easy social sciences

69 · 2023

Neue Daten und Methoden in der Sozialforschung: digital & transformativ

gesis Leibniz-Institut für Sozialwissenschaften

Julian Kohne, Josephine B. Schmitt & Johannes Breuer (Hrsg.)

Neue Daten und Methoden in der Sozialforschung: digital & transformativ

Inhalt

doi: 10.15464/easy.2023.07

Digitalisierungsforschung

Ein Einblick in die Bandbreite der Forschung zu und mit digitalen Daten

Julian Kohne, Josephine B. Schmitt & Johannes Breuer

*„Daten sind das neue Öl" – dieser plakative Slogan der Werbeindustrie verdeutlicht den Boom in der Auswertung und Nutzung digitaler Daten in den letzten beiden Jahrzehnten. Kommerzielle Anbieter nutzen diese Daten, um immer mehr und immer detailliertere Informationen über ihre Nutzenden und Kund*innen zu erheben und ihre Produkte so personalisieren und weiterentwickeln zu können. Aber digitale Daten können nicht nur zur Gewinnmaximierung genutzt werden. Auch die (sozial-) wissenschaftliche Forschung nutzt immer häufiger solche Daten und erforscht Verhalten im digitalen Kontext. Digitale Forschungsdaten bringen dabei, genau wie das „alte Öl", enorme Potenziale, aber auch große Herausforderungen mit sich. In dieser Ausgabe von* **easy_social_sciences** *möchten wir daher einen Einblick in die vielfältigen disziplinären, methodischen und inhaltlichen Ansätze zur Forschung mit und über digitale Daten geben, um einen Eindruck zu vermitteln, wie sie genutzt werden können, um neue Forschungspotenziale zu erschließen.*

"Data is the new oil" – this illustrative quote from the advertising industry underlines the boom in the analysis and use of digital data in recent decades. Commercial providers use this data to collect increasingly detailed information about their users and customers in order to develop and personalize their products and services. But digital data cannot only be used to maximize profits. (Social) scientific research is also making increasing use of such data and investigating behavior in a digital context. However, digital research data, just like the proverbial "oil", comes not only with enormous potentials but also great challenges. In this issue of **easy_social_sciences**, *we thus provide an overview of the diverse disciplinary, methodological, and substantuve approaches to research with and about digital data. In doing do, we aim to underline how these kinds of data can be used to exploit new research opportunities.*

Keywords: Digitale Forschungsdaten, Digitalisierung, digitale Transformation, Interdisziplinarität

„Daten sind das neue Öl". Mit diesem Satz beschrieb der Data Scientist Clive Humby schon 2006 in einem Vortrag auf der Association of National Advertisers Conference die Potenziale von digitalen Daten für die Werbeindustrie (Humby & Palmer, 2006). Auch wenn die Metapher oftmals kritisiert wurde (vgl. Sonderegger, 2021), hat sich die darin enthaltene Prognose im Wesentlichen bewahrheitet. Die Entwicklungen der letzten beiden Jahrzehnte können gewissermaßen in Anlehnung an den „Oil Boom" des 20. Jahrhunderts auch als „Data Boom" bezeichnet werden. Social-Media-Plattformen wie Facebook, reddit oder YouTube entwickelten Geschäftsmodelle, bei denen die Nutzung der Plattformen sich ausschließlich über zielgerichtete Werbung finanziert, während für Endnutzende keine

Kosten anfallen. Dieses Prinzip funktioniert, da die Plattformen Informationen über ihre Nutzenden sammeln können. Dies umfasst neben soziodemographischen Daten wie Alter, Geschlecht, Familienstand, Wohnort oder das Bildungsniveau auch Eigenschaften wie Hobbies, Interessen, politische Einstellungen oder Werte (z.B. Meta, 2022). Diese Informationen können bei der Nutzung der Plattformen entweder von Nutzenden selbst angegeben werden oder aber mithilfe von mathematischen Modellen aus dem Nutzungsverhalten abgeleitet werden. Laut Googles Chefökonomen Hal Varian (2014) sind dabei vier Punkte entscheidend: Datenextraktion und Analyse, Personalisierung und Anpassbarkeit, stetiges Experimentieren und neue Vertragsformen durch bessere Überprüfbarkeit. Damit kann Werbung zielgerichteter und individueller personalisiert werden als zuvor. Dieses Geschäftsmodell erweist sich als äußerst profitabel, wenn es auf Millionen oder gar Milliarden Nutzende angewendet wird. Aus diesem Grund wurde hierfür u.a. die Bezeichnung „Überwachungskapitalismus" (Englisch: surveillance capitalism) geprägt (Zuboff, 2015).

Aber nicht nur Social-Media-Plattformen haben das enorme Potenzial erkannt. Mittlerweile nutzen fast alle Anbieter von digitalen Services – von Betriebssystemen auf Computern und Smartphones (z.B. Microsoft 2023; Samsung, 2023), über Shopping-Plattformen wie Amazon oder eBay (Amazon, 2023; eBay, 2023), Entertainment-Anbietern wie Spotify (Spotify, 2023) oder Netflix (Netflix, 2022), bis zu speziellen Geräten wie Fitnesstrackern (z.B. Fitbit, 2023) – digitale Daten, um ihre Nutzenden zu quantifizieren und ihre Angebote damit zu optimieren und zu personalisieren. Dies muss nicht unbedingt immer im Interesse der Nutzenden selbst liegen: Das bekannteste Beispiel ist hier wohl das der personalisierten Werbung.

Die digitalen Daten, die Nutzende generieren, sind allerdings nicht nur interessant für die Unternehmen, die diese zu kommerziellen Zwecken erfassen. Auch die sozialwissenschaftliche Forschung ist inzwischen „auf Öl gestoßen". Sie hat die Potenziale für die Forschung zu und mit der Vielzahl an digitalen Daten erkannt und hat begonnen diese zu nutzen (Keuschnigg et al., 2018; Wagner et al., 2021).

Digitale Forschungsdaten: Mehr als nur Big Data

Wenn es um neue Datentypen und die Idee von Daten als dem „neuen Öl" geht, ist oft von Big Data die Rede. Obwohl der Begriff oft nicht genau definiert ist, können viele der neuen digitalen Forschungsdatentypen zu dieser Kategorie gezählt werden. Der Begriff Big Data umfasst aber nicht notwendigerweise *alle* digitalen Daten, die für die sozialwissenschaftliche Forschung von Interesse sind.

Während Big Data in der Regel durch fünf Merkmale definiert sind, die sich auf das Volumen, die Vielfalt, die Geschwindigkeit, die Genauigkeit und den Nutzen der Daten (im Englischen: volume, variety, velocity, veracity, and value) beziehen, gibt es auch digitale Daten, die für die Forschung wertvoll sind, aber nicht alle diese Merkmale aufweisen (s.u.). Zudem gibt es alternative Begriffe, die v.a. aus Sicht der Sozialwissenschaften, präziser sind als Big Data. So wird am GESIS – Leibniz-Institut für Sozialwissenschaften beispielsweise der Begriff „Digitale Verhaltensdaten" genutzt, der für alle Spuren von menschlichem Verhalten steht, die durch die Nutzung digitaler Technologien entstehen oder nutzbar gemacht werden können (Wilke et al., 2021). Ein weiterer gängiger Begriff ist „digitale Spurdaten", welche als „records of activity [...] undertaken through an online information system [...] that can be collected from a multitude of technical systems, such as websites, social media platforms, smartphone apps, or sensors" definiert werden können (Stier et al., 2020a; Howison et al., 2011).

Damit sind einerseits auch kleinere, homogenere Datensätze gemeint, die für die

Sozialwissenschaften interessant sind, andererseits werden Big Data ausgeschlossen, aus denen wenige oder keine Informationen über Menschen gewonnen werden können. So kann beispielsweise ein einzelner Twitter-Verlauf (jetzt X) einer politischen Persönlichkeit oder eines Parteiaccounts als digitaler Forschungsgegenstand relevant sein – selbst, wenn nicht alle Merkmale von Big Data auf ihn zutreffen. Andererseits gibt es viele Datensätze, auf welche die Definition von Big Data zutrifft, die aber für sozialwissenschaftliche Fragestellungen typischerweise nicht relevant sind. Dazu gehören beispielsweise astronomische Beobachtungen, physikalische Messungen oder Sensordaten, die in Produktionsmaschinen zur Prozessoptimierung gesammelt werden.

Neue Daten und Methoden als Treibstoff für die Forschung

Clive Humbys Metapher ist im Kontext der Forschung in mehreren Hinsichten überraschend treffend. Denn digitale Daten bringen nicht nur neue Möglichkeiten mit sich, sondern auch neue Herausforderungen. Genau wie für das sprichwörtliche Öl braucht es nämlich für digitale Forschungsdaten neue Werkzeuge und Wissen, um diese Daten „zu fördern". Zusätzlich sind „rohe" digitale Forschungsdaten, ähnlich wie Rohöl, meist nicht direkt nutzbar, sondern müssen aufwändig aufbereitet und weiterverarbeitet werden, bevor sie überhaupt ausgewertet – und damit genutzt – werden können. Dazu gehört beispielsweise die Anreicherung mit anderen Datensätzen. So wie Motorenbenzin viele Zusätze enthält, um optimal auf den jeweiligen Motor abgestimmt zu sein, ist es für digtiale Forschungsdaten in vielen Fällen sinnvoll oder sogar notwendig, diese um Umfragedaten oder qualitative Daten zu erweitern, um ihr volles Potenzial zu entfalten (Stier et al., 2020a).

Nicht zuletzt kann man mit Kerosin keinen Holzofen betreiben. Das bedeutet, dass für potenteren Treibstoff (in diesem Fall mehr und detailliertere Informationen) geeignete Methoden entwickelt werden müssen, um diesen effizient nutzen zu können. Für digitale Forschungsdaten sind dies oft Methoden aus den Bereichen Data Science und Machine Learning, die es ermöglichen, größere und unstrukturiertere Daten zu verarbeiten und komplexere Zusammenhänge abzubilden als dies die „klassischerweise" in den Sozialwissenschaften genutzten Methoden der deskriptiven und Inferenzstatistik können. Machine Learning ist dabei oft viel stärker datengetrieben als die sozialwissenschaftliche Inferenzstatistik. Statt ein Modell zu entwickeln und dann zu testen, ob dieses Modell zu den gesammelten Daten passt, geht Machine Learning typischerweise von den gesammelten Daten aus, und *lernt* das beste Modell, dass die Zusammenhänge in den Daten abbilden kann. Statt die linearen Zusammenhänge einiger weniger Faktoren auf kleinen Datensätzen zu modellieren, können diese komplexeren Modelle das Zusammenspiel von tausenden oder Millionen Einflussfaktoren in hochkomplexen Interaktionen darstellen.

Mit dieser Steigerung der Möglichkeiten im Umgang mit komplexen Datenstrukturen geht oft allerdings auch ein Verlust an Transparenz und Interpretierbarkeit einher. Neuronale Netzwerke sind beispielsweise als Machine-Learning-Ansatz gut geeignet, um komplexe Zusammenhänge zur Kategorisierung von Merkmalen zu erlernen, da sie anhand von beobachteten Daten „selbst lernen", welche Einflussfaktoren in welcher Kombination die größte Rolle bei der Vorhersage spielen. Die erlernten Muster sind allerdings häufig mathematisch so komplex, dass sie für Menschen nicht sinnvoll interpretierbar sind (z.B. Rudin, 2019). Konkret bedeutet dies, dass es mit solchen Modellen möglich ist, mathematisch gute Kategorisierungen zu entwickeln, ohne im Detail zu verstehen, *warum* eine bestimmte Kombination aus Merkmalen zu einem bestimmten Ergebnis führt (vgl. Abbildung 1). Diese und ähnliche Ansätze werden daher auch als „black box" bezeichnet (Rudin, 2019).

Digitale Forschungsdaten sind allerdings

nicht nur „das neue Öl“, wenn es um die Herausforderungen geht, die sich aus ihnen ergeben, sondern auch was ihre Möglichkeiten betrifft. Sie stellen für die Forschung einerseits eine Innovation in einzelnen, isolierten Disziplinen oder für ganz bestimmte Forschungsfragen dar. Andererseits fungieren sie als Innovationsmotor über Themenbereiche und disziplinäre Grenzen hinweg. So gibt es in fast allen (sozial-)wissenschaftlichen Disziplinen, von der Soziologie, über die Politikwissenschaft, die Kommunikations- und Medienwissenschaft oder die Psychologie immer mehr Forschungsarbeiten zu und mit digitalen Daten (Edelmann et al., 2020). Dabei ermöglichen diese Daten durch die Abbildung tatsächlichen Verhaltens in hoher Granularität einen neuen Blick auf etablierte Forschungsthemen wie z.B. Rassismus (z.B. Chaudhry, 2015), Sexismus (z.B. Samory et al., 2021), Extremismus (z.B. Aldera et al., 2021), Gruppendynamiken (z.B. Vega et al., 2021), Informationssuche und Nachrichtenkonsum (z.B. Stier et al., 2020b) oder Meinungsbildung (z.B. Kozitsin, 2022). Weiterhin ergeben sich durch digitale Daten neue Forschungsfragen, beispielsweise zu Phänomenen wie Filterblasen (z.B. Ross Arguedas, 2022), Interaktionen mit digitalen Technologien im Alltag (z.B. Faelens et al., 2021) oder dem Einfluss von Suchvorschlägen und Rankingalgorithmen auf menschliches Verhalten (z.B. Santos et al., 2021).

