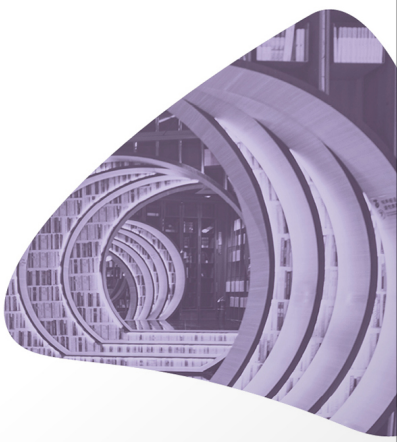
Melusina Press
Humanities



Reputation ohne Paywall?

Wissenschaftliches Publizieren im digitalen Wandel

Yuliya Fadeeva, Simone Franz, Torsten Kahlert, Dario Kampkaspar, Melanie Seltmann, Timo Steyer, Niels-Oliver Walkowski (Hrsg.)

Wissenschaft als datafizierter Raum

Renke Siems

Reputation ohne Paywall? Wissenschaftliches Publizieren im digitalen Wandel
Herausgegeben von Yuliya Fadeeva, Simone Franz, Dario Kampkaspar,
Melanie Seltmann, Timo Steyer und Niels-Oliver Walkowski

Melusina Press, 2025

Veröffentlicht durch die Universität Luxemburg - **Melusina Press**, 2025
11, Porte des Sciences
L-4366 Esch-sur-Alzette
https://www.melusinapress.lu

Verlagsleitung: Niels-Oliver Walkowski, Johannes Pause
Lektorat: Carolyn Knaup, Niels-Oliver Walkowski
Cover und Layout: Valentin Henning, Erik Seitz
Umschlagsbild: @vnwayne_fan;Foto 2020 veröffentlicht auf Unsplash

Die digitale Version dieser Publikation steht unter https://www.melusinapress.lu frei zur Verfügung.
Das PDF und die Druckvorlage werden mit Hilfe von princeXML erzeugt.

Bibliografische Information der Nationalbibliothek Luxemburg: Die Nationalbibliothek Luxemburg verzeichnet diese Publikation in der Luxemburgischen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über bnl.public.lu abrufbar.

ISBN (Online)	978-2-919815-83-8
ISBN (PDF)	978-2-919815-84-5
ISBN (EPub)	978-2-919815-85-2
DOI (Publikation)	10.26298/1981-5838-wadr
DOI (Band)	10.26298/1981-5838

Wissenschaft als datafizierter Raum

Renke Siems

Code/Space

Rob Kitchin und Martin Dodge veröffentlichten 2011 ihr Buch *Code/Space*. Als Humangeographen warfen Sie einen räumlichen Blick auf die digitale Transformation und analysierten, wie Software sich immer mehr in unser Alltagsleben hineinwebe und dabei unserer physischen Umgebung einen Charakter verleihe, den sie zuvor nicht gehabt hätte. Code schaffe Raum und gestalte ihn derart, dass der Raum ohne seinen digitalen Anteil nicht mehr in der Weise existiere wie gedacht: Ist der Server offline, wäre die Abfertigungshalle des Flughafens keine mehr, sondern nur noch ein chaotischer Wartesaal. Diese Entwicklung verändere unsere Wahrnehmung, unsere Interaktionen und damit auch die sozialen Relationen, sie sei damit keineswegs unschuldig. Kitchin und Dodge analysieren es als Foucaultsches Dispositiv — von Software gestalteter Raum sei immer auch eine Mikroökonomie der Macht.

Diese Entwicklung ist allgemein und deshalb auch in den Informationsinfrastrukturen zu erkennen, paradigmatisch im Essay *Libraries are Software* von Cody Hanson (2015). „We can only be as good as our software", erklärt er darin mit Blick darauf, dass Bestände, Recherche, bibliothekarische Entscheidungen und die Nutzererfahrung insgesamt sich in den vergangenen zwanzig Jahren in ein softwarebasiertes Konstrukt verwandelt hätten. All diese Kernbedingungen könnten nicht mehr ohne oder neben der Software, die sie gestalteten, existieren — wodurch sich auch hier die Frage von Macht und Verfügungsgewalt stellt: „We must face the fact that when we relinquish control over the software we provide, we effectively relinquish control of our most visible and effective public services." (Ebd.)

In den zurückliegenden Jahren ist sukzessive das Bewusstsein dafür gewachsen, auf welcher Basis Software unsere Umwelt und damit uns beeinflusst und verändert: Daten. Wir sind es immer noch gewohnt, von ‚Digitalisierung' zu reden, aber das trifft es nicht. Dinge maschinenlesbar zu machen, die es vorher nicht waren, ist zwar Voraussetzung für vieles, was zunehmend unser Leben bestimmt, aber damit erfassen wir noch nicht Ausmaß und Intensität dieser gesellschaftlichen Großunternehmung, weshalb Cukier und Mayer-Schoenberger (2013) von ‚Datafizierung' (*datafication*) sprechen:

> „Datafication is not the same as digitization, which takes analog content — books, films, photographs — and converts it into digital information, a sequence of ones and zeros that computers can read. Datafication is a far broader activity: taking all aspects of life and turning them into data. Google's augmented-reality glasses datafy the gaze. Twitter datafies stray thoughts. LinkedIn datafies professional networks. Once we datafy things, we can transform their purpose and turn the information into new forms of value." (Ebd.)

Datafizierung steht damit letztlich hinter vielen der kritisch diskutierten Phänomene der letzten Zeit — von den *prediction products*, die Shoshana Zuboff (2019) analysiert, bis hin zur *hidden security crisis* der *data broker*, die Ryan und Christl (2023a und 2023b) detailliert erläutern.[1] Die von Kitchin und Dodge eingeleitete spatiale Perspektive macht dabei den Charakter der Entwicklung besonders deutlich. Plattformkapitalismus mit mobilem Internet ist etwas völlig anderes als ohne, denn das Schleppnetz der Datafizierung allein hätte nie so viel transformieren und in ökonomische Entitäten verwandeln können. Konsequenterweise wenden wir deshalb mittlerweile den Blick und sprechen immer mehr — etwa in der Europäischen Datenstrategie — von ‚Datenräumen'.[2]

Usecase der Datafizierung

Das Muster von Datafizierung lässt sich vielleicht am einfachsten von seinem Extrem her beschreiben, der militärischen Anwendung. Als im Dritten Golfkrieg 2003 Bilder um die Welt gingen, wie Soldaten in Wüstenzelten auf ihren Laptops herumtippten, wurde deutlich, dass sich in der Kriegsführung etwas geändert hatte. *Network-centric warfare* ist der Ansatz einer vollständig vernetzten Operationsführung, die Daten aller militärischen Systeme zusammenführt und dadurch Informationsüberlegenheit und weitergehend die *full spectrum dominance* sichern soll.[3] Nicht nur die US-Army, sondern auch eine Reihe anderer, gerade Bündnis-Armeen, haben sich diesem Ansatz zugewendet, meist in kleineren, weniger umfangreicheren Modellen unter abweichenden Bezeichnungen wie *‚software-defined defence'*.

Diese Entwicklung ist offenkundig anspruchsvoll. Große Datenmengen müssen über Wissensmanagementsysteme und Künstliche Intelligenz (KI) aufbereitet und unter teils schwierigsten Bedingungen so ausgespielt werden, dass die einzelnen Aktor:innen auf dem Gefechtsfeld nicht vom Informationsfluss überfordert werden, sondern sich synchronisieren können. Diese Art von Militärdoktrin wird daher mit der Funktion von E-Commerce und vernetzten Unternehmen verglichen — man könnte es aber auch als Einzug des Plattformkapitalismus in die konventionelle Kriegsführung betrachten. Der immense Kapitalaufwand, die nötigen technischen Vorsprünge, die Skalenvorteile verfügbarer Datenbestände bewirken in der Summe eine Dominanz ganz weniger Player, während für alle anderen im Markt der eigenen Sicherheit zunehmend kein Platz mehr ist. So sind neben den klassischen Firmen wie Booz Allen Hamilton immer mehr der großen Plattformkonzerne wie Alphabet, Amazon und Microsoft auch bedeutende *military contractors*, neben neueren Spezialisten wie *Palantir* und *Anduril*.[4]

1 Vgl. auch die preisgekrönte Recherche Databroker Files von Netzpolitik, https://netzpolitik.org/databroker-files/ am 14.04.2025.
2 Vgl. https://digital-strategy.ec.europa.eu/en/policies/data-spaces am 14.04.2025.
3 Vgl. die Strategiepapiere Joint Vision 2010 (https://www.dtic.mil/jv2010/jv2010.pdf) und Joint Vision 2020 (https://www.dtic.mil/doctrine/concepts/ccjo_jointforce2020.pdf) beide am am 14.04.2025.
4 Vgl. dazu die Informationen auf dem Rechercheportal Tech Inquiry (https://techinquiry.org/) am 14.04.2025.

