Steffen Augsberg,
Petra Gehring (Hg.)

Datensouveränität

Positionen zur Debatte

campus

Steffen Augsberg ist Professor für Öffentliches Recht an der Justus-Liebig-Universität Gießen. *Petra Gehring* ist Professorin für Philosophie an der Technischen Universität Darmstadt. Beide leiteten im Jahr 2021 gemeinsam die Projektgruppe »Datensouveränität« am Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI). Das Zentrum wird gefördert durch die Hessische Ministerin für Digitale Strategie und Entwicklung.

Steffen Augsberg, Petra Gehring (Hg.)

Datensouveränität

Positionen zur Debatte

Campus Verlag
Frankfurt/New York

ISBN 978-3-593-51643-1 Print
ISBN 978-3-593-45194-7 E-Book (PDF)
DOI 10.12907/978-3-593-45194-7

Umschlaggestaltung: Campus Verlag GmbH, Frankfurt am Main.
Satz: le-tex xerif
Gesetzt aus der Alegreya
Druck und Bindung: Beltz Grafische Betriebe GmbH, Bad Langensalza
Beltz Grafische Betriebe ist ein klimaneutrales Unternehmen (ID 15985–2104-1001).
Printed in Germany

www.campus.de

Inhalt

Datentoxikalität: Eine technikethische Herausforderung

Gerhard Schreiber

Im biochemischen Kontext wird als toxisch[1] die schädigende Wirkung eines Stoffes bei Kontakt mit einem biologischen System (Mensch, Tier, Pflanze) bezeichnet. Als Weiterführung dieser naturwissenschaftlichen Verwendungsweise von »toxisch« bzw. »Toxizität« zur Beschreibung des Ausmaßes der Giftwirkung eines bestimmten Stoffes auf lebende Organismen wird »toxisch« seit einiger Zeit vermehrt auch auf destruktive Denk- und Verhaltensweisen bezogen, die das gemeinschaftliche oder gesellschaftliche Miteinander von Menschen vergiften (z. B. »toxische Männlichkeit«[2]). Der Begriff wird auch auf alles Mögliche übertragen, was mit Risiko und/oder Dysfunktionalität behaftet sein und negative Auswirkungen zeitigen kann (z. B. toxische Wertpapiere, toxische Beziehungen, toxisches Arbeitsumfeld bis hin zur zwanghaft optimistischen toxischen Positivität). Insofern wird durch den in diesem Beitrag zur Diskussion gestellten Begriff der Datentoxikalität die Erweiterung des Bedeutungsspektrums von »Toxizität« fortgesetzt und zugleich spezifiziert, indem mit der Rede von »toxikalisch« bzw. »Toxikalität«[3] anstelle von toxisch bzw. Toxizität speziell auf die sozialpsychologische Dimension einer Schädigungswirkung abgehoben wird, wie sie auf der Ebene zwischenmenschlicher Beziehungen und in Prozessen sozialer Interaktion zur Geltung kommt. Über Phänomene toxischer Wirkung auf pharmakologischer, biochemischer, genetischer, physikalischer oder physiologischer Ebene hinaus soll durch die Rede von der Toxikalität von

1 Eine Adjektivbildung zu griechisch τοξικόν, »Gift zum Bestreichen der Pfeilspitzen«, kurz: »Pfeilgift«; aus griechisch τοξικός, »zu Pfeil und Bogen gehörig« (Passow 1825: 876; Kluge 2011: 923).

2 Vgl. auch die althergebrachten Bezeichnungen eines boshaft-gehässigen Menschen als Giftzwerg, Giftnudel oder Giftkröte.

3 Zu dieser Begriffsneuschöpfung vgl. Gennermann 2020, die unter Toxikalität nicht nur als giftig empfundene und beschreibbare physikalische und chemische Wirkungen, sondern auch entsprechende »zwischenmenschliche oder interinstitutionelle Beziehungen« ([2]) subsumiert.

Daten[4] also deren mögliche Schädigungswirkung im Bereich menschlichen Zusammenlebens in den Begriff gebracht werden.

Bevor ausgewählte Beispiele für Datentoxikalität dargestellt und technikethische Überlegungen darüber angestellt werden, wie einer derartigen Schädigungswirkung von Daten begegnet werden könnte, gilt es den Aspekt der Schädigung zu konkretisieren.

1. Schädigung

Unter Schädigung[5] ist sowohl der Prozess des Geschädigt*werdens* als auch der Zustand des Geschädigt*seins* zu verstehen, wobei der zugefügte bzw. erlittene »Schaden« eine »negative, beeinträchtigende Einwirkung *und* das [umfasst], was sie an Verlust, Zerstörung oder Nachteil zur Folge hat« (Pfeifer 1989: 1486; meine Hervorhebung, GS). Schädigung meint also nicht allein den schädigenden Vorgang selbst, sondern auch das weite Spektrum möglicher sich dadurch unmittelbar oder mittelbar einstellender Folgen. Jedwede negative Einwirkung als Schädigung verstehen zu wollen, hätte freilich einen völlig entkonkretisierten Schädigungsbegriffs zur Folge, dessen praktische Handhabbarkeit zu entgleiten drohte. In Anlehnung an den berühmten Satz des Paracelsus ist demnach zu statuieren: *dosis facit venenum* – die Dosis macht das Gift.[6]

---

4 Das Verhältnis von Daten und Informationen sei im Folgenden der Einfachheit halber im Anschluss an Bernhard C. Witt dahingehend gefasst, dass Daten »kontextfreie Angaben« sind, »die aus interpretierten Zeichen bzw. Signalen bestehen«, während Informationen »Daten« sind, »die (i.d.R. durch den Menschen) kontextbezogen interpretiert werden und (insbesondere prozesshaft) zu Erkenntnisgewinn führen« (Witt 2010: 4 f.). Daten sind also noch nicht, sondern werden erst zu Informationen durch Kontextualisierung und Interpretation – sie werden sozusagen in Form gebracht (so die eigentliche Bedeutung von lateinisch *informare* als einformen).

5 Ich spreche an dieser Stelle bewusst von Schädigung bzw. schädigend anstelle von Schädlichkeit bzw. schädlich, um den kleinen, aber bedeutsamen Unterschied zu markieren, dass etwas unmittelbar oder mittelbar *schädigend* wirken, während *schädlich* auch etwas sein kann, das *nicht* unweigerlich zum Eintritt einer unmittelbaren oder auch nur mittelbaren Schädigung führt. Die dem Adjektiv *schädlich* üblicherweise gegebene Bedeutung »zu Schädigungen führend« (Duden [6]2020: 720) ist also nicht im Sinne einer Zwangsläufigkeit zu verstehen, so wie das bloße Vorhandensein einer giftigen Substanz in einem lebenden Organismus nicht unbedingt zu einer Vergiftung desselben führt.

6 Im Original der *Septem Defensiones* (1537/1538) allerdings umgekehrt formuliert: »alle ding sind gift und nichts on gift; alein die dosis macht das ein ding kein gift ist« (Paracelsus 1928: 138).

Eine Schädigung liegt erst vor, wenn ein normativ definierter Schwellenwert – juristisch gesprochen: eine Erheblichkeitsschwelle – erreicht und überschritten wird (Meyer 2005: 36–39). Dies ist zweifellos bei zugefügten Verletzungen physischer oder psychischer Art der Fall, aber auch bei körperlich-seelisch-geistig sich auswirkenden Verletzungen individueller Freiheits- und Selbstbestimmungsrechte, die sich, sofern in ihnen ein Moment fremdmächtiger Willensdurchsetzung zum Tragen kommt, zugleich als *gewalthaltig* qualifizieren lassen (Schreiber 2022: 84–86). Eine Schädigungswirkung im strengen Sinne setzt also stets Urheberschaft voraus, welche sowohl personal wie nicht-personal, also subjektanalog (Gerhardt 1996: 8) gedacht werden und damit konkret identifizierbaren Personen ebenso wie Strukturen und Verhältnissen zukommen kann.

