Häufig wird die transformative Dynamik der Digitalisierung jedoch nur verkürzt – etwa mit Verweis auf die territoriale Entgrenzung mit der Verbreitung des Internets oder der Netzwerkmacht transnationaler Digitalkonzerne – aufgegriffen und dabei genauso häufig nur als Unterpunkt der Globalisierung behandelt (siehe beispielsweise Voigt 2020: 17). Erst seit jüngerer Zeit scheint sich hier etwas zu verändern, zumindest dann, wenn – wie diese Abhandlung im Folgenden argumentiert – die Debatten um die »Digitale Souveränität« potenziell Anknüpfungspunkte für eine Vision des Staates im digitalen Zeitalter eröffnen. Zuvor sollen jedoch kurz einzelne zentrale Aspekte der dystopischen und utopischen Bilder auf den digitalen Staat aufgegriffen werden, da diese gewissermaßen die Gegenthese zur digitalen Souveränität verkörpern.

IV.4.1 Dystopischer Überwachungsstaat

Der dystopische Überwachungsstaat, bei dem der totale steuernde Staat ins Totalitäre kippt, hat spätestens mit Orwells »1984« Eingang in die Populärliteratur gefunden. Wegbereiter der von ihm erdachten Dystopie war die technologische Entwicklung. »Science and technology were developing at a prodigious speed, and it seemed natural to assume that they would go on developing« (Orwell 1949: 164). Aber in dem dystopischen Staat »technological progress only happens when its products can in some way be used for the diminution of human liberty« (ebd.: 111).

Aus Bentham (1791) architektonischem Panoptikum wird ein technikbasierter, allsehender und -wissender Staat,[5] wie auch Orwell ihn erdachte: »We control life, Winston, at all its levels« (ebd.: 156). Spätestens seit den Snowden Enthüllungen ist auch der Mehrheit der Gesellschaft deutlich geworden, dass Staaten die gegebenen Möglichkeiten der technischen Überwachung auch tatsächlich nutzen und die Gefahr gläserner Bürger:innen nicht rein theoretischer Natur ist. Wie die Gefangenen, die im Bentham'schen Panoptikum um den sie überwachenden Aufseher wissen, so ist auch das Wissen um die Überwachung im »age of digital surveillance« damit allgegenwärtig (McMullan 2015). Allerdings gibt es einen entscheidenden Unterschied zu Benthams Panoptikum. Seine Funktionalität ergab sich aus der Verhaltensanpassung aufgrund der jederzeit unbemerkt möglichen,[6] tatsächlich aber nicht unbedingt immer stattfindenden Beobachtung. Das Panoptikum setzte also auf das Gefühl, überwacht zu werden.[7] Dage-

5 »By comparison with that existing today, all the tyrannies of the past were half-hearted and inefficient. […] Part of the reason for this was that in the past no government had the power to keep its citizens under constant surveillance. […] With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end. Every citizen, or at least every citizen important enough to be worth watching, could be kept for twenty-four hours a day under the eyes of the police and in the sound of official propaganda, with all other channels of communication closed« (Orwell 1949: 120).

6 »The essence of it consists, then, in the centrality of the inspector's situation, combined with the well-known and most effectual contrivances for seeing without being seen« (Bentham 1791: 23).

7 »Not only so, but the greater chance there is, of a given person's being at a given time actually under inspection, the more strong will be the persuasion – the more intense, if I may say so, the feeling, he has of his being so« (Bentham 1971: 25).

gen kann im digitalen Zeitalter ein tatsächlich fast lückenloses Überwachungs- und Aufzeichnungssystem entstehen, das durch seine kontinuierliche Erfassung und Speicherung auch ein nachträgliches Erkennen oder Rekonstruieren und anschließendes Ahnden unerwünschten Verhaltens ermöglicht. Darüber hinaus erfolgt eine solche alltägliche Datenerfassung entgegen der panoptischen Überwachung verdachtsunabhängig.[8] Von den technischen Möglichkeiten aus gesehen sind wir heute einem solchen Überwachungsstaat näher denn je. So zeichnet sich etwa nach Reinhard (2007: 110) »die Möglichkeit eines durch neue technische Hilfsmittel ermöglichten und durch die Bekämpfung des Terrorismus legitimierten totalen Überwachungsstaates ab.«