Palantir ist angesichts der aktuellen Kriege in der Ukraine und im Gaza von besonderem Interesse. Während die vielfach sehr altmodisch wirkende Kriegsführung in der Ukraine anfangs überraschte, spielen dort Drohnen und andere Automaten eine bedeutende Rolle. Palantir verarbeitet die gesammelten Informationen mit dem ‚Wisch-und-Weg'-Ansatz seines KI-getriebenen Zielerfassungssystems.[5] Detailliertere Informationen hierzu gibt es mittlerweile durch Analysen der Aktivitäten im Gaza, wo das von Palantir in Kooperation mit Amazon, Google und Microsoft für die israelischen Streitkräfte entwickelte System *Lavender* im Einsatz ist (vgl. Abraham 2024 und Rehak 2024). Der Gaza ist in der Darstellung ein komplett datafizierter Raum: Alle Versorgungsleitungen werden von israelischem Gebiet zugeführt; Satellitenbilder geben detaillierte Informationen; Lokalisierungsdaten der Mobilgeräte sind verfügbar; bekannte Zielpersonen wie z.B. Hamas-Offiziere wurden vorab mit *Pegasus* oder vergleichbaren Spionagewerkzeugen angegriffen und biometrische Daten der Bevölkerung schon seit Jahren gesammelt (vgl. Loewenstein 2023). Die Datenlage bei Systemen wie Lavender ist damit wesentlich umfangreicher als bei klassischer network-centric warfare, da nicht nur die Daten militärischer Systeme, sondern vielerlei Datenquellen aus dem Web, aus Social Media, aus den Angeboten von Data Brokern in Cloudanwendungen verknüpft werden, was deshalb immer mehr als die ‚*kill cloud*' hinter den eigentlichen Waffensystemen diskutiert wird.[6] Auch über jede Person im Gaza liegen damit eine Vielzahl an Datenpunkten vor, die von Lavender algorithmisch in Scoringwerte umgesetzt werden. Personen ab einem bestimmten Scoring landen auf der Liste der anzugreifenden Ziele, die dann von den Waffensystemen abgearbeitet wird. Je nach Einstufung in *junior-* oder *senior-targets* wird dabei eine unterschiedliche Anzahl unbeteiligter Opfer in Kauf genommen.

Da die Listen über Scoringwerte befüllt werden, gelangen die Personen nicht über tatsächliche Ist-Zustände darauf, sondern über statistische Korrelationen der Art ‚ist so ähnlich wie X oder Y'. Gerade durch Datenbestände, die von Databrokern eingekauft wurden, hat das Ausgangsmaterial dabei quasi jeden vorstellbaren Bias: Zu einem bekannten Hamas-Offizier kommen also auf den Ziellisten nicht unbedingt weitere Offiziere hinzu, sondern auch Personen, die vom Algorithmus verfolgte Merkmale aufweisen — weil sie z.B. ein gebrauchtes Smartphone gekauft haben, welches einen falschen Vorbesitzer hatte. Die Listen werden dann durch weitere Programme verarbeitet wie *Where is Daddy?,* wodurch die Personen dann angegriffen werden, wenn sie z.B. abends im Kreis der Familie sind. Der Anteil an tatsächlicher KI sollte daher vielleicht nicht überschätzt werden. Rehak bezeichnet Lavender deshalb auch als „statistische Tötungsautomation" (Rehak 2024). Palantir selbst wirkt völlig überzeugt von diesem Vorgehen: „Palantir is here to disrupt and make all the institutions we partner with the very best in the world", erklärt CEO Karp (Palantir 2024). „And when it's necessary to scare enemies, and on occasion kill them. And we hope you are in favor of that. We hope you're enjoying being a partner, and we're really happy and very very focused on what we're doing." (Ebd.)

5 Vgl. https://www.sueddeutsche.de/projekte/artikel/kultur/ki-und-krieg-palantir-ukraine-e666421/ am 14.04.2025..

6 Vgl. z.B. https://www.disruptionlab.org/the-kill-cloud am 14.04.2025.

Lavender ist damit ein Muster für Michael Haydens berüchtigte Maxime „We kill people based on metadata" (vgl. Granick 2017) und eine Fortentwicklung der früheren *signature strikes*. Dabei sind Technologie und Paradigma durchaus als generisch zu verstehen, wie z.B. Molnar (2024) für *smart border technologies* zeigt, die nicht an der Grenze bleiben, sondern auch im Hinterland verwendet werden — etwa für den Fussballfan, der ins Stadion will — und die Basisinfrastruktur der *kill cloud* wie Microsoft *Azure* ist genauso in vielen Büros zu finden.

Größer als die Ankündigungen der Firmen sind dann meist nur noch die politischen Wünsche, wie die (Nicht-)Debatte in den europäischen Ländern um *Going Dark* zeigt, dem Programm zur Einführung umfassender Überwachungsmöglichkeiten in der EU (vgl. Siems 2024a). Umfangreiche Zugriffsrechte auf Daten, Ausnutzen von Schwachstellen, Knacken der Geräte und erzwungene Kooperation von Firmen betreffen alle Lebensbereiche und damit auch die Wissenschaft.

Datenkartelle

Geht man in die Historie dieser Entwicklung zurück, trifft man auf wissenschaftliche Infrastrukturen und die *Datenkartelle*, wie Sarah Lamdan (2023) sie nennt.[7] Lamdan analysiert anhand von *RELX* (früher *Reed Elsevier*) und *Thomson Reuters* einen Institutionentyp, der immer nach dem gleichen Muster vorgeht, nämlich öffentliche Ressourcen zu okkupieren und in ein Klubgut zu verwandeln, das die Datenkartelle dann privilegiert beherrschen und vermarkten können. Für das wissenschaftliche Informations- und Publikationswesen ist dieser Vorgang, bei dem die Big 5 Publisher (Elsevier, Springer, Wiley, Taylor & Francis, Sage) sich die Leistung der Forschenden weltweit zur Beute machen, bereits vielfach beklagt und beschrieben worden, sehr pointiert z.B. von Buranyi (2017). Lamdan beschreibt diesen Mechanismus aber für etliche Informationssparten wie Rechtsinformationen, Finanz- und Wirtschaftsinformationen, Nachrichtenwesen und — das soll hier weiter betrachtet werden — *risk solutions*.

Die Erfindung und Popularisierung des World Wide Web hatte in den Neunziger Jahren die wissenschaftlichen Informationsinfrastrukturen über Nacht ins Wanken gebracht. 1991 entstanden *arXiv* und *RePEc*, 1994 *SSRN*, 1996 *PubMed* (ab 2001 mit *PubMed Central*), 1997 *CiteSeer* und 2001 *PLoS*. War kurz davor noch das Paradigma der gedruckten wissenschaftlichen Zeitschrift erkennbar an den Rand seiner Leistungskraft geraten und sowohl Publizieren wie Lesen immer schwieriger und teurer geworden, eröffnete sich nun schlagartig für alle Wissenschaften, die Informationen, aber keine Bibliothek brauchen, ein strukturierter Weg ins Freie: Publizieren ohne Zeitverzug und frei von Paywalls; Verzeichnung der Beiträge in einer Datenbank; relevanzgerankte Suche. Die klassischen Intermediäre wie Verlage und Bibliotheken kamen spürbar unter Druck.

Gerade die ihren Investoren verpflichteten großen Wissenschaftsverlage wurden rasch aktiv. Sie bauten digitale Kompetenzen auf und erkannten die schwache Stelle im Infor-

7 Vgl. zum folgenden die Darstellung in Siems 2014, 2022, 2024b.

mationskreislauf — die Bibliotheken als institutionelle Nachfragerinnen, die oftmals ihre Entscheidungen nach den Präferenzen anderer Akteur:innen auf dem Campus treffen mussten. Ihnen konnten zunächst erfolgreich hochpreisige kombinierte Print- und Online-Abos angeboten werden, wodurch die Verlage ihr Geschäft migrieren konnten. Dann kamen die immer größeren Paketlizenzen, die den grünen Weg des Open Access austrockneten. Der Onlinegang des *Web of Science* verdrängte freie Alternativen. Zuletzt wurde die Laufrichtung des Geldes umgekehrt und durch die Einführung des APC-gesteuerten kommodifizierten Open Access anstelle des Lesens das Publizieren zum Klubgut. Damit waren die Position und Rendite insbesondere der Big 5 Publisher gesichert. Das kurzzeitige Knacken im Gebälk des eigenen Geschäftsmodells hatten sie aber nicht vergessen und es begann die Suche nach weiteren Standbeinen in der sich digital immer weiter transformierenden Welt. Reed Elsevier und Thomson Reuters entdeckten dabei das Thema *data brokerage*.