Als spezifische Form der Einwirkung ist Schädigung notwendig relational: Schädigung manifestiert sich stets im Verhältnis zu etwas oder jemandem, was nicht heißt, dass Schädigung von den sie Erleidenden immer auch *als* Schädigung wahrgenommen wird. Aus der Relationalität jeglichen Schädigungsgeschehens folgt deshalb, dass Schädigung *an sich* nicht existiert. Damit ist nicht behauptet, dass Schädigung immer auch von einem konkret identifizierbaren Subjekt gegenüber einem gleichermaßen konkret identifizierbaren Objekt erfolgt, wohl aber ist behauptet, dass es keine Schädigung ist, wenn sie in keiner Weise gegenüber etwas oder jemandem zur Wirkung kommt. Darin zeigt sich die pathische Seite einer Schädigungswirkung – pathisch entsprechend der Grundbedeutung von griechisch πάσχειν zunächst ganz allgemein als Erfahren einer Einwirkung von außen (Passow 1825: 399), noch ohne negative oder positive Bewertung, sodass das Feststellen einer Einwirkung und deren Bewertung zweierlei bleiben.

Mit der wesenhaften Relationalität von Schädigung korrespondiert der Umstand, dass die als Toxizität bezeichnete Schädigungswirkung eines bestimmten Stoffes auf der biochemischen Ebene dessen *Kontakt* mit einem lebenden Organismus voraussetzt, eine unvermittelt (akut) oder mit der Zeit (chronisch) auftretende Schädigungswirkung eines solchen in fester, flüssiger, gasförmiger oder plasmatischer Form vorliegenden Stoffes also erst dann bestehen kann, wenn ein Organismus diesem ausgesetzt (gewesen) ist und ihn in irgendeiner Weise (z. B. oral, dermal oder inhalativ) aufgenommen hat. So betrachtet sind auch Daten nicht *an sich* schädigend, sondern nur insofern, als sie gegenüber etwas oder jemandem eine entsprechende

Wirkung zeitigen.[7] Dies rechtfertigt den Vergleich von Daten mit einem Gefahrstoff wie beispielsweise Asbest (Véliz 2021: 107), chemisch an sich unbedenklichen faserförmigen Silikaten mit hervorragenden technischen Eigenschaften, die ihre Schädigungswirkung erst infolge einer Exposition gegenüber Asbestfasern entfalten können.

Kurzum: Was schädigend *wirkt*, muss nicht *an sich* schädigend *sein*. Dies gilt es auch bei der als toxikalisch bezeichneten Schädigungswirkung von Daten im Blick zu haben,[8] bei welcher zugleich, analog zur Toxizität als Schädigungswirkung eines Stoffes im biochemischen Kontext, zwischen einer quantitativen Komponente (Wirkstärke) und einer qualitativen Komponente (Wirkweise) unterschieden werden kann, was bei der nachfolgenden Konkretisierung von Datentoxikalität anhand ausgewählter Beispiele weiter zu bedenken sein wird.

2. Exemplarische Konkretisierungen

Angesichts der mannigfaltigen Mittel, Methoden und Möglichkeiten, Daten zu generieren, zu transferieren, zu analysieren und in irgendeiner Form nutzbar zu machen bzw. zu nutzen, haben wir es mit einem ebenso komplexen wie facettenreichen Phänomenbereich zu tun, dessen sachgemäße Erschließung eine multiperspektivische Betrachtungsweise erfordert, welche nicht nur differenziert genug ist, um Unterschiede zwischen einzelnen Phänomenen angemessen zu erfassen, sondern zugleich integriert genug, um ungerechtfertigte Trennungen zwischen ihnen zu vermeiden. Dies bedürfte einer wesentlich ausführlicheren systematischen Erörterung, wie sie im Rahmen dieses Beitrags nicht möglich ist. Im Folgenden kann es deshalb nur darum gehen, mit ständiger Rücksicht auf den spezifischen Unter-

7 Insofern kann gesagt werden: Daten sind weder gut noch schlecht, sondern indifferent (ἀδιάφορον). Sie befinden sich sozusagen in Möglichkeit (*in potentia*) gleichermaßen zum Guten wie zum Schlechten.

8 An dieser Stelle zeigt sich der Vorteil der Neubildung Datentoxikalität gegenüber der gleichermaßen denkbaren Rede von einer Toxizität von Daten (so z. B. Riedesel 2021: 412, der »data toxicity« allerdings versteht als »data that requires special handling«), welche die begriffliche Unschärfe in Kauf nehmen müsste, dass Gifte sowohl organische wie anorganische Stoffe sein können, während Toxine allein die von Lebewesen (einschließlich eukaryotischer Art) synthetisierten Gifte umfassen – ein Unterschied, der bei der Applikation des Toxizitätsbegriffs auf Daten sozusagen überschrieben wird.

suchungsgegenstand, für welchen ich zugleich mit Bedacht die zunächst eigens vorgestellte Begrifflichkeit verwende, ein paar strukturierende Breschen in dieses Dickicht zu schlagen.

In aller Vorläufigkeit kann hierzu zwischen Phänomenen unterschieden werden, in denen Daten – ungeachtet dessen, dass wir zumeist sagen, dass wir sie »nutzen« bzw. dass sie zur »Nutzung« existieren, was nahelegt, dass Daten gleichsam nur einen Nutzen haben – eine direkte Schädigungswirkung entfalten, und solchen mit indirekter Schädigungswirkung. Während bei ersteren eine Schädigung unmittelbar beabsichtigt und ganz bewusst angesteuert wird, erfolgt bei letzteren eine Schädigung mittelbar und wird sozusagen als Nebenwirkung in Kauf genommen. Während bei ersteren vornehmlich an Vorgänge zu denken ist, bei denen Daten von konkret identifizierbaren Subjekten gezielt zur Schädigung eines gleichermaßen konkret identifizierbaren Gegenübers eingesetzt werden und solche Schädigungen anzunehmenderweise auch leichter zum Vorschein kommen, handelt es sich bei Phänomenen indirekter Schädigungswirkung – jedenfalls wie sie hier im Blickpunkt stehen – um wesentlich schwieriger zu fassende Schädigungsvorgänge, die sich gegenüber einer breiteren Gemeinschaft oder der Öffentlichkeit überhaupt ereignen, ohne dass ein einzelner Urheber und eine direkte Verbindung zwischen Schädigendem und Geschädigtem identifizierbar ist.

Damit ist nicht bestritten, dass der so beschriebene Phänomenbereich wesentlich durch Übergängigkeit und Unabschließbarkeit charakterisiert ist und sich einzelne Phänomene zum Teil allenfalls schwerpunktmäßig einer der beiden Seiten zuordnen lassen. Ein Schubladendenken mit dem Anspruch, einzelne Phänomene in säuberlich getrennte Kategorien einzuordnen, ist auch an dieser Stelle fehl am Platz und demnach nicht der Anspruch der nachfolgenden orientierenden Bemerkungen.

