Energieverbrauch. Allein das Streamen von Videos verursachte im Jahr 2018 den Ausstoß von 306 Tonnen CO_2.[59] Unabdingbar für Informations- und Kommunikationstechniken sind die Rechenzentren. Im Jahr 2016 belief sich der Stromverbrauch der deutschen Rechenzentren auf 12,4 Terrawattstunden (TWh) und weltweit auf 287 TWh. Hierfür benötigte es alleine in Deutschland die Energieproduktion von fünf, weltweit von ca. 40 Großkraftwerken.[60] Nicht zu unterschätzen für das Klima ist auch die Produktion der Kryptowährung Bitcoin. Für die Produktion für das Jahr 2019 wird ein Stromverbrauch von 88,02 TWh pro Jahr berechnet, was einem Stromverbrauch entspricht, der den gesamten Verbrauch Finnlands überschreitet.[61]

Das Internet der Dinge wird diese Entwicklung weiter antreiben. Im Jahr 2022 soll die Vernetzung und somit die Kommunikation der Geräte bereits 6 Prozent des weltweiten Datenverkehrs ausmachen. Smart Homes können auf lange Sicht europaweit den Stromverbrauch um jährlich 70 Terrawattstunden (TWh) erhöhen. Dies entspricht dem Stromverbrauch aller privaten Haushalte Italiens.[62] Durch die Verwendung von Smart Homes könnte zwar ein großer Teil der Energie eingespart werden, allerdings wird auch hierfür wieder die passende Infrastruktur benötigt (Server, Rechenzentren etc.) und ein entsprechender Stromverbrauch zu veranschlagen sein. Die Evolution des automatisierten und autonomen Fahrens dürfte hier noch weitere Dynamik bringen. Autonome Autos brauchen für das Abscannen ihrer Umgebung, die Verwendung von GPS, Sensoren, Radar und die Produktion eigener Daten 20 bis 60 Megabyte lokales Datenvolumen pro Sekunde. Alle diese Dinge ermöglichen zwar einerseits den ressourcensparenden Einsatz von Technologie, benötigen für ihren Unterhalt aber eben auch wieder große Ressourcen.

---

[55] https://www.nabu.de/umwelt-und-ressourcen/abfall-und-recycling/kreislaufwirtschaft/26327.html (Download 14.11.2019).
[56] Lange und Santarius 2018: Kapitel: Leitprinzip 1: Digitale Suffizienz.
[57] a. a. O.: Kapitel: Die materielle Basis von Bits und Bytes.
[58] a. a. O.
[59] https://theshiftproject.org/wp-content/uploads/2019/07/Press-kit_Climate-crisis_The-unsustainable-use-of-online-video.pdf (Download 14.11.2019).
[60] https://www.swr.de/odysso/oekobilanz-des-internets/-/id=1046894/did=21791748/nid=1046894/1jsu4be/index.html (Download 14.11.2019).
[61] https://www.cbeci.org/comparisons/ (Download 25.2.2020).
[62] https://www.borderstep.de/digitalisierung-laesst-stromverbrauch-explodieren/ (Download 19.11.2019).

5.3.2 Nachhaltigkeit als Gestaltungsauftrag

Sehr schnell wird hier deutlich, dass die Digitalisierung keinesfalls automatisch zu einer nachhaltigen Wirtschaftsweise führt, sondern nach klugen Ansätzen ihrer Gestaltung verlangt. Es bedarf der weiteren Umsetzung der Energiewende und der umfassenden Bereitstellung ressourcen- und klimaschonender Energieträger, um den Energiehunger der Digitalisierung nachhaltig stillen zu können. Deutlich ist aber auch schon, dass die Digitalisierung das vorherrschende Verständnis von Nachhaltigkeit verändert hat. Nachhaltigkeit lässt sich nicht einfach als Bewahrung des Gestrigen und Konservierung bestehender Strukturen verstehen. Sie muss vielmehr als Auftrag zur progressiven Gestaltung einer sich rasant verändernden Umwelt verstanden werden, mit dem Ziel, der nächsten Generation möglichst große Entfaltungs- und Entwicklungsmöglichkeiten zu hinterlassen.

5.4 Sicherheit als neue Priorität

Sicherheit als Wert bezieht sich in einem umfassenden Sinn auf die Abwesenheit aktueller und zukünftiger Einschränkungen unserer ungestörten Selbstverwirklichung. Jede faktische oder auch nur befürchtete Einschränkung unserer Freiheit ist so verstanden ein Moment der Verunsicherung. Der Begriff der Sicherheit war bis in die jüngere Zeit kein expliziter gesellschaftspolitischer Wert. Ganz im Gegenteil. Der Begriff der Sicherheit stand seit dem Ende der Religionskriege im 17. Jahrhundert in einer Tradition staatsorientierten, herrschaftsbegründenden und in der Tendenz eher undemokratischen Denkens. Die Staatsräson und ein expansives Verständnis staatlicher Sicherheit lieferten die wesentlichen Rechtfertigungen für den Absolutismus in Europa sowie später für totalitäre Regime in Russland, Nordkorea und einer Reihe anderer Staaten. Für keinen der großen Demokratietheoretiker, von John Locke über Immanuel Kant und Jean-Jacques Rousseau und bis hin zu John Rawls oder Jürgen Habermas hatten sicherheitsbezogene Überlegungen einen zentralen Stellenwert. Sicherheit wurde, wenn überhaupt, dann als Sicherheit vor dem Staat gedacht.[63]

Auch neuere Beiträge zur politischen Theorie thematisierten den Begriff der Sicherheit lange Zeit eher negativ. Die sogenannte Kopenhagener Schule verbindet mit dem Begriff der „Versicherheitlichung“ einen Prozess der Auslagerung von politischen Gegenständen aus dem politischen Diskurs und deren Verlagerung in den Bereich gouvernementaler Diskretion. Versicherheitlichung konstruiert einen Ausnahmezustand, rechtfertigt außerordentliche Maßnahmen und setzt bestehende Entscheidungswege außer Kraft.[64]

Mit den neuen technologischen Möglichkeiten und den hiervon ausgelösten Gefahren im Bereich der Bedrohung kritischer Infrastrukturen und gefährdender Übergriffe auf private Freiheiten könnte sich dieser skeptische Blick auf Sicherheit relativieren. Sowohl auf der nationalen als auch europäischen Ebene ist in den letzten Jahren eine starke Nachfrage nach sicherheitsbetonenden Politiken entstanden. Mögliche negative Konsequenzen für individuelle Freiheitsrechte werden von weiten Teilen der Gesellschaft heute in Kauf genommen. Eine wesentliche Ursache für die Neubewertung des Wertes der Sicherheit findet sich in der Verwandlung moderner Gesellschaften in „Risikogesellschaften“.[65] Sicherheit wird heute zunehmend als Prozess verstanden, als eine kontinuierlich zu gewährleistende Abwehr von oftmals unbekannten Bedrohungen (Abbildung 7). Sicherheit gewinnt damit präventiven Charakter.

---

[63] Benjamin Franklin brachte dieses schwierige Verhältnis der politischen Theorie zum Begriff der Sicherheit auf den Punkt: „Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety” (Pennsylvania Assembly 1756: Reply to the Governor, 11 November 1755, in: Votes and Proceedings of the House of Representatives, 1755–1756, Philadelphia: 19–21, https://founders.archives.gov/documents/Franklin/01-06-02-0107; Download 1.2.2020)

[64] Buzan, de Wilde und Waever 1997.

[65] Beck 2015.

5.4.1 Infrastrukturschutz

Terroristische Angriffe auf kritische Infrastrukturen, schwer attribuierbare Cyberangriffe auf Unternehmen und Behörden, propagandistische Beeinflussungen des öffentlichen Raumes und die Manipulation von Wahlen sind nur die bekanntesten dieser Gefährdungen. Die Wahrnehmung von Unsicherheit in einem unkontrollierbaren Umfeld hybrider Bedrohungen ist zu einem diskursprägenden Paradigma in modernen Demokratien geworden. Die Werte der Freiheit, Toleranz und Offenheit sind zwar grundsätzlich weiter ohne Alternative; in ihrer praktischen Umsetzung müssen sie sich aber daraufhin befragen lassen, wie sie auf das radikal veränderte Umfeld eingestellt werden und sich hier gegen ihre Herausforderungen beweisen können. Die Demokratie ist heute gefordert, sich nicht nur als offen, sondern auch als wehrhaft zu beweisen. Sie muss sowohl ihren Werten verbunden bleiben als auch ihren Herausforderungen begegnen können.