Die Verbreitung des World Wide Web brachte nicht nur das wissenschaftliche Publikationswesen in Bewegung, sondern auch den Umgang mit den Daten der öffentlichen Hand. Funk (2023) zeichnet in seinem Porträt des Branchenpioniers Hank Asher nach, wie der frühere Drogenschmuggler sich das Datenbanksystem der *Drug Enforcement Agency* (DEA) zum Vorbild nahm, um seine eigene Datenfirma aufzumachen. Asher hatte immensen Erfolg, da er verstanden hatte, dass die Datenschutz- und Informationsfreiheitsgesetze seiner Zeit alle in der gleichen Weise angelegt waren, nämlich als Abwehrrecht gegenüber dem Staat. Dieser sollte keine Geheimnisse vor seinen Bürgern, aber sie sollten welche vor dem Staat haben können. Asher und seine Firma *Database Technologies* waren nun nicht der Staat, und so begannen er und andere Pioniere, die Daten aus den Behörden herauszuholen: Führerscheindaten, Fahrzeughalter, Firmenverzeichnisse, Standesamtsdaten wie Eheschließungen und Scheidungen, Schwerbehinderungen, Immobilieneigentum, Konzessionen und etliches mehr. Bis man durch die Fusion all dieser Daten in seinem Produkt *AutoTrack* gefangen war:

> „Most of what AutoTrack knew had little to do with the nascent internet. It had little to do with how careful you were. It had little to do with consent. AutoTrack knew what it knew not because you logged in to a website or filled out a warranty card and failed to read the fine print. AutoTrack knew you because in the universe of hard data Asher dealt in, there was rarely a mechanism to opt out. It was inescapable." (Funk 2023, 71)

Asher verkaufte zunächst an Kunden wie Versicherungen und Banken und begründete dadurch das, was heute ‚risk solutions' genannt wird, also Risiken datenbasiert kalkulieren. Sehr schnell erschloss er sich aber eine weitere Kundengruppe: die Polizei, die sich AutoTrack begeistert als Fahndungsinstrument zu eigen machte. Der Staat, der keine Geheimnisse haben sollte, mietete sich damit den Zugang zu denen seiner Bürger. Nach 9/11 kamen Nachrichtendienste dazu und die militarisierten Grenzpolizeien unter dem Dach des *Department of Homeland Security* wie *Immigration & Customs Enforcement* (ICE) und *Customs and Border Protection* (CBP). Da hatte Asher aber schon an einen

Konkurrenten im Markt verkauft, genauer an Reed Elsevier mit ihrem Produkt *LexisNexis*.

Auch in der Rechtsinformation war schon zunehmend datenbasiert gearbeitet worden. Zeugen wurden genauso gesucht wie Vermögenswerte — und so hatte LexisNexis parallel zu Asher seine Dienste sukzessive erweitert. Als Ashers Firma zum Verkauf stand, griff Reed Elsevier daher zu, auch wenn mit diesem Bieter zunächst niemand gerechnet hatte:

> „‚Everybody considered it a stodgy old British company that couldn't move fast enough to make something like that happen,' says Andy Perlmutter [...] who spent weeks holed up in the Embassy Suites as a consultant to Reed Elsevier. But for Reed Elsevier, whose leadership had their eyes opened to new opportunities by 9/11 just as their bread and butter – publishing – was being hit by the explosive growth of the World Wide Web, the fight felt existential. The company's business was more than three-quarters print, making it ‚a possible early contender to be entirely disintermediated by the internet,' as in-house venture capitalist Tony Askew put it to an interviewer years later. It had to quickly transition to something more durable, so it did." (Funk 2023, 137)

Reed Elsevier und Thomson Reuters teilten sich Ashers Erbe. LexisNexis Risk Solutions bietet das *Accurint Virtual Crime Center* an, Thomson Reuters *Special Services* das Konkurrenzprodukt *CLEAR*. Beide Firmen arbeiten auch eng mit Palantir zusammen, Reed Elsevier war dort zudem neben der CIA einer der frühen Investoren.[8] Mit Hilfe dieser Datenservices konnte ICE das *American Dragnet* aufspannen. ICE hat Zugang zu den Führerscheindaten von drei Viertel der erwachsenen Bevölkerung in den USA, hat von einem Drittel der Erwachsenen die Führerscheinbilder mit Gesichtserkennungssoftware gescant, verfolgt die Bewegungsmuster von drei Viertel der erwachsenen Bevölkerung in ihren Städten und kann ihre Wohnung durch Daten der Versorgungsunternehmen orten. Auf dieser Basis vollzieht ICE die gefürchteten Razzien und Deportationen und ist dabei der Aufsicht durch Institutionen wie dem Kongress völlig entglitten.[9]

Ashers Erbe zeigt sich auch im generischen Charakter, wie er bei Lavender deutlich wurde: Aus Daten werden Scores, Scores werden zu Handlungen. So sperrte *Automated Welfare*, die datengestützte Verwaltung und Überprüfung von Sozialleistungen ohne menschliche Nachkontrolle, Leistungen und forderte hohe Beträge zurück aufgrund eines aus der Datenlage geschlossenen Betrugsverdachts — der sich in bis zu 90% als falsch erwies (vgl. Gilman 2020). Bis dahin hatten Betroffene ihren Job und ihre Wohnung verloren, die Familien zerbrachen, manche nahmen sich das Leben. Die Pandemie gab der Branche dann die Gelegenheit, den Public-Health-Bereich zu durchsetzen, der sich lange gewehrt hatte, und mit Daten Triage-Entscheidungen zu unterfüttern. Wer an eins

8 Vgl. https://privateequitylist.com/investor/reed-elsevier-ventures-rev und https://web.archive.org/web/20180708032604/http://m.marketwired.com/press-release/thomson-reuters-palantir-technologies-enter-exclusive-agreement-create-next-generation-nyse-tri-1167653.htm beide am 14.04.2025.

9 Vgl. https://americandragnet.org/ am 14.04.2025.

der knappen Beatmungsgeräte durfte, hing dann eben vom Score ab (vgl. Funk 2023, 226ff.) — und dieses Prinzip weitet sich aus:

> „As the Obama era ended and the 2016 presidential election approached, America was already awash in consumer scores. There were renter scores, juror scores, voter scores, customer-lifetime-value scores, welfare-benefits scores, and now socioeconomic health scores, many of them built upon profiles first drawn by Asher. We were constantly stalked by secret identifiers. We were constantly stalked by secret scores. It was just that, unlike our counterparts in China, whose dystopia we mourned, most of us didn't know it." (Funk 2023, 208)

Auch die Wissenschaft wurde eingeholt. Im *Xandr*-Leak wurde publik, dass LexisNexis Daten von Forschenden sowie weiterer geschützter Berufsgruppen an den Databroker *LiveRamp* weitergegeben hat (vgl. das Datenrepositorium bei Keegan und Eastwood 2023). Auch ein Vertrag zwischen LexisNexis und ICE wurde mittlerweile geleakt und ist von einer Qualität, dass der Sicherheitsforscher Wolfie Christl nach der Lektüre feststellte: „it suggests, once again, that LexisNexis aka Elsevier aka RELX Group is a kind of outsourced domestic US intelligence agency."[10]

Surveillance Publishing

Datenkartelle kann man im Anschluss an Lamdan als *GAFAM* [11] *der kuratierten Information* betrachten. Dies beinhaltet einen Wandel in den wissenschaftlichen Informationsinfrastrukturen hin zu datengetriebenen Geschäftsmodellen, wobei risk solutions als erfolgreichstes neues Standbein der früheren Verlage einen Import der Überwachungslogik in die Wissenschaft bewirken. Seit Pooley (2022) wird dies verstärkt mit dem Begriff ‚*surveillance publishing*' beschrieben: „A scholarly publisher can be defined as a surveillance publisher if it derives a substantial proportion of its revenue from prediction products, fueled by data extracted from researcher behavior." (Ebd.)