2.1 Phänomene direkter Schädigungswirkung

Bei Phänomenen direkter Schädigungswirkung ist zunächst ganz allgemein an Situationen und Konstellationen zu denken, in denen personenbezogene, sicherheitsrelevante oder in irgendeiner Hinsicht sensible Daten – um einen in diesem Zusammenhang vielfach verwendeten somatischen Phraseologismus ebenfalls zu bemühen – »in falsche Hände« geraten (sind) und gezielt schädigend gegen andere Personen, Unternehmen oder Institutio-

nen eingesetzt werden. Diesen Formen des Datenmissbrauchs geht meist eine Variante des Datendiebstahls z. B. durch Phishing, Snarfing, Pharming oder Spoofing voraus[9], wobei die Motive durchaus unterschiedlich sein können, sei es primär pekuniär zur Löse- oder Schweigegelderpressung oder sei es primär um der Diskreditierung oder Desinformation eines Gegenübers willen, sodass vornehmlich dessen psychische oder soziale Schädigung bezweckt, eine gleichzeitige finanzielle Schädigung aber mehr oder weniger bewusst in Kauf genommen wird.

Persönliche Daten können durch andere aber auch gezielt als Waffe eingesetzt werden, wenn sie ohne Wissen der betreffenden Personen öffentlich gemacht werden, um diese bloßzustellen oder einzuschüchtern, wie es z. B. beim Doxxing der Fall ist (Douglas 2016: 199). Diese Form digitaler Gewalt wird vornehmlich gegen Prominente, Journalist*innen oder ehemalige Beziehungspartner*innen (zu Letzterem vgl. Bauer/Hartmann 2021: 76, 91), aber auch Vertreter*innen gegnerischer Positionen ausgeübt, was sowohl durch Einzelpersonen als auch durch Kollektive erfolgen kann. Letzteres etwa beim *Rénròu Sōusuǒ* (Chang/Leung 2015), einer vor allem in China und Taiwan verbreiteten Art virtuellem Lynchmob. Daten sind dann nicht nur in falschen Händen, sondern auch »am falschen Ort«.

Dieser Umstand, dass Daten eine schädigende Wirkung auch dadurch entfalten können, dass sie sich am falschen Ort befinden, macht solche deplatzierten Daten mit Schmutz vergleichbar – jedenfalls dann, wenn Schmutz im Anschluss an die britische Sozialanthropologin Mary Douglas allgemein und ohne Konnotation des Pathogenen und Unhygienischen definiert wird als »matter out of place« (1966: 36) – eine Sache nicht am Platz. Diese von Douglas wiederum dem britischen Diplomaten Philip Stanhope, 4. Earl of Chesterfield (1694–1773), zugeschriebene Schmutzdefinition (kritisch dazu Thompson 2021: 147 f.) setzt sowohl eine wie auch immer geartete Ordnung als auch zugleich einen Verstoß gegen dieselbe voraus, was Schmutz zu etwas Relativem macht. Schmutz ist demnach nie etwas Isoliertes, sondern steht immer in Beziehung zu einem ihn von sich ausschließenden System (Douglas 1966: 41). An einem Alltagsbeispiel verdeutlicht: »Essen ist nicht an sich schmutzig, aber es ist schmutzig, wenn

9 Für eine Übersicht vgl. Heartfield/Loukas 2018: 103 f. Als Spezialform von Datendiebstahl können Hackerattacken mittels datenlöschender Malware (Wiper) betrachtet werden, wie sie auch Teil der Kriegsführung – aktuell im Angriffskrieg Russlands gegen die Ukraine (Tidy 2022) – sein können.

man Kochutensilien im Schlafzimmer deponiert, oder Essen auf der Kleidung verschüttet« (ebd.: 36; meine Übersetzung, GS). Auf diesen bildlichen Vergleich von Daten mit Schmutz im angesprochenen Sinne, der freilich nicht überstrapaziert werden darf und doch die Ambivalenz von Daten auch im Blick auf ihre mögliche Schädigungswirkung gut zu veranschaulichen vermag, wird noch zurückzukommen sein.

Daten können toxikalisch schließlich auch dann sein, wenn sie manipuliert oder verfälscht werden – um im angesprochenen Bild zu bleiben: wenn man sie *ver*schmutzt. Charakteristisch für solches *data tampering* ist, dass Daten von anderen nicht einfach entwendet, sondern an Ort und Stelle belassen werden, und zwar gezielt verändert. Diese Veränderungen können ganz im Kleinen erfolgen, bis hin zur Modifizierung eines einzigen Pixels in einem Bild (Alberti u. a. 2019), was für die Betroffenen meist nur schwer ersichtlich ist, im Bereich etwa der Finanz- oder Betriebsbuchhaltung aber erheblichen Schaden verursachen kann. Selbst minimalinvasive Eingriffe in die Datenintegrität von Unternehmen können also von erheblicher wirtschaftlicher und damit zugleich sozialer Tragweite sein, was die von dem japanischen Ökonomen Hiroyuki Itami wirkmächtig vertretene Auffassung, die wertvollsten und für die Überlebensfähigkeit eines Unternehmens entscheidenden Vermögenswerte seien unsichtbar (Itami 1987: 12 f.), in einem anderen Licht erscheinen lässt. Die Erklärung von Daten – genauer: deren Monetarisierung,[10] Verwaltung und Erfassung – zum wichtigsten zukünftigen Vermögenswert von Unternehmen überhaupt, nicht nur, wie schon jetzt, im Bereich der Digitalwirtschaft, ist insofern dahingehend zu ergänzen, dass es sich hierbei zugleich um einen der gefährlichsten Vermögenswerte von Unternehmen handelt, der entsprechende Vorkehrungen und Schutzmaßnahmen unabdingbar macht. Die verschiedentlich, aber fälschlicherweise (Fanshawe 2022: 42 f.) dem US-amerikanischen Ökonom Peter F. Drucker zugeschriebene Managementweisheit »What gets measured gets managed« erweist sich in der heutigen Zeit von Big Data jedenfalls von ungeminderter, wenn nicht ungeahnter Aktualität.

Nicht weniger bedeutsam sowohl in wirtschaftlicher wie in sozialer Hinsicht ist die Sicherstellung und Sicherung der Datenintegrität im Bereich der kritischen Infrastruktur. Man denke, um ein Beispiel aus dem Sektor Transport und Verkehr anzuführen, an die bei einem zukünftigen digitalisierten Bahnbetrieb geplante Zug-zu-Zug-Kommunikation samt

10 Für einen Überblick vgl. Jentzsch 2019.

sensorbasierter Zuglokalisierung (Schomäcker 2019) oder, als Beispiel aus dem Gesundheitssektor, an die Arzneimittelherstellung (Schmitt 2019). Ganz grundsätzlich gilt dies auch für den Bereich der Wissenschaft, in dem schon kleinste, absichtliche oder unabsichtliche, Verfälschungen von Originaldaten und Datenbanken weitreichende Schädigungswirkungen auch im Sozialen entfalten können, wenn darauf z. B. die Verbreitung von Desinformation gründet oder sich daran anschließende gesellschaftliche Diskurse und politische Maßnahmen entsprechend kompromittiert sind. Das Streben nach höchstmöglicher Datenintegrität ist forschungspragmatischer Imperativ und, gemeinsam mit Datenqualität als einer die Verwendungsgerechtigkeit mit umschließenden Anforderung, geradezu *conditio sine qua non* für gute Wissenschaft, wobei eine Verletzung der Datenintegrität nicht nur bei fehlerhafter oder mangelnder Authentifizierung des Datenursprungs, sondern auch dann bestehen kann, wenn ambivalente, veraltete, redundante oder inkonsistente Datenbestände vorliegen (RfII 2019).

