Digitale Zensur als Kontrolle des Kontrollüberschusses

Daniel Moßbrucker

Einleitung: Zensur-Praktiken, die nicht als solche erscheinen

In vielen Teilen der Welt wenden Staaten Techniken an, um Inhalte im Internet zu zensieren. Ein Großteil dieser Techniken kann als 1 : 1-Kopie analoger Zensur beobachtet werden, leicht angepasst an das neue Übertragungsmedium Internet. Es geht darum, unerwünschte Kritik zu unterdrücken, indem beispielsweise Websites blockiert werden. Dies wird im Folgenden phänomenologisch am Beispiel China dargestellt. Im Zentrum des Beitrags steht das Argument, dass eine phänomenologische Analyse, die auf zu beobachtende Zensurtechniken abstellt, nicht vollends in der Lage ist, neue Facetten von Zensur sichtbar zu machen, die sich erst durch die Digitalisierung entwickelt haben. Es wird daher vorgeschlagen, Zensur funktional zu analysieren. Dies bietet den Vorteil, dass allein auf die Funktion von Zensur abgestellt werden muss. Eine solche funktionale Analyse öffnet den Blick für Phänomene, die auf den ersten Blick nicht wie vertraute Zensur-Praktiken aussehen, in der digitalen Gesellschaft jedoch eine Zensur-Funktion übernehmen. Es zeigt sich, dass sich digitale Zensur in der Zeitdimension paradoxerweise von der Intention des Zensors abkoppelt. Das heißt konkret: Manche Regulierungspraktiken demokratischer Rechtsstaaten entpuppen sich im Nachhinein als Zensur, obwohl dies gar nicht das Ziel der Maßnahmen war. Der Grund hierfür liegt in der Ubiquität digitaler Technologien, wodurch Überwachung zeitlich und räumlich entgrenzt wird, und einem damit einhergehenden „Kontrollüberschuss" (Baecker 2018), mit dem die Gesellschaft nur dann umgehen kann, wenn das Internet als Ganzes reguliert wird – mit dem Risiko, dass damit auch teilweise als wünschenswert angesehene Meinungsäußerungen zensiert werden.

Digitale Transformation analoger Zensur-Techniken: das Beispiel China

Nähert man sich digitaler Zensur rein phänomenologisch, stößt man rasch auf Praktiken, die schon vor der gesellschaftlichen Durchdringung des Internets als Zensur begriffen wurden. Das eindrücklichste und meistzitierte Beispiel ist die digitale Zensur-Infrastruktur Chinas (Liang 2010, Becker 2011, Noesselt 2014). Sie gilt als einzigartig und hocheffektiv, obwohl China seit 2008 das Land mit der absolut höchsten Zahl an Internetnutzerinnen und -nutzern ist (Kirchner 2017: 60). Für die Kontrolle von Inhalten sitzen heute nicht mehr nur Zensoren in Behörden, die Artikel prüfen, Musikstücke anhören oder Filme ansehen. Das erledigen größtenteils Algorithmen, die in Sekundenschnelle indizierte Wörter, Bilder oder Musik erkennen (Bamman et al. 2012). Sie löschen die Fundstücke entweder direkt oder melden sie einem Menschen zur Prüfung.

Gerade weil solche Systeme trotz aller Diskussionen um sogenannte künstliche Intelligenz kaum geeignet sind, den Kontext einer Aussage zu erfassen, ist der chinesische Zensurapparat auf tausende Mitarbeitende angewiesen (Kirchner 2017: 61). Es ist derzeit nicht absehbar, dass die Maschinen in Zukunft die Zensur vollständig automatisieren werden. Es bleibt auch im Digitalen bei einer „Zensur durch Menschen", aber von Maschinen unterstützt im Sinne einer Human-Computer Interaction (HCI), in der Mensch und Maschine die Stärken ihrer jeweiligen Intelligenz nutzen und funktional zusammenführen (Baecker 2019: 121–122).

Neben dieser inhaltlichen Zensur schottet die Kommunistische Partei das Internet des Landes vom Rest der Welt durch die Great Firewall ab. Der Vertrieb einer Zeitschrift wird heute nicht mehr mittels Verkaufsverboten verhindert, sondern durch Zugriffsblockade einer Website. Meistens verpflichtet die Regierung die nationalen Internetanbieter, den Traffic für indizierte Verbindungen nicht mehr durchzuleiten. Die Analogie zu Grossisten oder Kiosken, die Zeitschriften nicht mehr verkaufen dürfen, ist offenkundig. Solche Blockade-Technologien werden ständig verbessert und bilden damit ein zentrales Element der seit 2003 aufgebauten Great Firewall of China (Ensafi et. al 2015: 61). Die Beschränkungen lassen sich mit Virtual Private Networks (VPN) oder dem Tor-Netzwerk zwar umgehen (Scaife et al. 2017, Moßbrucker 2018), doch VPNs und Tor sind in China nicht so massenhaft verbreitet wie vielfach vermutet. 2017 nutzte nur rund ein Drittel der chinesischen Internetnutzerinnen und -nutzer gelegentlich einen VPN (Global Web Index 2017), seit 2018 ist die VPN-Nutzung außerdem verboten, wenn die VPNs nicht von der Regierung lizensiert wurden (Schulze 2017, Schulze/Voelsen 2020: 34-35; relativierend: Kipker 2018).

VPNs werden in China insgesamt eher sporadisch und anlassbezogen zur Zensurumgehung genutzt, was in jüngerer Forschung auch damit begründet wird, dass Teile der chinesischen Bevölkerung die „Western view of censorship" nicht teilen, sondern Zensur als legitimes Mittel zur Sicherung sozialer Ordnung sehen (Kou et. al 2017, Zitat: 378). Ähnlich dazu werden auch „Troll-Armeen" wie die „voluntary fifty-cent army", die weitestgehend freiwillig bei der Zensur helfen, als Argument angeführt, dass ein Zensurverständnis im Sinne von „staatliche Zensur vs. regimekritischer Aktivismus" zu trivial sei (Han 2015). Inwiefern solche Phänomene als Zensur zu verstehen sind oder nicht, soll an späterer Stelle nochmals aufgegriffen werden. Sie scheinen zumindest ein Indiz zu sein für eine Entdifferenzierung. Es verschwimmen die Grenzen zwischen Zensor und Zensierten, zwischen Zensur und Propaganda.