Die Diskussion über den Wandel im Status der Forschenden vom Versuchsleiter zur Laborratte (vgl. Brembs u.a. 2019) existiert dabei grundsätzlich schon seit längerem. Bereits Wood (2009) beschrieb den zunehmenden Handel mit personenbezogenen Daten durch *scholarly publishers*, fokussierte sich aber auf die Diversifizierung von Geschäftsbereichen bei Reed Elsevier durch deren Vordringen in den Bereich data brokerage und nicht auf die datengetriebene Auswertung des Forschungsverhaltens selbst. Hellman (2015) wies dann auf die Durchsetzung der Verlagsplattformen mit Trackern von *advertising technology* hin, was Lynch (2017) in seiner Betrachtung des Lesens im digitalen Zeitalter wieder aufnahm. Aber erst die Beiträge von Hanson (2019) bewirkten eine Debatte, da sie sich mit der zeitgleich im wissenschaftlichen Bibliothekswesen engagiert geführten Auseinandersetzung zu Authentifizierungsmethoden für digitale Medien verknüpften (vgl. Siems 2021, 2022). In der Folge wurden die Stellungnahme der *American*

10 https://x.com/WolfieChristl/status/1671309669111873538 am 14.04.2025.
11 Akronym der Internetkonzerne Google, Apple, Facebook, Amazon, Microsoft.

Library Association (2019) zu *data surveillance* veröffentlicht, die Reports der *Scholarly Publishing and Academic Resources Coalition SPARC* (2019, 2020, 2021, 2023, 2024), das Informationspapier der Deutschen Forschungsgemeinschaft (2021) und die Petition *Stop Tracking Science*.[12]

Alle relevanten Untersuchungen wiesen, wie zuletzt Lindstrot (2025), Spuren zahlreicher digitaler Analyseinstrumente auf den großen Verlagsplattformen nach. Ein Teil sind vom Anbieter selbst verantwortete Instrumente zur Webseitenanalyse, dazu kommen aber jede Menge Tracker von *third parties* aus der digitalen Werbeindustrie, *audience management tools* zum *microtargeting* sowie *fingerprinter*, um privacy-orientierte Nutzer:innen aufzuspüren. Die DFG-Task Force Datentracking (2024) zeigte zudem, dass nicht nur das Portal selbst, sondern auch alle Kommunikationskanäle im Umfeld, wie Newsletter etc. verseucht sind. Aber nicht nur Personen werden getrackt, sondern auch jeder individuelle Download, um das *scholarly sharing* zu überwachen.[13] Es entstehen damit feingranulare Bewegungsbilder der Forschung, die aufgrund der Einbindung von third parties auch nicht bei den Anbietern verbleiben, sondern zu weiteren Data Brokern abfließen und von dort aus zu jedem/jeder Akteur:in, der/die bereit ist, dafür Geld auszugeben. Das bedeutet nicht nur Risiken für individuelle Forschende, sondern auch Risiken des Technologie- und Wissensabflusses. Dies passiert nicht nur in der Wissenschaft, sondern aufgrund der geteilten Infrastruktur auch in den Bereichen Transfer, Startups und forschende Unternehmen generell, weshalb der Verein Deutscher Ingenieure verlangt, „dem Thema Tracking in der Wissenschaft weitere Aufmerksamkeit im Rahmen der Forschungs- und Innovationspolitik zu widmen und dabei Implikationen für die Wirtschaft in den Blick zu nehmen" (VDI 2024).

Die datenbasierten Geschäftsmodelle der früheren Verlage reichen mittlerweile auch innerhalb wissenschaftlicher Infrastrukturen weit über die Verlagsplattformen hinaus: Suchinstrumente, Literaturverwaltung, elektronische Laborbücher, Schreibtools, Outreach-Plattformen, Forschungsinformationssysteme und Assessment. Posada und Chen (2017) zeigen beispielhaft an Elsevier, wie die großen Player mittlerweile im gesamten Forschungszyklus Fuß fassen, um alle Bereiche nach den Bedürfnissen des surveillance publishing umzugestalten. Das Endziel fassen Koivisto und Sly (2022) dann bündig zusammen:

> „It is becoming increasingly clear that the core functions of higher education are destined to be quantified and that this data will be harvested, curated, and repackaged through a variety of enterprise management platforms. All aspects of the academic lifecycle, such as research production, publication, distribution, impact determination, citation analysis, grant award trends, graduate student research topic, and more can be sold, analysed, and gamed to an unhealthy degree." (Ebd.)

Damit zeigt sich die Bedeutung des Kernsatzes von Cukier und Mayer-Schoenberger — „Once we datafy things, we can transform their purpose and turn the information into

12 Vgl. https://stoptrackingscience.eu/ am 14.04.2025.
13 Vgl. https://x.com/json_dirs/status/1486120144141123584 am 14.04.2025.

new forms of value“ (Cukier, Mayer-Schoenberger 2013) — für die Wissenschaft. Auch sie erweist sich als datafizierter Raum mit einer langen Genese und muss durchaus auch als Ideengeberin angesehen werden. Vieles, was sich dann im Überwachungskapitalismus wiederfand, stammt ursprünglich aus der Wissenschaft, so wie er auch insgesamt ohne vielfältige wissenschaftliche Qualifikationen nicht zu betreiben ist. Ein Beispiel für eine bis heute aktuelle Verbindung ist der Bereich Personen-Identifier. Individuen als solche identifizieren, um sie dann kontinuierlich verfolgen zu können, ist ein zentrales Anliegen von data brokerage, das sich auch in weiteren Wirtschaftsbereichen findet. Wittmann (2025) stellt z.B. im Bereich E-Commerce heraus, „warum Unternehmen das Thema Wallets so spannend finden: Um einen offiziellen Marktplatz für garantiert echte Daten einer Person zu schaffen.“ Über echte Daten echter Menschen zu verfügen ist der Königsweg für alle anschließenden Verwertungen und Handlungen, weshalb die ehemaligen Verlage sich über Initiativen wie RA21, Seamless Access und GetFTR[14] bemühten, die Hand auf die Authentifizierungswege auf dem Campus zu bekommen (vgl. DBV 2019).

Ähnliches gilt für Personen-Normdaten. Ein Dienst wie *ORCID* befriedigt einerseits legitime Interessen hinsichtlich besserer Metadaten, kreiert aber ebenfalls einen offiziellen Marktplatz für garantiert echte Daten einer Person. Solche Identifier lassen sich dann prinzipiell gut mit anderen wie der *LexID* von LexisNexis Risk Solutions verknüpfen, was einen Beitrag zum *identity graph* der jeweiligen Person leistete: ein *shadow knowledge graph*, der das Wissen zu dieser Person über alle Bereiche und Devices hinweg bündelt und verwertbar macht.[15] Und da dieser Marktplatz wie die Literaturproduktion von den Forschenden selbst in kostenloser Heimarbeit erstellt wird, fand er das Interesse der ehemaligen Verlage, die zu den Mitgründern von ORCID gehören.

Die Ausdehnung datengetriebener Geschäftsmodelle in den gesamten Forschungszyklus bewirkt eine entsprechende Ausdehnung auch der Entwicklung, die Schonfeld (2022) in den Publikationsinfrastrukturen als „supercontinent“ beschreibt. Die naive Form der Umstellung auf Open Access, die nur die Laufrichtung des Geldes umkehrt und den gleichen Unternehmen die gleichen *windfall profits* — jetzt eben durch Publikations- statt Subskriptionsgebühren — zugesteht, ermöglicht den früheren Verlagen eine zuvor nicht mögliche Vertiefung ihrer Datenanalysen. War zuvor jeder Anbieter durch die urheberrechtsbedingte Parzellierung des Gesamtgeschehens auf seine eigenen *ip bits* zurückgeworfen, sind jetzt übergreifende Auswirkungen möglich, und neben der Überwachung des Informationsverhaltens auf den Verlagsplattformen dann auch jeder folgende Schritt: von der minutiösen Ausprotokollierung eines Literaturverwaltungssystems wie Mendeley, wie Fried (2023) zeigt, bis hin zu Forschungsinformation und Assessment.

Mirowski (2022) sieht Open Science daher auch als Türöffner zur Plattformisierung der Wissenschaft. Den Big 5 Publishern sei die zunehmende Erschöpfung ihres klassischen Erlösmodells völlig bewusst gewesen und nun seien sie ihren Kritiker:innen in der Wissenschaft wieder die entscheidenden Schritte voraus, indem sie unter der Fahne von

14 Vgl. https://seamlessaccess.org und https://www.getfulltextresearch.com/ beide am 14.04.2025.
15 Vgl. https://piwikpro.de/blog/cross-device-tracking-am-besten-mit-id-graph/ am 14.04.2025.