Wichtig ist dabei, dass digitale Forschungsdaten und Analysemethoden keinesfalls etablierte Datentypen und Methoden vollständig ersetzen können (Wilke et al., 2021). Diese Ansätze können sich im Gegenteil sehr gut gegenseitig ergänzen (Stier et al., 2020a). Umfragedaten erfassen oft subjektive Meinungen, Einstellung und Werte, Experimente können kausale Zusammenhänge offenlegen und qualitative Ansätze bieten mehr Möglichkeiten für tiefere Einblick in Prozesse (etwa des Verstehens) und Theorieentwicklung als die quantitative Arbeit mit digitalen Forschungsdaten. Im Gegenzug erfassen digitale Daten tatsächliches Verhalten, haben eine höhere

Abbildung 1
Cartoon zur problematischen Nutzung von Machine-Learning-Algorithmen. Statt interpretierbarer, theoriegeleiteter Hypothesen arbeiten diese Modelle oft mit rein datengetriebenen Vorhersagen. Sie können dafür allerdings komplexere Muster in großen Datensätzen besser abbilden als „klassische“ statistische Ansätze.
Quelle: https://m.xkcd.com/1838/

zeitliche und räumliche Auflösung, können oft in großem Umfang automatisiert erhoben werden und sind dabei zum Teil weniger umständlich in der Erhebung.

Eine letzte Gemeinsamkeit zwischen dem „Oil Boom“ und der Nutzung digitaler Forschungsdaten stellt das Potenzial für Schaden dar, der aus unsachgemäßem Gebrauch resultieren kann und die Notwendigkeit von klaren Regeln, die dies verhindern sollen. So wie in fossilen Brennstoffen eine enorme Menge Energie gespeichert ist, die nur zur richtigen Zeit, am richtigen Ort und zum richtigen Zweck freigesetzt werden sollte, enthalten digitale Daten oft persönliche und möglicherweise sensible Informationen über uns und unser soziales Umfeld, deren Nutzung u.U. „explosiv“ sein kann (um im Bild zu bleiben). So wie es für den Umgang mit fossilen Brennstoffen industrielle Sicherheitsstandards gibt, gibt es daher auch für digitale Forschungsdaten Leitlinien für einen ordnungsgemäßen Umgang. Dazu

gehören neben einem gesetzlichen Rahmen, wie ihn zum Beispiel die europäische Datenschutzgrundverordnung (DSGVO) vorgibt, auch ethische Richtlinien und Empfehlungen innerhalb der wissenschaftlichen Forschung zum Umgang mit solchen Daten (z.B. franzke et al., 2020).

Digitale Forschungsdaten als „das neue Öl“ bringen also sowohl zahlreiche Chancen und Potenziale als auch spezifische Herausforderungen und Risiken für die sozialwissenschaftliche Forschung mit sich. Aber was bedeutet das konkret für einzelne Forschungsprojekte? Das lässt sich für die Digitalisierungsforschung als methodisch, theoretisch und disziplinär enorm heterogenes Feld nicht pauschal beantworten (zur allgemeinen Entwicklung des Feldes siehe auch Schmitt et al., 2023). Mit der vorliegenden Ausgabe von *easy_social_sciences* wollen wir trotzdem den Versuch unternehmen, den Lesenden anhand von ausgewählten Forschungsarbeiten die Vielfalt an digitalen Forschungsdaten, -fragen und -methoden sowie die damit verbundenen Potenziale und Herausforderungen näher zu bringen.

Ein Einblick in die Digitalisierungsforschung aus fünf Perspektiven

In der letzten Ausgabe easy 68 „Digitale Gesellschaft(en)“ haben wir uns bereits der Digitalisierungsforschung gewidmet und eine Auswahl an Querschnittsthemen aus der Vogelperspektive betrachtet. Unser Fokus spannte sich von einer initialen Begriffserklärung über die Identifizierung relevanter Forschungsfragen, Erläuterungen zur Qualität neuer Datentypen sowie der Potenziale und Herausforderungen bei der Verknüpfung verschiedener Datentypen bis zur Kommunikation von Ergebnissen der Digitalisierungsforschung in die Gesellschaft. Die einzelnen Beiträge haben dabei bewusst Themen aufgegriffen, die die Forschung eher von einer Metaperspektive betrachten und sind weniger auf einzelne, inhaltliche Forschungsarbeiten eingegangen.

Im Gegensatz dazu möchten wir in dieser Ausgabe inhaltliche Arbeiten in den Mittelpunkt stellen, die sich aus verschiedenen disziplinären, methodischen und inhaltlichen Perspektiven mit Fragen der Digitalisierungsforschung sowie der Nutzung digitaler Forschungsdaten auseinandersetzen. Dazu haben wir Forschende aus verschiedenen sozialwissenschaftlichen Bereichen eingeladen, uns einen Einblick in ihre Forschungsprojekte zu geben.

Im ersten Beitrag, „Digitale Methoden in der Politikwissenschaft – Auf dem Weg in virtuelle Welten?“, beschreibt *Isabelle Borucki* aus politikwissenschaftlicher Perspektive die Kategorisierung von analogen, digitalen und nativ-digitalen Daten und Methoden und erläutert, wie eine Integration von neuen Daten und Methoden in etablierte Forschungsprozesse erfolgreich sein kein. Der Beitrag unterstreicht vor allem, dass digitale Forschungsdaten und -methoden nicht in Konkurrenz zu etablierten Ansätzen stehen, sondern im Gegenteil große Kombinationspotenziale aufweisen.

Im zweiten Beitrag, „The Dark Web. A Brief Introduction“, nimmt *Felix Soldner* die Lesenden mit in das sogenannte Dark Web – also den Teil des Internets, der nur über Verschlüsselungs- und Anonymisierungsdienste wie z.B. das TOR-Netzwerk zugänglich ist. Wenngleich die Zugänglichkeit zu diesen Daten für Forschende erschwert ist, ermöglicht der Blick ins Dark Web Einsichten in Interaktionen und Prozesse, die sich Forschenden oftmals entziehen. Dazu gehören vor allem kriminelle Handlungen wie der Handel mit illegalen Waren und Dienstleistungen oder Fälschungen, aber auch Interaktionen von politischen Aktivist*innen in Ländern, in denen Zensur herrscht.

Im dritten Beitrag, „Jung, weiblich und extrem rechts. Die narrative Kommunikation weiblicher Akteurinnen auf der Plattform Instagram“, zeigt *Sandra Kero* auf, wie Daten der Plattform Instagram – insbesondere Bil-

der aus Instagram-Stories – genutzt werden können, um detaillierte Einblicke in die Kommunikationsstrategien rechter Accounts zu erhalten. Dabei betrachtet sie eine Gruppe, die bisher im öffentlichen Diskurs und der wissenschaftlichen Forschung kaum beachtet wird: Frauen, die rechte Inhalte erstellen und teilen. Methodisch verbindet sie digitale Daten der Plattform mit qualitativer Inhaltsanalyse und quantitativer Auswertung.

Im vierten Beitrag, „Periods in the Public Eye – Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications" von *Annika Deubel* und *Pauline Heger*, geht es im weitesten Sinne um „Sensoren" – allerdings nicht für die Erfassung von öffentlich verfügbaren Daten, sondern von persönlichen Gesundheitsinformationen. Konkret betrachten die Autor*innen basierend auf Daten einer Online-Befragung den Zusammenhang zwischen der Nutzung von Apps zur Erfassung des eigenen Menstruationszyklus und den Einstellungen der Nutzenden zum Datenschutzrisiko, welches diese Apps bei der Verarbeitung von sensiblen, gesundheitsbezogenen Daten mit sich bringen.

Im letzten Beitrag der Ausgabe, „Making Sense of the Big Data Mess. Why Interdisciplinarity Matters in Smart Cities", verlassen wir mit den Autor*innen *Niklas Frechen, Pauline Heger, Christoph Bieber* und *Mennatullah Hendawy* das Internet und erhalten einen Überblick über digitale Daten, die von Sensoren wie Stromzählern, Wetterstationen oder Ampelschaltungen im Alltag von Stadtbewohnenden erhoben werden. Die Autor*innen beschreiben mit kritischem Blick die Potenziale dieser vielfältigen Datentypen in sogenannten „Smart Cities" und wie diese durch interdisziplinäre Zusammenarbeit und öffentliche Zugänglichkeit zur politischen Entscheidungsfindung genutzt werden können.

Wir hoffen, mit diesen vielfältigen Beiträgen einen Einblick in die Themen und Methoden der Digitalisierungsforschung geben zu können, und ein Bewusstsein dafür zu schaffen, wie digitale Forschungsdaten über Fachdisziplinen hinweg die Erforschung sowohl neuer als auch etablierter Fragen ermöglichen, welche Herausforderungen sich dabei für die Forschenden ergeben, und wie mit diesen produktiv umgegangen werden kann. Wir können dabei natürlich nur einen kleinen Einblick in ein dynamisches, thematisch sowie methodisch breites und sehr heterogenes Forschungsfeld liefern, hoffen aber trotzdem, den Leser*innen dieser Ausgabe die Forschung zu und mit digitalen Daten ein Stück näher bringen zu können.

Referenzen

Aldera, S., Emam, A., Al-Qurishi, M., Alrubaian, M. & Alothaim, A. (2021). Online extremism detection in textual content: A systematic literature review. *IEEE Access, 9*, 42384–42396. https://doi.org/10.1109/ACCESS.2021.3064178

Amazon (2023, 30. Juni). Amazon.com Privacy Notice. Abgerufen am 10.07.2023, von https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

Borucki, I. (2023). Digitale Methoden in der Politikwissenschaft. Auf dem Weg in virtuelle Welten. *easy_social_sciences, 69*, 11–17. https://doi.org/10.15464/easy.2023.08

Chaudhry, I. (2015). #Hashtagging hate: Using Twitter to track racism online. *First Monday, 20*(2). https://doi.org/10.5210/fm.v20i2.5450

Deubel, A & Heger, P. (2023). Periods in the Public Eye. Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications. *easy_social_sciences, 69*, 37–44. https://doi.org/10.15464/easy.2023.11

eBay (2023, 24. März). eBay User Privacy Notice. Abgerufen am 10.07.2023, von https://www.ebayinc.com/company/privacy-center/privacy-notice/

Edelmann, A., Wolff, T., Montagne, D. & Bail, C. A. (2020). Computational social science and sociology. *Annual Review of Sociology, 46*, 61–81. https://doi.org/10.1146/annurev-soc-121919-054621

Faelens, L., Hoorelbeke, K., Soenens, B., Van Gaeveren, K., De Marez, L., De Raedt, R. & Koster, E. H. (2021). Social media use and well-being: A prospective experience-sampling study. *Computers in Human Behavior, 114*, 106510. https://doi.org/10.1016/j.chb.2020.106510

Fitbit (2023, 6. Juni). Fitbit Privacy Policy. Abgerufen am 10.07.2023, von https://www.fitbit.com/global/us/legal/privacy-policy#how-we-use-info

Frechen, N., Heger, P., Bieber C., & Hendawy, M. (2023). Making Sense of the Big Data Mess. Why Interdisciplinarity Matters in Smart Cities. *easy_social_sciences, 69*, 45–52. https://doi.org/10.15464/easy.2023.12

franzke, a. s., Bechmann, A., Zimmer, M., Ess, C. & Association of Internet Researchers (2020). Internet research: Ethical guidelines 3.0. https://aoir.org/reports/ethics3.pdf

Howison, J., Wiggins, A. & Crowston, K. (2011). Validity issues in the use of social network analysis with digital trace data. *Journal of the Association for Information Systems, 12*(12), 767–797. https://doi.org/10.17705/1jais.00282

Humby, C. & Palmer, M. (2006, 3. November). Data is the new oil. Abgerufen am 10.07.2023, von https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Keuschnigg, M., Lovsjö, N. & Hedström, P. (2018). Analytical sociology and computational social science. *Journal of Computational Social Science, 1*, 3–14. https://doi.org/10.1007/s42001-017-0006-5