„Zensursula": Reflexe in demokratischen Regulierungsdebatten

Die Beobachtung gegenwärtiger Zensurtechniken ließe sich nun zu einer Liste ausbauen. Was wäre bei einem solchen Beitrag phänomenologischer Beobachtungen zu erwarten? Im Hinblick auf eingesetzte Technologien werden diese immer präziser und subtiler. Vielfach diskutiert ist beispielweise die sogenannte Deep Packet Inspection (DPI), mit der ein Internetanbieter jedes einzelne Internetpaket seiner Kundinnen und Kunden live analysieren und „tief" hineinschauen kann. Er kann dabei pro Paket nicht nur die Metadaten – wer kommuniziert mit wem – erfassen, sondern auch die Inhalte lesen. Das ist an sich schon invasiv, doch mit einer DPI kann ein Provider den Internet-

verkehr hunderttausender Menschen gleichzeitig überwachen, und ganz gezielt blockieren oder sogar manipulieren. Die Deep Packet Inspection hat zwar einen legitimen technischen Nutzen für Internet-Provider, birgt aber auch Potential für umfassende Zensur (Wagner 2009).

Im Hinblick auf die zensierenden Länder ist in einigen Ländern eine Orientierung an der chinesischen Great Firewall zu beobachten. Angestrebt ist eine „Renationalisierung" des Internets, um den Kommunikationsraum wieder an die nationalen Grenzen anzupassen. Prominentestes Beispiel ist Russland, das ein „RU-Net" aufbauen will (Reporter ohne Grenzen 2019: 60–62). An der Spitze einer solchen Liste würden insbesondere die Länder stehen, die in anderen Länder-Rankings wie der Rangliste der Pressefreiheit von Reporter ohne Grenzen regelmäßig hinten stehen. Die Botschaft: Diktaturen und Autokratien bedienen sich tradierter, für das Internet optimierter Zensurformen, während die Zensur in Demokratien historisch besiegt wurde.

Im Folgenden soll es um eine Beobachtung gehen, die mit der Unterscheidung Demokratie/Diktatur nicht zu erklären ist: Dass nämlich in Demokratien „Zensur" befürchtet wird, wenn über die Regulierung des Internets diskutiert wird. Zwei Beispiele aus Deutschland: 2008 erhielt die damalige deutsche Familienministerien Ursula von der Leyen den Spitznamen „Zensursula". Sie wollte den Zugriff auf Server sperren, auf denen nachweislich kinderpornografisches Material abrufbar war (Schallbruch 2018: 9–13). Kritisiert wurde mittels Online-Petitionen, dass Sperrlisten geführt werden sollten, was einer verfassungswidrigen Vorzensur gleichkomme. Gefordert wurde stattdessen „Löschen statt sperren" (Bieber 2014). Auch ein Jahrzehnt später wurde der Zensurbegriff in Debatten um die Regulierung des Internets in Deutschland intensiv genutzt. Dieses Mal wollte die Bundesregierung mit dem Netzwerkdurchsetzungsgesetz (NetzDG) die Anbieter sozialer Netzwerke wie Facebook, Twitter und YouTube verpflichten, binnen 24 Stunden zu löschen, was strafbar ist, ansonsten drohten teils millionenschwere Bußgelder (Eifert/Gostomzyk 2018). Radikale Kritiker nannten dies ein „Zensurgesetz" (Steinhöfel 2018), und auch in juristischen Fachkreisen wurde gefragt, ob es sich beim NetzDG um Zensur handeln könnte (Richter 2017). Teilweise werden Zensurrufe sogar laut, wenn Anbieter wie Facebook ohne staatlichen Druck Inhalte löschen (Adelberg 2019: 55–61).

Zensur oder nicht? Die aufgeworfenen Fragen werden mannigfaltig juristisch geprüft, phänomenologisch beobachtet, politikwissenschaftlich interpretiert oder auf ihren technologischen Innovationsgehalt hin untersucht. Der Erkenntnisgewinn dieser fachspezifischen Analysen soll nicht bestritten werden, im Gegenteil. Ich rege dennoch an, die Betrachtungsweise nochmals zu erweitern und stärker auf die Funktion von Zensur in einer Gesellschaft abzustellen. Gegenüber den genannten Perspektiven kann eine funktionale Analyse den Blick öffnen für Phänomene, die auf den ersten Blick nicht wie Zensur anmuten, rechtlich nicht als solche definiert würden oder politisch nicht als solche gemeint sind – in der digitalen Gesellschaft jedoch die Funktion von Zensur übernehmen. Damit soll dem Umstand Rechnung getragen werden, dass das Internet nicht nur ein zusätzliches Verbreitungsmedium ist, sondern sich durch digitale Technologien die Gesellschaftsform als solche ändert. Es geht im Folgenden also darum, den Blickwinkel zu erweitern, ohne zu behaupten, andere Analysen korrigieren oder gar ersetzen zu können.

Funktionale Äquivalente analoger Techniken

Zensur kann man im Anschluss an Roßbach (2018) beschreiben als eine umfassende, strukturell und institutionell verankerte Kontrolle, Beschränkung oder Verhinderung von zur Veröffentlichung bestimmter oder veröffentlichter Meinungsäußerungen. Entscheidender als diese (recht weite) Definition ist für das Folgende jedoch, mit der Definition die Funktion von Zensur zu bestimmen. Diese besteht ganz allgemein darin, Komplexität zu reduzieren. Reduktion von gesellschaftlicher Komplexität ist Voraussetzung dafür, Strukturen zu bilden und zu etablieren. Im Falle von Staaten ist *eine* Form von Zensur also die umfassende Kontrolle von Meinungsäußerungen vor ihrer Veröffentlichung mit der Funktion, das staatliche Gewaltmonopol zu sichern. Im Folgenden soll versucht werden, von dieser Ausgangslange aus die Analyse zu konkretisieren, indem herausgearbeitet wird, was „Komplexität" der digitalen Gesellschaft ausmacht und wie sie konkret reduziert werden kann.