Die Betonung der Sicherheit hat mit der zentralen Rolle von Infrastrukturen in der modernen Gesellschaft zusätzliche Bedeutung erlangt. Wo immer wir uns auch bewegen und was immer wir auch tun, wir sind umgeben von und leben in Infrastrukturen.[66] Das Internet, der Markt, das Straßen- und Verkehrsnetz, das Bildungs- und Forschungssystem und viele andere Infrastrukturen bilden das Rückgrat moderner Gesellschaften, sozusagen ihr unsichtbares Fundament. Infrastrukturen sind für uns so selbstverständlich, dass wir sie oft gar nicht mehr wahrnehmen. Modern zu sein heißt, in den Worten von Paul Edwards, nicht nur mit, sondern in Infrastrukturen zu leben.[67] Die Idee offener Infrastrukturen als demokratiebefördernde Instrumente findet sich heute in den öffentlichkeitsgenerierenden Verfahren der liberalen Demokratie, in öffentlich zugänglichen digitalen Verwaltungen, in nutzergenerierten sozialen Medien, in Open-Source-Software und Datenbanken, in Open Educational Resources, Blockchain-Anwendungen und vielem mehr. Auch große öffentliche Infrastrukturen wie das Stromnetz brauchen sowohl angebots- als auch nutzerseitige Offenheit und Kooperation, um intelligent („smart“) arbeiten zu können. Nur die kommunikative Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Netzbetriebsmitteln ermöglicht eine Optimierung der Energieversorgung auf Basis eines effizienten und zuverlässigen Systembetriebs.

Die Offenheit von kritischen Infrastrukturen ist gleichwohl nicht unproblematisch. Je breiter der Zugang für einen unbegrenzten Konsumentenkreis ist, desto verwundbarer werden Infrastrukturen für Störungen und Angriffe von

[66] Infrastrukturen lassen sich als langfristige Einrichtungen definieren, die den Austausch von materiellen oder immateriellen Gütern ermöglichen.
[67] Edwards 2003: 185–225.

außen.[68] Die Entwicklung riskanter Technologien hat die moderne Gesellschaft in eine „Risikogesellschaft“ transformiert, „in der der Ausnahmezustand zum Normalzustand zu werden droht“.[69] Moderne Infrastrukturen sind gekennzeichnet von Konnektivität (alles ist vernetzt/Kaskadeneffekte), Komplexität (vielfach überlagerte und interdependente Kausalitäten) und damit einhergehender Kontingenz (beschränkte Vorhersehbarkeit). Die zunehmende Konnektivität und Komplexität unterschiedlicher Lebensbereiche haben zu einem Zustand „systemischer Vulnerabilität“[70] geführt. Das Systemversagen ist das Erwartbare geworden, welches das Zufällige infrage stellt.[71] Die Maßgabe lautet, „sich auf das forcierte Bewusstsein ungewisser Zukünfte einzustellen und sich auf das Nichtvorbereitbare vorzubereiten“.[72]

Wenn Sicherheit nicht mehr als Zustand, sondern nur noch als Prozess gedacht werden kann, dann erfordert sie ein Denken in Kategorien permanenter Herausforderung und der Bereitschaft zur Anerkennung struktureller Unsicherheit: Die Fiktion, zukünftige Gefahren vorhersehen zu können, zerfällt endgültig. Wir konnten zwar noch nie wissen, was morgen auf uns zukommen würde, werden uns dieser strukturellen Unsicherheit jetzt aber nochmals bewusster.[73] Nicht bloß Prävention gegenüber dem Wiederauftreten des Bekannten, sondern Reaktionsfähigkeit gegenüber dem Unbekannten ist die zentrale Herausforderung in der Gestaltung moderner offener Infrastrukturen.[74] In der neuen Welt von Konnektivität, Komplexität und Kontingenz kann sich die Frage der sicheren Gestaltung von Infrastrukturen nicht mehr auf die Minimierung von Wahrscheinlichkeit und Risiko beschränken, sondern wird in Begriffen von Möglichkeit und Plausibilität gedacht werden. Das Denken in Kategorien des Konfliktmanagements von der Vorsorge bis hin zur Nachsorge wird abgelöst durch ein Denken in den Kategorien von Resilienz.[75]

5.4.2 Sicherheit als Cybersicherheit

Die Cybersicherheit gilt in der EU als ein Querschnittsthema, das den Binnenmarkt, die Innen- und Justizpolitik sowie die Außen- und Sicherheitspolitik umfasst. In allen diesen Bereichen operiert die EU mit der Betonung hoher Gefährdung und Dringlichkeit der zu ergreifenden Maßnahmen. Diese wahrgenommene Dringlichkeit bringt sich zuerst einmal in der Strategie der EU für den digitalen Binnenmarkt zum Ausdruck. Die Vernetzung der europäischen digitalen Wirtschaft erfordere zusätzliche und für alle Mitgliedstaaten verbindliche Anstrengungen zur Gefahrenabwehr. Insbesondere müsse die Marktintegration weiter vorangetrieben werden, da nur in einem integrierten europäischen Markt für Cybersicherheitsprodukte die nötige Expertise und unternehmerische Wettbewerbsfähigkeit entstünde, um globalen Herausforderungen begegnen zu können. Die EU, so die Europäische Cybersicherheitsagentur (European Network and Information Security Agency, ENISA), sei ein „ICT-Taker und nicht ein ICT-Maker“, der dringend zusätzlicher Maßnahmen bedürfe, um die Widerstandsfähigkeit gegenüber kriminellen oder auch militärischen Angriffen zu erhöhen. Unternehmen müssten daher technologisch in die Lage versetzt und gleichzeitig regulativ dazu verpflichtet werden, Minimumstandards für Cybersicherheit und verbindliche Cyberhygienemaßnahmen umzusetzen.[76]

Mit der europäischen Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) und der Cybersicherheitsverordnung hat die EU eine politikübergreifende Maßnahme zur Gewährleistung von Mindeststandards an Sicherheit in europäischen Netz- und Informationssystemen sowie für Hard- und Software beschlossen.[77] Die

---

[68] Bendiek 2017: 19.
[69] Beck 2015: 31.
[70] Edwards 2013.
[71] Paul Virilio spricht vom „integralen Unfall“: Ob Blackout, Börsencrash oder Bevölkerungsexplosion, ob Stau oder Super-GAU, Server-Breakdown, nervous breakdown oder neuerdings der „Klimakollaps“ – Virilio 2009: 7. Siehe auch Perrow 1999.
[72] Blum et al. 2016: 155.
[73] Vgl. Scharte und Thoma 2016: 123–150 und 132–133.
[74] Vgl. Bendiek 2017: 19, https://www.swp-berlin.org/fileadmin/contents/products/studien/2017S19_bdk.pdf (Download 1.2.2020); Bendiek 2018.
[75] Resilienz wird daher auch als „a technology of governing the unknowable“ verstanden (Kaufmann 2013: 65). Einen guten Überblick über die aktuelle Forschungslandschaft in unterschiedlichsten wissenschaftlichen Disziplinen bieten Wink 2016 sowie Karidi, Schneider und Gutwald 2018.
[76] Bendiek, Bossong und Schulze 2017: 3.
[77] Bendiek und Schallbruch 2019, https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A60_bdk_Schallbruch_WEB.pdf (Download 1.2.2020).

EU-Kommission beschränkt sich in ihrer Sicherheitspolitik nicht auf Fragen der technologischen Resilienz, sondern beansprucht ebenfalls eine Rolle in der Regulierung von kommunikativen Inhalten. Ihr Vorschlag für eine Verordnung zur Unterbindung von terroristischen Inhalten im Internet sieht vor, dass Internetplattformen eine positive Verpflichtung zur Identifizierung und Verhinderung haben und entsprechende Inhalte innerhalb von einer Stunde löschen müssen. Die EU-Grundrechteagentur (FRA) äußerte sich bereits besorgt darüber, dass die Verordnung im Widerspruch zur Meinungsfreiheit stehe. Der Vorschlag sehe zwar formal lediglich vor, „das reibungslose Funktionieren des digitalen Binnenmarkts zu gewährleisten“[78], greife faktisch aber tief in demokratische Grundrechte ein. Wie innere und äußere Sicherheit in einem resilienzbasierten Sicherheitsverständnis ineinandergreifen, bringt sich deutlich in der Europäischen Sicherheitsagenda und dem Ziel der Schaffung einer Sicherheitsunion zum Ausdruck. Lang etablierte Verfassungsprinzipien, wie das Verbot des Einsatzes von Militär im Innern, das Trennungsgebot zwischen polizeilicher und nachrichtendienstlicher Arbeit sowie die parlamentarische Kontrolle des Militärs, werden in der Cybersicherheitspolitik infrage gestellt.