Kero, S. (2023). Jung, weiblich und extrem rechts. Die narrative Kommunikation weiblicher Akteurinnen auf Instagram. *easy_social_sciences, 69*, 28–36. https://doi.org/10.15464/easy.2023.10

Kozitsin, I. V. (2022). Formal models of opinion formation and their application to real data: Evidence from online social networks. *The Journal of Mathematical Sociology, 46*(2), 120–147. https://doi.org/10.1080/0022250X.2020.1835894

Meta (2022, 11. Januar). Facebook Datenrichtlinie. Abgerufen am 10.07.2023, von https://www.facebook.com/about/privacy/update/printable

Microsoft (2023, April). Data collection summary for Windows. Abgerufen am 10.07.2023, von https://privacy.microsoft.com/en-us/data-collection-windows

Netflix (2022, 1. November). Netflix Privacy Statement. Abgerufen am 10.07.2023, von https://help.netflix.com/legal/privacy

Ross Arguedas, A., Robertson, C., Fletcher, R. & Nielsen, R. (2022). Echo chambers, filter bubbles, and polarisation: A literature review. Reuters Institute for the Study of Journalism.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature machine intelligence, 1*(5), 206–215. https://doi.org/10.1038/s42256-019-0048-x

Samory, M., Sen, I., Kohne, J., Flöck, F. & Wagner, C. (2021). "Call me sexist, but...": Revisiting sexism detection using psychological scales and adversarial samples. *Proceedings of the International AAAI Conference on Web and Social Media, 15*(1), 573–584. https://doi.org/10.1609/icwsm.v15i1.18085

Samsung (2023). Samsung Privacy Policy Overview. Abgerufen am 10.07.2023, von https://privacy.samsung.com/policy/overview

Santos, F. P., Lelkes, Y. & Levin, S. A. (2021). Link recommendation algorithms and dynamics of polarization in online social networks. *Proceedings of the National Academy of Sciences, 118*(50), e2102141118. https://doi.org/10.1073/pnas.2102141118

Schmitt, J. B., Kohne, J. & Breuer, J. (2023). Digitalisierungsforschung. Wie wir die digitale Transformation wissenschaftlich erfassen können. *easy_social_sciences, 68*, 4–11. https://doi.org/10.15464/easy.2023.01

Soldner, F. (2023). The Dark Web. A Brief Introduction. *easy_social_sciences, 69*, 18–27. https://doi.org/10.15464/easy.2023.09

Sonderegger, P. (2021, 4. März). Data hits peak metaphor. Abgerufen am 10.07.2023, von https://paulsonderegger.com/2021/03/04/data-hits-peak-metaphor/

Spotify (2023, 22. Februar). Datenschutzrichtlinie von Spotify. Abgerufen am 10.07.2023, von https://www.spotify.com/de/legal/privacy-policy/

Stier, S., Breuer, J., Siegers, P. & Thorson, K. (2020a). Integrating survey data and digital trace data: Key issues in developing an emerging field. *Social Science Computer Review, 38*(5), 503–516. https://doi.org/10.1177/0894439319843669

Stier, S., Kirkizh, N., Froio, C. & Schroeder, R. (2020b). Populist attitudes and selective exposure to online news: A cross-country analysis combining web tracking and surveys. *The International Journal of Press/Politics, 25*(3), 426–446. https://doi.org/10.1177/1940161220907018

Varian, H. R. (2014). Beyond big data. *Business Economics, 49*(1), 27–31. https://doi.org/ 10.1057/be.2014.1

Vega, L., Mendez-Vazquez, A. & López-Cuevas, A. (2021). Probabilistic reasoning system for social influence analysis in online social networks. *Social Network Analysis and Mining, 11*(1). https://doi.org/10.1007/s13278-020-00705-z

Wagner, C., Strohmaier, M., Olteanu, A., Kıcıman, E., Contractor, N. & Eliassi-Rad, T. (2021). Measuring algorithmically infused societies. *Nature, 595*, 197–204. https://doi.org/10.1038/s41586-021-03666-1

Wilke, R., Knoblauch, H., Kohne, J., Miller, B., Strohmaier, M., Wagner, C., Wolf, C., Hanekop, H., Heuer, J-O, Hollstein, B. & Mozygemba, K. (2021). Symposion Forschungsdateninfrastruktur. *Soziologie, 50*(4), 430–472.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of information technology, 30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Julian Kohne
GESIS – Leibniz-Institut für Sozialwissenschaften

E-Mail julian.kohne@gesis.org

Julian Kohne ist wissenschaftlicher Mitarbeiter bei GESIS, Köln und Doktorand der Psychologie an der Universität Ulm. Bei GESIS arbeitet er an der Entwicklung zugänglicher Smartphone-Datenerfassungsinfrastrukturen für Sozialwissenschaftler*innen. In seinem Promotionsprojekt entwickelt er transparente Methoden zur Datenspende für WhatsApp-Chatprotokolle und untersucht, wie unterschiedliche soziale Beziehungen in Online-Kommunikationsmustern ausgedrückt werden. Sein übergreifendes Forschungsinteresse gilt der Nutzung digitaler Verhaltensdaten, insbesondere der Text- und Netzwerkdaten, um sozialwissenschaftlicher Forschungsfragen zu bearbeiten.
https://www.juliankohne.com

Josephine B. Schmitt
Center for Advanced Internet Studies (CAIS)

E-Mail Josephine.Schmitt@cais-research.de

Josephine B. Schmitt ist wissenschaftliche Koordinatorin am Center for Advanced Internet Studies (CAIS). Dort befasst sie sich u.a. mit der Erforschung und Entwicklung von innovativen Konzepten für die interdisziplinäre Zusammenarbeit in der Digitalisierungsforschung. Sie forscht weiterhin zu Inhalt, Verbreitung und Wirkung von Hate Speech, extremistischer Propaganda und (politischen) Informations- und Bildungsangeboten im Internet.
https://orcid.org/0000-0002-4689-3049

Johannes Breuer
GESIS Leibniz-Institut für Sozialwissenschaften &
Center for Advanced Internet Studies (CAIS)

E-Mail johannes.breuer@gesis.org

Johannes Breuer ist Senior Researcher im Team Digital Society Observatory bei GESIS, Köln und Leiter des Teams Research Data & Methods am Center for Advanced Internet Studies (CAIS). Seine Forschungsinteressen sind die Nutzung und Wirkung digitaler Medien, Computational Methods, digitale Spurdaten, Datenmanagement und Open Science.
https://www.johannesbreuer.com

doi: 10.15464/easy.2023.08

Digitale Methoden in der Politikwissenschaft

Auf dem Weg in virtuelle Welten?

Isabelle Borucki

Big Data, digitale Methoden und Computational Social Science sind Begriffe, die in einem großen gemeinsamen Feld aus Politikwissenschaft, Soziologie und anderen Sozialwissenschaften, Kulturwissenschaften und Informatik miteinander verschmelzen. Um geeignete Methoden und Werkzeuge für die zunehmend größer werdenden Datenmengen zu finden, ist eine angemessene Kategorisierung und Systematik für diese Bereiche notwendig. Der Zugang hierzu wird in diesem Artikel über eine Beschreibung der verschiedenen Daten und der zu deren Erhebung und Verarbeitung geeigneten Methoden geliefert. Abschließend präsentiert dieser Beitrag Gedanken zu weiteren Implikationen für gesamtgesellschaftliche Zusammenhänge.

Big Data, digital methods and computational social science are terms that merge in a large interdisciplinary field of political science, sociology and other social sciences, cultural studies, and computer science. To find appropriate methods and tools for the increasingly large amounts of data, appropriate categorization and systematics for these fields is necessary. This article provides a description of the different data and the methods suitable for their collection and processing. Finally, this article discusses further implications for the overall societal context.

Keywords: Digitale Methoden, Computational Social Science, Big Data, Digital Literacy, Digitalkompetenz, Politikwissenschaft

Was sind digitale Methoden und wozu brauchen wir sie?

Digitale Methoden (etwa computerunterstützte oder automatisierte Analyseverfahren) können verstanden werden als das im Digitalen und mit digitalen Quellen arbeitende systematische Vorgehen zur Generierung von Erkenntnissen. In der Politikwissenschaft basieren diese vor allem auf Onlinedaten – Daten also, die im Internet anfallen und zudem oft auch nicht dezidiert für Forschungszwecke generiert wurden (daher werden diese Daten häufig auch als „found data“ bezeichnet). Es können allerdings auch von Forschenden geplant generierte Daten (sogenannte „designed data“) wie etwa Simulationen oder (Online-)Experimente weitere Datenquellen aus dem digitalen Repertoire sein. Es handelt sich also um geplant generierte oder protokollierte versus generische oder hinterlassene Daten, die entweder „gefunden“ (found data: z.B. öffentlich verfügbare Social-Media-Posts) oder geplant mittels eigener Erhebungsverfahren generiert werden (designed data: z.B. Webtracking-,

Smartphone-Studien). All diese können in den Bereich der digitalen Methoden fallen.

Wirkt sich die ‚Messiness' auf die Genauigkeit bzw. Güte der darauf basierenden Auswertungen aus?

Generische, gefundene Daten stehen oftmals in der Kritik: Sie seien aufgrund ihrer wenig organisierten Datenstruktur scheinbar unvollständig und zusätzlich „messy", weil sie nicht in einer üblichen Tabellenstruktur geliefert werden und daher ungeordnet bzw. unstrukturiert sind (Salganik, 2018). Eine Frage ist, ob und wie sich diese „Messiness" auf die Genauigkeit bzw. Güte der darauf basierenden Auswertungen auswirken kann. Wir differenzieren demnach zwischen I) analogen Daten (z.B. Umfragedaten), II) digital migrierten Daten (solche also, die wir erst digitalisieren müssen, wie z.B. handschriftliche Feldnotizen) sowie III) digital-nativen Daten (etwa Social-Media-Daten).

Dem Unterschied zwischen den verschiedenen Datenursprüngen und wie Daten genutzt werden, wollen wir im Folgenden nachspüren und dabei aufzeigen, welche Möglichkeiten, aber auch Grenzen digitale Methoden in der Politikwissenschaft mit sich bringen. Das trifft insbesondere auf Datensätze zu, die eine Möglichkeit zur Verknüpfung mit anderen Datensätzen über eindeutig identifizierbare Kennungen oder IDs ermöglichen. Beispiele für solche Verknüpfungen können etwa die Zusammenführung von Daten zur Verbreitung von Themen im Parlament und in Parlamentsdebatten mit Wahlumfragen und anderen Umfragedaten sein. Doch zunächst soll nachfolgend genauer erklärt werden, was digitale Methoden eigentlich sind und woher sie kommen.

Ihren Ursprung haben digitale Methoden im sogenannten „Computational Turn" (Alvarez, 2016; Berry, 2011; Blätte et al., 2018). Dieser war insbesondere in den „Digital Humanities", den digitalen Kultur- und Geisteswissenschaften, und hier speziell der Arbeit mit und an Texten mit Hilfe von Computern wegweisend für die Erschließung und Bearbeitung von Quellen zur späteren Analyse (Schanze, 1972). In den Kulturwissenschaften werden etwa historische Handschriften digitalisiert und dann mit Hilfe von Computerprogrammen analysiert, um beispielsweise Vernetzungen zwischen Urkunden oder Briefen herauszuarbeiten. Dieser Turn der 1970er Jahre liegt aus Sicht der digitalen Kultur- und Geisteswissenschaften lange zurück. Früh stand die Frage im Zentrum, wie handschriftliche Dokumente und Daten digitalisiert und für die Nachwelt in einer gut nutzbaren Fassung für Analysen konserviert werden können. Für die Politik- und Sozialwissenschaften ist dieser Turn mittlerweile ebenso aktuell wie für die Kulturwissenschaften, allerdings geht es heutzutage vornehmlich um die Erhebung, Aufbereitung und Analyse von Daten, die originär digital entstehen, wie z.B. große Textmengen aus sozialen Netzwerken.

Um die Nutzung digitaler Methoden (etwa automatisierte Textanalysen, soziale Netzwerkanalysen) für die Sozialwissenschaften grundlegend einzuführen und zu beleuchten, ist zunächst die Bedeutung der Begrifflichkeit klarzumachen. Digitale Methoden kennzeichnen sich durch die Nutzung eines Mediums im Digitalen (etwa eine browsergestützte Anwendung zum Verfassen von Texten). Ziel der digitalen Methoden ist es, digitale Objekte (wie z.B. Social-Media-Daten oder Webseiten) für die sozialwissenschaftliche Forschung generell nutzbar zu machen. Gleichzeitig soll dabei eine Erschließung im Digitalen (also z.B. eine im Browser bereitgestellte grafische Benutzeroberfläche für Endnutzende), gewährleistet sein (Rogers, 2021), d.h. die Daten sollen für Forschungszwecke in einem Format vorliegen, welches von Computern gelesen und verarbeitet und von Forschenden an digitalen Geräten genutzt werden kann. Insofern grenzen sich digitale Methoden durch diese Nutzung von klassischen analogen Methoden ab. Ziel der Verlagerung von Erschließungs- und Analyseinstrumenten ins Internet, ist eine möglichst

anwendungsorientierte Umgebung. Diese soll es erlauben, ohne viel Vorwissen Daten zu erkunden (bspw. die grafischen Interaktionsmöglichkeiten mit den V-Dem-Datensätzen oder interaktive *Social-Media-Monitoring Boards*). In einer solchen Virtualisierung wird ohne die Notwendigkeit von Kenntnissen in Programmiersprachen mit digitalen Methoden an digitalen Daten operiert.