Die Methode hierfür bietet die funktionale Analyse. „Die Funktion ist keine zu bewirkende Wirkung, sondern ein regulatives Sinnschema, das einen Vergleichsbereich äquivalenter Leistungen organisiert. (…) In diesem Blickwinkel erscheinen die einzelnen Leistungen dann als gleichwertig, gegeneinander austauschbar, fungibel, während sie als konkrete Vorgänge unvergleichbar verschieden sind." (Luhmann 1991a: 14) Die funktionale Analyse erlaubt es zum Beispiel, zwischen historisch unterschiedlich ausdifferenzierten Gesellschaftssystemen zu vergleichen, um funktionale Äquivalente zu finden. Im Folgenden soll die funktional differenzierte Gesellschaft der Moderne mit der Netzwerkgesellschaft verglichen werden. Funktionale Äquivalente im Sinne Luhmanns sind also Leistungen, die in beiden Gesellschaftssystemen erbracht werden, selbst wenn sie je für sich unterschiedlich sind in ihrer Ausgestaltung, zum Beispiel weil die Leistung in System A intentional und in System B kausal erklärt werden kann (Luhmann 1991b). Als triviales Beispiel ließe sich anführen, dass das staatliche Bildungssystem heute gesellschaftliche Leistungen in der Erziehung von Kindern übernimmt, die traditionell von der Familie erbracht wurden – wobei mit dieser Äquivalenz der Leistung eben nichts über Einheit oder Differenz von Erziehungsinhalten, Erziehungsmethoden oder Erziehungszielen zwischen Familie (früher) und Bildungssystem (heute) gesagt sein soll.

Hinter diesem Ansatz steht die These der Theorie sozialer Systeme, wonach sich Gesellschaften evolutionär ausdifferenzieren und Medienrevolutionen zu neuen Differenzierungsformen geführt haben. Zensur war demnach eine Lösung speziell für die Funktionssysteme Religion und Politik, um mit dem Kritiküberschuss umzugehen, den der Buchdruck ermöglicht hatte. Der Buchdruck steigerte die Lesefähigkeit in der Bevölkerung sowie die Publikationsfähigkeit von Ansichten, die Staat und Religion widersprachen (Luhmann 1997: 729). Man konnte nun Bücher nebeneinanderlegen, vergleichen und fand unterschiedliche Meinungen. Das Bezugsproblem der Gesellschaft war ein Kritiküberschuss, der die Komplexität immens steigerte. Um mit Komplexität in Form des Kritiküberschusses umgehen zu können, muss ein System selektieren, also bestimmte Handlungen anderen vorziehen, um damit handlungsfähig zu bleiben (Luhmann 1984: 47). Zensur war und ist eine solche Selektionstechnik, um mit zu viel Kritik umzugehen. Auf Dauer hat sie sich nur selten bewährt und ist gerade im demokratischen Rechtsstaat, der von Diskurs und divergierenden Meinungen lebt, zumeist überflüssig.

Erkennt man nun an, dass digitale Medien das Kommunikations- und Gesellschaftssystem grundlegend verändern, sodass wir nach Sprache, Schrift und Buchdruck eine vierte Medienrevolution erleben (Baecker 2018, Nassehi 2019), dann ändert sich im Übergang von der funktionalen Gesellschaft in eine Netzwerkgesellschaft auch das Bezugsproblem der Gesellschaft. Baecker (2018: 54) nennt dies den neuen „Kontrollüberschuss" der elektronischen Medien. Dieser besteht in der „Erweiterung der Kontrollmöglichkeiten menschlichen Handelns und Erlebens durch den Computer. Der neue Verweisungsüberschuss im Medium des Sinns ist umso mehr ein Kontrollüberschuss, als jegliche erdenkliche Kommunikation auf Daten beruht, die von Computern gesammelt, aufbereitet, verarbeitet, vernetzt und ausgegeben werden, so verständlich oder unverständlich sie sein mögen." (Baecker 2019: 117–118) Kritiküberschuss verschwindet damit nicht als Bezugsproblem, genauso wie die Lüge weiterhin ein Problem ist, die erst möglich wurde, als die Menschen Sprache entwickelten. Tradierte Zensurtechniken wie die Löschung von Kritik und Zugriffssperren bleiben bestehen, wie das Beispiel China zeigt.

Aber es genügt offensichtlich nicht, Kritik zu löschen, um gesellschaftliche Komplexität zu reduzieren, wie die chinesische „voluntary fifty-cent army" belegt: Das Regime weiß sehr genau, wer es in den sozialen Medien kritisiert, es könnte alle Kritiker sanktionieren, aber das nur theoretisch, denn es sind so viele, dass es einen Überschuss an kontrollierbarem Handeln gibt. So paradox das klingen mag: Das Regime weiß zu viel über die Menschen, die sozialen Medien fluten die Behörden mit detailliertesten Informationen über jegliche Regung der Gesellschaft, und das führt nicht zu mehr, sondern zu weniger Kontrolle. Wer jedes Verhalten kontrollieren könnte, wird gerade dadurch handlungsunfähig, und muss wiederum selektieren. Die Technik zur Reduktion dieser Komplexität besteht bei der „voluntary fifty-cent army" darin, Inhalte von Freiwilligen produzieren zu lassen, um die Kritik so weit im Sumpf von Meinungen untergehen zu lassen, dass Kritiker nicht immer verfolgt werden, aber die staatliche Ordnung nicht mehr gefährden. Was wie Propaganda von Partisanen anmutet, erfüllt in der digitalen Gesellschaft die Funktion von Zensur. „Die Idee der Komplexität wird stark gemacht, weil sie es ermöglicht, sich eine Kontrolle der Kontrolle unter Bedingungen der Unmöglichkeit von Kontrolle vorzustellen." (Baecker 2018: 72)