Für die modernen Staaten westlicher Prägung findet sich diese Problematik immer wieder im Spannungsverhältnis zwischen Sicherheit und Freiheit. Konkret diskutiert wird dies etwa im Rahmen der neuen Polizeigesetzgebung auf Länderebene, der Frage nach dem Umgang mit Staatstrojanern auf Länder- und Bundesebene sowie der Einführung umfassender Videoüberwachung, Gesichtserkennung[9] und perspektivischer Software zur automatisierten Verhaltenserkennung (vgl. Kurpjuweit 2017). Deutlich wird dies aber auch an den Interessenkonflikten im Spannungsfeld zwischen Verschlüsselung und Datenschutz auf der einen Seite sowie öffentlicher Sicherheit und Zugriffsmöglichkeiten der Ermittlungsbehörden auf der anderen Seite (vgl. Winkel 2022).

Diese Ausprägung unterscheidet sich jedoch immer noch deutlich von den Entwicklungen, wie sie etwa aus westlicher Perspektive für China postuliert und zumindest in Teilen bereits jetzt praktiziert werden. Angeführt werden hier etwa die vielen Schritte zur Einführung eines Social Credit System (SoCS), Berichte über Testphasen zur Videoüberwachung in Klassenräumen, die mittels Gesichtserkennung die Aufmerksamkeit der Schüler:innen erfassen soll, zu Gehirnwellen messenden EEG-Stirnbändern mit der gleichen Funktion oder zu smarter Schulkleidung, die die Anwesenheit und Wachheit der Schüler:innen erkennen soll (vgl. Pluta 2018; Tautz 2018; Rötzer 2019). Aus der medial-öffentlichen Perspektive der westlichen Welt erscheint das chinesische Social Credit System als Paradebeispiel des Überwachungsstaates. In der Realität existiert dieses System allerdings bislang nicht in dieser Form, und es ist noch völlig unklar, ob es jemals mit der diskutierten Funktionalität eingeführt werden wird (siehe auch Krempl 2019). Vielmehr besteht das System zurzeit aus drei einzelnen Teilen. Der erste Teil entspricht weitgehend den bekannten Kredit-Scoring-Verfahren, wie sie etwa auch die Schufa in Deutschland nutzt. Hier arbeitet der chinesische Staat mit Unternehmen wie Tencent oder Alibaba zusammen beziehungsweise lizenziert das Errechnen der Scores an solche Unternehmen, die ohnehin bereits über einen Großteil der zu nutzenden Daten verfügen. Der zweite Teil besteht aus schwarzen Listen, die sektorspezifisch und nicht gesamtstaatlich geführt, zum Teil aber durchaus miteinander verknüpft werden. Auf diesen Listen kann landen, wer gegen chinesische Gesetze verstoßen hat. Mit dem Listeneintrag sind dann je nach Sektor bestimmte Einschränkungen im Sinne von Strafen ver-

8 Erst die vorsorgliche Erfassung von Daten ermöglicht Konzepte wie *predictive policing*.

9 Siehe dazu etwa die Debatten um die Testphase der Videoüberwachung mit Gesichtserkennungsfunktion am Berliner Bahnhof Südkreuz, die nicht nur mit Blick auf Bürger:innenrechte, sondern auch ihren (Miss-)Erfolg kontrovers diskutiert wurde (vgl. Borchers 2018; erdgeist 2018).

bunden. Diese können etwa im Untersagen von Flugbuchungen bestehen oder im ausschließlichen Zugang zu schlechteren Sitzkategorien in Zügen.