Mittels digitaler Methoden können und sollen andere Methoden und Formen der Datenerhebung und -analyse angepasst und integriert werden. Bei der Arbeit mit digitalen Textdaten können beispielsweise sowohl quantitative (z.B. Analysen von Worthäufigkeiten) aber auch qualitative Ansätze (Inhaltsanalyse, Annotation nach festgelegten Kriterien) von digitalen Ansätzen profitieren. Digitale Methoden können somit durch die Kombination verschiedener methodischer Ansätze eine ganzheitliche Herangehensweise im Rahmen sozialwissenschaftlicher Analyse bieten.

Digitale Daten und Methoden: Eine Annäherung

Die Grundlage jeglicher empirischen Methodik sind Daten (etwa Texte, Zahlen, Bilder, Videos). Demnach können in diesem Sinne alle betrachteten Untersuchungseinheiten als Daten angesehen werden. Zur genaueren Kategorisierung und Systematisierung der verschiedenen Datenarten und korrespondierender Analysewege soll die folgende Unterscheidung dienen, die nach Ursprung und Art der Daten unterscheidet. Dabei soll jedoch nicht aus dem Blick geraten, dass es gerade ein Vorteil digitaler Methoden ist, dass diese sowohl auf digitalen Daten wie auf analog erstellten Texten anwendbar sind.

Zunächst eine grundlegende *Differenzierung* in verschiedene Kategorien (vgl. Rogers, 2014): Die sogenannten nativ-digitalen Daten (Daten aus dem Digitalen, wie etwa Social-Media-Daten), digitalisierte Daten (z.B. transkribierte Interviewmitschnitte, die als Textdaten vorliegen) und die damit verbundenen genuinen Methoden sowie migrierte, also angepasste Methoden, sollen im Folgenden näher betrachtet werden; und zwar spezifisch unter dem Gesichtspunkt, eine Verbindung zu klassischen Methoden (wie etwa der Umfrageforschung und Statistik) und Herangehensweisen aufzuzeigen.

Die Frage, in welchem Format welche Art von Daten zugänglich sind oder zugänglich gemacht werden, stellt eine zentrale Herausforderung in diesem Gebiet dar: Denn Daten werden entweder strukturiert (in klar definierten Formaten wie z.B. eine Datei mit Reihen und Spalten und einem Wert pro Zeile wie in Excel) oder unstrukturiert (zum Beispiel eine Sammlung von PDF-Dateien mit ganz unterschiedlichem Layout) auf Datenträgern unterschiedlicher Art gespeichert. Die Unterscheidung in strukturiert/unstrukturiert sagt jedoch noch nichts über die Zugänglichkeit dieser Daten aus. Metadatenschemata, Übersichten darüber, welche Informationen ein Datensatz enthält, erleichtern auch den Zugang zu zunächst unstrukturierten Daten, wie Social-Media-Daten (Stier et al., 2018).

Digitale Daten von Nutzenden werden aber nicht nur für Forschungszwecke verwendet, sondern auch zwischen Plattformbetreibenden und Werbetreibenden ausgetauscht und somit an andere Akteur*innen weitergegeben. Problematisch wird dies, wenn dadurch rechtlicher Regelungsbedarf entsteht, der die Nachvollziehbarkeit einer Datennutzung und -verwertung erschwert.

Analog erhobene Daten unterliegen der direkten Kontrolle der Forschenden, bei den meisten digitalen Daten ist das jedoch nicht der Fall. Äquivalent zur obigen Differenz der Daten, lassen sich auch Methoden unterscheiden in i) digitalisierte bzw. migrierte Methoden und ii) nativ-digitale Methoden. Diese Unterscheidung ist stark von den Daten her gedacht, reduziert auf found data und nicht von den methodologischen Ursprüngen abgeleitet (siehe Tabelle 1; vgl. Borucki, 2022).

Die in Tabelle 1 aufgeführten Daten und Methoden können unterschiedliche Ausprä-

Tabelle 1 Übersicht der verschiedenen Daten und Methoden. Eigene Darstellung orientiert an Rogers, 2014

		Methoden		
		i) klassische Methoden	ii) digitalisierte Methoden	iii) nativ-digitale Methoden
Daten	I) analoge Daten	Umfragen, Expert*innen-interviews, Experimente	Digitale Analyse von analog erhobenen Expert:inneninterviews, Surveys	
	II) digitalisierte Daten	Online-Surveys, Video-Interviews, Online-Beobachtung und -Aufzeichnung von Onlineevents, Experimente, Textanalyse		Künstliche Intelligenz und Machine Learning/Natural Language Processing, Textanalyse
	III) nativ-digitale Daten	Soziale Netzwerkanalyse, Bibliometrie, Altmetrics, Social-Media-Kommentare/Posts, Textkorpusanalysen		Digitale Spurendaten, Social-Media-Textkorpusdaten

gungen annehmen: Eine Textanalyse kann digitalisiert durchgeführt werden, es können z.B. meistgeteilte Inhalte oder meistgeteilte URLs in Twitter-Tweets analysiert werden. In diesem Fall handelt es sich um eine *nativ-digitale Methode*. Befragungen über Facebook-Nutzung und Wahrnehmung von Desinformation sind als *klassische Methode* anzusehen, wohingegen beispielsweise die computergestützte und maschinell automatisierte Big-Data-Analyse von Posts und Kommentaren hinsichtlich der Verbreitung von Desinformation *nativ-digital* ist. Die interpretative Praxisforschung des Kommunikationsverhaltens (also die Auswertung von Handlungen und Äußerungen mittels qualitativer Methoden) stellt eine *digitalisierte, klassische* Herangehensweise dar. Interviews mit Akteur*innen aus dem politischen Bereich zur Problematisierung jeweiliger strategischer oder inhaltlicher Fragestellungen können als *klassisch* angesehen werden.

Darüber hinaus sind weitere Datenarten in die Betrachtung mit einzubeziehen: *Digitale Spurendaten* sind protokollierte und hinterlassene Daten, die eher etwas über das Nutzungsverhalten der Nutzenden aussagen als über Kommunikationsinhalte. Ebenso können diese Daten mit *Umfragedaten* verknüpft werden und über digitalisierte oder digital-native Korpora erschlossene große Textdaten analysiert werden. Hier kann ein Anknüpfungspunkt zu Cultural Data und Digital Humanities gesehen werden, wo bereits seit langem auf derlei Methoden zurückgegriffen wird (vgl. Stier et al., 2020).

Abgesehen von diesen Fragen, kann man mit digitalen Daten und orientiert an digitalen Methoden ähnlich arbeiten wie mit analogen Daten, weshalb diese hier nicht gesondert aufgeführt sind.

Digitale Spurendaten bilden also, je nach Verständnis, den nativ-digitalen Bereich. Denn diese Daten fallen nur digital an und können insofern mit entsprechenden Methoden des maschinellen Lernens oder automatisierten Analysen erschlossen werden (Breuer et al., 2020).

Digitale Analysemethoden

Die schier unglaubliche Menge von Big Data macht es, im Gegensatz zu kleineren Mengen digitaler Daten, unmöglich, allein mit menschlicher Analyse- und Codierarbeit

Texte und andere Datentypen zu bearbeiten. Hierzu sind sogenannte Machine-Learning-Algorithmen (Programme also, die in der Lage sind, nach Mustern in den Daten zu suchen) notwendig. Zudem kann es für die sozialwissenschaftliche Forschung hilfreich sein, Daten aus dem Bereich Big Data mit anderen (klassischen) Datentypen zu kombinieren. So werden digitale Spurendaten zusehends auch als zusätzliche Informationsquelle in der Umfrageforschung genutzt (Stier et al., 2020).

> ***Wir brauchen eine Debatte darüber, was digitale Methoden leisten können – und was nicht.***

Nach Rogers (2021) geht es bei der Entwicklung und Nutzung von digitalen Methoden v.a. darum, digitale Objekte für eine sozialwissenschaftliche Perspektive nutzbar zu machen, allerdings nicht ohne zu hinterfragen, wie digitale Methoden online „verankert" werden können (S. 26) – welchen Ort sie also finden sollen, bzw. wo mit digitalen Methoden operiert wird. Insofern ist die oben vorgenommene Unterscheidung in found data und generierte Daten (designed data) zielführend. Grundlegender Unterscheidungspunkt ist die Frage nach der Nativität – der ursprünglichen Herkunft – von Daten und Methoden: „Insgesamt geht es bei digitalen Methoden also darum, Online-Objekte und -Methoden zu rekombinieren und nutzbar zu machen" (Rogers, 2021, S. 43).

Die Frage nach der Verankerung digitaler Methoden zeigt auch die wesentliche Unterscheidung zur Datenwissenschaft (Data Science) und Datenverarbeitung auf: Hier kann zwischen generierten, also produzierten und protokollierten (etwa Social-Media-Interaktionen oder Kommunikation über Apps) versus generischen, natürlich vorkommenden oder hinterlassenen Daten (etwa Nutzungsdaten von Apps wie die Häufigkeit, Tageszeit und Ort der Nutzung) unterschieden werden. Eng mit methodischen Fragen verbunden sind Fragen zu Datenzugriff und -nutzung: Welche unterschiedlichen Anforderungen ergeben sich an eine Analyse generierter oder found data in Bezug auf die Datenherkunft als willkürlich anfallende Daten oder bewusst produzierte, generierte Daten? Dies führt zum Ausgangspunkt der Überlegungen im Hinblick auf den Stellenwert digitaler Methoden als eigener Zugang aber auch als Querschnittsbereich zwischen verschiedenen methodischen Zugängen. Quer liegen digitale Methoden insofern zu anderen Methoden, als sie eine vermittelnde Instanz einnehmen und beispielsweise die Verknüpfung der genannten Datenarten erst ermöglichen. Querschnittscharakter erhalten digitale Methoden aber auch durch mögliche Verknüpfung der eben genannten gefundenen und generierten Daten.

Weiterentwicklung sozialwissenschaftlicher Methoden

Was wir letztlich brauchen, ist eine umfassende Debatte darüber, was digitale Methoden leisten können – und was nicht. Ein wichtiger Aspekt in diesem Zusammenhang ist die Frage nach der Nachnutzung von eigentlich privaten und/oder persönlichen Daten, beispielweise aus Interviews mit Expert*innen oder Zeitzeug*innen, die entsprechend zunächst pseudonymisiert oder anonymisiert werden müssen, insbesondere wenn das Einverständnis zur Veröffentlichung und Nachnutzung durch die Datengebenden nicht eingeholt werden kann. Im Big-Data-Kontext ist dies oftmals nicht gegeben bzw. eine Nachnutzung nur unter der Einschränkung einer Pseudonymisierung oder Anonymisierung überhaupt möglich. Hier kollidieren zudem oftmals die stark einschränkenden Richtlinien der Plattformbetreibenden mit der Anforderung an Transparenz, Nachvollziehbarkeit und Nachnutzbarkeit von Forschung und Daten im Sinne von Open Science durch diese Plattformen. Dieses Spannungsverhältnis birgt für Forschende in diesem Bereich die Gefahr, zwi-

schen diesen beiden Polen insofern zerrieben zu werden, als dass gerade Forschende vor der Herausforderung stehen, sowohl Daten für ihre Forschung erheben und bestenfalls auch zur Nachnutzung bereitstellen zu wollen und gleichzeitig Datenschutzanforderungen und Vorgaben durch die Plattformen zu berücksichtigen (speziell für personenbezogene Daten).