Ob Regierungen offensive Cyberabwehrfähigkeiten auch zur Strafverfolgung in Friedenszeiten miteinschließen müssen, ist politisch umstritten. Das Vorhalten von defensiven und offensiven Cyberabwehrfähigkeiten ist zwar im Rahmen der Bündnisverteidigung in der Nato und EU legitimiert, die damit einhergehenden Gefahren einer Proliferation von Schadsoftware rechtfertigen, so die Kritiker, noch lange nicht die kurzfristigen Vorteile des vermeintlich kurzfristigen größeren Abschreckungspotenzials. Friedensforscher betonen demzufolge die Notwendigkeit, vertrauens- und sicherheitsbildende Maßnahmen der Cyberdiplomatie sowie der Rüstungskontrolle durch die Vereinten Nationen, der OSZE und EU zu forcieren. Cyberverteidigung könne nur ein Element einer gesamtstaatlichen Cybersicherheit darstellen, da sie immer in Gefahr stünde, Eskalationsspiralen zu befördern.

Zusammengenommen entsteht hier das Bild eines sich schleichend verändernden Integrationsprozesses, in dem die Versicherung gegen externe Bedrohungen zur treibenden Kraft von Integration wird. Die EU wird zunehmend zu einer „Resilienzgemeinschaft“, die in der Abwehr externer und interner digitaler Bedrohungen einen zentralen Gegenstand ihres legislativen Handelns sieht. Hiermit gehen sowohl der Anspruch auf neue Kompetenzen für die europäischen Institutionen als auch einer substanziellen Ausdehnung ihres Gestaltungsanspruches einher.

[78] European Union Agency for Fundamental Rights 2019: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf (Download 1.2.2020)

6 Europäische digitale Werte in der Weltrisikogesellschaft

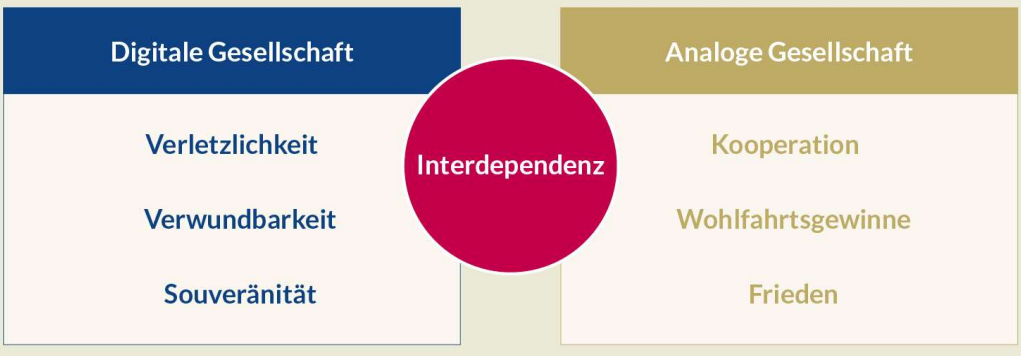
Die europäische Werteordnung verändert sich nicht nur aufgrund innerer Prozesse und Politiken, sondern ist ebenfalls Gegenstand globaler Strukturveränderungen. Die sich in den letzten Jahren zuspitzende politische Konfrontation zwischen den USA und China hat zu einer Neubewertung ökonomischer Verflechtungen und politischer Strukturen geführt. Transnationale Netzwerke in der Finanzpolitik, der Energiepolitik und der Technologiepolitik werden heute kaum noch als Orte globaler Kollektivgutproduktion, sondern zunehmend als Orte harter Machtpolitik und des Ringens um Einfluss verstanden.[79] Sie generierten aufgrund der ungleich verteilten Einflusskanäle und Knotenpunkte die Möglichkeit, Informationsflüsse zu steuern und Interdependenz als Waffe in der internationalen Politik zu benutzen:[80] „Interdependenz, einst als Verhinderer von Konflikten gepriesen, ist zu einem Machtmittel geworden, weil Staaten versuchen, die Asymmetrien in ihren Beziehungen auszunutzen. Sie haben nur zu gut verstanden, dass es gilt, eigene Abhängigkeiten zu reduzieren und das ‚Gleichgewicht des Schadens' in Richtung des Gegners zu verändern, um sich selbst größere Handlungsspielräume zu eröffnen."[81]

6.1 Neue Konflikthaftigkeit

In der alten Welt der Nachkriegszeit hatten ökonomische Interdependenzen eine nur nachgelagerte Bedeutung für Europa. Sie entwickelten sich im Wesentlichen zwischen den Verbündeten der westlichen Welt und waren von einem hohen Maß an Vertrauen begleitet. Die wirtschaftliche Interdependenz mit Russland und China bewegte sich zu keinem Zeitpunkt auf einem Niveau, das als bedrohlich wahrgenommen wurde.

In der digitalen Weltrisikogesellschaft des 21. Jahrhunderts verringert die Digitalisierung die Distanzen zwischen Gesellschaften und führt zu einer intensiveren Begegnung (Abbildung 8). Die weltwirtschaftlichen Verflechtungen haben im Zuge der Globalisierung stark zugenommen und umfassen heute eine ganze Reihe von Produktkategorien, die von strategischer Bedeutung für die europäische Entwicklung, Sicherheit und Werteordnung sind. Diese Verflechtungen in Bereichen wie der Kommunikationsinfrastruktur, der künstlichen Intelligenz oder auch spezialisierten Hochleistungsrechnern sind in vielen Fällen stark asymmetrisch ausgeprägt und finden nur selten europäische Unternehmen als Weltmarktführer. Immer öfter sieht sich die EU daher mit einer Situation konfrontiert, in der sie notwendige Technologie auch dann importieren muss, wenn dieses nur schwer mit dem Wunsch nach „technologischer Souveränität" zu vereinbaren ist.

ABBILDUNG 8 **Interdependenz in der digitalen Weltrisikogesellschaft**



Quelle: eigene Darstellung

BertelsmannStiftung

[79] Leonard 2016: 95: „Schlachtfeld ist die vernetzte Infrastruktur der globalen Wirtschaft und als Waffe dient die Unterbrechung oder Reduzierung unserer globalen Verknüpfungen: Handel und Investitionen, internationales Recht, Internet, Transportwege und Personenfreizügigkeit. Willkommen im Zeitalter der Verknüpfungskriege."
[80] Farrell und Newman 2019: 42–49.
[81] Leonard 2016: 95.

Komplexe digitale Systeme wie die Netzwerkinfrastruktur haben zudem eine hohe Bedeutung für moderne staatliche Souveränität. Sie werden für Jahrzehnte in den Infrastrukturen eines Staates verbaut und drohen bei einer Auftragsvergabe an Unternehmen aus autoritären Staaten, fremder politischer Kontrolle zu unterliegen. Netzwerkprodukte entwickeln sich derzeit zu einer im Wesentlichen durch Software definierten Technologie weiter, deren regelmäßige Updates für den einsetzenden Betreiber:innen kaum nachvollziehbare Funktionalitätsveränderungen bringen. Gleichzeitig verändert die digitale Transformation alle Marktsegmente, von landwirtschaftlichen Produkten über die Medizintechnik bis zum Maschinenbau. Handelsfragen werden immer stärker verschränkt mit dem Ringen um digitale Kontrollfähigkeit.[82]

Die Relevanz der aktuellen wirtschafts- und handelspolitischen Konflikte zwischen den USA, China und der EU geht daher weit über rein ökonomische Fragen hinaus. Digitale Technologien sind die Kommunikationsinfrastruktur hoch entwickelter Informationsgesellschaften. Wer die Kontrolle über Hard- und Software hat, bestimmt auch, wer zu welchem Zeitpunkt und zu welchem Preis Zugriff auf welche Informationen hat. Mit der Digitalisierung geht eine neue Konflikthaftigkeit in der globalen Politik, eine neue Auseinandersetzung um global gültige Standards und damit letztlich auch um die Gültigkeit europäischer Werte einher.

Globale Normen und Regulierungen in Fragen der Cybersicherheit sind nach über zehn Jahren erfolgloser Verhandlungen und in einem Klima der Cyberrivalität zwischen den USA und China nach wie vor weit entfernt. Die Debatten über staatliches Verhalten im Cyberraum, die globale Ächtung oder Beschränkung von Cyberangriffen und eine völkerrechtlich abgesicherte Organisation zur Cyberabwehr wurden zwar in fünf Verhandlungsrunden der Gruppe von Regierungsexperten auf Ebene der Vereinten Nationen (Group of Governmental Experts, GGE) verhandelt, blieben aber erfolglos. In der aufgeladenen Konfliktsituation zwischen den USA und China und aufgrund der erheblichen Interessendivergenzen zwischen liberalen Demokratien und autoritären Staaten sind baldige Fortschritte der derzeitigen Verhandlungsrunden der GGE und der von Russland und China initiierten Open Ended Working Group (OEWG) auch weiter unwahrscheinlich.