Der mediale Fokus liegt auf dem dritten Teil, bei dem es um die Erziehung zu sozial-adäquatem Verhalten geht. Gerade für diesen existieren aber bislang nur etwa 40 regionale Pilotprojekte. Über deren perspektivische gesamtstaatliche Relevanz lässt sich zum jetzigen Zeitpunkt nur spekulieren (vgl. ebd.). Im Kern geht es darum, Verhalten von Menschen (bei technischer Machbarkeit durchaus auch automatisch in Echtzeit) zu bewerten. Konformes Verhalten führt zu Pluspunkten, nonkonformes beziehungsweise unerwünschtes Verhalten zu Abzügen im Score. Alle drei Teile zeichnen sich durch die Verbindung zwischen dem chinesischen Staat und Privatunternehmen aus. Dieser »corporate-state nexus […] complicated the process of state surveillance in China, since previous surveillance systems rarely included the private sector« (Liang et al. 2018: 434). Solche Public Private Partnerships »erzeugen in der Datengesellschaft« eine neue »Art des Panoptikums«, das die Überwachung nicht mehr wie bei Bentham »in einem zentralen Beobachtungsposten bündelt, sondern zentrumslos und damit potentiell allgegenwärtig ist« (Houben/Prietl 2018b: 344). Drinhausen und Brussee (Drinhausen/Brussee 2022: 1, 4) konstatierten im Jahr 2021 zwar eine Entwicklung des Social Credit Systems »from fragmentation towards integration« und damit den Eintritt in eine neue Phase nach dem Ende der »key construction phase.« Allerdings ist dessen Funktionalität weiterhin grundsätzlich beschränkt.

> »The SoCS itself is not tasked with conducting political surveillance of individual behaviour. Its role is more clearly limited in recent party and policy documents. Instead, these functions and political needs are addressed by other domestic security systems. In addition, a variety of commercial scoring systems have popped up across China, which operate independently of the SoCS« (ebd.: 4).

Das Social Credit System stellt demnach nur einen Baustein des chinesischen Staates im digitalen Zeitalter bei seinem Streben nach autoritärer Souveränität dar. Weitere Aspekte wie die Great Firewall wurden bereits in Kapitel II.2 erwähnt.

Aber auch jenseits autoritärer Regime hält mit der Digitalisierung von Gesellschaft und Politik »eine Logik der Kontrolle« in Bereiche Einzug, »die traditionell durch eine Balance von Autonomie und Kontrolle geprägt sind« (Weyer 2019: 21). Dabei besteht gerade im digitalen Raum die Gefahr, dass der Staat seine Aufgabe, die Sicherheit und den Schutz seiner Bürger:innen aufrechtzuerhalten, durch den Einsatz digitaler Kontrollmittel in Richtung Überwachung kippen lässt (vgl. Jäger et al. 2022: 195). In Deutschland zeigt sich dies an den breiten (medialen) Debatten um den Einsatz von Staatstrojanern bei der Quellentelekommunikationsüberwachung oder von Videoüberwachung (mit Gesichtserkennung) an Bahnhöfen (vgl. Borchers 2018; erdgeist 2018).

Darüber hinaus wird für die westlichen demokratischen Staaten das größere Potenzial für eine negative Entwicklung in Bezug auf Überwachungsfantasien jedoch eher in der Verbindung zwischen modernem Staat und Kapitalismus gesehen. Insbesondere Zuboff (2018) hat diese Debatte mit dem Überwachungs*kapitalismus* anstelle des Überwachungs*staates* begrifflich geprägt.