Mit diesen grundlegenden Fragen verbunden ist auch ein Umdenken im Hinblick auf die Methodenausbildung im Fach Politikwissenschaft sowie anderen Fachbereichen. Wichtig ist in diesem Kontext, mittels entsprechender Anreizstrukturen Digital Data Literacy, d.h. den informierten Umgang mit digitalen Daten und entsprechende Kompetenzen, sowohl in Forschungskontexten als auch der Allgemeinbevölkerung zu vermitteln bzw. zu fördern. Data Literacy, oder eben Daten- und Digitalkompetenz ist als eine Kombination aus logischen, statistischen und technischen Fähigkeiten zu verstehen. Anreizstrukturen sowohl für Forschende als auch interessierte Bürger*innen können etwa über kleinere Laborformate (z.B. zum Einüben von Arbeit mit Daten bzw. des Interpretierens von Daten) oder Interaktions- und Diskussionsforen zielgruppengenau gestaltet werden. Folgerichtig argumentieren Gray et al. (2018) für eine Erweiterung des Konzepts der Digitalkompetenz zu einer Datenkompetenz, welche im Konzept der Digital Data Literacy aufgehen. Dies ist wichtig um deutlich zu machen, dass nur auf Grundlage solcher Kompetenzen digitale Daten sinnvoll genutzt und analysiert werden können. Datenkompetenz beinhaltet, im erweiterten soziotechnischen Kontext einordnen und erklären zu können, was warum mit welchen Daten erklärt werden kann. Ein Verständnis davon, wie mit welchen Daten gearbeitet wird und woher diese stammen, kann die Sensibilität für Probleme bzw. Leerstellen dieser Daten und der Notwendigkeit eines bewussten Umgangs auch mit den eigenen Daten schärfen.

Digitale Daten und Methoden: Perspektiven

In der Summe diente dieser Beitrag als Einführung in die vielschichtigen Dimensionen, diversen Kategorien und unterschiedlichen Formate digitaler Daten, sowie in Methoden zu deren systematischer Erschließung. Dabei stand grundlegend die Frage im Vordergrund, was sich durch die Digitalisierung in methodischer Sicht ändert und was konstant bleibt bzw. lediglich neu interpretiert werden muss. Zentral ist an dieser Stelle hervorzuheben, dass digitale Methoden zwar quer zu anderen Methoden liegen und somit für die Forschung ein immenses Kombinationspotenzial aufweisen, sich aber teilweise mit anderen Methoden decken. Die Herkunft der jeweiligen Daten macht hier einen Unterschied, was die Analyse und Methoden, die zur Anwendung gelangen angeht. Fest steht, dass sich durch die neuerliche Skalierbarkeit in großen Datenmengen, die verbesserte (oder stark eingeschränkte) Zugänglichkeit zu Daten auch die Art und Weise der Arbeit mit Daten verändert hat. Insofern hat die Erweiterung des Arbeitsspektrums und Werkzeugkastens der sozialwissenschaftlichen digitalen Methoden gerade erst begonnen.

Literatur

Alvarez, R. M. (2016). *Computational Social Science*. Cambridge University Press.

Berry, D. M. (2011). *The Computational Turn: Thinking About the Digital Humanities*.

Blätte, A., Behnke, J., Schnapp, K.-U., & Wagemann, C. (Eds.). (2018). *Computational Social Science: Die Analyse von Big Data*. Nomos. https://doi.org/10.5771/9783845286556

Borucki, I. (2022). Methoden in der Regierungsforschung. In K.-R. Korte & M. Florack (Hg.), *Handbuch Regierungsforschung* (S. 37–53). Springer VS. https://doi.org/10.1007/978-3-658-30071-5_3.

Breuer, J., Bishop, L. & Kinder-Kurlanda, K. (2020). The practical and ethical challenges in acquiring and sharing digital trace data: Negotiating public-private partnerships. *New Media & Society, 22*(11), 2058–2080. https://doi.org/10.1177/1461444820924622.

Gray, J., Gerlitz, C. & Bounegru, L. (2018). Data infrastructure literacy. *Big Data & Society, 5*(2). https://doi.org/10.1177/2053951718786316

Rogers, R. (2015). Digital Methods for Web Research. In R. Scott & S. Kosslyn (Eds.), *Emerging trends in the social and behavioral sciences* (pp. 1–22). Wiley.

Rogers, R. (2021). Digitale Methoden: Zur Positionierung eines Ansatzes. *M&K Medien & Kommunikationswissenschaft, 69*(1), 25–45. https://doi.org/10.5771/1615-634X-2021-1-25.

Salganik, M. (2018). *Bit by Bit: Social research in the digital age.* Princeton University Press. https://press.princeton.edu/books/paperback/9780691196107/bit-by-bit.

Schanze, H. (1972) Literatur und Datenverarbeitung. Bericht über die Tagung im Rahmen der 100-Jahr-Feier der Rheinisch-Westfälischen Technischen Hochschule Aachen. Max Niemeyer.

Stier, S., Bleier, A., Bonart, M., Mörsheim, F., Bohlouli, M., Nizhegorodov, M., Posch, L., Maier, J., Rothmund, T. & Staab, S. (2018). Systematically monitoring social media: The case of the German federal election 2017. *GESIS Papers, 2018*(4). GESIS – Leibniz-Institut für Sozialwissenschaften. https://www.ssoar.info/ssoar/bitstream/handle/document/56149/ssoar-2018-Stier_etal-Systematically_Monitoring_Social_Media.pdf.

Stier, S., Breuer, J., Siegers, P. & Thorson, K. (2020). Integrating survey data and digital trace data: Key issues in developing an emerging field. *Social Science Computer Review, 38*(5), 503–516. https://doi.org/10.1177/0894439319843669.

Isabelle Borucki

Philipps-Universität Marburg

E-Mail isabelle.borucki@uni-marburg.de

Isabelle Borucki ist Professorin für politikwissenschaftliche Methoden und Demokratie im digitalen Wandel am Institut für Politikwissenschaft der Philipps-Universität Marburg. Sie leitete ein Forschungsprojekt zum digitalen Wandel von Parteien und arbeitet wesentlich zu Fragen der demokratischen Qualität im Digitalen, zu Partizipationsmustern und Beteiligung in der digitalen Demokratie.

doi: 10.15464/easy.2023.09

The Dark Web

A Brief Introduction

Felix Soldner

The dark web is a highly anonymized section of the Internet in which some users share sensitive and illicit content. Users on the dark web generate digital traces, allowing researchers to study previously difficult-to-observe phenomena, such as trading illegal products or services. Trading occurs on darknet markets, platforms that provide the infrastructure for vendors and buyers to convene, similar to surface web platforms, such as eBay. Listings on such markets predominantly include drugs but also fraud items, counterfeits, or cybercrime-related services, such as hacking. Studying the dark web can be challenging due to technical and ethical considerations. This article introduces the dark web and Tor, the most prominent used dark web network. The article continues with a brief overview of how users engage with the dark web and darknet markets and discusses past research as well as possible future avenues for further research.

*Das Dark Web ist ein stark anonymisierter Teil des Internets, in dem einige Nutzer*innen sensible und illegale Inhalte teilen. Sie hinterlassen dabei digitale Spuren, die es Forscher*innen ermöglichen, zuvor schwer zu beobachtende Phänomene zu untersuchen, wie zum Beispiel das Handeln mit illegalen Produkten oder Dienstleistungen. Solcher Handel findet auf Darknet-Märkten statt, Plattformen, die ähnlich wie etwa eBay eine Infrastruktur für Käufer*innen und Verkäufer*innen bereitstellen. Die Angebote auf solchen Märkten umfassen überwiegend Drogen, beinhalten aber auch Fälschungen, Betrugsanleitungen oder kriminelle Dienstleistungen wie Hacking Attacken. Allerdings wird die wissenschaftliche Erforschung des Dark Webs oft durch technische und ethische Hürden erschwert. Dieser Artikel stellt das Dark Web vor und erläutert die Funktionsweise von Tor, dem am häufigsten genutzte Dark-Web-Netzwerk. Darüber hinaus wird erklärt, wie Darknet-Märkte operieren und wie diese genutzt werden. Abschließend werden mögliche Forschungsrichtungen, sowie rechtlich und ethische Probleme diskutiert.*

Keywords: darknet markets, crypto markets, tor network

The dark web is often imagined as an outlandish section of the Internet and mentioned in the context of illegal activity, such as drug trading, hacking, or contract killings. Since the dark web anonymizes user activity on the Internet, it is also called an anonymous network, which is used for illicit trading and enables users to overcome governmental censorship and communicate more securely. Thus, investigating such anonymized networks is worthwhile for a broad range of researchers that are not only interested in crime-related behavior (e.g., drug usage, fraud, hacking) but also in wider societal phenomena, such as extremism, political attitudes, organized movements (e.g., protests), whistleblowing, or conspiratorial beliefs.

After providing a basic understanding of

the dark web, followed by explanations of darknet markets (platforms used to trade goods and services), I will illustrate how such markets operate, and how users interact with them.

> ***The deep web is considered the largest and fastest-growing part of the Internet.***

What is the Dark Web?

The *dark web* describes a section of the Internet in which the communication between computers differs from the Internet we use daily. The "everyday" Internet with which we primarily interact is also called the surface web (see Figure 1) and includes websites, such as news sites or shopping platforms, that are accessible with traditional browsers (e.g., Chrome, Firefox) and are indexed by search engines (e.g., Google, Bing, DuckDuckGo). In contrast, online content that is protected through barriers, hidden from the public, and not indexed by search engines is considered part of the so-called deep web (Figure 1). The deep web includes personal cloud storage (e.g., Dropbox, OneDrive), paywalled content (e.g., streaming services), or databases. Communications between computers on the surface and deep web are identifiable through their Internet Protocol (IP) address and unique *cookie* settings[1]. In most cases, communication between computers is recorded and stored, making our online behavior visible to others, often resulting in tracking and targeted actions, such as personalized advertisements.

The *dark web* can be regarded as a small sub-part of the *deep web* (Figure 1), on which the communication between computers is anonymized, thus, also called an anonymized network (Gehl, 2018; Ghosh et al., 2017; Mansfield-Devine, 2009). The Tor network is the most known access point to such a *network*, but other technologies can also facilitate anonymity, such as the *Invisibility Internet Project (I2P)* or *Freenet* (Gehl, 2018). These technologies provide anonymity by sending the computers' encrypted communication through a network that conceals the true IP address. The Tor, I2P, or Freenet networks can be accessed through standard web browser technology. (The Tor client is built onto Firefox and can be downloaded *here*.) Accessing websites on such networks requires exact addresses since the software facilitating the creation of the network prevents classical search engines from finding and indexing websites on the network. However, lists of websites exist and are published on forums or websites, such as *reddit.com*, *thehiddenwiki.org*, or *dark.fail*.

Making size comparisons between the different parts of the Internet is difficult due to the unindexed content of the anonymized networks. Currently (January 16th, 2023), the surface web seems to contain over 1,1 billion websites (Netcraft, 2023), while only 18% of them contain and load content (Huss, 2022). Thus, most websites seem to be inactive or unused. Estimations about the number of dark web sites on the Tor network vary considerably but are thought to be much lower than on the surface web. While past investigations found

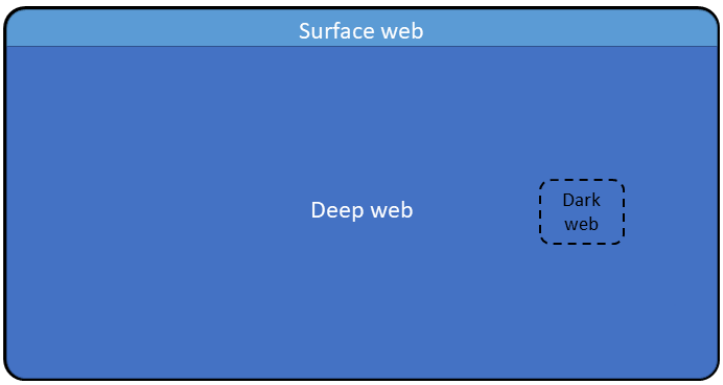


Figure 1 The Internet can be subdivided into the surface, deep, and dark web. The proportions of each part are rough approximations for illustration purposes; figure from (Soldner et al., 2022).

1 Saved websites & user settings.

around 32,000 sites on the Tor network, fewer than half of those seem active (Ghosh et al., 2017; Gray, 2019; Lewis, 2017). By contrast, the deep web is considered the largest and fastest-growing part of the Internet, with some estimating it to contain 400-500 times more data (i.e., stored information) than the surface web (Bergman, 2001; He et al., 2007).

The Tor Network

Tor (**T**he **O**nion **R**outing) uses *onion routing* to protect the user's privacy and was created by the US Naval Research Laboratory in the mid-1990s (Syverson, 2005; The Tor Project, Inc., 2020). Onion routing entails encrypting and relaying messages from the client (i.e., user) to a server, thereby anonymizing the user's internet activity. Tor uses three random relays that forward the messages from the client to the server (Figure 2).