Digitale Zensur als Kontrolle von Kontrollüberschuss

Wenn die Gesellschaft insgesamt mit einem durch elektronische Medien ausgelösten Kontrollüberschuss überfordert wird, sind all' ihre Teilsysteme davon betroffen. Die Politik spürt dies zum Beispiel darin, dass sie aus jedem Bereich kritisiert werden kann und jede Kritik potentiell aufnehmen, bestätigen und widerlegen könnte. Es bleibt eine gute Maxime, die klassischen Leitmedien zu rezipieren, aber es genügt nicht mehr, denn auch twitternde Eltern können mit einem Tweet über schlechte Kita-Bedingungen eine nationale Diskussion über das Bildungssystem lostreten. Die PR-Abteilung des Familienministeriums hätte es merken müssen, denn der Tweet war ihnen prinzipiell zugänglich, aber es sind zu viele Tweets und Posts in den sozialen Netzwerken, um sich mit jeder Kritik auseinanderzusetzen. Das Dilemma: Die Kritik ist nicht mehr das alleinige Problem. Vielleicht gab es wenige Tage zuvor bereits einen ähnlichen Tweet,

dessen Kritik schärfer und fundierter war, aber er verschwand unbeachtet in den Tiefen des Internets.

Besonders deutlich spüren diese Überforderung die Sicherheitsbehörden, deren genuine Aufgabe ja ohnehin schon Kontrolle ist. Der Terrorismus beispielsweise hat sich internationalisiert, und eine kleine Gruppe von Individuen kann die nationale Sicherheit gefährden (Lahl/Varwick 2019: 81–87). Trotz aller Diskussionen um den Ausbau von Überwachungsbefugnissen ist die Herausforderung der Zukunft wohl weniger, Daten über die Bevölkerung zu sammeln. Der Blogger Sascha Lobo recherchierte 2017, dass bis dahin 24 identifizierte Täter 13 islamistische Anschläge in der EU verübt hatten – und alle waren den Sicherheitsbehörden zuvor als gewaltaffin bekannt (Lobo 2017). Um die viel zitierte Metapher zu bemühen: Nicht das Aufstocken des Heuhaufens ist das Problem der Netzwerkgesellschaft, sondern das Aufspüren der Nadel darin.

Weil das Internet rein technisch gesehen immer überwachbar ist, wird durch die zunehmende Vernetzung der Welt – beschleunigt durch das Internet der Dinge (Weiser/Brown 2015) – Überwachung ubiquitär (Andrejevic 2012). Jeder Mensch speist durch sein Verhalten sein „data double" (Haggerty/Ericson 2000), das immer präziser das Verhalten des „echten Menschen" digital abbildet. Sein eigenes „data double" ist für den Menschen jedoch nicht einsehbar, sondern unterliegt dem Zugriff durch Internetunternehmen und Staaten. Beide haben ein Interesse an einer Steigerung der Überwachung, zum Zwecke der wirtschaftlichen Profitsteigerung und des staatlichen Machterhalts (Zuboff 2018). Sicherheitsbehörden können diese „data doubles" prinzipiell einsehen und damit arbeiten, um zu kontrollieren. Es ist kaum mehr eine Herausforderung, sogenannte „Gefährder" (ein Begriff, der erst in den letzten Jahren Konjunktur erlangte [Kretschmann/Legnaro 2019]) zu identifizieren. Aber wann wird ein „Gefährder" zum Massenmörder?

Sieht man die Lösung des Bezugsproblems des Kontrollüberschusses also darin, Kontrollüberschuss zu kontrollieren (d.h. Reduktion von Komplexität), dann geht dies bei der digitalen Zensur über die reine Unterdrückung von Kritik, ob als Vor- oder Nachzensur, hinaus. Es läuft auf Techniken hinaus, die in ihrer Selektivität so indifferent wie möglich sind, einfacher gesprochen: die potentiell das gesamte Netzwerk (das ist die digitale Gesellschaft) erfassen. Das konkrete Handeln, die einzelne Kommunikation, ob kritisch oder nicht, sind erst einmal egal, denn potentiell kann ja jede Äußerung zu einer Kritik werden, die Struktur gefährdet. Es rücken damit digitale Techniken als funktionale Äquivalente zu „analogen Zensurtechniken" der Kritikbeseitigung ins Blickfeld, die Kontrolle automatisieren. Damit ist nicht nur eine maschinelle Automatisierung gemeint (Andrejevic 2019).

Ein Beispiel für die Automatisierung der Kontrolle des Kontrollüberschusses sind datengestützte Verhaltensprognosen zur Kriminalitätsbekämpfung, an denen Regierungen weltweit arbeiten. Diskutiert wird dies meist unter dem Begriff „predictive policing". Die Vision: Da Daten (im doppelten Sinne des Wortes) gegeben sind (Kontrollüberschuss), errechnen Systeme eine Prognose und die menschliche Intelligenz (z.B. „Data-Analysts") befasst sich nur mit den Prognosen der höchsten Verbrechenswahrscheinlichkeit. In der Strafverfolgung zeigt die Polizei also dort Präsenz, wo die Einbrecher höchstwahrscheinlich auftauchen werden. „Vor die Lage kommen" beschreibt Knobloch (2018) die Idee treffend. Der Trend der maschinengestützten Automatisierung lässt sich in vielen Bereichen der Sicherheitspolitik beobachten (Lobe 2019), zum Bei-

spiel auch in der demokratischen Geheimdienstkontrolle, also der Kontrolle der Kontrolle des Kontrollüberschusses. Weil die Geheimdienstkontrolleure, die überprüfen, dass sich Geheimdienste an Recht und Gesetz halten, von der schieren Masse der Kontrolle von Kontrollüberschuss in den Diensten überfordert werden, wollen (oder müssen) sie „intelligente Technologien" einsetzen, die ihnen als Entscheidungshilfen dienen (Vieth/Wetzling 2019).