Eine Mehrheit von 61 Prozent der Wahlberechtigten machte sich 2019 große oder sehr große Sorgen wegen etwaigen Missbrauchs ihrer persönlichen Daten im Internet. Gar keine Sorgen machten sich nur vier Prozent (infratest dimap 2019).[10] Mit Blick auf die Nutzer:innen besteht das eingängige Modell der plattformisierten Dienste im Internet (wie Suchmaschinen oder Mailservices von Google oder Soziale Netzwerke und Messenger von Facebook) heute in einem Tausch: dem Tausch persönlicher Daten gegen die kostenlose Nutzung des angebotenen Dienstes. Dieser ist also nur insofern kostenlos, als sich die jeweilige Plattformen nicht direkt von den Nutzer:innen bezahlen lässt, sondern von Dritten. Diese Dritten – die eigentlichen Kund:innen der Plattformen – sind Unternehmen, Werbekund:innen und andere, die entweder erhobene Nutzer:innendaten direkt kaufen oder indirekt auf diese für das zielgruppenspezifische Ausspielen von Werbung auf der Plattform zurückgreifen.[11]

Wenn die Verfügung über große Datenmengen diejenige über andere Produktionsmittel als Ausgangspunkt für Macht und Reichtum ablöst, stellen sich – aufgrund der ungleichen Verteilung des Dateneigentums zugunsten monopolartiger Digitalkonzerne – Fragen von Gleichheit, Gerechtigkeit, Freiheit und Umverteilung neu. Es ist daher nicht verwunderlich, dass zwei zentrale Frage die Debatten prägen: Wem gehören die Daten, die an unterschiedlichsten Stellen anfallen oder erhoben werden? Und wie kann ihre souveräne Nutzung sichergestellt werden? Im Kern geht es damit um den Umgang mit Dateneigentum und Algorithmen, bei dem auch immer wieder die Rolle des Staates im Zentrum der Debatten steht.

> »Wenn man Regierungen erlaubt, die Daten zu verstaatlichen, wird das vermutlich die Macht großer Unternehmen eindämmen, aber es kann auch zu gruseligen digitalen Diktaturen führen« (Harari 2018: 120).

Mit Blick auf den Staat besteht in einer umfassenden Datensammlung die inhärente Gefahr von Überwachung und Kontrolle unabhängig von dessen Einordnung zwischen Demokratie und Diktatur. Howard (2016: 20f.) führt dies zu dem Vorschlag, bezogen auf Staaten, Regierungen und Politik, von soziotechnischen statt von repräsentativen Systemen zu sprechen. Dies würde eine differenziertere Verortung von Staaten im Spektrum zwischen offenen (Demokratie) und geschlossenen technischen Systemen (Diktatur) erlauben. Ähnlich weist Harari (2017: 505) darauf hin, dass, wenn unter einer datenfokussierten Perspektive alle Organismen und Organisationen als Datenverarbeitungssysteme verstanden werden, Demokratien und Diktaturen wie auch Kapitalismus und

10 Mit 49 % deutlich weniger Sorgen macht sich die Altersgruppe der 18- bis 34-Jährigen. Zwischen den anderen Altersgruppen sowie nach Bildungsgruppen unterscheiden sich die Anteile derjenigen, die sich große oder sehr große Sorgen machen, dagegen kaum (vgl. infratest dimap 2019).

11 Unter anderem durch die auf Websites von Dritten befindliche Werbung sowie die Einbindung von Nachrichten oder Like-Buttons erhalten große Plattformen wie Google oder Facebook nicht nur die Daten der direkten Nutzer:innen ihrer Website. Facebook kann so im Durchschnitt über 50 % der besuchten Webseiten und 40 % der im Internet verbrachten Zeit nachvollziehen – wobei sich die Beobachtbarkeit des Surfverhaltens zwischen Facebook-Nutzer:innen und Nichtnuzter:innen kaum unterscheidet (vgl. Ullrich et al. 2022: 403).