Each relay provides an encryption layer that will either decrypt (when the client sends a message to the server) or encrypt (when the server sends a message to the client) the message with its encryption key (K). Multiple encryption keys are held by the client (who can decrypt and encrypt all messages) and by the individual relays. For example, the message is encrypted multiple times when the client wants to visit a website (i.e., sending a message to a server) through the Tor network. The first relay can decrypt the first layer of encryption, the second relay the second, and so forth. Thus, like layers in an onion, the relays decrypt each layer with a decryption key, hence the term "onion routing". Similarly, messages can be encrypted multiple times when sent from the server to the client, which can then decrypt all layers.

Since Tor relies on a decentralized network, more computers using the software create more *relays* (also called *nodes*) through which the network traffic is sent. A more extensive network facilitates a more secure space since more relays can be utilized, making tracking more difficult. To expand the decentralized network, Tor was released to the public in 2002 (Syverson, 2005; The Tor Project, Inc., 2020). The Tor project became a nonprofit organization in 2006. From 2007 onwards, changes were implemented to allow users to access the open web, circumventing censorship, for which the Tor browser is often used today. Those implementations can overcome local internet restrictions for specific countries (e.g., Russia, China). However, visiting surface websites with Tor is less anonymous than visiting sites within the Tor network, which is why some US governmental agencies (e.g., CIA, FBI), as well as other organizations (e.g., BBC, The New York Times, Facebook), also operate websites on the Tor network. Websites on the Tor network are also called "onion sites", and their administrative markers or country codes, such as ".de" or ".com", are replaced by the top-level domain ".onion".

Due to the anonymous and secure communication provided by Tor, the network is valuable for individuals who want to share sensitive information and want to protect their identity (e.g., journalists, whistleblowers). Similarly,

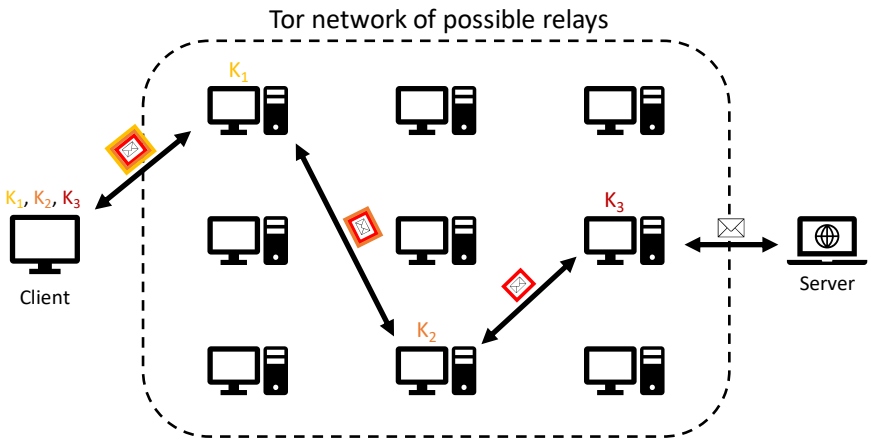


Figure 2 Visualization of how messages are sent from a client to a server through the Tor network; adapted from The Tor Project, Inc. (2020).

individuals use Tor to circumvent internet restrictions (often imposed by authoritarian regimes) and prevent tracking by state or industry actors. However, the Tor network is also used for illicit trading, including drugs, stolen goods, or digital items and services (e.g., hacking services). Trades of illicit goods are often carried out on darknet markets, which provide an infrastructure where users can transact goods and services with each other, similar to the surface web platform eBay. The Tor network, on which many markets exist, will be the focus for the remainder of this text due to its relatively widespread and larger-scale usage compared to other networks.

What are Darknet Markets?

At the beginning of 2011, the infamous online market "Silk Road" started operating on the Tor network, offering many illicit goods, predominantly drugs (e.g., cannabis, ecstasy, opioids), but also digital goods (e.g., hacking guides), apparel, electronics and more (Christin, 2013). In late 2013, the alleged site operator, Ross Ulbricht, was arrested, and US authorities shut the market down (CNN, 2013; EMCDDA-Europol, 2017). Around one month after the closure, Silk Road 2.0 was launched next to many similar sites (e.g., Pandora, Sheep Marketplace, BuyItNow). Since then, dark markets have been abundantly present on the network, but many operate only for a few months due to low traffic, voluntary closures, authority interventions, or "exit scams"[2] (EMCDDA-Europol, 2017).

Darknet markets, also called "black markets" or "crypto markets", mainly use cryptocurrencies for monetary exchanges, further supporting user anonymity, which is explained in more detail below. Some specialized markets offer only one product type, such as cannabis or stolen credit card information (Marin et al., 2016; Soska & Christin, 2015). Others are more general and offer a range of products, including fake documents (e.g., Passports), counterfeits (e.g., money, clothes), or firearms (Baravalle & Lee, 2018). Figure 3 provides an example of a listing on the market "Darkode". Sellers often customize offers for specific buyers, which can be arranged through chats, and name the listings "custom listing for [Username]".

Furthermore, markets often self-impose rules on what can be offered and sold. Next to general and specialized markets, more exclusive markets are also present, which are only accessible through invitations. However, invitations can sometimes be bought on other markets. While marketplaces are currently the predominant sales platforms, more shops are emerging that offer goods from a single seller, resembling retailer platforms (Oosthoek et al., 2023).

Accessing and browsing darknet markets often requires registration. Beyond having to solve unusually difficult Captchas, creating an account resembles registrations on surface web platforms. However, further interactions (e.g., posting, chatting, purchasing) mostly require *PGP keys* (Pretty Good Privacy), which encrypt messages and enable secure communications between users (Ailipoaie & Shortis, 2015). Each user requires a public and private PGP key for this encryption technology. For example, if a customer wants to send a message to a vendor, the customer uses the vendor's public key (often available on the vendor's profile) to encrypt a message. The message is then sent to the vendor, who can decrypt the message with their private key. In short, public keys are available to everyone to encrypt messages, while the private key is only known to the message receiver and is used to decrypt messages (For more details on PGP see: *openpgp.org*). Since vendors operate across platforms, PGP keys are also used as an identity verification tool (Ailipoaie & Shortis, 2015).

Payments on crypto markets are handled through *cryptocurrencies* (e.g., Bitcoin, Ethereum), which can be acquired through online exchanges, such as *Coinbase*, *Bitstamp*, or

2 A scam in which all the monetary user funds stored with the market website are stolen by hackers or the operators of the website, resulting in a closure.

direct transfers from other individuals. Cryptocurrencies are decentralized, anonymous, and rely on a peer-to-peer system, circumventing a governing third party, such as a bank (Rickens, 2019). The currencies can be held online on exchanges, the markets, or a local machine. Storing the currency locally with software is often preferred since it reduces the risk of theft through exit scams or hacks (EMCDDA-Europol, 2017). Since many cryptocurrency exchanges do not require personal information for registrations, the users' true identities often remain unknown. Further currency laundering through online *mixers* (*tumblers*)[3] makes the transactions virtually anonymous, complicating tracking for law enforcement (Europol, 2021; Möser et al., 2013). Thus, combining the Tor network and cryptocurrencies enables a highly anonymous environment for communication and trading.

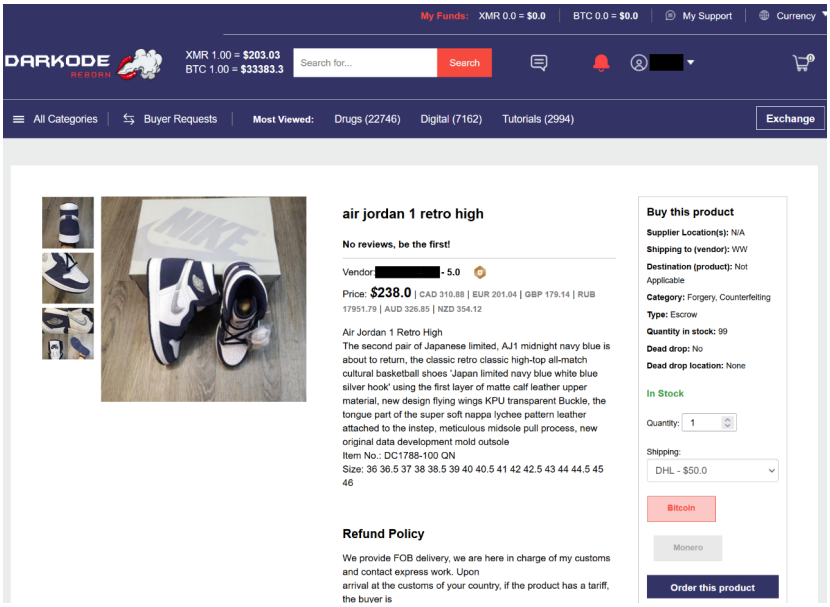


Figure 3 Screenshot of a counterfeit (Air Jordan shoes) sold on the darknet market "Darkode" on the Tor network.

The minimal oversight on cryptomarkets makes both customers and vendors vulnerable to fraud, such as sending payments without receiving the product or vice versa. To curb fraud, markets often implement escrow systems, mostly integrated within the markets. Buyers who want to make a purchase deposit the required funds into the escrow system. These funds are withheld until the buyer receives the product, allowing for a more secure transaction. Market operators often take commissions through escrow and oversee transactions (Christin, 2013). Large funds held in the markets owned escrow system are also believed to have led to past exit scams (EMCDDA-Europol, 2017).

Why and How to Research the Dark Web?

The dark web has mostly been researched within security-related disciplines and computer science. For example, researchers have examined the infrastructures of the dark web, tested potential security issues (e.g., how well communications are kept anonymous), or developed new encryption methods (Alidoost Nia & Ruiz-Martínez, 2018; Alsabah & Goldberg, 2016). An extensive overview of such security and encryption research is provided by Huete Trujillo & Ruiz-Martínez (2021). At the same time, recent years have seen increased research on crypto markets, forums, and their users, but mostly with quantitative approaches (Gehl, 2018). Fewer researchers investigate users' behavior, motivations, and opinions on dark web platforms qualitatively through observations or interviews (Barratt et al., 2016; Barratt & Maddox, 2016). Since many researchers take a quantitative approach, some research attention has shifted to automated large-scale data collection methods (Ball et al., 2019; Yannikos et al., 2022). Collecting data automatically from the dark web is difficult due to the long loading times of

3 For more details on Tumblers see: Möser et al. (2013).

the websites (due to the many relays through the network) and implemented security features (e.g., advanced Captchas, extended registration procedures) or anti-crawling measures (e.g., detection of fast navigation behavior on the website) (Georgoulias et al., 2021). Data collection is further complicated by the uniqueness of the websites, requiring custom-made scrapers (programs that automatically collect web data) for almost every website. Because of these difficulties, incomplete data is a common issue, and automated solutions can be unreliable (Munksgaard et al., 2016), which led some to argue that manual collection approaches should be preferred to ensure adequate data quality (Van Buskirk et al., 2014, 2015).[4]

According to past research, the earliest known market, the Farmer's Market, seemed to have started operating in 2010 and closed in 2012 (EMCDDA-Europol, 2017). The Silk Road 1 closely followed (2011-2012), which was the first platform to receive more in-depth scholarly attention, followed by many more market openings. Silk Road 1 contained around 220 product categories, and Christin (2013) estimated that it harbored around 30,000-150,000 customers, with vendors generating a monthly revenue of around $1.2 million in 2012. Later studies also focused on single big markets, such as Alphabay (Baravalle & Lee, 2018) or Hydra (Goonetilleke et al., 2022). Alphabay was one of the biggest markets at its time (2015-2017), with estimated sales values of $79.8 million over the two years. Drugs were the predominant listings of the market, contributing around $69.2 million to all sales on the market, while other products, such as fraud-related items (e.g., guides), counterfeits, or services (e.g., hacking) were also present (Baravalle & Lee, 2018). Hydra, operated from 2015 to 2022, grew bigger than Alphabay and was estimated to account for around $5 billion in transactional value over its lifespan (Goonetilleke et al., 2022). Drugs were also the predominant product category, but unlike other markets, it also implemented drop-offs (products were dropped at hidden locations where buyers could collect them from after the purchase) as an alternative to postal deliveries to circumvent authority inspections, which seemed to be one of the reasons for the market's success.

Other cryptomarket studies expanded to include multiple markets in an attempt to estimate the scale of the entire dark web economy, both in general and for specific product categories, such as COVID-19-related products (e.g., masks, vaccines, personal protective equipment) (Bracci et al., 2022; Oosthoek et al., 2023; Soska & Christin, 2015). For example, Soska & Christin (2015) collected data on 35 markets between 2013 and 2015 and estimated an accumulated peak daily sales volume of up to $600,000 in mid-2014, and over 9,000 sellers were estimated to be operating across markets. Estimating sales volumes can be challenging and is often achieved through counting unique reviews. Buyer feedback through reviews is very important in crypto markets due to the lack of vendor verifications (Batikas & Kretschmer, 2018; Tzanetakis et al., 2016).