Die vorstehend dargestellten Phänomene direkter Schädigungswirkung durch entwendete, böswillig veröffentlichte oder in irgendeiner Hinsicht problembehaftete Daten machen deutlich, dass und inwiefern Daten toxikalisch nicht nur in Prozessen sozialer Interaktion, sondern auch auf der gesamtgesellschaftlichen Ebene wirken können. Wie die Oxforder Philosophin Carissa Véliz (2021: 107–139) anhand einschlägiger Beispiele aus Geschichte und Gegenwart darlegt, kann der falsche Umgang mit personenbezogenen Daten nicht nur die nationale Sicherheit eines Staates bedrohen (Stichwort: Equifax-Hack) oder zur Korrumpierung repräsentativ-demokratischer Regierungssysteme beitragen (Stichwort: Cambridge Analytica), sondern auch die gegenwärtige Sinn- und Orientierungskrise liberaler Gesellschaften noch weiter vorantreiben, etwa indem auf Social-Media-Plattformen eine Kultur narzisstischer Selbstdarstellung und selektiver Selbstjustiz befördert wird, was eine Korrektur des allgemeinen Umgangs mit personenbezogenen Daten unabdingbar macht. Dass vor dem Hintergrund der Auswirkungen einer zunehmend digitalisierten Lebenswelt überdies eine Re-Evaluation der bisherigen Vorstellung und Wahrnehmung von Privatsphäre und Öffentlichkeit in ihrem Verhältnis zueinander erforderlich ist, verdeutlichen auch die von Jürgen Habermas neuerlich angestellten Überlegungen »zu einem *erneuten* Strukturwandel der politischen Öffentlichkeit« (Habermas 2021: 470; meine Hervorhebung, GS) im Zuge

seiner ebenso bedenkenswerten wie nachdenklich stimmenden Revision der eigenen Theorie der politischen Öffentlichkeit.[11]

Mit letzteren Bemerkungen ist bereits der Übergang zur Reflexion darüber vollzogen, inwiefern Daten auch eine indirekte Schädigungswirkung entfalten können, die den bislang angesprochenen Phänomenen in ihrem Wirkpotenzial in nichts nachstehen müssen, auch wenn – oder vielleicht: gerade weil – die Schädigungswirkung prozesshaft schleichend, gleichsam hinter dem Rücken des Einzelnen und damit zunächst weniger augenfällig verlaufen mag.

2.2 Phänomene indirekter Schädigungswirkung

Ausgangspunkt für die im Vergleich zu Phänomenen direkter Schädigungswirkung ungleich schwieriger lokalisierbare und insofern potentiell weiterreichende, wenn auch in ihrer ganzen Tragweite noch nicht überschaubare indirekte Schädigungswirkung von Daten ist der Umstand, dass wir nicht lediglich durch gezielte Eingaben, sondern durch *jegliche* Internetaktivität und Nutzung digitaler Dienste permanent und unweigerlich Datenspuren hinterlassen (Wenhold 2018: 33–35).[12] Diese Datenspuren »zeichnen« gewissermaßen »ein digitales Abbild unseres Lebens« (Stampfl 2012: 394) und eröffnen Dritten nicht nur vielfältige, noch bis vor wenigen Jahren ungeahnte reale Möglichkeiten der Kontrolle und Bevormundung, aber auch der Gefahrenabwehr und Strafverfolgung, sondern können, durch gezielte Auswertung zu Nutzungs-, Kauf- und Bewegungsprofilen verdichtet, zugleich Aufschluss geben über Eigenschaften und Persönlichkeitsmerkmale eines Menschen einschließlich seiner sozialen Bezüge und Beziehungen.

---

11 So wie nicht alles Private auch politisch (hier im umfassenden aristotelischen Sinne als »die Polis betreffend«; πολιτικός von πολίς) sein muss, so muss nicht alles Private auch öffentlich sein – eine Aussage, die in der heutigen digital vernetzten Welt womöglich seltsam anmuten mag. Tatsächlich scheint Digitalität die Grenzlinie zwischen dem Privaten und dem Öffentlichen bei allem Haschen nach Likes und bei aller Gier nach Followern zunehmend zu verwischen.

12 Zur möglichen Unschärfe der Rede von Datenspuren vgl. Stäheli 2021: 66: »Die von den Verbindungen [der globalen Vernetzungsinfrastrukturen] produzierten Daten und Metadaten werden häufig als Datenspuren verstanden, wobei diese Metapher irreführend sein kann, da sie die arbiträre Beziehung zwischen dem Verbindungsgeschehen und den Daten übersieht. Die Akkumulation dieser Daten ist in der *corporate surveillance* zu einer der primären ökonomischen Kräfte geworden. Ihre Sammlung, Extraktion, Filterung, Prozessierung und Manipulation ermöglichen neue Formen der ökonomischen Wertschöpfung.«

Die Gesamtheit dieser z. B. beim Betreten der Online-Welt – jedenfalls ohne Proxy-Server oder Anonymisierungsnetzwerke – durch IP-Adresse, Cookies, Suchanfragen, Hardware- und Browsereinstellungen, Betriebssystem, installierte Software etc. generierten, individuell rückverfolgbaren Daten ist als »digitaler Fußabdruck« (Lambiotte u. a. 2014) eines Menschen nicht nur unverwechselbar, sondern auch gewissermaßen unhintergehbar: »Unlike footprints in the sand, digital traces in silica are not wiped away by the tide; instead, they accrete, leaving incredibly detailed records of social interaction« (Welser u. a. 2010: 117, Hervorhebung im Original weggelassen, GS). Das von Menschen in der Welt der Bits und Bytes bewusst oder unbewusst, absichtlich oder unabsichtlich hinterlassene Nebenprodukt der Datenspuren ist deshalb keineswegs wertloser Abfall,[13] sondern erweist sich für Dritte vielmehr als »Rohstoff« von unschätzbarem Wert, den es durch den Einsatz datenbasierter Technologien entsprechend abzubauen und ohne Rücksicht auf den ursprünglichen Kontext für neue Kontexte und Zwecke verwertbar zu machen gilt.[14] Selbst die augenscheinlich kostenlose Teilnahme am digitalen Leben kann sich damit als teuer erkauft erweisen – data non sunt gratis data.

Analog zu den beispielsweise mit der Gewinnung und Förderung mineralischer Rohstoffe einhergehenden unerwünschten Nebeneffekten für Mensch und Natur können negative realweltliche Folgen der Sammlung, Auswertung und Verarbeitung schier unendlicher Datenmengen beschrieben werden. Neben den enormen ökosozialen und sozioökonomischen Kosten der Digitalisierung und Datafizierung mitsamt ihrer globalen Ungleichverteilung (Parlamentarischer Beirat für nachhaltige Entwicklung des Deutschen Bundestages 2019: 2) ist auf die schädlichen Umwelteinwirkungen hinzuweisen, die direkt oder indirekt auf datengetriebene

13 Wenn überhaupt und mit Blick speziell auf den Schädigungsaspekt könnten Datenspuren als eine Art »Sondermüll« ganz eigener, nämlich *digitaler* Art bezeichnet werden, der dem Recycling zur Wieder- und Neuverwendung zugeführt wird, wohingegen unter »dark data« oder »zombie data« primär »unutilized or underutilized data« zu verstehen sind – »typically data that was collected and used for a single purpose, then forgotten about and often archived« (Laney 2018: 42).