Kommunismus »konkurrierende Mechanismen zur Sammlung und Analyse von Informationen« darstellen. Bei Ersteren finde eine dezentrale, verteilte Verarbeitung statt, bei Letzteren eine zentralisierte. Eine Diskussion über Datensammlung und -nutzung des Staates im digitalen Zeitalter kann aus dieser Perspektive daher fruchtbar geführt werden, ohne dass es dabei immer gleich um die Abwehr des Überwachungsstaates und »Datenpaternalismus« gehen muss (Krönke 2016: 319). Zugleich sollten die dabei gesehenen Potenziale aber auch nicht in eine neue technologische Steuerungseuphorie umschlagen.

IV.4.2 Utopischer Mikro-Steuerungsstaat

Die zunächst utopisch anmutende Vorstellung eines potenten Steuerungsstaates setzt auf einen Staat, der die Digitalisierung nutzt, um die effektivsten und effizientesten Antworten auf gesellschaftliche Probleme zu finden und umzusetzen. Basis dieser Utopie ist die Voraussetzung, dass die Verdatung aller Dinge und Lebewesen diese in einer immer höheren Auflösung widerspiegelt – was Kucklick (2015) mit dem Begriff der Granularität bezeichnet (siehe Kapitel II.2.4). Aus der vermeintlichen Eindeutigkeit der gemessenen Zahlen, der gewonnenen Daten, wird ein Verschwinden der Ambiguität geschlussfolgert (vgl. Bauer 2018: 94).[12] Damit führen Entscheidungen nicht mehr zu einem ambivalenten Ergebnis aufgrund von Abwägung, Interpretation sowie Verhandlung und Kompromiss. Vielmehr ließe sich so die Wahrheit, also die perfekte Lösung, finden. Es geht also um die Wunschvorstellung, es gebe einfache und eindeutige Lösungen für komplexe Probleme. Morozov (2013a: 25ff.) spricht von der Ideologie des Solutionismus, die insbesondere bei den Technikeuphorist:innen des Silicon Valley verbreitet ist. Für diese stehen zum einen nicht die Probleme und ihre Definitionsnotwendigkeit (aufgrund von Komplexität und Mehrdeutigkeit) im Mittelpunkt, sondern ausschließlich das Finden von Lösungen.[13] Zum anderen zielt der Begriff darauf ab, dass unter ihnen der Glaube – und das durchaus im Wortsinn[14] – verbreitet ist, dass sich für alle gesellschaftlichen, sozialen, wirtschaftlich und politischen Probleme effiziente technologische Lösungen finden lassen[15] – sich also alle diese Probleme als technologische Probleme definieren las-

12 Unabhängig davon gilt: »Dass Bürokratisierung und Technisierung auf Eindeutigkeit abzielen, ist naheliegend« (Bauer 2018: 87).

13 Diese Perspektive entspricht dem Vorgehen der Suche nach Antworten, ohne dass man die Frage kennen würde, wie es sich etwa beispielhaft an der Datenanalyse und dem Data-Mining bei der Auswertung von Big Data zeigt (siehe Kapitel II.2.5).

14 Weidenfeld (2019) spricht nicht grundlos von »Digitalisierungspropheten«, die die Digitalisierung mit einer »Erlösungshoffnung« verbinden. Denn letztlich ist der Solutionismus genau das: der Glaube daran, dass sich in (nicht allzu ferner) Zukunft die Probleme durch die technologische Entwicklung (quasi automatisch) lösen lassen. Negativ gewendet könnte man aber auch sagen: Es geht um Fortschritt um jeden Preis, denn um die Lösung damit einhergehender Probleme (wie etwa Umweltverschmutzung, soziale Ungleichheit etc.) braucht man sich in der Gegenwart nicht zu kümmern, denn die technische Innovation von heute lässt sich einfach durch die technische Innovation von morgen korrigieren (vgl. Mamczak 2014: 99).

15 Der Solutionismus knüpft damit direkt an der kybernetischen Idee der Wunschmaschine an, der nur »ein Ziel vorgegeben wird […] aber der Weg dorthin unbestimmt ist und den installierten