Open Science den gesamten Forschungszyklus aufkaufen, zu übergreifenden Ökosystemen zusammenbauen und monetarisieren. Open Science, und nicht nur Open Access, in eine solche marktförmig kontrollierte Form zu bringen, verändere das Wissenschaftsverhältnis und eskaliere jede Problematik, die jetzt schon zu sehen ist — ähnlich den rasch zirkulierenden Projektkräften, wie sie in Deutschland unter dem Hashtag *#IchbinHanna* diskutiert werden (vgl. Bahr, Eichhorn und Kubon 2022). Hanna ist aus dieser Sicht kein Fehler in einem solchen System, sondern — entsprechend der von Digitalkonzernen in anderen Sektoren bereits durchgesetzten Prekarisierung — Teil einer Entwicklung, die Forschenden die Macht über ihre eigene Agenda zu nehmen und stattdessen einen Status ähnlich von *ghost work* zuzuweisen bestrebt ist (vgl. Gray und Suri 2019). Kommt dann der aktuelle Trend zum verstärkten Einsatz von KI-Systemen hinzu, verstärken sich für Lamdan bestehende Ungleichheiten und Verzerrungen nochmals, denn

> „machine-generated journal impact metrics and researcher ranking systems incorporate the same biases, white supremacy, and systemic racism that permeate academia, favoring the work of white men at elite institutions. Academic data analytics don't repair the racist and misogynistic decisions made in university tenure committees and college boards, they datafy them." (Lamdan 2022, 63f.)

Die Sprachlosigkeit und die Folgen

Während dieser Artikel geschrieben wird,[16] erfährt das mächtigste Land der Welt einen Staatsstreich neuen Typs (vgl. Snyder 2025), bei dem bislang nicht wie in einem klassischen Militärputsch Panzer rollen, sondern Gruppen fanatisierter junger Ingenieure im Auftrag des reichsten Mannes der Welt Daten bewegen. Der *Network State Coup* (vgl. Duran 2025) bringt die Abwehrmechanismen einer freiheitlichen Demokratie durch einen DDoS-Angriff der Illegalität zum Erliegen und den *civil service* unter eine Art Besatzerregime (vgl. Applebaum 2025). Internationale Verträge werden gebrochen, Kriegsverbrechen größten Ausmaßes angekündigt, den Nachbarstaaten wird mit gewaltsamer Intervention und wirtschaftlicher Zerstörung gedroht. Guantanamo soll als Auffanglager für die Opfer der ICE-Razzien dienen, zentrale staatliche Behörden werden im Stundentakt gefleddert, Informationsressourcen — darunter sensibelste Daten der Bürger:innen — werden zugunsten von Datenkonzernen geplündert und für die Allgemeinheit zerstört (vgl. Scheppele 2025, Brockschmidt 2025). Betroffen ist auch die Wissenschaft durch die Zerstörung von Webressourcen, Entfernung von Datenzugängen, Reise- und Publikationsverbote, politisch gezieltes Defunding und Vandalismus gegen zentrale Institutionen.[17] Wie sich die Lage bei der Publikation dieses Textes darstellen wird, ist mitten im Gewirr kaum absehbar. Allem Anschein nach will sich erneut eine Atommacht in eine Kleptokratie verwandeln, nach dem Muster von Putins Russland: Organisierte Kriminalität wird staatenbildend als eine Oligarchie, die das Gemeinwesen aus der Perspek-

16 Januar-Februar 2025, Anm. d. Red.
17 Vgl. den Silencing Science Tracker (https://climate.law.columbia.edu/Silencing-Science-Tracker) am 14.04.2025.

tive einer Beutegemeinschaft betrachtet und auch genauso behandelt (vgl. Burgis 2020 und Michel 2021). Während in Putins Oligarchie die Ausbeutung fossiler Ressourcen und die daraus erwachsenen imperialen Träume im Vordergrund stehen, treten in der sich neu entwickelnden Kleptokratie die Schattenfinanzwirtschaft sowie verstärkt digitale Ressourcen als Grundlage der Plattformkonzerne und des digitalen Kolonialismus ergänzend hinzu, weshalb sich hier der Terminus ‚*broligarchy*' etabliert hat.[18]

Angesichts dessen ist die allgemeine Sprachlosigkeit, die die Transformierung von Wissenschaft in einen datafizierten Raum bisher begleitet hat, umso erstaunlicher. Nahezu unkommentiert verflechten die Datenkartelle eine Vielzahl Tools und Workflows sukzessive zu einer im Hintergrund durchgängigen Verhaltensbiometrie des akademischen Lebens, die sich still durchsetzt. „So far the publishers' data-hoovering hasn't galvanized scholars to protest", schreibt Pooley (2024) zur bisherigen Diskussion. „None of this has translated into much, not even awareness among the larger academic public." (Ebd.) Dabei muss man nur auf ein aktuelles Vergleichsbeispiel zurückgreifen, um besorgniserregende Möglichkeiten zu konstatieren. Als der Supreme Court das Abtreibungsurteil *Roe vs. Wade* kippte, wurden in den USA kommerziell gehandelte Trackingdaten über Nacht zur Bedrohung: Die von Frauen in Notlagen konsultierten Klinikwebseiten hatten Facebook-Trackingpixel installiert; Perioden-Apps sammelten und verteilten Daten; *Meta* übergab auf Social Media getauschte Nachrichten an die Behörden. Frauen wurden in der Folge verhaftet und zu Gefängnisstrafen verurteilt, weshalb Hoffman zur Wachsamkeit aufruft, unabhängig von der individuellen technischen Kompetenz: „you don't have to be an automotive engineer to unterstand that a truck can run you over." (Hoffman 2022, 8)

Von welchem Unternehmen auch immer dies als Produkt angeboten werden wird — in einer Situation, wo wissenschaftliche Publikationen, Förderentscheidungen und Webressourcen wissenschaftlicher Einrichtungen in Massen zurückgezogen und gesperrt werden, um sie nach Listen verbotener Wörter zu prüfen,[19] können auch die über viele Jahre gesammelten Trackingdaten von Forschenden zur Drohung geraten und genutzt werden, um einen *loyalty score* bisherigen Wohlverhaltens zu erzeugen. Wer arbeitete an den falschen Themen? Was sind seine/ihre Netzwerke? Was sind die sonstigen Aktivitäten, räumlichen Bewegungen, der Lebensstil, die familiären Beziehungen? Dadurch entstünden analog zu Lavender Listen von Zielpersonen, ohne dass bislang absehbar wäre, wie sie genutzt würden. Absehbar ist nur, dass bislang geäußerte Vermutungen nicht haltbar sind, dass ein Tracking von Forschenden auch ein Potential für die Wissenschaft selbst haben könnte, wenn es nur forschungsgerecht ins Werk gesetzt würde (vgl. z.B. DFG 2021). Solche Datenbestände wurden von extrem kapital- und technikgetriebenen Konzernen aufgebaut, die darüber ihre Marktposition sichern und sie für immer neue Produktvarianten nutzen, welche qua Design die Machtposition der Anbieter:innen stets weiter ausbauen. Deshalb gibt es von solchen Datensammlungen kei-

18 Vgl. https://broligarchy.substack.com/ (am 14.04.2025) sowie Dachwitz und Hilbig 2025.

19 Vgl. z.B. https://bsky.app/profile/darbysaxbe.bsky.social/post/3lhcvn4hxwk2o und https://www.washingtonpost.com/science/2025/02/04/national-science-foundation-trump-executive-orders-words/ beide am am 14.04.2025.

ne Version *ad usum delphini*, sondern sie haben vor allem das Potential einer geduldig wartenden Schlagfalle, die in einer entsprechenden Konstellation unterschiedslos und empathiefrei von uns allen ausgelöst werden kann. Ausgenommen sind eben diejenigen, die sie mit viel Sorgfalt aufgestellt haben, um ihren Nutzen daraus zu ziehen. Dennoch scheinen entsprechende Mentalitäten ungebrochen — so bewirbt aktuell ein zentraler deutscher Wissenschaftsakteur Systeme wie Lavender als herausragende Lerngelegenheit für Deutschland.[20]

Unterdessen kommen alle Ideologien, die in den vergangenen Jahren im Silicon Valley umliefen, von *Singularity* bis *Long Terminism*, zu einer bizarren Blüte und die maßgeblichen Personen machen keinerlei Hehl aus dem, was sie vorhaben. „We're going to have supervision", erklärte Oracle-Gründer Larry Ellison gegenüber Investoren.[21] „Every police officer ist going to be supervised at all times, and if there's a problem, AI will report that problem and report it to the appropriate person. Citizens will be on their best behavior because we are constantly recording and reporting everything that's going on." (Ebd.) AI-Drohnen würden Polizeiautos ersetzen, Kameras und Sensoren von Amazons *Ring Doorbell* bis zum vernetzten Auto eingesetzt. Eine solch unterschiedslose maschinelle Überwachung sowohl von Bürger:innen wie auch der Vertreter:innen der traditionellen Staatsmacht wäre viel weitergehender als alles, was Funk (2023) in seiner Genealogie der risk solutions entfaltet. Es ist das Bild einer Überwachungsgesellschaft, deren *service provider* die Macht ergriffen haben.