Digitale Zensur entkoppelt sich zeitlich von der Intention des Zensors

Der Grenzwert der Automatisierung der Kontrolle des Kontrollüberschusses ist erreicht, wenn jedes kontrollfähige Element im Netzwerk (z.B. ein Mensch) kontrolliert wird nach dem Leitwert einer externen Kontrollinstanz (z.B. Staaten). Es geht um automatisierte Verhaltenskonditionierung, was der Zensurforschung unter dem Begriff der „Selbstzensur" keineswegs fremd ist. Techniken der digitalen Zensur bestehen beispielsweise darin, über die Kontrolle des Kontrollüberschusses aktiv zu kommunizieren. Sicherheitsbehörden melden aktuelle Statistiken über die „Zahl der Gefährder im Land", sie fordern in der Rechtsordnung möglichst umfassende Rechte zur Überwachung oder sie verfolgen Whistleblower, die Missstände aufgedeckt haben. Das Paradoxe: All' dies muss gar nicht geschehen mit der Intention, zensieren zu wollen. Transparenz über die Arbeit von Sicherheitsbehörden ist ebenso eine demokratische Notwendigkeit wie die Maßgabe, dass Grundrechtseingriffe wie Überwachung nur auf Grundlage eines Gesetzes erfolgen dürfen. Und so sehr Whistleblower im Einzelfall auch Missstände aufdecken, hat der Staat auch ein berechtigtes Interesse an vertraulicher Beratung. Hinter allem steht jedoch unweigerlich auch die Botschaft: „Wir können alles sehen, was Ihr macht, und Ihr haltet Euch besser an die Regeln, andernfalls treffen Euch drakonische Strafen." Eine Intention von Überwachung war immer schon ein solcher Abschreckungseffekt (Foucault 1977), doch mit der Ubiquität digitaler Netzwerke wird diese Überwachung räumlich und zeitlich entgrenzt, was zu einer permanenten Überwachbarkeit und Abschreckung führt (Deleuze 1992, Haggerty 2006). Es gibt Hinweise darauf, dass es durch den digitalen Wandel zu einem sogenannten „Chilling Effect" kommt, wodurch zum Beispiel Menschen aus Furcht vor Überwachung ihr Verhalten konditionieren, obwohl dies der Überwacher (zumeist Staaten) gar nicht geplant hatte (Assion 2015, Staben 2016).

Hier gelangt man an die für den Zensurbegriff im Digitalen entscheidende Stelle: Wenn automatisierte Kontrolle die Antwort der digitalen Netzwerkgesellschaft auf das Bezugsproblem des Kontrollüberschusses ist, dann überzeugt es auf den ersten Blick nicht, jede Form von Kontrolle als Zensur zu begreifen. „Predictive Policing" oder die Verfolgung von Whistleblowern, um die Beispiele wieder aufzugreifen, scheinen ja nicht automatisch in Zensur überzugehen. Man gelänge zur Paradoxie, dass rechtsstaatliches Handeln immer dann rechtsstaatliches Handeln ist, wenn es Zensur ist. Aus der Perspektive eines Beobachters gesprochen, der zwischen legitim und illegitim unterscheidet: Staatliches Handeln ist legitim, wenn es illegitim ist. Kann ein Zensurverständnis in einer Gesellschaft des Kontrollüberschusses überhaupt noch an Kontrolle anknüpfen? Man sollte sich zumindest von der Paradoxie nicht abschrecken lassen, sondern nach Lösungen suchen, sie zu entfalten (Baecker 2002: 91).

Das eigentlich Neue am Begriff der *digitalen* Zensur wird sichtbar, wenn man die Paradoxie in der Zeitdimension entfaltet. Kontrolle ist immer Kontrolle, und manchmal auch Zensur. Manche Kontrolltechniken können weiterhin ex ante als Zensur bewertet werden (die gezielte Blockade kritischer Websites in China), d.h. die Technik wird gewählt mit der Intention, zu zensieren. Bei manchen Kontrolltechniken ist eine Bewertung nur noch ex post möglich. Früher war es noch möglich, gezielt nur das zu zensieren, was man nicht sehen wollte. Heute muss man nicht mehr jede Kritik löschen, sondern die Kontrolle so weit automatisieren, dass sie allumfassend anknüpft, um den ubiquitären Kontrollüberschuss zu kontrollieren. Die Zensur trennt sich nicht von der Kontrolle als Technik ab, aber paradoxerweise von der Intention des Zensors. Rechtsstaatliches Handeln zensiert, wenn es gar nicht zensieren soll. Journalistinnen und Journalisten wissen zum Beispiel, dass die Kommunikation mit ihren Quellen erfasst wird und schränken sich ein (Mills 2018, Moßbrucker 2019a), obwohl die allumfassende Kommunikationsüberwachung mit dem Zweck der Terrorbekämpfung legitimiert wird. Soziale Netzwerke erhöhen die Löschquoten aus Furcht vor hohen Bußgeldern und schrecken damit gegebenenfalls ihre Nutzerinnen und Nutzer ab, obwohl der Staat die Maßnahme vor allem eingeführt hat, um Opfer von Hassrede besser zu schützen. Was Zensur war, weiß man immer erst hinterher. Ganz auf Kontrolle zu verzichten, kann keine erfolgsversprechende Vermeidungsstrategie für Politik sein, denn damit würde man in der digitalen Gesellschaft handlungsunfähig und auch gesamtgesellschaftlich gewünschte Kontrolle in Form von Rechtsstaatlichkeit, Regulierung, Strafverfolgung oder Friedenssicherung unterlassen. Im Grenzwert formuliert heißt dies: rechtsstaatliches Handeln zur Kontrolle des Kontrollüberschusses kann es nur geben, wenn dies auch in digitale Zensur münden kann.