Since the dark web is highly anonymized, estimating unique vendors can also be complicated but is often achieved through PGP-key identifications or comparisons of image or text styles from product listings (Ho & Ng, 2016; Wang, 2018). Studying crypto markets, specifically, their products and services, allows researchers to better understand the economic breadth of illicit markets that were difficult to observe previously. Thus, helping to understand the possible impact of specific products or services, their demand, and availability. Most research concerns drug market behavior, but fraud or hacking-related offers are investigated as well. For example, previous studies examined fraud and hacking-related services, including the registration of fake businesses, the procurement of airplane tickets, or the capabilities of denial-of-service attacks (Hutchings, 2018; Hyslip & Holt, 2019). Examining how such services are used and implemented helps us understand how to protect against or

4 Some open available data can be found here: https://gwern.net/DNM-archives (Branwen et al., 2015).

deal with them. However, crypto markets also allow researchers to examine user interactions and behaviors to better understand their attitudes and motivations. Drug user behavior is most prominent, but trust building, accountability, advertising, and other vendor or buyer behaviors can also be studied.

Since market closures are common, researchers have investigated the effects of market disruptions on vendor and buyer migrations, vendor resilience across platforms, and offline crime (Décary-Hétu & Giommoni, 2017; ElBahrawy et al., 2020; Zambiasi, 2022). Some research has found that market closures due to authority interventions or other reasons seem to have limited effects, with buyers and sellers adapting and migrating to other markets quickly. Prices seem stable even after market shutdowns, and larger vendors, often present on multiple markets, show stronger resilience than smaller vendors (Décary-Hétu & Giommoni, 2017; ElBahrawy et al., 2020). There is also evidence that offline drug sales seem to increase shortly after big market closures but quickly drop to pre-closure levels (Zambiasi, 2022). However, intervention or disruption approaches to reduce crime-related activity in crypto markets are not well studied, with some research examining warning messages or rumor spreads as alternatives to market shutdowns (Howell et al., 2022; Hutchings & Holt, 2017).

Research Challenges and Ethical Considerations

Due to the challenges associated with collecting data from anonymous networks, large-scale analyses are not as abundant, and data is scarce. Contributing to data collection approaches and extending existing data repositories are still open issues that could be addressed by making methods and data more readily available. Such data scarcity is further exacerbated for anonymous networks other than Tor and market dissimilar platforms, such as forums. With such data, researchers could explore differences in user behavior across anonymized and surface web platforms, including research on political opinions, conspiracy beliefs, or extremism.

> ***Researchers could explore differences in user behavior, including research on political opinions, conspiracy beliefs, or extremism.***

Cryptomarkets often have associated forums that could be linked with listing data to better understand the behavior and motivations of vendors and users. For example, understanding why and how cybercrime-related services are used (e.g., for misinformation campaigns) could facilitate better implementations of preventative measures. Furthermore, examining whether and how political movements utilize anonymous networks could be interesting.

Research around anonymous networks, specifically crypto markets, is often faced with legal and ethical considerations that are not always easy to address, along with common issues such as data protection. Notably, depending on the level of engagement from the researchers (e.g., observations, survey), the legal and ethical situation can become complicated quickly. For example, many institutional ethical guidelines recommend that researchers inform potential participants about their study and intentions, which collides with the principle of most users not to share personal information on anonymous networks (Gehl, 2018). Sharing personal information from and about the researchers has led at least once to threats and abuse to the investigators in the past (Martin & Christin, 2016).

However, conducting observational studies can also bring challenges. For example, collecting data on illegal products onto a local machine may be unlawful. Furthermore, ethical considerations may differ for users on anonymous networks, depending on their roles (e.g., site administrators, vendors, and

consumers) (Martin & Christin, 2016). As an example, estimating sales volumes for specific vendors could – in theory – be used against them if they were brought to trial. Further information around legal issues (e.g., when to report a possible crime) for the German context can be found in (RatSWD, 2023). Although essential to reproducibility, publicly sharing data is even more complicated as it may contain personal identifiable information, potentially harming users, especially in illegal contexts. The previous considerations only briefly touch on some key ethical considerations; the interested reader can look at the more in-depth discussion of these issues by Martin and Christin (2016).[5]

Technical and Legal Hurdles Complicate Dark Web Research

This paper introduced the dark web (anonymous networks), such as Tor and crypto market research, and provided starting resources for anyone interested in researching this space. Since users openly share sensitive information and conduct illicit businesses on anonymous networks, such spaces allow researchers to examine previously difficult-to-observe phenomena. However, anonymous networks are still understudied, especially outside of market environments. Technical and ethical hurdles surrounding collecting and sharing data from such networks are notable barriers. To address those barriers, collection methods and data should be shared more openly and documented to enable or facilitate reuse.

5 Some of the cited studies in this paper also include ethical or legal assessments related to their research (Barratt et al., 2016; Barratt & Maddox, 2016; Christin, 2013; Gehl, 2018; Soska & Christin, 2015).

References

Ailipoaie, A., & Shortis, P. (2015). *From Dealer to Doorstep – How Drugs Are Sold On the Dark Net.* Global Drugs Policy Observatory.

Alidoost Nia, M., & Ruiz-Martínez, A. (2018). Systematic literature review on the state of the art and future research work in anonymous communications systems. *Computers & Electrical Engineering, 69*, 497–520. https://doi.org/10.1016/j.compeleceng.2017.11.027

Alsabah, M., & Goldberg, I. (2016). Performance and Security Improvements for Tor: A Survey. *ACM Computing Surveys, 49*(2), 32:1-32:36. https://doi.org/10.1145/2946802

Ball, M., Broadhurst, R., Niven, A., & Trivedi, H. (2019). *Data Capture and Analysis of Darknet Markets.* 15.

Baravalle, A., & Lee, S. W. (2018). Dark Web Markets: Turning the Lights on AlphaBay. In H. Hacid, W. Cellary, H. Wang, H.-Y. Paik, & R. Zhou (Eds.), *Web Information Systems Engineering – WISE 2018* (Vol. 11234, pp. 502–514). Springer International Publishing. http://link.springer.com/10.1007/978-3-030-02925-8_35

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24–31. https://doi.org/10.1016/j.drugpo.2016.04.019

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research, 16*(6), 701–719. https://doi.org/10.1177/1468794116648766

Batikas, M., & Kretschmer, T. (2018). Entrepreneurs on the Darknet: Reaction to Negative Feedback. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3238141

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing, 7*(1). http://dx.doi.org/10.3998/3336451.0007.104

Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2022). Vaccines and more: The response of Dark Web marketplaces to the ongoing COVID-19 pandemic. *PLOS ONE, 17*(11), e0275288. https://doi.org/10.1371/journal.pone.0275288

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, El Presidente, Anonymous, Lau, D., Sohhlz, Kratunov, D., Cakic, V., Whom, McKenna, M., & Goode, S. (2015). *Dark Net Market archives, 2011-2015* (2015-07-12). https://www.gwern.net/DNM-archives

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13*, 213–224. https://doi.org/10.1145/2488388.2488408

CNN, B. T. H. (2013, October 5th). *How the FBI caught Ross Ulbricht, alleged creator of Silk Road*. CNN. https://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports, 10*(1), 18827. https://doi.org/10.1038/s41598-020-74416-y

EMCDDA-Europol. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Publications Office of the European Union.

Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Publications Office of the European Union. https://data.europa.eu/doi/10.2813/75468

Gehl, R. W. (2018). Archives for the Dark Web: A Field Guide for Study. In lewis levenberg, T. Neilson, & D. Rheams (Eds.), *Research Methods for the Digital Humanities* (pp. 31–51). Springer International Publishing. https://doi.org/10.1007/978-3-319-96713-4_3

Georgoulias, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E. (2021). A qualitative mapping of Darkweb marketplaces. *2021 APWG Symposium on Electronic Crime Research (ECrime)*, 1–15. https://doi.org/10.1109/eCrime54498.2021.9738766

Ghosh, S., Porras, P., Yegneswaran, V., Nitz, K., & Das, A. (2017). ATOL: A Framework for Automated Analysis and Categorisation of the Darkweb Ecosystem. In *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*.

Goonetilleke, P., Knorre, A., & Kuriksha, A. (2022). Hydra: A Quantitative Overview of the World's Largest Darknet Market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4161975

Gray, H. (2019). *Dark Web Map*. https://www.hyperiongray.com/dark-web-map/#zoom=0.8521016982969332&x=0.5064520330563047&y=0.572866049039204

He, B., Patel, M., Zhang, Z., & Chang, K. C.-C. (2007). Accessing the deep web. *Communications of the ACM, 50*(5), 94–101. https://doi.org/10.1145/1230819.1241670

Ho, T. N., & Ng, W. K. (2016). Application of Stylometry to DarkWeb Forum User Identification. In K.-Y. Lam, C.-H. Chi, & S. Qing (Eds.), *Information and Communications Security* (Vol. 9977, pp. 173–183). Springer International Publishing. https://doi.org/10.1007/978-3-319-50011-9_14

Howell, C. J., Maimon, D., Perkins, R. C., Burruss, G. W., Ouellet, M., & Wu, Y. (2022). Risk Avoidance Behavior on Darknet Marketplaces. *Crime & Delinquency,* 00111287221092713. https://doi.org/10.1177/00111287221092713

Huete Trujillo, D. L., & Ruiz-Martínez, A. (2021). Tor Hidden Services: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 1*(3), Article 3. https://doi.org/10.3390/jcp1030025

Huss, N. (2022, April 6). How Many Websites Are There in the World? (2023). *Siteefy*. https://siteefy.com/how-many-websites-are-there/

Hutchings, A. (2018). Leaving on a jet plane: The trade in fraudulently obtained airline tickets. *Crime, Law and Social Change, 70*(4), 461–487. https://doi.org/10.1007/s10611-018-9777-8

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*(1), 11–30. https://doi.org/10.1080/17440572.2016.1197123

Hyslip, T. S., & Holt, T. J. (2019). Assessing the Capacity of DRDoS-For-Hire Services in Cybercrime Markets. *Deviant Behavior, 40*(12), 1609–1625. https://doi.org/10.1080/01639625.2019.1616489

Lewis, S., Jamie. (2017, March 6th). *OnionScan Report: Freedom Hosting II, A New Map and a New Direction*. Mascherari Press. https://mascherari.press/onionscan-report-fhii-a-new-map-and-the-future/

Mansfield-Devine, S. (2009). Darknets. *Computer Fraud & Security, 2009*(12), 4–6. https://doi.org/10.1016/S1361-3723(09)70150-2

Marin, E., Diab, A., & Shakarian, P. (2016). Product Offerings in Malicious Hacker Markets. *ArXiv:1607.07903 [Cs]*. http://arxiv.org/abs/1607.07903

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy, 35*, 84–91. https://doi.org/10.1016/j.drugpo.2016.05.006

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *2013 APWG ECrime Researchers Summit*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

Munksgaard, R., Demant, J., & Branwen, G. (2016). A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network." *International Journal of Drug Policy, 35*, 92–96. https://doi.org/10.1016/j.drugpo.2016.02.027

Netcraft. (2023, January 16th). *Web Server Survey*. Netcraft News. https://news.netcraft.com/archives/category/web-server-survey/

Oosthoek, K., Van Staalduinen, M., & Smaragdakis, G. (2023). Quantifying Dark Web Shops' Illicit Revenue. *IEEE Access, 11*, 4794–4808. https://doi.org/10.1109/ACCESS.2023.3235409

RatSWD. (2023). Handreichung Umgang mit der Kenntnisnahme von Straftaten im Rahmen der Durchführung von Forschungsvorhaben. *RatSWD Output Paper Series*. https://doi.org/10.17620/02671.74

Rickens, E. (2019). *What Are Cryptocurrencies: The Basics*. https://blog.blockport.io/what-are-cryptocurrencies/

Soldner, F., Kleinberg, B., & Johnson, S. (2022). Trends in online consumer fraud: A data science perspective. In *A Fresh Look at Fraud*. Routledge.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Proceedings of the 24th USENIX Security Symposium*, 33–48.

Syverson, P. (2005). *Onion Routing*. https://www.onion-router.net/

The Tor Project, Inc. (2020). *The Tor Project | Privacy & Freedom Online*. https://torproject.org

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy, 35*, 58–68. https://doi.org/10.1016/j.drugpo.2015.12.010

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: What has this meant for online drug trading?: Editorial. *Addiction, 109*(4), 517–518. https://doi.org/10.1111/add.12422

Van Buskirk, J., Roxburgh, A., Naicker, S., & Burns, L. (2015). A response to Dolliver's "Evaluating drug trafficking on the Tor network." *International Journal of Drug Policy, 26*(11), 1126–1127. https://doi.org/10.1016/j.drugpo.2015.07.001

Wang, X. (2018). *Photo-based Vendor Re-identification on Darknet Marketplaces using Deep Neural Networks* [Master Thesis]. Faculty of the Virginia Polytechnic Institute and State University.