Diese neue Konflikthaftigkeit ist eng mit dem Aufstieg Chinas zur technologischen Großmacht verbunden. Über die chinesische Marktmacht erhalten auch die in chinesischer Technologie von beispielsweise Huawei und Zhong Xing Telecommunication Equipment Company Limited (ZTE) beinhalteten Werte Einzug nach Europa. Gesichtserkennungssoftware, Social Scoring und andere Überwachungsinstrumente werden bereits auf dem europäischen Markt angeboten und können leicht von interessierten Staaten (selbst in der Europäischen Union) für die Kontrolle oppositioneller Gruppen angewandt werden. Der Aufstieg der USA zur globalen Hegemonialmacht ging nach 1945 mit einer Ausbreitung des *American Way of Life* einher. Genauso könnte der Aufstieg Chinas eine vergleichbare Attraktivität seines Gesellschaftsmodells nach sich ziehen.

Das chinesische Cybersicherheitsgesetz von 2017 hat in diesem Kontext für viel Irritation gesorgt. Es sieht unter anderem die Registrierung von Vollnamen für Internetnutzer:innen vor und verbietet Virtual Private Networks (VPN), verlangt verschärfte Sicherheitsauflagen für kritische Infrastrukturen und für Anbieter:innen „kritischer Informationsinfrastruktur“. Der Staat behält sich das Recht vor, die privaten Datenschutzansprüche seiner Bürger:innen dann einzuschränken, wenn Fragen der nationalen Sicherheit oder der nationalen Wirtschaft berührt sind. Individuelle Freiheitsrechte stehen hiermit faktisch unter dem Vorbehalt ihrer Vereinbarkeit mit staatlichen Interessen. Hinzu kommt, dass chinesische Unternehmen unter einem Generalverdacht stehen, von der chinesischen Regierung ferngesteuert zu sein oder sich zumindest im Konfliktfall einer derartigen Instrumentalisierung nicht entziehen zu können. Am Streit um den chinesischen Technologiekonzern Huawei ist diese Befürchtung jüngst deutlich geworden.[83] Das Angebot Huaweis, auf dem europäischen Markt den Aufbau der 5G-Infrastruktur mit voranzutreiben, stößt auf massive Vorbehalte seitens der US-amerikanischen sowie einer Reihe europäischer Regierungen. Die US-Regierung betrachtet Huawei als das trojanische Pferd einer gegnerischen Regierung, deren Politik mit den

[82] Vgl. Bendiek und Schallbruch 2019.
[83] Dokumentationen des Konfliktes sind zu finden in Johnson und Groll 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/ (Download 7.7.2019) sowie in Rühlig, Seaman, und Voelsen 2019.

amerikanischen Interessen unvereinbar ist.[84] Der Konflikt um Huawei droht einen grundlegenden Bruch mit der Logik einer globalen Marktwirtschaft zu signalisieren. Er könnte eine neue Phase des internationalen Merkantilismus einleiten, in der der Gewinn einer Partei als identisch mit dem Verlust einer anderen Partei verstanden wird.[85] In dieser neuen Wahrnehmung des Nullsummenaustauschs ist die Konvergenz der Märkte nicht mehr nur eine Chance für Wohlstand, sondern zunehmend eine Bedrohung für die öffentliche Sicherheit. Neue Konzepte wie technologische Souveränität und wirtschaftliche Verwundbarkeit beginnen den Glauben an eine globale Wirtschaftsordnung des gemeinsamen Marktes zu ersetzen.[86]

Die neue Konflikthaftigkeit in der digitalisierten Politik beschränkt sich nicht auf die Beziehungen zwischen dem Westen und China. Auch in den transatlantischen Beziehungen sind die normativen Vorstellungen oftmals nur schwer in Einklang zu bringen.[87] Die viel beschworene transatlantische Wertegemeinschaft kollidiert immer häufiger mit grundlegend unterschiedlichen Vorstellungen zum Umgang mit Daten, der Regulierung des Wettbewerbs und dem Schutz von Privatheit. Während die US-Regierung für ihre Sicherheitsdienste den Zugriff auch auf sensible Daten fordert, im Verhältnis zwischen Konzernen und Konsumenten die Vertragsfreiheit betont und sich gegen die Regulierung des Marktes durch europäische Institutionen wehrt, sind die Europäer stolz darauf, in allen diesen Bereichen ihre eigenen Wertvorstellungen zum Ausdruck zu bringen. Ein klares Beispiel für die zunehmende Kluft zwischen den USA und Europa ist die Reaktion der Regierung Trump auf die Strafen, die die Europäische Kommission Google wiederholt wegen Verstößen gegen das europäische Wettbewerbsrecht auferlegt hat. Unter völliger Missachtung der verfassungsrechtlichen und regulatorischen Gründe für diese Entscheidungen bewertete US-Präsident Donald Trump sie als eine reine Racheaktion einer „tax lady who hates the US".[88] Dies ist mehr als ein Tweet. Es ist ein Beweis für die Lücke zwischen zunehmend schwierig zu vereinbarenden Regulierungsphilosophien auf beiden Seiten des Atlantiks.

6.2 Strategische Autonomie und Verflechtung

Der wachsenden internationalen Konflikthaftigkeit wird in Europa mit der Forderung nach mehr europäischer Eigenständigkeit und der Etablierung einer „strategischen Autonomie der EU"[89] begegnet. Die alte Idee einer globalen liberalen Ordnung, die auf der Basis konsentierter Werte und Normen einen rechtlichen Rahmen globalen Regierens herstellt, tritt immer stärker in den Hintergrund und wird zunehmend von der Forderung nach einem selbstbewussteren Auftreten Europas, verstärkter „Datensouveränität" oder gar „digitalen Grenzkontrollen" überlagert.[90]

Die Debatte über die Frage nach der strategischen Ausrichtung Europas im Wettbewerb mit den USA und China ist allerdings noch lange nicht entschieden. Trotz der Einführung eines Investitions-Screenings von ausländischen Unternehmen im Binnenmarkt und der Vorschläge für eine Industriepolitik bleibt die EU einer multilateralen Handels- und Investitionsordnung verpflichtet, die nicht Abschottung und Autonomie, sondern strategische Verflechtung als zentrales Ziel betont. Die Kommission setzt nach wie vor auf die *Welthandelsorganisation* (WTO) als zentralen Ort der Gestaltung globaler Wirtschaftsbeziehungen und lehnt alle Schritte ab, die die multilaterale Ordnung unterminieren. Auch für die Investitionsbeziehungen vertritt die EU-Kommission weiterhin eine Linie, die das Prinzip der Anwenderneutralität betont und jede Diskriminierung aufgrund nationaler Herkunft ablehnt. Es

[84] Marcus 2019, https://www.bbc.com/news/business-48397081 (Download 25.6.2019).
[85] a. a. O.
[86] Für die Debatte über technologische Souveränität vgl. Benner 2015.
[87] Für eine aufschlussreiche Analyse über die Ursache der Krise der liberalen Ordnung vgl. Ikenberry 2018: 7–23.
[88] https://www.politico.com/news/2019/11/27/margarethe-vestager-eu-tax-promotion-074181 (Download 1.2.2020).
[89] Strategische Autonomie ist „the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society and their institutions", vgl. Timmers 2019: 2.
[90] In Deutschland gibt es mit GAIA-X inzwischen konkrete Pläne, der deutschen und europäischen Industrie eine eigene europäische Datenplattform anzubieten, die nach deutschen Sicherheitsstandards und damit – so die Bundesregierung – „unter vertrauenswürdigen Bedingungen" funktioniert.

müsse anstelle dessen darum gehen, die Kontrolle des Datenverkehrs und eine transparente Softwarebereitstellung zu verbessern, Redundanzen in Mobilfunknetzen zu stärken, Rechenzentren zu dezentralisieren und Monokulturen in Netz- und Systemkomponenten zu vermeiden.[91] Die europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) sowie die Cybersicherheitsverordnung folgen diesem Weg bereits.[92] Die NIS-Richtlinie fördert den Informationsaustausch zwischen den Mitgliedstaaten, um eine rasche und wirksame operative Zusammenarbeit bei Cybersicherheitsvorfällen und den Austausch von Informationen über Risiken zu fördern. Auch beabsichtigt die Cybersicherheitsverordnung, die Resilienz von Produkten, Dienstleistungen und Anwendungen von Informations- und Kommunikationstechnologien (IKT) im Binnenmarkt zu stärken, ohne unnötige Konfrontationen und Abschottungen aufzubauen.