Die große Herausforderung wird darin bestehen, die Erscheinungsformen digitaler Zensur, die nur ex post als solche zu bewerten ist, theoretisch und praktisch sichtbar zu machen. Das ist alles andere als selbstverständlich. Theoreme wie die „Chilling Effects" sind wichtige Ausgangspunkte, aber zu unterkomplex. Dahinter steht schließlich die Idee, dass soziale Effekte ontologisch prognostiziert werden könnten. Tritt dann ein Ereignis wie zum Beispiel Überwachung auf, ändern Menschen ihr Verhalten und „lassen sich abschrecken". Wenn aber doch Überwachung und Kontrolle allumfassend wird, weil sie sich räumlich und zeitlich entgrenzen, lässt sich nichts anderes prognostizieren als diese eine „abgeschreckte Gesellschaft". Die Normabweichung kann nicht beobachtet werden, weil Abweichung die Norm ist, neben der es keine Referenz gibt, mit der man sie vergleichen könnte. Man sollte sich weiterhin nicht der Illusion hingeben, die Gesellschaft von außen beobachten und an einer externen Referenz messen zu können (Luhmann 1984: 9–11), nur weil die Welt sich in Daten digital dupliziert. Digitale Zensur ist daher nicht mit individueller Selbstzensur gleichzusetzen, denn bei der Selbstzensur liegt ein aktives Unterdrückungshandeln des Zensierten vor im Sinne jener Abschreckung. Digitale Zensur hingegen ist, wenn man so will, systemimmanent und löst die Differenz zensiert/unzensiert vollends auf.

Die Gesellschaft auf der Suche nach funktionalem Ersatz

Die Folgen der „digitalen Zensur ex post" lassen sich eher an evolutionären Strukturentwicklungen der Gesellschaft durch funktionale Äquivalente ablesen, wie ich abschließend am Beispiel der Kritikfunktion des Journalismus zeigen möchte. Ist es also Aufgabe des Journalismus, durch zugespielte Informationen von Quellen Missstände aufzudecken, um damit staatliches Handeln zu kontrollieren (Blöbaum 2016: 157), dürfte dieser Zufluss an Informationen sich gerade bei hochsensiblen Dokumenten („streng geheim") abschwächen, wenn Mitarbeitende in Ministerien oder streng kontrollierten Sicherheitsbehörden wissen, dass eine Kontaktaufnahme mit einer Redaktion protokolliert würde (Lashmar 2017). Es schien zunächst, dass genau das Gegenteil passiere, nämlich dass das Internet das Ende der Geheimhaltung und damit eine „monitoring democracy" einleiten könnte (Keane 2009) – man denke nur an Wikileaks und die Snowden-Veröffentlichungen. In den USA jedoch sind mittlerweile alle Whistleblower identifiziert, sitzen größtenteils lange Haftstrafen ab oder werden international verfolgt. Quellen können also in Einzelfällen durchaus streng geheime Papiere leaken, sie bezahlen es nur mit der individuellen Freiheit, weil sie mit höchster Wahrscheinlichkeit auffliegen (Moßbrucker 2019b).

Die Gesellschaft muss sich dieser Herausforderung stellen, wenn sie die Kritikfunktion des Journalismus bewahren und eine Vertrauensbeziehung zwischen Redaktion und Quelle ermöglichen will. Sie braucht funktionale Äquivalente, die sich in der neuen Gesellschaftsform bewähren. Die meistgenutzte Technik ist ein Relikt der funktionalen Gesellschaft und besteht in einer Verrechtlichung (Luhmann 1975: 44–46), sodass Überwachung und Auswertung von Kommunikation auf einen legitimen Zweck beschränkt wird. Die Überwachung soll damit zur legitimen Macht werden. In vielen Fällen erweist sich dies in einer technisch total überwachbaren Gesellschaft allerdings als unmöglich, weil Überwachung als Kontrolltechnik ja eben nicht prinzipiell ausgeschlossen werden kann. So werden Überwachungsmaßnahmen rechtlich nie ganz ausgeschlossen werden können, sondern „an den Einzelfall" und eine „Verhältnismäßigkeitsprüfung" gebunden, was den potentiell Überwachten jedoch nicht hilft. Es würde bei einer Telefonüberwachung ja wenig Sinn ergeben, den Überwachten mitzuteilen, dass sie gerade aktiv belauscht werden. Sie müssen immer damit rechnen, dass sie überwacht werden, nicht obwohl, sondern weil in der Rechtsordnung etwas von „Einzelfällen" und „Verhältnismäßigkeit" steht. In diesem Kontext ist bemerkenswert, dass zunehmend Verbote für die Weiterentwicklung digitaler Technologien wie KI-gestützter Gesichtserkennung gefordert werden, weil nicht absehbar ist, ob sich diese Technologien jemals wieder rechtlich einhegen und damit demokratisch kontrollieren lassen werden (Stolton 2020). Auch Ideen wie die „Technikfolgenabschätzung" oder „Human Rights Impact Assessments" bei digitalen Technologien avancieren in der Politik zunehmend zu Entscheidungshilfen (Grunwald 2010: 41–64).

In Großbritannien wird außerdem diskutiert, ob Geheimdienste der Presse „Foren" bieten müssen, um mit Geheimdienst-Mitarbeitenden sprechen zu können (Lashmar 2015). So sehr das der aktuellen journalistischen Logik widerspricht und der Erfolg fraglich ist, trägt es zumindest der Realität Rechnung, dass die Dienste geschwätzige Beamtinnen und Beamte mit an Sicherheit grenzender Wahrscheinlichkeit auffinden können (Lashmar 2017, Snowden 2019: 241–254). Auch das Erlassen von Whistleblo-

wer-Schutzgesetzen könnte ein solches funktionales Äquivalent darstellen. Dass Hinweisgeberinnen und Hinweisgeber eine wichtige Rolle für die Gesellschaft erfüllen, ist ein altes Argument und der Grund, warum Medien einen Informantenschutz genießen. Aber erst im Zeitalter der Digitalisierung scheint es notwendig zu werden, diese Whistleblower rechtlich zu schützen und gesellschaftlich breit zu stützen, weil es höchstwahrscheinlich ist, dass ihr Tun publik wird (Moßbrucker 2019b).