Ausblick

Während die digitale Entwicklung der zurückliegenden Jahrzehnte insgesamt die Möglichkeiten von Wissenschaft und Forschung potenziert, neue Methoden und Fragestellungen eröffnet und eine bessere Qualitätssicherung ermöglicht hat, bedroht die aktuelle Form der Transformation von Wissenschaft in einen datafizierten Raum zugleich ihre Freiheit, Unabhängigkeit und geradezu ihre Überlebensfähigkeit, da die generische Logik dieser Art Datafizierung den Grundlagen freier Wissenschaft völlig konträr ist. Die mit Hilfe von Lavender weggebombten Kinder, die in den Selbstmord getriebenen Opfer von Automated Welfare und auch der Forschende, der sich das Leben nimmt, weil er metrifizierte Zielvorgaben nicht erfüllen kann[22] — sie sind alle keine Belege für die Qualität oder Präzision der eingesetzten Systeme. Es sind Belege dafür, dass sich hier Machtrelationen mit steilen Hierarchien und klaren Trennungen in Beobachtete und Beobachtende etabliert haben, denen solche Konsequenzen offenbar strukturell nahezu gleichgültig sind. Obwohl diese Bedrohung daher keineswegs nur abstrakt zu verstehen ist, sondern Forschende ganz individuell betreffen kann, ist die Awareness bislang

20 Vgl. https://table.media/security/events/side-event-msc-software-defined-defence-was-deutschland-von-israel-lernen-kann/ am 14.04.2025.

21 Vgl. https://www.businessinsider.com/larry-ellison-ai-surveillance-keep-citizens-on-their-best-behavior-2024-9 am 14.04.2025.

22 Vgl. https://www.timeshighereducation.com/news/imperial-college-professor-stefan-grimm-was-given-grant-income-target/2017369.article am 14.05.2025.

gering. Welche Untiefen im routinierten Umgang mit den gängigen wissenschaftlichen Infrastrukturen verborgen liegen können, wird genauso wenig reflektiert wie das alltägliche Wegklicken von Cookiebannern.

Dies ist umso kritischer zu betrachten, als im Paradigma datengetriebener Wissenschaft Forschung und Infrastruktur sich immer mehr amalgamieren, bis eine Grenzziehung kaum mehr möglich ist. Nur noch über stabile und leistungsfähige Infrastrukturen sind Spitzenleistungen in der datengetriebenen Forschung möglich. Umso wichtiger ist es, dass sie keine eigene und im Zweifel nicht wissenschaftsdienliche Agenda entwickeln.

Der Rat für Informationsinfrastrukturen (2024) hat sich in seiner Analyse der *Federated Data Infrastructures* dieser Frage gewidmet. Die vergleichende Analyse von der *Nationalen Forschungsdateninfrastruktur* (NFDI), der *European Open Science Cloud* (EOSC), der *European Common Data Spaces* und von *GAIA-X* stellt ihren gemeinsamen Charakter als politische Strategieentwicklung heraus, wobei die Rolle der Politik weiterhin wachsen wird, da die Grundgedanken zu allen dieser Initiativen noch aus der Zeit vor der Polykrise stammen. Die geopolitischen Veränderungen der letzten Zeit werden sich in den Infrastrukturen daher erst noch niederschlagen, z.B. in Folge der aktuellen Diskussionen über Forschungssicherheit.[23] Auch der Charakter von *Open Science* wird sich absehbar verändern, denn der Zerfall der Welt in multipolare Einfluss-Sphären und die absehbare Aufspaltung des bislang gemeinsamen Technologiestacks durch den *Tech Cold War* wird das Regime des Datenzugangs beeinflussen (vgl. Augsberg, Düwell und Müller 2024 sowie Baums und Butts 2025). Die den *Common Data Spaces* zugrunde liegende Idee des Europäischen Datenbinnenmarkts legt dies bereits nahe: Datenzugang haben in dessen Logik EU-Ansässige, die das *level playing field* und die Europäischen Grundwerte anerkennen. Entsprechend wird sich auch die im Rahmen der aktuellen Berichte[24] von Letta und Draghi diskutierte fünfte Grundfreiheit von Forschung, Innovation und Bildung etablieren.[25]

Aus der aktuellen Publikation der DFG (2025) zur digitalen Forschungspraxis ergibt sich ein ähnliches Bild. Kooperative Infrastrukturen müssten dem Anforderungsdruck datengetriebener Forschung standhalten können. Berufsbilder, Verantwortungen und Interessen sortierten sich neu, um Daueraufgaben wie die Kuratierung von Daten, Software und Diamond-Open-Access-Infrastrukturen auch nachhaltig betreiben zu können.

Letztendlich geht es wieder einmal um digitale Souveränität. Auch wenn der Begriff mittlerweile nicht mehr den besten Ruf hat und teils im Verdacht steht, einem Rückzug ins Nationale das Wort zu reden, so muss man festhalten, dass es in der Wissenschaft da-

23 Vgl. z.B. https://www.dfg.de/de/service/presse/pressemitteilungen/2024/pressemitteilung-nr-37 am 14.04.2025.

24 Vgl. https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf und https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf beide am 14.04.2025.

25 Vgl. https://de.euronews.com/business/2024/06/11/bildung-soll-funfte-freiheit-werden-enrico-letta-uber-den-eu-binnenmarkt am 14.04.2025.

bei keineswegs darum geht, eine virtuelle schwarz-rot-goldene Flagge auf das Dach einer ebenso virtuellen Alma Mater zu pflanzen. Sowohl die denkbar knappe, auf das einzelne Individuum bezogene Definition „Die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum" (BMWi 2017) wie auch die allgemeine, institutionsbezogene längere Version „Die Souveränität eines demokratischen Staates besteht in der Sicherung der Selbstbestimmungsfähigkeit seiner Bürgerinnen und Bürger mit ihren unveräußerlichen Rechten" (Pohle 2020, 6) zeigen deutlich, dass es um die Wiederherstellung und Sicherung von Autonomie und Handlungsfähigkeit der freien Wissenschaft geht. Dazu gehört auch, das Versprechen von Open Science nicht korrumpieren zu lassen.

„Souveränität und Sicherheit im digitalen Raum" sind daher auch aus Sicht des Wissenschaftsrats (2023) „zentral für ein resilientes Wissenschaftssystem" und Gegenstand einer Reihe an Empfehlungen zur Förderung der digitalen Selbstbefähigung der Wissenschaftseinrichtungen. Aktuell steht es damit offenkundig nicht zum Besten, denn Rechenzentren sehen sich engen Grenzen gegenüber, welche Hardware überhaupt beschafft und wie sie dann eingesetzt werden kann. Bibliotheken wie andere Informationseinrichtungen haben die Hoheit über ihre digitalen Angebote nahezu völlig verloren. Die lange Historie der Paketlizenzen hat den kontrollierbaren Anteil des Angebots ausgelöscht, da es das einzig freie Volumen zur Kündigung zugunsten immer größerer Big Deals war. Jetzt ist es in den übergroßen Transformationsverträgen nicht einmal mehr möglich, klare Rechtsverletzungen und Gefahren für die Forschenden — wie das Datentracking — wirksam auszuschließen.