Auch der große Erfolg der Datenschutzgrundverordnung (DSGVO) der EU kann als Beispiel für die Möglichkeit einer Bewahrung europäischer Werte bei gleichzeitiger Verfolgung einer Strategie der Verflechtung verstanden werden. Die DSGVO zielt darauf ab, Unternehmen auf einen sparsamen und Privatheit respektierenden Umgang zu verpflichten. Sie ist damit erst einmal nur auf den europäischen Markt ausgerichtet und beansprucht keine unmittelbare Geltung für außereuropäische Räume, sofern von diesen nicht die Daten von Bürger:innen in der Europäischen Union verarbeitet werden. Gleichzeitig allerdings setzt die DSGVO Maßstäbe, die von vielen Unternehmen außerhalb Europas angewendet werden.[93] Die Auswirkungen der DSGVO auf den US-amerikanischen Markt sind bereits heute für viele Beobachter:innen verblüffend. „Ironically, many Americans are going to find themselves protected from a foreign law“,[94] so Rohit Chopra, der demokratische Kommissar bei der Federal Trade Commission (FTC). Die EU hat sich als die mächtigste Regulierungsbehörde des Silicon Valley herauskristallisiert: Sie ist dort eingetreten, „where Washington has failed or simply has been unwilling – to limit some of the United States' most lucrative and politically influential companies“ (ebd.).

Der wesentliche Grund für diesen sogenannten „Brüssel-Effekt“[95] findet sich zuerst einmal darin, dass es für globale Unternehmen wie Google, Facebook oder Amazon weder eine Option ist, den europäischen Markt zu verlassen, noch ihr Geschäft nach zwei unterschiedlichen gesetzlichen Vorschriften zu organisieren. Die inhärente Mobilität von Daten erfordert de facto eine transnationale Regulierung, auch wenn dies auf einigen Märkten politisch nicht erwünscht ist. Es ist für Unternehmen oftmals weitaus kosteneffizienter, die anspruchsvollen europäischen Vorschriften auf globaler Ebene umzusetzen, als auf unterschiedlichen Märkten mit unterschiedlichen Standards zu operieren. Im Ergebnis erweitert die EU de facto die territoriale Reichweite ihres Datenschutzrechts und stellt starke Anreize für ausländische Marktteilnehmer:innen bereit, sich auch außerhalb der EU an das EU-Recht zu halten. Das Beispiel zeigt, dass in der globalen Produktregulierung die gleiche Logik gilt wie in der EU: Hohe Standards verdrängen niedrige Standards, wenn sie in relevanten Teilmärkten rechtsverbindlich sind.[96]

Ergänzend zu diesem marktbasierten Effekt der Externalisierung europäischer Standards werden Drittländer zunehmend durch bilaterale Abkommen dazu verpflichtet, europäische Datenschutzstandards zu übernehmen. Die EU erlaubt Datenübermittlungen in ein Drittland grundsätzlich nur dann, wenn ein „angemessenes Schutzniveau“ gewährleistet ist, das demjenigen in der EU grundsätzlich gleichwertig ist.[97]

---

[91] Rühlig, Seaman und Voelsen 2019: 4–5.
[92] RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)
[93] Bendiek und Römer 2019: 37.
[94] Romm, Timberg und Birnbaum 2018.
[95] Bradford 2012; Bendiek und Römer 2019.
[96] Vogel 2009: 250.
[97] Die Ernsthaftigkeit, mit der die EU das Ziel verfolgt, ihre Datenschutzstandards auch für Drittstaaten faktisch verbindlich zu machen, kam deutlich in der Stellungnahme des Europäischen Gerichtshofes zum bilateralen Abkommen zwischen der EU und Kanada über Fluggastdatensätze (PNR) zum Ausdruck. Der EuGH hat hier die EU verpflichtet, das Abkommen neu zu verhandeln, da es keinen ausreichenden Datenschutz bieten würde.

Strategische Verflechtung und nicht Abschottung ist daher die Strategie, die mit smarter Resilienz zu vereinbaren ist. Sicherheit wird in diesem Denken als Ergebnis eines Prozesses der ökonomischen und politischen Integration und der Steigerung wechselseitiger Abhängigkeit erreicht. Kooperatives Schnittstellenmanagement wie die gegenseitige Anerkennung in der Produktsicherheit durch Zertifizierung tritt an die Stelle konfrontativer Abgrenzung.

Es gibt Stimmen, die diesen europäischen Weg „naiv“ nennen und befürchten, dass die hohen Standards der EU Wettbewerbsnachteile bedeuten. Konsument:innen wollten effektive Produkte und wären nicht bereit, für anspruchsvolle Standards zu bezahlen. Wie zuvor schon beim Datenschutz stellt sich auch hier die Frage der Relevanz und Durchsetzungsfähigkeit europäischer Vorgaben: Muss Europa erst globaler Technologieführer werden, um sich anspruchsvolle lokale Standards leisten zu können? Ein genauerer Blick auf das Argument zeigt schnell, dass es auf unplausiblen Annahmen beruht. Europa, so die erste Annahme, sei nicht in der Lage, eigenständige Standards zu setzen, da der Ort der Standardsetzung nicht der Binnenmarkt, sondern der Weltmarkt sei. Hier aber würden, so die zweite Annahme, die USA und China so lange dominieren, wie sie die leistungsfähigeren Produkte entwickelten. Diese Vorherrschaft durch Leistungsfähigkeit sei wiederum dadurch begründet, so die dritte Annahme, dass Konsument:innen nicht bereit wären, ethische Standards als Leistungsmerkmale zu bewerten und entsprechend dafür zu bezahlen.

Keine der drei Annahmen hält allerdings einer näheren Überprüfung stand: Die Datenschutzgrundverordnung (DSGVO) hat deutlich gezeigt, dass Europa durchaus in der Lage ist, eigenständig anspruchsvolle Standards zu setzen und ihre Anwendung europaweit zu gewährleisten. Europäische Standards wirken sogar weit über die EU hinaus. Für viele global operierende Konzerne ist es sinnvoller, die anspruchsvollen EU-Regularien global anzuwenden, als für unterschiedliche Märkte mit unterschiedlichen Standards zu operieren. Gerade in Drittmärkten außerhalb Europas, der USA, Chinas und Russlands haben europäische Standards gute Erfolgschancen. Im Bereich der globalen Produktregulierung greift letztlich die gleiche Logik, die sich auch schon bei der Produktregulierung in der EU beobachten ließ: Der sogenannte California-Effekt sorgt dafür, dass hohe Standards niedrige Standards dann verdrängen, wenn sie in relevanten Teilmärkten gesetzlich verbindlich sind. Hiermit ist dann auch die dritte Annahme falsifiziert, dass Konsument:innen nicht bereit wären, für hohe ethische Standards zu bezahlen. Die hohe Qualität europäischer Normen, angefangen bei der Maschinensicherheit und bis hin zur Lebensmittelreinheit, ist eine wesentliche Erfolgsgeschichte der europäischen Integration und ein zentraler Wettbewerbsvorteil gegenüber anderen Regionen. Es gibt wenig Grund zu der Annahme, dass sich diese Logik nicht auch auf digitale Produkte und deren Cybersicherheit übertragen lässt, zukünftig vielleicht auch auf Komponenten künstlicher Intelligenz.

7 Die digitale Werteordnung

7.1 Resümee

Die Digitalisierung hat tief greifende Auswirkungen auf die europäische Werteordnung. Sie stellt eine technologische Umgebung bereit, in der sich sowohl die individuelle Bedeutung der Werte von Freiheit, Nachhaltigkeit, Verantwortung und Sicherheit als auch ihr Verhältnis zueinander verändert. Damit verändert sich die normative Infrastruktur von Gesellschaft insgesamt. Es entsteht eine insgesamt individualistischere, gestaltungsorientiertere und gleichzeitig sich auf Europa zurückbesinnende Gesellschaft. Zur Beschreibung dieses Prozesses bietet sich der Begriff der „smarten Resilienz“ an. Sie lässt sich als eine Form der Widerstandsfähigkeit verstehen, die auf die technologische Herausforderung des digitalen Wandels nicht mit dem bloßen Versuch der Bewahrung oder Wiederherstellung eines bereits vergangenen Zustands reagiert, sondern Lernfähigkeit und Adaption beinhaltet. Die europäische Werteordnung gibt nicht den Wert der Freiheit auf, sondern reinterpretiert ihn als Eröffnung neuer Gestaltungsspielräume. Der Wert der Verantwortung geht nicht in einer generellen Krise des Allgemeinen auf, sondern drückt sich in neuen Formen gesellschaftspolitischen Engagements aus, die es so zu analogen Zeiten noch gar nicht gegeben hat. Nachhaltigkeit hat als Wert heute eine zentrale Bedeutung erhalten, auch wenn seine Praxis noch immer höchst defizitär ist. Auch die Idee von Sicherheit löst sich nicht auf, sondern verändert sich hin zu einem Infrastrukturschutz, der kontinuierlich angepasst werden muss. Im Einzelnen:

- Das Verständnis von *Freiheit in Europa individualisiert sich* zunehmend. Viele Nutzer:innen digitaler Medien scheinen bereit zu sein, erhöhte staatliche und private Kontrollen und Überwachungen (negative Freiheit) im Austausch für größere Gestaltungsmöglichkeiten (positive Freiheit) in Kauf zu nehmen. Freiheit insgesamt verändert damit ihren Charakter. Sie wird zunehmend zu einer individuell interpretierten Größe, deren positive und negative Komponenten interpersonell stark divergieren. Freiheit in Europa dürfte damit langfristig weniger eine Kategorie zur Beschreibung gesamtgesellschaftlicher und mehr zur Beschreibung individueller Lebenszustände werden.