Die journalistische Recherche ist nur ein Beispiel dafür, wie die Gesellschaft derzeit funktionale Äquivalente für eine neue Gesellschaftsform ausprobiert, um die Funktionserfüllung in einer sich ändernden Umwelt gewährleisten zu können. Ob sich solche Entwicklungen als funktionale Äquivalente bewähren, lässt sich wiederum nur im Nachhinein beobachten. Es kann funktionieren, muss aber nicht. Gelingt es nicht, entsteht eine Gesellschaft, in der digitale Zensurtechniken mit Kontrolle gleichgesetzt werden. Dann, und nur dann, rücken Dystopien vom Ende der Demokratie durch totale digitale Kontrolle in den Bereich des Möglichen.

Literatur

Adelberg, Philipp Nikolaus (2019): Rechtspflichten- und grenzen der Betreiber sozialer Netzwerke. Zum Umgang mit nutzergenerierten Inhalten. Wiesbaden, Springer Fachmedien.

Andrejevic, Mark (2012): Ubiquitous surveillance. In: Ball, Kristie/Haggerty, Kevin/Lyon, David (Hrsg.): Routledge Handbook of Surveillance Studies. Abindon: Routledge, S. 91–98.

Andrejevic, Mark (2019): Automating Surveillance. In: Surveillance & Society (17) 1–2, S. 7–13.

Assion, Simon (2015): Überwachung und Chilling Effects. In: Telemedicus (Hrsg.): Überwachung und Recht, S. 31–82.

Baecker, Dirk (2002): Wozu Systeme? Berlin, Kulturverlag Kadmos.

Baecker, Dirk (2018): 4.0 Oder die Lücke, die der Rechner lässt. Leipzig, Merve.

Baecker, Dirk (2019): Intelligenz, künstlich und komplex. Leipzig, Merve.

Bamman, David/Brendan, O'Connor/Smith, Noah (2012): Censorship and deletion practices in Chinese social media. In: First Monday (17) 3, https://doi.org/10.5210/fm.v17i3.3943

Becker, Kim-Björn (2011): Internetzensur in China. Aufbau und Grenzen des chinesischen Kontrollsystems. Wiesbaden: Springer Fachmedien.

Blöbaum, Bernd (2016): Journalismus als Funktionssystem der Gesellschaft. In: Löffelholz, Martin/Rothenberger, Liane (Hrsg.): Handbuch Journalismustheorien. Wiesbaden, Springer VS, S. 151–164.

Bieber, Christoph (2014): "NoBailout" und "Zensursula": Online-Kampagnen in der Referendumsdemokratie. In: Scholten, Heike/Kamps, Klaus (Hrsg.): Abstimmungskampagnen. Politikvermittlung in der Referendumsdemokratie. Wiesbaden, Springer VS, S. 323–338.

Deleuze, Gilles (1992): Postscript on the Societies of Control. In: October (59) Winter, S. 3–7.

Eifert, Martin/Gostomzyk, Tobias (2018): Netzwerkrecht. Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation. Baden-Baden: Nomos.

Ensafi, Roya/Winter, Philipp/Abdullah, Mueen/Jedidiah, R. (2015): Analyzing the Great Firewall of China over Space and Time. In: Proceedings on Privacy Enhancing Technologies (1), S. 61–76.

Foucault, Michel (1977): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main, Suhrkamp.

Global Web Index (2017): VPN Usage Around the World. https://cdn2.hubspot.net/hubfs/304927/Downloads/VPN-Usage-Around-the-World-Infographic.pdf , 21. April 2020.

Grunwald, Armin (2010): Technikfolgenabschätzung: eine Einführung. Berlin, edition sigma.

Haggerty, Kevin (2006): Tear down the walls: on demolishing the panopticon. In: Lyvon, David (Hrsg.): Theorizing Surveillance. The panopticon and beyond. Oregon, Willan Publishing, S. 23–45.

Haggerty, Kevin/Ericson, Richard (2000): The surveillant assemblage. In: British Journal of Sociology (51) 4, S. 604–622.

Han, Rongbin (2015): Defending the authoritarian Regime Online: China's "Voluntary Fifty-cent Army". In: The China Quarterly (224), S. 1006–1025.

Keane, John (2009): The Life and Death of Democracy. New York, W. W. Norton & Co.

Kipker, Dennis-Kenji (2018): VPN-Tunnelabschaltung und "Chinese Cybersecurity Law" – wohl mehr Mythos als Realität. In: Datenschutz und Datensicherheit (DuD) (42) 9, 574–575.

Kirchner, Ruth (2017): Situation von Medien und Internet. In: Bundeszentrale für politische Bildung (Hrsg.): Informationen zur politischen Bildung / izpb. Volksrepublik China. Bonn, bpb.

Knobloch, Tobias (2018): Vor die Lage kommen: Predictive Policing in Deutschland. Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit. Berlin/Gütersloh, Stiftung Neue Verantwortung/Bertelsmann Stiftung.

Kou, Yubo/Semaan, Brian/Nardi, Bonnie (2017): A Confucian Look at Internet Censorship in China. In: Bernhaupt, Regina/Dalvi, Girish/Joshi, Anirudha/Balkrishan, Devanuj K./O'Neill, Jacki/Winckler, Marco (Hrsg.): Human Computer Interaction – INTERACT. Cham, Springer Nature, S. 377–398.

Kretschmann, Andrea/Legnaro, Aldo (2019): Abstrakte Gefährdungslagen. Zum Kontext der neuen Polizeigesetze. In: Aus Politik und Zeitgeschichte. Polizei (69) 21–23, S. 11–17.

Lahl, Kersten/Varwick, Johannes (2019): Sicherheitspolitik verstehen. Handlungsfelder, Kontroversen und Lösungsansätze. Bonn, Bundeszentrale für politische Bildung.

Lashmar, Paul (2015): Spies and journalists. Towards an ethical framework? In: Ethical Space: the international journal of ethics (12) 3–4, S. 4–14.