Angesichts dieser Gegebenheiten und vor allem angesichts der aktuellen Situation, in der die bisherige westliche Führungsmacht sich u.a. anschickt, in einem machtpolitischen Bullying zu versuchen, die europäische Digitalgesetzgebung niederzureißen,[26] erscheinen die Empfehlungen des Wissenschaftsrats mittlerweile als übervorsichtig und zu begrenzt. Umso mehr ist allerdings weiterhin seiner Schlussfolgerung zuzustimmen:

> „Souveränität und Sicherheit lassen sich langfristig nur sichern, wenn auch die strukturellen und finanziellen Rahmenbedingungen des digitalen Wissenschaftsbetriebs weiterentwickelt werden. Daher bekräftigt der Wissenschaftsrat seine Position, dass die *Gestaltung des digitalen Raumes als Daueraufgabe von Wissenschaftseinrichtungen* zu verankern und dem auch in finanzieller Hinsicht Rechnung zu tragen ist. Zugleich sind alle Angehörigen der Einrichtungen gefordert, sich dieser Aufgabe anzunehmen und daran mitzuwirken." (WR 2023, 8, Hervorhebung im Original)

Der Aufbau der Nationalen Forschungsdateninfrastruktur, die Einrichtung eines nationalen Hubs für Diamond Open Access, der — wenn auch extrem langsame — Wandel in der Forschungsbewertung sind alles Kristallisationskeime, aus denen ein alternatives Ökosystem mit allen nötigen Funktionalitäten sukzessive erwachsen kann (vgl. dazu

26 Vgl. https://www.heise.de/news/DSA-und-Co-US-Praesident-laesst-Digitalgesetze-im-Ausland-pruefen-10292156.html am 14.04.2025.

Brembs u.a. 2023). Dies braucht die Hilfe aller Beteiligten. Daher ist zu wünschen, dass der aktuelle Aufruf der DFG zu einem Dialog über digitale Forschungspraxis und kooperative Informationsinfrastrukturen Erfolg hat.

Literatur

Abraham, Yuval. 2024. „‚Lavender': The AI machine directing Israel's bombing spree in Gaza." *+972 Magazine*, 03.04.2024. Abgerufen am 14.04.2025. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

American Library Association. 2021. *Resolution on the Misuse of Behavioral Data Surveillance in Libraries*. Abgerufen am 14.04.2025. https://www.ala.org/advocacy/intfreedom/datasurveillanceresolution .

Applebaum, Anne. 2025. „There's a Term for What Trump and Musk Are Doing. How Regime Change is Happening in America". *The Atlantic*, 13.02.2025. Abgerufen am 14.04.2025. https://www.theatlantic.com/ideas/archive/2025/02/doge-civil-servant-purge/681671/.

Augsberg, Steffen, Düwell, Marcus und Müller, Benjamin, Hrsg. 2024. *Datenzugangsregeln. Zwischen Freigabe und Kontrolle*. Frankfurt/M., Campus Verlag.

Bahr, Amrei, Eichhorn, Kristin, Kubon, Sebastian. 2022. *#IchBinHanna. Prekäre Wissenschaft in Deutschland*. Frankfurt/M., Suhrkamp.

Baums, Ansgar und Butts, Nicholas. 2025. *Tech Cold War. The Geopolitics of Technology.* Boulder, Colorado, Lynn Rienner Publishers.

BMWi. 2017. *Kompetenzen für eine Digitale Souveränität*. Berlin, Bundesministerium für Wirtschaft und Energie. Abgerufen am 14.04.2025. https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html.

Brembs, Björn u.a. 2020. „Auf einmal Laborratte. Wie Großverlage Wissenschaftler überwachen". *Frankfurter Allgemeine Zeitung 0*2.12.2020. https://doi.org/10.5281/zenodo.4317252.

Brembs, Björn u.a. 2023. „Replacing Academic Journals". *Royal Society Open Science* 10: 230206. https//doi.org/10.1098/rsos.230206 .

Brockschmidt, Annika. 2025. „Staatsstreich mit USB-Drives: der digitale Putsch des Elon Musk". *Blätter für deutsche und internationale Politik* März 2025. Abegrufen am 14.04.2025. https://www.blaetter.de/ausgabe/2025/maerz/staatsstreich-mit-usb-drives-der-digitale-putsch-des-elon-musk .

Burgis, Tom. 2020 *Kleptopia. How Dirty Money is Conquering the World*. London, Harper Collins.

Dachwitz, Ingo und Hilbig, Sven. 2025. *Digitaler Kolonialismus. Wie Tech-Konzerne und Großmächte die Welt unter sich aufteilen.* München, C.H. Beck.

DBV. 2019. *Empfehlungen zu Methoden zur Kontrolle des Zugriffs auf wissenschaftliche Informationsressourcen. Ein gemeinsames Papier von Deutscher Bibliotheksverband e.V. (dbv) und Schwerpunktinitiative Digitale Information der Allianz der deutschen Wissenschaftsorganisationen*. Berlin, Deutscher Bibliotheksverband. Abgerufen am 14.04.2025. https://dbv-cs.e-fork.net/sites/default/files/2020-11/2019_11_27_dbv_Stellungnahme_Empfehlungen%20zu%20Methoden%20zur%20Kontrolle%20des%20Zugriffs%20auf%20wissenschaftliche%20Informationsressourcen.pdf.

DFG. 2021. *Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage. Ein Informationspapier des Ausschusses für Wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft*. Bonn, Deutsche Forschungsgemeinschaft. https://doi.org/10.5281/zenodo.5900759.

[DFG] Altschaffel, Robert u.a. 2024. „Datentracking und DEAL. Zu den Verhandlungen 2022/2023 und den Folgen für die wissenschaftlichen Bibliotheken". *Recht und Zugang* 5 (1): 23–40. https://doi.org/10.5771/2699-1284-2024-1-23.

DFG. 2025. *Digitale Forschungspraxis und kooperative Informationsinfrastrukturen. Ein Diskussionspapier der Deutschen Forschungsgemeinschaft (DFG) zu Förderung und Finanzierung wissenschaftlicher Informationsinfrastrukturen*. Bonn, Deutsche Forschungsgemeinschaft. https://doi.org/10.5281/zenodo.14621979.

Duran, Gil. 2025. „The Network State Coup is Happening Right Now". *The Nerd Reich*, 01.02.2025. Abgerufen am 14.04.2025. https://thenerdreich.com/the-network-state-coup-is-happening-right-now/.

Fried, Eiko. 2022. „Welcome to Hotel Elsevier. You can check out any time you like ... not". *Eiko Fried Blog*, 09.05.2022. Abgerufen am 14.04.2025. https://eiko-fried.com/welcome-to-hotel-elsevier-you-can-check-out-any-time-you-like-not/.

Funk, McKenzie. 2023. *The Hank Show. How a House-Painting, Drug Running DEA-Informant Built the Machine That Rules Our Lives*. New York, St. Martin's Press.

Gilman, Michelle. 2020. „How algorithms intended to root out welfare fraud often punish the poor". *PBS News* 17.02.2020. Abgerufen am 14.04.2025.. https://www.pbs.org/newshour/economy/column-how-algorithms-to-root-out-welfare-fraud-often-punish-the-poor.

Granick, Jennifer Stisa. 2017. "We Kill People Based on Metadata." In *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It* , 53–66. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316216088.006 .

Gray, Mary L., Suri, Siddhart. 2019. *Ghost Work. How to Stop Silicon Valley from Building a New Global Underclass.* Boston, Massachusetts, Houghton Mifflin Harcourt Company.

Hanson, Cody. 2015. *Libraries are Software.* Abgerufen am 14.04.2025. https://www.codyh.com/writing/software.html und https://www.youtube.com/watch?v=fNr-nsTGV8w.

Hanson, Cody. 2019. *User Tracking on Academic Publisher Platforms*. Abgerufen am 14.04.2025. https://www.codyh.com/writing/tracking.html und https://www.youtube.com/watch?v=uAzt-iJEkvU.

Hellman, Eric. 2015. „16 of the top 20 research journals let ad networks spy on their readers". *Go to Hellman*, 12.03.2015. Abgerufen am 14.04.2025. https://go-to-hellman.blogspot.com/2015/03/16-of-top-20-research-journals-let-ad.html.

Hoffman, Bob. 2022. *ADSCAM. How Online Advertising Gave Birth to One of History's Greatest Frauds, and Became a Threat to Democracy* . Oakland, Type A Group.

Keegan, Jon und Eastwood, Joel. 2023. „From ‚Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650.000 Ways Advertisers Label You". *The Markup 0*8.06.2023. Abgerufen am 14.04.2025. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you .

Kitchin, Rob und Dodge, Martin. 2011. *Code/Space. Software and Everyday Life.* Cambridge, Massachusetts, The MIT Press. https://doi.org/10.7551/mitpress/9780262042482.001.0001 .

Koivisto, Joseph und Sly, Jordan. 2023. „Publication and data surveillance in academia". *Research Information Yearbook 2022/2023*. Abgerufen am 14.04.2025. https://www.researchinformation.info/feature/publication-and-data-surveillance-academia .

Kukier, Kenneth Neil und Mayer-Schoenberger, Viktor. 2013. „The Rise of Big Data. How It's Changing the Way We Think About the World". *Foreign Affairs* Mai/Juni 2013. Abgerufen am 14.04.2025. https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data.