- Auch *Verantwortung wird zunehmend als ein individuell zu interpretierender Wert verstanden*. Während in früheren Dekaden der Begriff der Verantwortung als bürgerliche Pflicht zur materiellen Solidarität innerhalb der nationalen Gemeinschaft verstanden wurde, entstehen im digitalen Raum neue Formen selbstgewählter funktionaler Zugehörigkeit und der Wahrnehmung von Verantwortung. Zum Ausdruck kommt hier weniger eine Krise des Allgemeinen als vielmehr ein Prozess der Restrukturierung politischer Zugehörigkeit. Die nationale Gemeinschaft verliert hier in dem Ausmaß an Zusammenhalt, wie sich neue Räume von Verantwortungswahrnehmung konstituieren.

- Der Wert der *Nachhaltigkeit gewinnt in der digitalen Transformation neue Relevanz als progressiver Gestaltungsbegriff*. Die rasante technologische Veränderung erlaubt keinen rein konservativen Nachhaltigkeitsbegriff mehr, sondern verlangt eine Politik der digitalen Risikofolgenabschätzung von Veränderungen in Gesellschaft und Technologie.

- Mit der digitalen Transformation hat der *Begriff der Sicherheit eine neue Bedeutung als Schutz von Infrastrukturen* erhalten. Die technologischen Möglichkeiten von Überwachung und Kontrolle sowie die qualitativ gestiegene globale Verflechtung haben zu einem spiegelbildlich gestiegenen Bedürfnis nach Sicherheit und Schutz geführt. Die Europäische Union befördert diese Wahrnehmung aktiv und findet gleichzeitig neue Legitimation und Handlungsräume in der Bedienung dieser Nachfrage („l’Europe qui protège“). Sie wandelt sich zunehmend von einer Gestalterin einer offenen Marktgesellschaft hin zu einer politischen Sicherheitsunternehmerin.

- Das politische Verhältnis zwischen den vier Werten der Freiheit, Verantwortung, Nachhaltigkeit und Sicherheit *verschiebt sich zugunsten der Sicherheit*. Politiken der Beförderung negativer Freiheit stehen unter einem wachsenden Legitimationsdruck und müssen sich auf ihre Vereinbarkeit mit

Sicherheitsanforderungen befragen lassen. Zum Ausdruck kommt hier ein doppelter Prozess der erhöhten gesellschaftlichen Bereitschaft zur Nutzung der Versicherungschancen digitaler Technologien sowie der aktiven europäisch-institutionellen Beförderung der Wahrnehmung von Sicherheitsgefährdungen und der Formulierung politischer Antworten. Am politischen Horizont deutet sich heute die Möglichkeit einer europäischen Identität an, die in Begriffen von strategischer Autonomie und technologischer Souveränität denkt und beides als Notwendigkeit einer verstärkten Selbstvergewisserung Europas in einer zunehmend konfliktiven internationalen Umgebung begreift.

7.2 Perspektiven für die weitere Forschung

Die hier präsentierten Erkenntnisse bewegen sich notwendigerweise auf einem hohen Abstraktionsniveau und können weder den unterschiedlichen empirischen Ausprägungen von Wertewandel in einzelnen Politikfeldern und Mitgliedstaaten Rechnung tragen noch das ganze Feld relevanter Werte und deren Wandels ausleuchten. Diese Expertise kann insofern nur den Beginn einer Debatte über die Veränderung grundlegender europäischer Werte unter den Bedingungen der digitalen Transformation darstellen, nicht aber bereits ihr Ende.

7.2.1 Empirische Vergleichsstudien

Die hier präsentierten Ergebnisse tragen weder unterschiedlichen Ausprägungen in den einzelnen Mitgliedstaaten noch Variationen zwischen gesellschaftlichen Gruppen oder zwischen Politikfeldern Rechnung. Es ist durchaus anzunehmen, dass die Wahrnehmung der Veränderung von Werten und ihres Verhältnisses zueinander in den mittel- und osteuropäischen Staaten anders ausgeprägt ist als etwa in Frankreich oder Skandinavien. Denkbar wäre ebenfalls, dass sich zwischen der Dynamik des Wertewandels in der Innen- und in der Außenpolitik gravierende Unterschiede beobachten lassen. Es könnte durchaus sein, dass die Außenpolitik aufgrund ihrer geringeren Nähe zum Grundrechtsschutz noch sehr viel stärker vom Sicherheitsdenken geprägt ist als die Innenpolitik. Genauso gut ließe sich allerdings auch argumentieren, dass gerade in der Innenpolitik kritische Infrastrukturen zu schützen sind und dass deswegen hier größere Dynamiken insbesondere auf Kosten der negativen Freiheit zu erwarten sind. Um hier zu mehr Klarheit zu gelangen, wäre es hilfreich, detailliertere Fallstudien anzustellen, die die Dynamik von Werten und ihre Veränderung sowohl politikfeldspezifisch als auch länderspezifisch erheben und kontrastierend gegenüberstellen.

Sinnvoll wäre ebenfalls die Ergänzung der hier vorgenommenen sozialwissenschaftlichen Betrachtungsweise gesellschaftlichen Wertewandels durch eine stärker kulturwissenschaftliche Analyse. Der mögliche Wandel wichtiger gesellschaftlicher Werte wie Würde, Glück, Harmonie oder Erfolg unter dem Einfluss der Digitalisierung und ihrer Rückwirkungen auf die Entwicklung neuer Technologien wäre eine wichtige zusätzliche Dimension für das Verständnis gesellschaftlichen Wertewandels in der digitalisierten Gesellschaft.

7.2.2 Politik der smarten Resilienz

Smarte Resilienz ist nicht nur ein analytischer Begriff zur Beschreibung der Ko-Konstituierung von gesellschaftlichen Werten und digitaler Technologie, sondern hat auch politisch praktische Bedeutung. Über klug gewählte Instrumente der wertebasierten Technologiegestaltung kann die Politik aktiv die Entwicklung smarter Resilienz fördern. Die Einführung neuer Technologien mit disruptivem Potenzial sollte von Anbeginn begleitet werden durch Maßnahmen der vorausschauenden Technikfolgenabschätzung. Es sollten frühzeitig gesellschaftliche Interessengruppen in den Prozess der Evaluation und gegebenenfalls der proaktiven Entwicklung von Maßnahmen mit dem Ziel eingebunden werden, negative Folgen zu minimieren.

Derartige Politiken existieren bereits. Sowohl die Europäische Union und ihre Institutionen als auch eine Vielzahl von privaten Unternehmen haben Ethikkommissionen eingesetzt, um die Entwicklung künstlicher Intelligenz zu begleiten. Ebenfalls gibt es eine Reihe von Expertisen zu den Gefahren autonomer Fahrzeuge, des Einsatzes von künstlichen Intelligenzen in der Personalgewinnung oder des Einsatzes von Algorithmen zur Kontrolle von Arbeitsabläufen. In der Entwicklung der Datenschutzgrundverordnung (DSGVO) gab es eine intensive Auseinandersetzung mit der organisierten Zivilgesellschaft über ethische Standards und genauso gibt es eine

breite Debatte über die Entwicklung militärischer Drohnen, autonomer Waffensysteme und anderer, potenziell Menschen gefährdender Technologien. Hier finden sich wichtige Ansätze einer Politik der smarten Resilienz.

Was uns bisher allerdings noch fehlt, ist ein systematischer Überblick über die zahlreichen existierenden Digital- und Ethikkommissionen unter der Fragestellung, welche Maßnahmen und Verfahren dafür zuträglich sind, dass Technologieentwicklung ein Maximum an Verantwortung gegenüber der gesellschaftlichen Werteordnung aufweist. Welche Beteiligungsformen und welches Verbindlichkeitsniveau sind nötig, um gleichzeitig gesellschaftliche Akzeptanz zu befördern und die Einhaltung zentraler Werte zu gewährleisten? Wo und im Rahmen welcher Verfahren ergänzen sich private und staatliche Expertise sinnvoll mit dem Ziel, smart resiliente Technologiepolitiken umzusetzen?