14 Zu diesem Prozess und den verschiedenen metaphorischen Sprechweisen im Sinne des Data-Mining vgl. van Dijck 2014: 198–201; Thylstrup 2019: 2 f. Kritisch zum Bild von Daten als Rohstoff und dessen Abbau – zumindest, wenn damit ein allgemeingültiger »Mechanismus der Rekontextualisierung und Verarbeitung von Daten« suggeriert und die Aufwertung von »Daten zu faktisch Vorfindlichem« (Püschel 2014: 17) praktiziert werde, vgl. Püschel 2014: 10 u. 14 ff. Speziell zu den Prozessen der De- und Rekontextualisierung von Daten speziell für den Gesundheitsbereich vgl. Deutscher Ethikrat 2018: 14 f., 47 f. und 86–88.

Infrastrukturen zurückgehen (Bietti/Vatanparast 2020). Es wird geschätzt, dass die Informations- und Kommunikationstechnologiebranche bis zum Jahr 2040 – ohne entsprechende Gegenmaßnahmen – für über 14 % der globalen Treibhausgasemissionen (bei Zugrundelegung der Zahlen von 2016) verantwortlich sein wird (Belkhir/Elmeligi 2018), während aktuellen Berechnungen zufolge der Anteil allein der Rechenzentren (»Server-Farmen«) am weltweiten Stromverbrauch von 1,15 % im Jahr 2016 auf knapp 2 % im Jahr 2030 steigen wird und dieser Anstieg auch durch etwaige Effizienzgewinne aufgrund von technologischen Innovationen nicht gänzlich aufgefangen werden kann (Koot/Wijnjoven 2021: 7 f. u. 11). Um ein Beispiel zu nennen: Die Rechenzentren in der selbsternannten Internet-Hauptstadt Europas Frankfurt am Main verbrauchen mittlerweile deutlich mehr Strom als der Frankfurter Flughafen und sind, wie Zahlen aus dem Jahr 2018 zeigen, für rund ein Fünftel des Gesamtstromverbrauchs der Stadt Frankfurt verantwortlich (Wacket 2020); die enorme, bislang ungenutzte Abwärme der Rechenzentren soll in verschiedenen Pilotprojekten für das Heizen von Büro- und Wohngebäuden nutzbar gemacht werden (Rittel 2021), gewissermaßen »Heizen mit Datenverkehr« (Janović 2021). Die Rede von schädlichen Daten ist also mehrdeutiger als es zunächst scheint.

Auch digitale Datenspuren selbst sind, wie die dänische Kommunikationswissenschaftlerin Nanna Bonde Thylstrup argumentiert, nicht adiaphorisch, als aus ethischer Sicht neutrale Phänomene, sondern insofern als »Schadstoff« zu betrachten, als sie der ökonomischen Logik der Extraktion folgten, während sie zugleich durch die Spuren der Körper gekennzeichnet blieben, von denen sie ursprünglich stammten (Thylstrup 2019: 2 und 4). Überhaupt gründe, so die Autorin, die Logik der Datafizierung »on a logic of waste and recycling, with significant implications for how we consider datafication's politics and ethics« (Thylstrup 2019: 1). Wie Thylstrup unter Rekurs auf Sarah Myers West weiter ausführt, etabliere die Kommerzialisierung von Daten[15] eine Logik des Datenkapitalismus, welche der Macht der Netzwerke dadurch den Vorrang einräume, dass sie quer zur wirtschaftlichen, politischen und sozialen Dimension der Technologie aus den in den Netzwerken generierten Datenspuren Werte schaffe (Thylstrup 2019: 2; dazu West 2019: 21). Darin zeige sich eine deutliche Affinität zum Konzept des Überwachungskapitalismus (*surveillance capitalism*) von Shoshana

15 Zu Chancen und Risiken datenbasierter bzw. datengetriebener Geschäftsmodelle vgl. Kretschmer 2018: 459–462.

Zuboff, die darunter eine neue »Unterart des Kapitalismus« versteht, »bei dem die Gewinne aus der einseitigen Überwachung und Veränderung menschlichen Verhaltens stammen« (Zuboff 2016; dazu Myers West 2019: 23). Diese datenkapitalistische Wertschöpfungskette, aber auch die von datenintensiven Unternehmen zuweilen bewusst durch die Überproduktion von Daten gleichermaßen produzierte wie reproduzierte »organisatorische Ignoranz« (Schwarzkopf 2020: 197) gilt es im Blick zu behalten, wenn Daten als strategische Gegenwartsressource (»das neue Öl«; vgl. Spitz 2017: 9) und Datenökosysteme[16] als »Betriebssysteme der zukünftigen globalen datengetriebenen Wirtschaft« (Fraunhofer-Verbund IUK-Technologie [2021]) betrachtet werden.

Die mit der digitalen Transformation aller Lebensbereiche (»Vierte industrielle Revolution«) einhergehende Datafizierung unseres Daseins[17] mit entsprechenden Folgen auch für unser Verständnis desselben erweist sich spätestens dann aber als selbstgestellte Falle, wenn die *scheinbare* digitale Freiheit, ob bewusst oder nicht, um den Preis *realer* Unfreiheit erkauft wird und Menschen dadurch, dass ihnen die Möglichkeit digitaler Selbstbestimmung[18] verwehrt wird, an der Ausschöpfung potenzieller individueller

16 Für eine aktuelle Definition von »Datenökosystem« auf fachliterarischer Basis vgl. Putnings 2021: 7: »Ein Datenökosystem ist das prägende, ganzheitliche Umfeld, in dem verschiedene Akteure zusammenkommen, um Daten zu produzieren, anzubieten, zu finden und zu »konsumieren« (d.h. nachzunutzen, zu verarbeiten, anzureichern, zu archivieren, zu publizieren, Entscheidungen darauf zu fällen etc.). Die Einflüsse des Datenökosystems wirken in alle Phasen der Datenlebenszyklen hinein, es schafft die entsprechenden *Rahmen-, Netzwerk- und regulativen Bedingungen* für die (Zusammen-)Arbeit mit Daten bzw. stellt diese konkret dar.«

17 Digitalisierung (»Umwandlung analoger Informationen in ein maschinenlesbares Format« [Mayer-Schönberger/Cukier 2017: 106) und Datafizierung (»Umwandlung von allem nur Vorstellbaren […] in Datenform, um sie damit quantifizieren zu können« [Mayer-Schönberger/Cukier 2017: 24]) sind dahingehend zu differenzieren, dass Digitalisierung zwar als »Turbolader der Datafizierung«, nicht aber als »Ersatz dafür« (ebd.) fungiert. Zur immer weiter fortschreitenden Digitalisierung unseres Alltags, einschließlich der zunehmenden Verlagerung wesentlicher Aspekte der Persönlichkeit ins Digitale, und der Datafizierung des Sozialen vgl. Filipović 2015: 7 ff. und die Beiträge bei Houben/Prietl 2018.

18 Zum Begriff der »digitalen Selbstbestimmung« vgl. Mertz u. a. 2016: 18, die darunter – im Rückgriff auf die Definition »allgemeiner« Selbstbestimmung durch den Deutschen Ethikrat (2013: 120 f.) – »[d]ie konkrete Entfaltung einer menschlichen Persönlichkeit bzw. die Möglichkeit der Realisierung von je eigenen Handlungsentwürfen und Handlungsentscheidungen« verstehen, »soweit dies eine bewusste Verwendung digitaler Medien betrifft oder dies von der Existenz oder Funktionsweise digitaler Medien (mit-)abhängig ist«, und insgesamt sieben Begriffskomponenten identifizieren: Kompetenz, Informiertheit, Werte, Freiwilligkeit, Wahlmöglichkeit, Willensbildung und Handlung (Mertz u. a. 2016: 21–26).