Lamdan, Sarah. 2022. *Data Cartels*. *The Companies That Control and Monopolize Our Information*. Stanford, California, Stanford University Press.

Lindstrot, Barbara. 2025. „Wissenschaftsverlage und Third-Party-Tracking. Wer sind diese Third-Partys? – Codefragmente im Seitenquelltext von Verlagen führen zu diversen Firmen". *ABI Technik*, *45*(1): 28-49. https://doi.org/10.1515/abitech-2025-0001.

Loewenstein, Antony. *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World* . London, Verso Books 2023.

Lynch, Cliff. 2017. „The Rise of Reading Analytics and the Emerging Calculus of Reader Privacy in the Digital World". *First Monday* 4 (22). https://doi.org/10.5210/fm.v22i4.7414 .

Michel, Casey. 2021. *American Kleptocracy. How the U.S. Created the World's Greatest Money Laundering Scheme in History*. New York, St. Martin's Press.

Mirowski, Philip. 2022. *A Science Worth Trusting? Platform Capitalism Reorganizes the Science of the Future*. Presentation at Max Planck Institute for the History of Science 18.01.2022. Abgerufen am 14.04.2025. https://www.mpiwg-berlin.mpg.de/video/science-worth-trusting-platform-capitalism-reorganizes-science-future .

Molnar, Petra. 2024. *The Walls have Eyes. Surviving Migration in the Age of Artificial Intelligence*. New York, The New Press.

Palantir. 2024. Palantir Technologies | Q4 2024 Earnings Webcast. Abgerufen am 14.04.2025. https://www.youtube.com/watch?v=MW0zvoEMdRA.

Pohle, Julia. 2020. *Digitale Souveränität: Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa*. Berlin, Konrad Adenauer Stiftung.

Pooley, Jeff. 2022. „Surveillance Publishing". *The Journal of Electronic Publishing* 25(1). https://doi.org/10.3998/jep.1874.

Pooley, Jeff. 2024. „Large Language Publishing". *Upstream*, 02.01.2024. https://doi.org/10.54900/zg929-e9595.

Posada, Alejandro und Chen, George. 2017. „Publishers are increasingly in control of scholarly infrastructure and why we should care". *The Knowledge G.A.P.* 20.09.2017. Abgerufen am 14.04.2025. https://knowledgegap.org/index.php/sub-projects/rent-seeking-and-financialization-of-the-academic-publishing-industry/preliminary-findings/ .

Rehak, Rainer. 2024. „Der Mythos der ‚gezielten Tötung'. Zur Verantwortung von KI-gestützten Zielsystemen am Beispiel ‚Lavender'". Vortrag auf dem 38. Chaos Communication Congress 28.12.2024. Abgerufen am 14.04.2025. https://media.ccc.de/v/38c3-der-mythos-der-gezielten-ttung-zur-verantwortung-von-ki-gesttzten-zielsystemen-am-beispiel-lavender.

RfII. 2024.*Federated Data Infrastructures for Scientific Use. NFDI, EOSC, Gaia-X, and the European Data Spaces: Comparison and Recommendations for a Committed Engagement to Shape the European Research Data Ecosystem*. Göttingen, Rat für Informationsinfrastrukturen.

Ryan, Johnny und Christl, Wolfie. 2023a. *Europe's hidden security crisis. How data about European defence personnel and political leaders flows to foreign states and non-state actors*. Abgerufen am 14.04.2025. https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf .

Ryan, Johnny und Christl, Wolfie. 2023b. *America's hidden security crisis. How data about United States defence personnel and political leaders flows to foreign states and non-state actors.* Abgerufen am 14.04.2025. https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf.

Scheppele, Kim Lane. 2025. „Trumps Gegenverfassung. ‚He who saves his Country does not violate any Law.'" *Verfassungsblog*, 21.02.2025. Abgerufen am 14.04.2025. https://verfassungsblog.de/trumps-gegenverfassung/.

Schonfeld, Roger C. 2018. "The Supercontinent of Scholarly Publishing?" *The Scholarly Kitchen,* 03.05.2018. Abgerufen am 14.04.2025. https://scholarlykitchen.sspnet.org/2018/05/03/supercontinent-scholarly-publishing/ .

Siems, Renke. 2014. „Innere und äußere Kreise". *Bibliotheksdienst* 48(8-9): 612–632. https://doi.org/10.1515/bd-2014-0077.

Siems, Renke. 2021. „When your journal reads you – user tracking on science publisher platforms". *Elephant in the Lab* 14.04.2021. https://doi.org/10.5281/zenodo.4683778 .

Siems, Renke. 2022. „Das Lesen der Anderen: Die Auswirkungen von User Tracking auf Bibliotheken". *O-Bib. Das Offene Bibliotheksjournal Herausgeber VDB*, *9*(1): 1-25. https://doi.org/10.5282/o-bib/5797.

Siems, Renke. 2022. „Rezension zu: Data Cartels: The Companies That Control and Monopolize Our Information“. *O-Bib. Das Offene Bibliotheksjournal Herausgeber VDB* 9 (4): 1-8. https://doi.org/10.5282/o-bib/5902.

Siems, Renke. 2023. „‚Überwachen und Strafen‘ – Tracking und Kontrolle des Forschungszyklus“. *ABI Technik*, *43*(2): 86-95. https://doi.org/10.1515/abitech-2023-0016.

Siems, Renke. 2024a. „‚Going Dark‘. Datentracking und Datenzugriff auf europäischer Ebene.“ *ZEVEDI-Verantwortungsblog* 13.08.2024. https://doi.org/10.60805/5c9w-7n74 .

Siems, Renke. 2024b „Subprime Impact Crisis. Bibliotheken, Politik und digitale Souveränität“. *Bibliothek Forschung und Praxis*, *48*(2): 311-321. https://doi.org/10.1515/bfp-2024-0008 .

Siems, Renke. 2024c. „Rezension zu: The Hank Show: How a House-Painting, Drug Running DEA Informant Built the Machine That Rules Our Lives“. *O-Bib. Das Offene Bibliotheksjournal Herausgeber VDB* 11 (1): 1-8. https://doi.org/10.5282/o-bib/6021.

Snyder, Timothy. 2025. „Of course it’s a coup. Miss the obvious, lose your republic“. *Thinking About...* 05.02.2025. Abgerufen am 14.04.2025**.** https://snyder.substack.com/p/of-course-its-a-coup.

[SPARC] Aspesi, Claudio u.a. 2019. *SPARC Landscape Analysis* . https://doi.org/10.31229/osf.io/58yhb .

[SPARC] Aspesi, Claudio u.a. 2020. *2020 Update: SPARC Landscape Analysis & Roadmap for Action* . https://doi.org/10.31229/osf.io/2pwft .

[SPARC] Aspesi, Claudio u.a. 2021. *2021 Update: SPARC Landscape Analysis & Roadmap for Action* . Abgerufen am 14.04.2025. https://infrastructure.sparcopen.org/media/posts/report-landscape-analysis-2021-update.pdf.

[SPARC] Yoose, Becky und Shockey, Nick. 2023. *Navigating Risk in Vendor Data Privacy Practices: An Analysis of Elsevier's ScienceDirect (Version v1).* https://doi.org/10.5281/zenodo.10078610.

[SPARC] Yoose, Becky und Shockey, Nick. 2024. *Navigating Risk in Vendor Data Privacy Practices: An Analysis of Springer Nature's SpringerLink (Version v1).* https://doi.org/10.5281/zenodo.13886473.

[VDI] Zweck, Axel, Holtmannspötter, Dirk und Freund, Sebastian. 2024. „Tracking in der Wissenschaft“. *VDI Research-Paper 17* . Düsseldorf, VDI Technologiezentrum. Abgerufen am 14.04.2025. https://www.vditz.de/service/publikationen/details/tracking-in-der-wissenschaft.

WR. 2023. *Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum*. Köln, Wissenschaftsrat. https://doi.org/10.57674/m6pk-dt95.

Wittmann, Lilith. 2025. „Warum die EUDI-Wallet Menschenleben gefährdet“. *Payment & Banking* 04.02.2025. Abgerufen am 14.04.2025. https://paymentandbanking.com/warum-die-neue-eudi-wallet-menschenleben-gefaehrdet/.

Wood, David Murakami. 2019. „Spies in the Information Economy: Academic Publishers and the Trade in Personal Information“. *ACME: An International Journal for Critical Geographies*, 8(3): 484–493. https://doi.org/10.14288/acme.v8i3.846 .

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* . London, Profile Books.