Lashmar, Paul (2017): No More Sources? The impact of Snowden's revelations on jounalists and their confidential sources. In: Journalism Practice, (11), 3-4, S. 665–688.

Liang, Bin/Hong, Lu (2010): Internet Development, Censorship, and Cyber Crimes in China. In: Journal of Contemporary Criminal Justice (26) 1, S. 103–120.

Lobe, Adrian (2019): Speichern und Strafen. Die Gesellschaft im Datengefängnis. München, C. H. Beck.

Lobo, Sascha (2017): Unsere Sicherheit ist eine Inszenierung. Anschläge in Europa. https://www.spiegel.de/netzwelt/web/islamistischer-terror-in-europa-unsere-sicherheit-ist-eine-inszenierung-a-1150015.html, 23. April 2020.

Luhmann, Niklas (1975): Macht, 3. Auflage. Stuttgart, UTB.

Luhmann, Niklas (1984): Soziale Systeme. Grundriß einer allgemeinen Theorie. Frankfurt am Main, Suhrkamp.

Luhmann, Niklas (1991a): Funktion und Kausalität. In: ders. (Hrsg.): Soziologische Aufklärung 1. Aufsätze zur Theorie sozialer Systeme, 6. Auflage. Opladen, Westdeutscher Verlag, S. 9–30.

Luhmann, Niklas (1991b): Funktionale Methode und Systemtheorie. In: ders. (Hrsg.): Soziologische Aufklärung 1. Aufsätze zur Theorie sozialer Systeme, 6. Auflage. Opladen, Westdeutscher Verlag, S. 31–53.

Luhmann, Niklas (1997): Die Gesellschaft der Gesellschaft. Frankfurt am Main, Suhrkamp.

Mills, Anthony (2018): Now You See Me – Now You Don't. Journalists' Expercience With Surveillance. In: Journalism Practice, https://doi.org/10.1080/17512786.1555006, 23. April 2020.

Moßbrucker, Daniel (2018): Überwachbare Welt: Wird das Darknet zum Mainstream digitaler Kommunikation? In: Regierungsfoschung.de. Das wissenschaftliche Online-Magazin der NRW School of Governance. https://regierungsforschung.de/ueberwachbare-welt-wird-das-darknet-zum-mainstream-digitaler-kommunikation/, 23. April 2020.

Moßbrucker, Daniel (2019a): Digitaler Informantenschutz. Was Daten über Journalisten verraten. In: Schröder, Michael & Schwanebeck, Axel (Hrsg.): Big Data – In den Fängen der Datenkraken. Die (un-)heimliche Macht der Algorithmen. Baden Baden, Nomos, S. 87–105.

Moßbrucker, Daniel (2019b): PSSSST! So ist es um den Schutz von Whistleblowern bestellt. In: politik & kommunikation, Nr. 127, S. 40–43.

Nassehi, Armin (2019): Muster. Theorie der digitalen Gesellschaft. München: C. H. Beck.

Noesselt, Nele (2014): Internationale Dimensionen des „chinesischen" Internets. In: Zeitschrift für Internationale Beziehungen (21) 1, S. 161–177.

Reporter ohne Grenzen (2019): Alles unter Kontrolle? Internetzensur und Überwachung in Russland. www.reporter-ohne-grenzen.de/russlandbericht, 21. April 2020.

Richter, Philipp (2017): Das NetzDG – Wunderwaffe gegen "Hate Speech" und "Fake News" ode rein neues Zensurmittel? In: ZD-Aktuell, 05623.

Roßbach, Nikola (2018): Achtung, Zensur! Über Meinungsfreiheit und ihre Grenzen. Berlin: Ullstein.

Scaife, Nolen/Carter, Henry/Lidsky, Lyrissa/Jones, Rachael L./Traynor, Patrick (2017): OnionDNS: a seizure-resistant top-level domain. In: Int. J. Infor. Secur. (17), S. 645–660.

Schallbruch, Martin (2018): Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt. Wiesbaden: Springer Fachmedien.

Schulze, Matthias (2017): Verschlüsselung in Gefahr. Weltweit schwächen Staaten die Cyber-Sicherheit – Deutschland sollte dagegenhalten. In: SWP-Aktuell (56) August 2017.

Schulze, Matthias/Voelsen, Daniel (2020): Einflusssphären der Digitalisierung. In: Lippert, Barbara/Perthes, Volker (Hrsg.): Strategische Rivalität zwischen USA und China. Worum es geht, was es für Europa (und andere) bedeutet. SWP Studie 1, Februar 2020, Berlin: Stiftung Wissenschaft und Politik.

Snowden, Edward (2019): Permanent Record. London, Macmillan.

Staben, Julian (2016): Der Abschreckungseffekt auf die Grundrechtsausübung. Strukturen eines verfassungsrechtlichen Arguments. Tübingen, Mohr Siebeck.

Steinhöfel, Joachim (2018): Heiko Maas' Anschlag auf die Meinungsfreiheit. In: The European. Das Debatten-Magazin. https://www.theeuropean.de/joachim-nikolaus-steinhoefel/13404-neues-zensurgesetz-ist-verfassungswidrig, 21. April 2020.

Stolton, Samuel (2020): LEAK: Comission considers facial ecognition ban in AI 'white paper'. https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/, 23. April 2020.

Vieth, Kilian/Wetzling, Thorsten (2019): Data-driven Intelligence Oversight. Recommendations for a System Update. Berlin, Stiftung Neue Verantwortung.

Wagner, Ben (2009): Deep Packet Inspection and Internet Censorship: International convergence on an "Integrated Technology of Control", http://dx.doi.org/10.2139/ssrn.2621410, 21.04.2020.

Weiser, Mark/Brown, John Seely (2015): Das kommende Zeitalter der Calm Technology. In: Sprenger, Florian/Engemann, Christoph (Hrsg.): Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt. Bielefeld, Transcript, S. 59–72.

Zuboff, Shoshana (2018): Das Zeitalter des Überwachungskapitalismus. München: Piper.