7.2.3 Technologische Souveränität und strategische Verflechtung

Ein dritter zentraler Bereich für die weitere Forschung ist die Auseinandersetzung mit dem Begriff und den politischen Inhalten technologischer Souveränität. Es bedarf auf der begrifflichen Ebene einer grundlegenden Klärung dessen, was unter technologischer Souveränität eigentlich verstanden werden soll. Souveränität ist traditionell eine juristische Kategorie, die wenig mit der autonomen Verfügung über Technologie zu tun hat. In seiner aktuellen Verwendung wird der Begriff gleichwohl in einer Vielzahl von hochpolitisierten Kontexten aus der Sicherheitspolitik und als Instrument für die Forderung verwandt, entweder auf der europäischen oder der nationalen Ebene zusätzliche industriepolitische Anstrengungen zu unternehmen, um strategische Unabhängigkeit von den USA und China zu erzielen. In diesem Kontext bedarf es der empirischen Klärung, ob und inwiefern es Politiken der Beförderung technologischer Souveränität ebenfalls in China und den USA gibt und inwiefern die EU genötigt ist, hierauf zu reagieren. Diese Bestandsaufnahme ist von grundlegender Bedeutung für die Beantwortung der Frage, wie sich die europäische Technologiepolitik zu dem Ziel der technologischen Souveränität verhalten soll und ob Europa hier eher ein Getriebener oder selbst zu einer treibenden Kraft geworden ist.

Forschungsbedarf besteht ebenfalls hinsichtlich der Frage, welche gesellschaftlichen und wirtschaftlichen Gruppen in Europa von einer souveränitätsorientierten Technologiepolitik betroffen sein würden. Wer wären die Gewinner:innen und wer die Verlierer:innen? Wie würde sich eine (partielle) Autonomisierung der EU auf Handel, Investitionen und die Sicherheitspolitik auswirken? Und welche längerfristigen Konsequenzen für die multilaterale Ordnung und das globale System der liberalen Welthandelsordnung wären hiervon zu befürchten?

Auf der Basis dieser Erkenntnisse ließen sich letztlich Leitlinien für eine kluge Politik strategischer Verflechtung ableiten. Es wären diejenigen Bereiche zu identifizieren, in denen bewusst wechselseitige Verflechtungen mit dem Ziel angestrebt werden sollten, Abhängigkeiten symmetrisch zu balancieren, um Situationen zu vermeiden, in denen Europa erpressbar werden könnte. Strategische Technologiepolitik sollte sich auf die Förderung von solchen Bereichen konzentrieren und gleichzeitig in möglichst vielen anderen Bereichen die Prinzipien einer offenen und multilateralen Welthandels- und Investitionsordnung hochhalten. In einem klugen Mix aus grundsätzlichem Liberalismus und strategisch angeleiteter Technologiepolitik ließe sich dann möglichweise das Beste der liberalen Ordnung mit dem Notwendigen einer umstrittener werdenden postliberalen Ordnung verbinden.

8 Literaturverzeichnis

Alloway, Tracy, Rachel Runac, Mueez Qureshi und George Kemp (2014). „Is Facebook Linked to Selfishness? Investigating the Relationships among Social Media Use, Empathy, and Narcissism“. *Social Networking* 3. 150–158.

Anderson, Benedict (1983). *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London.

Beck, Ulrich (2015). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Berlin.

Bendiek, Annegret (2018). *Europa verteidigen. Die Gemeinsame Außen- und Sicherheitspolitik der EU*. Stuttgart.

Bendiek, Annegret (2017). *Gemeinsame Außen- und Sicherheitspolitik der EU: Von der Transformation zur Resilienz*. SWP-Studie. Berlin. https://www.swp-berlin.org/fileadmin/contents/products/studien/2017S19_bdk.pdf (Download 1.2.2020).

Bendiek, Annegret, Raphael Bossong und Matthias Schulze (2017). „The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges“. *SWP Comment* No. 47, November 2017.

Bendiek, Annegret, und Magnus Römer (2019). „Externalizing Europe: the global effects of European data protection“. *Digital Policy, Regulation and Governance* (21) 1. 32–43

Bendiek, Annegret, und Martin Schallbruch (2019). „Europas dritter Weg im Cyberraum. Die Cybersicherheitsverordnung der EU“. *SWP-Aktuell* A60. https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A60_bdk_Schallbruch_WEB.pdf (Download 1.2.2020).

Benkler, Yochai (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven CT und London.

Benner, Thorsten (2015). „Technological Sovereignty: Blind Rage Against the US is Not Enough“. *Global Public Policy Institute* 1. Februar. https://www.gppi.net/2015/02/01/technological-sovereignty-blind-rage-against-the-us-is-not-enough (Download 9.3.2020).

Biselli, Anna (2019). „Upload-Filter: Alle Demos auf einen Blick“. https://netzpolitik.org/2019/upload-filter-alle-demos-auf-einen-blick/ (Download 18.6.2019).

Blank, Grant (2017). „The digital divide among Twitter users and its implications for social research“. *Social Science Computer Review* (35) 6. 679–697.

Blum, Sabine, Martin Endreß, Stefan Kaufmann und Benjamin Rampp (2016). „Soziologische Perspektiven“. *Multidisziplinäre Perspektiven der Resilienzforschung*. Hrsg. Rüdiger Wink. Wiesbaden. 151–177.

Bostrom, Nick (2016). *Superintelligenz: Szenarien einer kommenden Revolution*. Berlin.

Bridle, James (2019). *New Dark Age. Der Sieg der Technologie und das Ende der Zukunft*. München.

Bradford, Anu (2012). „The Brussels Effect“. *Northwestern University Law Review* (107) 1.

Brodnig, Ingrid (2019). *Übermacht im Netz. Warum wir für ein gerechtes Internet kämpfen müssen.* Wien.

Brunkhorst, Hauke (1997). *Solidarität unter Fremden*. Frankfurt/M.

Burkhardt, Christoph (2018). *Don't be a Robot. Seven Survival Strategies in the Age of Artificial Intelligence*. St. Gallen/Zürich.

Bughin, Jacques, Eric Hazan, Sree Ramaswamy, Michael Chui, Terra Allas, Peter Dahlström, Nicolaus Henke und Monica Trench (2017). *Artificial Intelligence. The Next Digital Frontier?* MGI Report, McKinsey Global Institute.

Bundesministerium für Ernährung und Landwirtschaft (2018). Digitalisierung in der Landwirtschaft. Chancen nutzen – Risiken minimieren. Bonn.

Buzan, Barry, Jaap de Wilde und Ole Waever (1997). *Security: A New Framework for Analysis*. Boulder CO.

Castells, Manuel (1996). *The Network Society. The Information Age: Economy, Society and Culture*. 1. Auflage. Oxford.

Council of Europe (Hrsg.) (2019). „Unboxing Artificial Intelligence: 10 steps to protect Human Rights". Straßburg. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64 (Download 11.3.2020).

Degner, Anne, und Eva Kocher (2018). „Arbeitskämpfe in der ‚Gig-Economy'? Die Protestbewegungen der Foodora- und Deliveroo-‚Riders' und Rechtsfragen ihrer kollektiven Selbstorganisation". *KJ Kritische Justiz* (51) 3. 247–265.

Deleuze, Gilles (1993). *Unterhandlungen – 1972–1990*. Frankfurt/M.

European Commission (2018). „Artificial Intelligence for Europe, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions", COM(2018) 237 final. Brüssel. https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF (Download 12.3.2020).

Edwards, Paul N. (2013). *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming (Infrastructures)*. Cambridge MA.

Edwards, Paul N. (2003). „Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems". *Modernity and Technology*. Hrsg. Thomas J. Misa, Philip Brey und Andrew Feenberg. Cambridge MA.

European Commission (2019). „ Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence". Brussels. https://ai.bsa.org/wp-content/uploads/2019/09/AIHLEG_EthicsGuidelinesforTrustworthyAI-ENpdf.pdf (Download 12.3.2020).

Farrell, Henry, und Abraham Newman (2019). „Weaponized Interdependence: How Global Economic Networks Shape State Coercion". *International Security* (44) 1. 42–49.

Foer, Franklin (2018). *Welt ohne Geist. Wie das Sillicon Valley freies Denken und Selbstbestimmung bedroht*. München.

Frey, Carl Benedikt (2019). *Technology Trap: Capital, Labor, and Power in the Age of Automation*. Princeton NJ.

Häußling, Roger (2019). *Techniksoziologie. Eine Einführung*. Stuttgart.

Hofstetter, Yvonne (2016a). *Das Ende der Demokratie: Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt*. München.

Hofstetter, Yvonne (2016b). *Sie wissen Alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen*. München.