Entfaltungs- und Verwirklichungsmöglichkeiten wirksam gehindert werden. Auf diese Aktualisierungsbedürftigkeit des Konzepts der strukturellen Gewalt[19] unter digitalen Vorzeichen und die aufgrund umfassender digitaler Vernetzung heute nicht mehr nur als Orwell'sche Dystopie, sondern als allzu reale Gefahr erscheinende ubiquitäre und omnipräsente Überwachung von Menschen »bis in die Tiefe der Gefühls- und Gedankenwelt« (Lobo 2014) hinein – kurz: auf die Gefahr einer ›digitalen Diktatur‹ (Aust/Ammann 2014: 7 ff.)[20], deren Vorboten keineswegs allein in autoritären Regimen, sondern auch in Staaten der »Freien Welt« (Stichwort: Gläserne Belegschaft[21]) sichtbar sind, sei an dieser Stelle wenigstens hingewiesen.

Mit all dem soll keinem ostentativen Fortschrittsskeptizismus das Wort geredet, geschweige denn unter Zuhilfenahme düsterer Weltuntergangsmetaphorik die Unausweichlichkeit derselben beschworen, wohl aber die realistische Einsicht in die alles durchstimmende Ambivalenz menschlicher Lebenswirklichkeit ausgesprochen werden, wonach sich durch den rasanten Fortschritt im Bereich der Informations- und Kommunikationstechnologien nicht nur neue Möglichkeiten und Wege eines lebensdienlichen Gebrauchs dieser Technologien, sondern zugleich immer auch neue Möglichkeiten und Wege auftun, sie zur Verfolgung, Unterdrückung und Schädigung anderer zu missbrauchen. Doch allein in Form skeptischer Negation scheinen technikethische Bemerkungen wenig zielführend. Daher sollen im abschließenden Abschnitt in aller Kürze noch einige kritisch-konstruktive Überlegungen aus technikethischer Perspektive dazu angestellt werden, wie einer Schädigungswirkung von Daten begegnet werden könnte.

19 Zur Unterscheidung zwischen personaler und struktureller Gewalt vgl. Galtung 1971: 9 ff.; dazu Schreiber 2022: 80–92. Es sei bemerkt, dass die Identifizierung von Gewalt*verhältnissen* bereits lange Zeit vor Galtung erfolgt ist, z. B. bei Marx 1962 [1867]: 765 u. 790.

20 Vgl. dazu Stefan Aust in einem Interview von 2014: »Diese totale Kontrolle, der der Mensch sich teils freiwillig, teils unfreiwillig unterwirft, ist, wenn Sie so wollen, eine Art von Diktatur. Und ich glaube, es ist wahrscheinlich die strengste Diktatur, was die Überwachung anbetrifft, die es jemals auf dieser Erde gegeben hat« (zitiert nach Baetz 2014: Abs. 2).

21 Vgl. dazu die umfangreiche Studie von Christl 2021.

3. Vergessenwerden durch Unauffindbarmachen

Wie im biochemischen Kontext die Toxizität von Stoffen nicht einfach eliminiert, aber der Umgang mit toxischen Stoffen entsprechend gestaltet und, wann immer notwendig, angepasst werden kann, so ist angesichts des vorstehend beleuchteten Phänomens der Datentoxikalität zu fragen, wie einer Schädigungswirkung von Daten im Bereich menschlichen Zusammenlebens begegnet werden kann. Dies zum Anlass zu nehmen, um über die Sinnhaftigkeit dessen zu räsonieren, dass überhaupt Daten in gegebenem, weitreichenden Umfang mittels digitaler Techniken gesammelt und gespeichert werden, wäre freilich müßig, zumal ein generelles Verbot des Sammelns und Speicherns beispielsweise speziell von personenbezogenen Daten[22] – von Fragen der politischen Durchsetzbarkeit und praktischen Umsetzbarkeit desselben einmal abgesehen – mit allem potentiell oder tatsächlich Schädlichen zugleich auch das potentiell oder tatsächlich Förderliche dieser Praxis beseitigen würde.[23] Nicht das Sammeln und Speichern von Daten als solches, sondern die Art und Weise, *wie* Daten aller Arten und Komplexitätsgrade gesammelt und gespeichert werden und zukünftig gesammelt und gespeichert werden sollten, steht zur Diskussion. Hierbei rückt – nicht nur, aber nicht zuletzt – im Falle personenbezogener Daten Fragen der Ver- und Entschlüsselung, der Zugangs- und Zugriffskontrolle, aber auch der Löschung und Löschbarkeit in den Fokus.

Es ist an dieser Stelle nicht der Ort, das aus dem Recht auf informationelle Selbstbestimmung[24] folgende »Recht auf Vergessenwerden«, wie es in

22 Hierauf scheinen mir die Überlegungen z. B. bei Véliz 2021: 108 u. 112 hinauszulaufen, die im Sammeln und Speichern personenbezogener Daten »a ticking bomb, a disaster waiting to happen« (108) sieht. Und weiter: »Personal data is dangerous because it is sensitive, highly susceptible to misuse, hard to keep safe, and desired by many – from criminals to insurance companies and intelligence agencies. The longer our data is stored, and the more it is analysed, the more likely it is that it will end up being used against us. Data is vulnerable, which in turn makes data subjects and anyone who stores it vulnerable too« (108). Nicht unähnlich Schneier 2019: 212 f.

23 Ebenso wenig lösungsorientiert (jedenfalls aus gesamtgesellschaftlicher Perspektive) wäre daher eine gemeinschaftliche Suche nach dem Heil in der Flucht in eine digitale Wüste, gewissermaßen ein Eremitentum »2.0«, aber auch pauschale Forderungen nach einer »Entdatafizierung«. Reflexionen über »Taktiken der Entnetzung« (Zurstiege 2019) und Fragen der Verantwortlichkeit des Einzelnen als Daten-Prosumer sind gleichwohl keineswegs obsolet.

24 Zur Herleitung des Rechts auf informationelle Selbstbestimmung (im Sinne eines Datenschutz-Grundrechts) aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG vgl. BVerfG 1983. Kritisch dazu z. B. Assion 2014.

Art. 17 der neuen EU-Datenschutz-Grundverordnung (DSGVO) verbrieft ist, en détail zu erörtern.[25] Dies soll nur insofern geschehen, als damit die Frage der Löschung und Löschbarkeit von Daten tangiert ist. Die Möglichkeit und Sicherstellung der Löschung und Löschbarkeit von Daten erweist sich nämlich als Schlüssel, wenn auch nicht als Allheilmittel, um insbesondere Phänomenen direkter Schädigungswirkung von Daten, wie sie aus deren Diebstahl, böswilliger Veröffentlichung oder Verfälschung resultieren können, entgegenzuwirken und bereits eingetretene Schädigungswirkungen abzumindern. Dabei ist einerseits zu bedenken, wie eine solche Löschung zu verstehen ist – in der DSGVO wird der Begriff »Löschen« nicht näher definiert.[26] Und andererseits muss gefragt werden, wie die dann so oder so verstandene Löschung auch im Falle toxikalischer Daten umgesetzt werden kann.