Ikenberry, G. John (2018). „The End of Liberal International Order? “. *International Affairs* (94) 1. 7–23.

Jasanoff, Sheila (Hrsg.) (2004). *States of Knowledge: The Co-production of Science and the Social Order*. London.

Johnson, Keith, und Elias Groll (2019). „The Improbable Rise of Huawei. How did a private Chinese firm come to dominate the world’s most important emerging technology? “. *Foreign Policy* 3.4. https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/ (Download 7.7.2019).

Kaufmann, Mareile (2013). „Emergent Self-Organisation in Emergencies: resilience Rationales in interconnected Societies“. *Resilience. International Policies, Practices and Discourses* (1) 1. 53–68.

Karidi, Maria, Martin Schneider^und Rebecca Gutwald (Hrsg.) (2018). *Resilienz. Interdisziplinäre Perspektiven zu Wandel und Transformation*. Wiesbaden.

Kielmannsegg, Peter Graf (2003). „Integration und Demokratie“. *Europäische Integration*, Hrsg. Markus Jachtenfuchs und Beate Kohler-Koch. Wiesbaden.

Knüpfer, Curd, Barbara Pfetsch und Annett Heft (2020). „Demokratischer Wandel, dissonante Öffentlichkeit und die Herausforderungen vernetzter Kommunikationsumgebungen“. *Digitale Demokratie*. Hrsg. Isabelle Borucki und Michael Oswald. Berlin.

Kurz, Constanze, und Frank Rieger (2018). *Cyberwar. Die Gefahr aus dem Netz*. München.

Lange, Steffen, und Tilman Santarius (2018). *Smarte Grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit*. München.

Leonard, Mark (2016). „Interdependenz als Waffe. Die EU muss die Zeichen der geoökonomischen Zeit erkennen“. *Internationale Politik* 2. 94–103.

Lobe, Adrian (2019). *Speichern und Strafen. Die Gesellschaft im Datengefängnis*. München.

Lovink, Geert (2019). *Digitaler Nihilismus. Thesen zur dunklen Seite der Plattformen*. Bielefeld.

Marcus, Jonathan (2019). „What the Huawei battle tells us about US-China relations“. *BBC News* 25.5. https://www.bbc.com/news/business-48397081 (Download 25.6.2019).

Min, Seong-Jae (2010). „From the Digital Divide to the Democratic Divide: Internet Skills, Political Interest, and the Second-Level Digital Divide in Political Internet Use“. *Journal of Information Technology & Politics* (7) 1. 22–35.

Norris, Pippa (2010). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. New York NY

Morgenroth, Markus (2016). *Sie kennen Dich. Sie haben Dich. Sie steuern Dich. Die wahre Macht der Datensammler*. München.

O´Neil, Cathy (2017). *Angriff der Algorithmen. Wie sie Wahlen manipulieren, Berufschancen zerstören und unsere Gesundheit gefährden*. München.

Pariser, Eli (2012). *Filter Bubble: Wie wir im Internet entmündigt werden*. München.

Perrow, Charles (1999). *Normal Accidents. Living with High-Risk Technologies*. Princeton NJ.

Reckwitz, Andreas (2017). *Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne*. Berlin.

Reich, Robert (1991). *Work of Nations: Preparing Ourselves for 21st Century Capitalism*. New York NY.

Romm, Tony, Craig Timberg und Michael Birnbaum (2018). „Europe, not the U.S., is now the most powerful regulator of Silicon Valley". *The Washington Post* 25 Mai.

Rühlig, Tim, John Seaman und Daniel Voelsen (2019). „5G and the US-China Tech Rivalry – a Test for Europe's Future in the Digital Age". *SWP Comment* 29.

Scharte, Benjamin, und Klaus Thoma (2016). „Resilienz – Ingenieurwissenschaftliche Perspektive". *Multidisziplinäre Perspektiven der Resilienzforschung*. Hrsg. Rüdiger Wink. Wiesbaden. 123–150.

Sherman, Lauren E., Minas Michikyan und Patricia M. Greenfield (2013). „The effects of text, audio, video, and in-person communication on bonding between friends". *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (7) 2, article 3.

Shirkey, Clay (2010). *Cognitive Surplus: Creativity and Generosity in a Connected Age*. London.

Selwyn, Neil (2004). „Reconsidering Political and Popular Understandings of the Digital Divide". *New Media Society* (6) 3. 341–362.

Sommer, Andreas Urs (2016). *Werte. Warum man sie braucht, obwohl es sie nicht gibt*. Stuttgart.

Stalder, Felix (2016). *Kultur der Digitalität*. Berlin.

Timmers, Paul (2019). „Ethics of AI and Cybersecurity When Sovereignty is at Stake". *Minds and Machines* 29. 635–645.

Virilio, Paul (2009). „Der integrale Unfall". *Die Unordnung der Dinge. Eine Wissens- und Mediengeschichte des Unfalls*. Hrsg. Christian Kassung. Bielefeld.

Vogel, David (2009). *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Cambridge MA.

Vossen, Helen G.M., und Patti M. Valkenburg (2016). „Do social media foster or curtail adolescents' empathy? A longitudinal study". *Computers in Human Behavior* 63. 118–124.

Welzer, Harald (2016). *Die smarte Diktatur. Der Angriff auf unsere Freiheit*. Frankfurt/M.

Wink, Rüdiger (Hrsg.) (2016). *Studien zur Resilienzforschung*. Wiesbaden.

Xiang, Feng (2018). „AI will spell the end of capitalism". *The Washington Post* 3.5. https://www.washingtonpost.com/news/theworldpost/wp/2018/05/03/end-of-capitalism/?noredirect=on&utm_term=.6d94e627b16e Download 8.7.2019).

Zuboff, Shoshana (2018). *Das Zeitalter des Überwachungskapitalismus*. Frankfurt/New York.

9 Index

10 Abkürzungsverzeichnis

DSGVO	Datenschutzgrundverordnung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
ENISA	Agentur der Europäischen Union für Cybersicherheit
FRA	Agentur der Europäischen Union für Grundrechte
FTC	Federal Trade Commission
GGE	Group of Governmental Experts
ICT	Information and Communication Technology
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
KI	Künstliche Intelligenz
NIS	Netz- und Informationssicherheit
NSA	National Security Agency
OSCE	Organization of Security and Cooperation in Europe
PNR	Passenger Name Record (Fluggastdatensätze)
OEWG	Open-ended Working Group
TWh	Terrawattstunden
VPN	Virtual Private Networks
WTO	World Trade Organization (Welthandelsorganisation)
ZTE	Zhong Xing Telecommunication Equipment Company Limited

11 Über die Autoren

Dr. Annegret Bendiek ist Politikwissenschaftlerin in der Forschungsgruppe „EU/Europa“ bei der Stiftung Wissenschaft und Politik (SWP). Seit 2005 forscht sie zu Grundsatzthemen europäischer Außen- und Sicherheitspolitik und ist Dozentin im Postgradudiertenstudiengang „Master of European Studies“ der Freien Universität Berlin und Technischen Universität Berlin. 2014 wurde sie für das Projekt „Review 2014: Außenpolitik neu denken“ in den Planungsstab des Auswärtigen Amts berufen. 2013 war sie Robert-Bosch-Fellow an der Transatlantic Academy „The Future of the Liberal Order” und Visiting Fellow beim German Marshall Fund in Washington, D.C. Sie publiziert regelmäßig in Fachzeitschriften und ist Autorin und Herausgeberin mehrerer Bücher. Neben ihrer Forschungs- und Publikationstätigkeit berät sie Regierungen, internationale Institutionen und Unternehmen in den Bereichen Europäische Außen- und Sicherheitspolitik sowie zu Regulierungsfragen in der Cybersicherheit und Digitalisierung auf EU-Ebene.

Prof. Dr. Jürgen Neyer leitet den Lehrstuhl Europäische und Internationale Politik an der Europa-Universität Viadrina und ist Gründer der European New School of Digital Studies. Er forschte und lehrte an der Johann-Wolfgang-Goethe Universität Frankfurt am Main, der Universität Bremen, der University of California at Berkeley, dem European Institute Florence und der Freien Universität Berlin. Neyer veröffentlichte zahlreiche Arbeiten zu den Themen European Governance und Deliberative Demokratie. Der Titel seines letzten Buchs lautet "The Justification of Europe. A Political Theory of Supranational Integration, Oxford University Press". Seit 2018 ist er Vize-Präsident der Europa-Universität Viadrina Frankfurt (Oder).

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0

Falk Steiner
Senior Expert Digitalpolitik
Telefon +49 30 275788-132
falk.steiner@bertelsmann-stiftung.de

Ralph Müller-Eiselt
Director Programm Megatrends
Telefon +49 5241 81-81456
ralph.mueller-eiselt@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de

BertelsmannStiftung