Was zunächst das *Verständnis* betrifft, ist entscheidend, dass das vielerorts in der öffentlichen Diskussion, zuweilen auch im juristischen Kontext missverständlich verkürzend[27] als »Recht auf Vergessen« bezeichnete »Recht auf Vergessenwerden« einen *aktiven* und *selektiven* Prozess zum Gegenstand hat. Dieser entspricht dem gleichermaßen aktiven und selektiven Prozess der Erinnerung (ανάμνησις), im Unterschied zum passiven Gedächtnis (μνήμη) – wenn auch eben im Modus der Verkehrung. Im Unterschied zur alltagssprachlichen Rede von Vergessen, aber auch der alltagsweltlichen Erfahrung von Erinnern und Vergessen[28] meint Vergessen*werden* in diesem Zusammenhang also etwas anderes als dass etwas *von selbst*, durch einen natürlichen Vorgang bzw. mit der Zeit, aus dem Gedächtnis verloren geht und so allmählich in Vergessenheit gerät. Vielmehr beschreibt Vergessen-

25 Für eine solche vgl. Luch u. a. 2014; Abbt 2016a und b.

26 Interessanterweise wird in den Begriffsbestimmungen von Art. 4 DSGVO »Löschen« als eine Variante der »Verarbeitung« von Daten betrachtet, wobei »Löschen« (*erasure*) und »Vernichtung« (*destruction*) mit der Konjunktion »oder« einander nebengeordnet (»[…] die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung«) werden, was – selbst wenn das »oder« als einschließendes (lateinisch *vel*) und nicht als ausschließendes (lateinisch *aut*) »oder« gemeint sein sollte – einen semantischen Unterschied zwischen Löschen und Vernichtung markiert.

27 Selbst von seinem Begriffsschöpfer, dem österreichischen Rechtswissenschaftler Viktor Mayer-Schönberger (Mayer-Schönberger 2012), sowie vom Bundesverfassungsgericht (BVerfG 2019a; 2019b). Zum Hintergrund vgl. ferner Hunzinger 2018: 34–38.

28 Pointiert z. B. Jahnel/Pallwein-Prettner 2022: 111 (unter Rekurs auf Mayer-Schönberger): »Für unser Gehirn [ist] das Erinnern die Ausnahme und das Vergessen die Regel. Für ein digitales Gerät ist es aber genau umgekehrt, hier erfordert das Vergessen einen aktiven Akt, das Erinnern geschieht automatisch.«

werden das Ergebnis eines intentional geleiteten und methodisch angeleiteten Löschungs*vorgangs*. Gleich ob Löschung dabei im strengen Sinne als Auslöschung (Eliminierung) oder im weiten Sinne als Beseitigung oder Entfernung verstanden wird – das Recht auf Vergessenwerden bezeichnet das Recht auf die unverzügliche Durchführung von Löschungsvorgängen[29], die im Falle personenbezogener Daten *zugleich* die »Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten« (Art. 17 Abs. 2 DSGVO) beinhaltet. Löschung von Daten im Sinne des Rechts auf Vergessenwerden bedeutet demnach nicht einfach nur »Erschwerung des Zugriffs auf Daten« (Abbt 2016a: 353; vgl. Abbt 2016b: 927), sondern Löschung von Daten *sowohl* »am Ort ihrer ersten Speicherung und Veröffentlichung« *als auch* an allen anderen Stellen, an denen die betreffenden Daten »veröffentlicht, archiviert oder verlinkt worden sind« (Buchner 2020: 307). Es geht mit einem Wort darum, diese Daten, einschließlich möglicher Datenrückstände in Archivspeichern, »aus der (Online-)Welt zu schaffen« (Herbst 2020: Rn. 49; zitiert bei Buchner 2020: 307).

Nun ist allerdings, und dies betrifft die *Umsetzung* solcher Löschungsvorgänge, nicht zu Unrecht die Frage aufgeworfen worden, ob das Löschen von Daten in einem Informationszeitalter wie dem unseren, in dem Menschen ständig und allerorten von einer Flut von Informationen überschüttet werden[30] und das, wie angesprochen, vom rasanten Fortschritt im Bereich der Informations- und Kommunikationstechnologien nachhaltig geprägt, wenn nicht gar getrieben ist, überhaupt »noch eine Zukunft« habe und nicht vielmehr als »Utopie der Moderne« (Hunzinger 2018: 213; vgl. 240)

---

29 Dass derartige Löschungsvorgänge auch vor dem Hintergrund des in Abschnitt 2.1. angestellten Vergleichs toxikalischer Daten mit Schmutz sowie der in Abschnitt 2.2 angesprochenen Grundlegung der Logik der Datafizierung in einer Logik von Abfall und Recycling bei Thylstrup beschrieben werden können – letzteres insofern, als Recycling selbst ein »Prozess zur Abfallvernichtung« durch Transformation von Abfall und Wiederzuführung durch Neubewertung, mithin ein Löschungsprozess ist, nämlich der »Zukunft des Dings als eben dieses Ding sowie dessen Vergangenheit« (Gehrlein 2020: 110) –, ist nur offensichtlich. Ebenso der radikale Widerspruch zum Vergessenwerden der Namen und Werke von Menschen nach ihrem Tod, wie es z. B. in der altägyptischen, klassisch-griechischen, aber auch biblischen Tradition gerade als »Unglück« gilt: »Der, der sein Vergessen beklagt, fühlt sich bereits wie ein Toter« (120; vgl. 119–122). Zu entsprechenden Lösungsansätzen für einen »digitalen Nachlass« vgl. Brucker-Kley 2013: 82–84.

30 Zur informationstechnischen Aufladung der Umgebung des Menschen wie überhaupt der »informatorische[n] Aufladung der physischen Welt« durch eine allgegenwärtige IKT vgl. Grunwald 2010: 85 f.

zu betrachten sei. In der Tat scheint eine endgültige und vollständige Löschung von Daten samt aller Datenrückstände zumindest im Internet in seiner heutigen Form, aber auch in Systemen der Künstlichen Intelligenz (KI), die von einer gleichermaßen komplexen Verarbeitung wie einer schnellen und unabsehbaren Verbreitung von Daten gekennzeichnet sind (Jorzig/Sarangi 2020: 138), nahezu unmöglich. Selbst wenn das Recht auf Vergessenwerden als »Menschenrecht« (Gstrein 2016) oder »Internet-Grundrecht« (Boehme-Neßler 2014) *geltend gemacht* werden kann, ist damit also noch nichts darüber gesagt, wie einem solchen Recht auch *Geltung verschafft* werden kann, wird doch in der Diskussion über das Recht auf Vergessenwerden geradezu gebetsmühlenartig betont, dass das Internet nichts vergesse.[31] Das sprichwörtliche Steckerziehen oder eine einfache, sichere Vernichtung von Daten wie durch die physische Zerstörung als Unbrauchbarmachung eines Speichermediums ist hier gerade nicht möglich und widerspricht überdies der »Logik digitaler Archive« (Stähli 2021: 416), zumal Löschungsvorgänge selbst wiederum Spuren erzeugen können, die dann ebenfalls zu beseitigen wären, woraus sich theoretisch ein infiniter Regress ergäbe.

So berechtigt die Forderung nach einem Recht auf Vergessenwerden ist, so illusorisch erscheint die Vorstellung einer einfachen praktischen Umsetzung desselben. Dies gilt umso mehr im Falle toxikalischer Daten, die als solche ja nicht nur in der Online-Welt, sondern auch in der Offline-Welt Spuren hinterlassen haben[32], sodass es nicht lediglich um ihre Löschung, sondern zugleich um ihre möglichst effektive realweltliche »Unschädlichmachung« gehen müsste. Was jedenfalls die Online-Welt betrifft, scheint mir ein theoretisch gangbarer Weg in der Rekonzeptualisierung des traditionellen Löschungsbegriffs zu liegen. Angesichts des oben bereits angesprochenen Umstandes, dass wir in der Online-Welt sozusagen auf Schritt und Tritt rückverfolgbare Datenspuren hinterlassen, kann es bei dem allgemein als Löschung bezeichneten Vorgang im Grunde nur darum gehen, ebendiese Rückverfolgbarkeit an einer bestimmten, und zwar der (jeweils) richtigen, Stelle zu un-

31 Zu diesem »Ewigkeitseffekt« vgl. Stumpf 2017: 40–44.

32 In der Offline-Welt allerdings kann »Vergessen« gerade der *falsche* Weg sein, selbst wenn er als »Therapeutikum« betrachtet werden sollte, wird doch das Trauma einer Vergangenheit nicht durch Vergessen bewältigt, sondern gerade durch »Erinnern, um zu überwinden« (Assmann 2020: 202). Zu dieser ethischen Verpflichtung zum Erinnern als Vergegenwärtigung der Vergangenheit und Chance kritischer Selbstreflexion, bei der Vergessen *kein* angemessenes therapeutisches Mittel ist, vgl. Assmann 2020: 180–202, hier bes. 191 ff.

terbrechen, um damit eine Wiederauffindbarkeit auszuschließen.[33] Es geht dann also »nicht mehr um das (letztlich unmögliche) physische Auslöschen von Datenspuren, sondern um die Nichtlokalisierbarkeit von Daten« (Stähli 2021: 416). Kurzum: Das Recht auf Vergessenwerden wird – zumindest in den Fällen, in denen eine dauerhafte und irreversible »Entfernung« von Daten nicht möglich ist – nicht durch Löschung qua »Tilgung« von Daten, sondern durch deren *Unauffindbarmachung* umgesetzt.[34]

Wie der Schweizer Soziologe Urs Stäheli in seiner Studie *Soziologie der Entnetzung* (2021) darlegt, lässt sich das Konzept der »Unauffindbarkeit« (*irretrievability*) von Daten, verstanden als »dritte Kategorie zwischen Speichern und Löschen« (417), bis auf Ideen zu einer »›Kompostierung‹ überflüssiger Daten« in den 1990er Jahren zurückverfolgen. An die Stelle eines auf Konservierung ausgerichteten Digitalarchivs, dessen größtes *Risiko* in der Unauffindbarkeit von Daten besteht, ist eine solche in einer Sammlung »entnetzte[r] Daten« gewissermaßen Programm: »einzelne Elemente wie etwa Links oder Formulare bleiben funktionsfähig, sind nun aber herausgerissen aus jedem intelligiblen Zusammenhang. Der Datenabfall kann so gesammelt, aber nicht mehr durchsucht werden.« (Ebd.) Angesichts der angedeuteten Schwierigkeiten der Umsetzung und Sicherstellung einer Löschung von Daten scheint das Konzept der Unauffindbarkeit und damit eine Realisierung des Vergessenwerdens durch Unauffindbarmachen nicht nur bedenkenswert, sondern auch intuitiv nachvollziehbar. Dies sei abschließend an einem Beispiel erläutert.

Am Ende des Films *Raiders of the Lost Ark* (deutscher Filmtitel: *Jäger des verlorenen Schatzes*) von Steven Spielberg und George Lucas, dem ersten Teil der Abenteuerfilmreihe *Indiana Jones* aus dem Jahr 1981, fragt Universitätskurator Brody in einer Besprechung mit amerikanischen Regierungsvertretern, wo sich denn jener von Dr. Jones vor den Händen der Nazis für die ameri-

33 Derartige Ansätze zu anonymen Kommunikationsverfahren gibt es in der Informatik bereits seit Anfang der 1980er Jahre, vgl. Schwenke 2006: 245–249.

34 »Entfernung« und »Tilgung« in Anführungszeichen, um dem Umstand Rechnung zu tragen, dass ein konventioneller Löschungsvorgang technisch gesehen *nicht* die Entfernung (im Sinne von Wegschaffung) von Daten, sondern lediglich deren Markierung als gelöscht zur Folge hat, was allenfalls bloß deren Wiederauffindbarkeit erschwert. Beim konventionellen Löschen werden also nur »die Verweise auf die Daten im Index, dem Inhaltsverzeichnis der Festplatte, gelöscht und der Bereich zum Überschreiben freigegeben. Dieses Überschreiben findet aber möglicherweise nie statt. Die vermeintlich entsorgten Daten befinden sich auch weiterhin auf der Festplatte, sind aber für den Nutzer nicht mehr mit normalen Mitteln erreichbar« (Bundesamt für Sicherheit in der Informationstechnik o. J.).

kanische Regierung gerettete »verlorene Schatz« – nichts Geringeres als die alttestamentliche Bundeslade, einer aus Akazienholz verfertigten, mit Gold überzogenen Truhe – nun befinde, worauf er von Major Eaton zur Antwort erhält, dass sich die Lade »an einem sehr sicheren Ort« befinde (»The Ark is somewhere very safe«), um von Topspezialisten untersucht werden zu können. In der Schlussszene sieht man dann, wie ein Lagerarbeiter die Lade in eine einfache Holzkiste samt Aufschrift »Top Secret Army Intel 9906753 Do Not Open!« verstaut, welche daraufhin, mit einem simplen Vorhängeschloss gesichert, in ein schier unendlich großes Lager gebracht wird und in der Masse tausender und abertausender ähnlich aussehender Holzkisten untergeht.

Eine Erörterung der vielfältigen Deutungen, die dieses Filmende erfahren hat, kann an dieser Stelle unterbleiben. Ich beschränke mich auf eine von Rainer Erlinger (2019: 127–132) vorgeschlagene Deutung, die – auf unseren Zusammenhang übertragen – zugleich eine anschauliche Antwort auf die Frage liefert, wie das Unauffindbarmachen auch toxikalischer Daten verstanden werden könnte. In der Tat befindet sich die Bundeslade, die ja nicht nur von unschätzbarem Wert, sondern auch von ungeahnter Macht und Kraft im Guten wie im Schlechten ist, »an einem sehr sicheren Ort«, indem sie zwischen unzählig vielen ähnlich aussehenden Dingen versteckt ist, was einen Versuch, sie zu finden, als praktisch aussichtslos erscheinen lässt. Das sicherste Versteck eines Gegenstandes ist nicht unbedingt ein bestimmter Ort (klischeehaft: der Dachboden oder der Keller), sondern ein ganz und gar *un*bestimmter Ort. Was Erlinger in Bezug auf das Bild mit den unzähligen Holzkisten in der Schlussszene des Films *kritisch* über die Unterdrückung von Wahrheit sagt, die heutzutage eben nicht mehr nur durch Zensur oder Gewalt, sondern durch ein Untergehen inmitten anderer Informationen erfolgen könne, kann im *positiven* Sinne als Veranschaulichung der Entnetzung von Daten zum Zwecke ihrer Unauffindbarmachung verstanden werden:

> »Es reicht, so viele andere Kisten zu produzieren, dass man kaum mehr eine Chance hat, die eine Kiste, in der sich die Wahrheit befindet, zu finden oder, wenn man sie gefunden hat, sicher zu identifizieren. Die Wahrheit ist nur eine Information unter vielen, die sich von den anderen lediglich dadurch unterscheidet, dass sie der Realität entspricht. Das lässt sich aber der Kiste von außen nicht unbedingt ansehen.« (Erlinger 2019: 128 f.)

Inwieweit nun ein solches theoretisches Konzept des »Ablegens in einen falschen Ordner« zur Unauffindbarmachung von Daten praktisch realisiert

werden kann, um damit Phänomenen der Datentoxikalität zu begegnen, steht freilich auf einer anderen Seite.