Yannikos, Y., Heeger, J., & Steinebach, M. (2022). Data Acquisition on a Large Darknet Marketplace. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–6. https://doi.org/10.1145/3538969.3544472

Zambiasi, D. (2022). Drugs on the Web, Crime in the Streets. The Impact of Shutdowns of Dark Net Marketplaces on Street Crime. *Journal of Economic Behavior & Organization, 202*, 274–306. https://doi.org/10.1016/j.jebo.2022.08.008

Felix Soldner

GESIS – Leibniz Institute for the Social Science, Köln, Germany

Dawes Centre for Future Crime, Department of Security and Crime Science, University College London, UK

E-Mail felix.soldner@gesis.org

Felix Soldner arbeitet als wissenschaftlicher Mitarbeiter bei GESIS im Department Computational Social Science. Seine Forschung umfasst Themen wie online Betrug, Cryptomärkte, Täuschungserkennung und Datenverzerrungen. Dabei interessieren ihn die Nutzung von Methoden in Bereichen von Natural Language Processing (NLP) und maschinelles Lernen.

doi: 10.15464/easy.2023.10

Jung, weiblich und extrem rechts

Die narrative Kommunikation weiblicher Akteurinnen auf Instagram

Sandra Kero

In der extremen Rechten wird in der Regel eine starke Dominanz männlicher Akteure beobachtet. Dass Frauen eine substanzielle Rolle innerhalb der Bewegung spielen, wird dabei oftmals übersehen: Diese erscheinen im Diskurs – wenn nicht gänzlich ausgeblendet – häufig nur als Nebenfigur, ihre eigene ideologische Verfasstheit sowie Handlungsfähigkeit werden dabei unterschätzt. Dieser Beitrag verdeutlicht, dass weibliche Mitglieder der extremen Rechten als ideologische Multiplikatorinnen agieren, die politische Agenda mitgestalten und sich aktiv an der öffentlichen Mobilisierung beteiligen. Ich habe anhand einer qualitativen Analyse von Instagram-Stories aufgedeckt, wie die Plattform zur Verbreitung menschenfeindlicher Ideologien genutzt wird und soziale Medien als neue Möglichkeitsräume für Frauen in der politischen Sphäre dienen. Die Ergebnisse der Untersuchung zeigen, dass Frauen innerhalb der extremen Rechten keine marginale Rolle einnehmen und eine Randerscheinung sind, sondern als aktive Gestalterinnen der politischen Einflussnahme agieren.

In the political extreme right, a strong dominance of male actors has been observed. However, the fact that women play a substantial role within the spectrum is often overlooked: In the discourse within the extremist community, they often appear – if not completely absent – as minor figures, and their own ideological constitution and capacity for action is underestimated. Contrary to this perception, this article shows that female members of the extreme right act as ideological multipliers, help shape the political agenda, and actively participate in public mobilization in the far right. To this end, a qualitative analysis of Instagram communication, with a particular focus on the story function, illustrates how the platform is used to spread propaganda by the extreme right, and how social media serves as a new possibility space for women in the political sphere. The findings from the study illustrate that women within the extreme right do not occupy a marginal role as a peripheral phenomenon but act as active subjects of political influence.

Keywords: Neue Rechte, digitaler Rechtsextremismus, Gender, soziale Medien, Instagram-Stories, politische Online-Kommunikation, qualitative Inhaltsanalyse

Frauen in der extremen Rechten: Übersehen und unterschätzt

Konservative, traditionelle Vorstellungen von Geschlecht sind ein wesentliches Merkmal des rechtsextremen[1] Denkens: Die Vorstellung einer biologischen Zweigeschlechtlichkeit, einer heteronormativen Sexualität oder das

1 Rechtsextremismus, oder ‚extreme Rechte', wird hier u.a. anlehnend an Jaschke, 2001; Salzborn, 2020; Stöss, 2010 als Sammelbegriff für verschiedenartige ideologische Einstellungen, Ausprägungen sowie Agitationsformen verstanden.

konservative Familienmodell von Vater, Mutter, Kind sind für die Konstruktion und den Erhalt der idealisierten ‚Volksgemeinschaft' im Rechtsextremismus zentral (Bitzan, 2016). Im klassischen rechtsextremen Weltbild werden Frauen vor allem reproduktive Aufgaben zugewiesen, das heißt die primäre Rolle der Mutterschaft und Kindererziehung.

» Frauen rücken zunehmend in den Vordergrund rechtsextremer politischer Aktivitäten. «

Betrachtet man die Geschlechterunterschiede innerhalb der extremen Rechten scheinen Frauen im Vergleich zu männlichen Akteuren unterrepräsentiert zu sein.[2] Aktuelle Schätzungen beziffern eine weibliche Beteiligung bei rechtsextrem motivierten Straf- und Gewaltdelikten auf lediglich 10% bis 15% (Counter Extremism Project (CEP), 2020). Dass die extreme Rechte primär als ein männliches Phänomen diskutiert wird, überrascht daher nicht – ist aber nicht unproblematisch. Daten der Mitte-Studie der Friedrich-Ebert-Stiftung verdeutlichen, dass sich Frauen in ihren rechtsextremen Einstellungen nicht signifikant von Männern unterscheiden (Bitzan, 2016; Zick et al., 2019). Es zeichnet sich außerdem ab, dass Frauen zunehmend in den Vordergrund rechtsextremer politischer Aktivitäten rücken (Bitzan, 2016); sei es als Spitzenpolitikerinnen wie Alice Weidel (AfD), Organisatorinnen und Aktivistinnen verschiedener (Straßen-)Bewegungen (z.B. ‚Mütter gegen Gewalt') oder als ideologische Multiplikatorinnen im Internet wie bei der selbstbezeichneten Fraueninitiative ‚Lukreta'. Dies ist insbesondere bedenklich, weil die gesamtgesellschaftliche (unbewusste) Stereotypisierung von geschlechtsspezifischen Eigenschaften und Verhaltensweisen eine unvoreingenommene Wahrnehmung des potenziell problematischen Einflusses weiblicher Akteurinnen verhindert. Während Männer mit Eigenschaften wie Kompetenz, Selbstbehauptung und Handlungsfähigkeit assoziiert werden (Eagly & Mladinic 1989; Eckes, 2008), werden Frauen häufig als fürsorglich, friedlich, gewaltfrei und unpolitisch wahrgenommen (Amadeu Antonio Stiftung, 2014; Radvan & Voigtländer, 2015). Diese unzureichende Wahrnehmung wird oft als *doppelte Unsichtbarkeit* bezeichnet: Wenn nicht gänzlich übersehen und ausgeblendet, werden rechtsextreme Einstellungen von Frauen oft nicht erkannt, sodass sie selbst als Akteurinnen aus dem Fokus geraten (Lehnert, 2015; Radvan & Voigtländer, 2015). Dies führt dazu, dass weibliche Akteurinnen oftmals ungehindert ihre rechtsextremistische Ideologie verbreiten können.

Mit dem allgemeinen Erstarken geschlechterpolitischer Themen rücken geschlechtsspezifische Anliegen auch zunehmend in den Fokus rechtsextremer Kampagnen. So instrumentalisieren insbesondere weibliche Akteurinnen die Feminismus-Debatte um angebliche Frauenrechte, um ihre ideologischen Vorstellungen und rassistischen Weltbilder subtil und breitenwirksam in gesellschaftliche Diskurse zu tragen. Geschlechter- und frauenpolitische Themen werden dabei entlang migrationsfeindlicher, (antimuslimischer) rassistischer Narrative verhandelt und eröffnen dem rechtsextremen Spektrum neue (weibliche) Zielgruppen (Lang, 2020; Lehnert, 2021; Trültzsch, 2019). Zugleich werden unter dem Deckmantel des ‚wahren Feminismus' politische Feindbilder gestärkt, die sowohl politische Gegner*innen als auch emanzipatorische Errungenschaften delegitimieren. Weiterhin spielt der Fokus auf die konservative Frauenrolle und Mutterschaft trotz politischer Aktivitäten rechtsextremer Frauen eine entscheidende Rolle für die Mobilisierung der weiblichen Zielgruppe (Lehnert, 2021). Beispielhaft verdeutlicht wird dies durch ein Instagram-Posting der AfD-Politikerin Mary

2 Als Beispiel kann hier etwa der – v.a. im Vergleich zu den anderen im deutschen Bundestag vertretenen Parteien – sehr geringe Frauenanteil von 13,8% in der AfD-Fraktion genannt werden, siehe Statista, 2021.

Abbildung 1 Betonung von Mutterschaft bei gleichzeitiger politischer Tätigkeit.

Khan (August 2021), welche neben ihrer politischen Tätigkeit die Rolle von Kindern als das „Wichtigste im Leben einer Frau“ betont (siehe Abbildung 1).

Um die Dynamiken der extremen Rechten der letzten Jahre zu ergründen, bedarf es einer tiefgreifenden Auseinandersetzung mit den neu geschaffenen Mitteln der politischen Agitation. Dazu gehören insbesondere auch Äußerungen in sozialen Medien wie Instagram. Diese sind ein wichtiges Medium in der Gestaltung des öffentlichen Diskurses und der Meinungsbildung (Hölig et al., 2021). Sie spielen außerdem für die Verbreitung von extremen Ideologien und Narrativen eine wichtige Rolle (Fielitz & Marcks, 2019; Rau et al., 2022). So bietet die (non-)verbale Interaktion, also die Kommunikation von ideologischen und politischen Ideen und Meinungen, etwa durch das Teilen eines Bildes oder Videos, ein niedrigschwelliges Angebot politischer Partizipation.

Zwar haben Ereignisse wie die rechtsterroristischen Anschläge in Christchurch und Halle oder die Erstürmung des Kapitols in Washington den digitalen Rechtsextremismus zu einem wachsenden Forschungsfeld werden lassen, eine geschlechterspezifische Untersuchung des Phänomens ist bislang jedoch eine Nische. An dieser Stelle setzt dieser Artikel an. Durch eine explorativ angelegte qualitative Analyse der narrativen Kommunikation weiblicher Akteurinnen der extremen Rechten auf der Plattform Instagram soll die strategisch-erzählerisch politische Mobilisierung und Ideologisierung in den Blick genommen werden.

Instagram als ideologischer Schauplatz weiblicher Akteurinnen im Rechtsextremismus

In einer Untersuchung von Feed-Beiträgen auf Instagram stellte das Recherchenetzwerk CORRECTIV (2020) fest, dass Frauen eine Schlüsselrolle auf der Plattform spielen. Sie bilden „die Brücke von der vorgeblich unpolitischen Ästhetik auf Instagram in ein rechtes Weltbild und letztlich in rechtsextreme Kreise“ (Abs. 2). Die Bilder ihrer Accounts verfolgen eine harmlose Inszenierung und damit eine politisch subtile Strategie der Propagandaverbreitung. So handele es sich oftmals um Motive von „Frauen in traditionellen Kleidern, mit geflochtenen, langen Haaren, in freier Natur“ (CORRECTIV, 2020, Abs. 10), durch welche traditionelle Geschlechterkonstruktionen transportiert werden sollen. Die Verbreitung von Angst und emotionalisierten Inhalten sei zudem ein zentraler Faktor ihrer strategischen Kommunikation über soziale Medien.

Einen besonderen Stellenwert in der Verbreitung der radikaleren Inhalte habe die Story-Funktion der Plattform (CORRECTIV, 2020). Anders als die Feed-Beiträge, welche innerhalb des Feeds sowie auf dem Instagram-Profil veröffentlicht werden und dauerhaft sichtbar sind, erscheinen die Instagram-Stories nicht in fortwährender Form im Feed oder auf dem Profil des postenden Accounts: ausschlaggebend ist hier die Schnelllebigkeit, da die geposteten Inhalte nach 24 Stunden von der Plattform verschwinden. Während der Schwerpunkt der CORRECTIV-Recherche auf den Feed-Beiträgen der Akteurinnen lag,

nimmt der vorliegende Artikel die Story-Funktion von Instagram in den Blick. Wie sich diese veränderte Zeitlichkeit von Stories auf die Sichtweisen und Interaktionen von Nutzenden auswirkt, wurde bereits in verschiedenen Arbeiten untersucht (z.B. Bainotti et al., 2020). Ein Hauptfokus lag bisher auf der Untersuchung von Selbstdarstellung, Intimität und Sexual- und Beziehungskulturen von Jugendlichen. Allgemein wird von einem höheren Maß an Selbstoffenbarung ausgegangen: Im Vergleich zu dauerhaften Inhalten werden die Bedenken hinsichtlich der Selbstdarstellung geringer (Bainotti et al., 2020). Diese potenziellen Effekte flüchtiger Medienformate sind für die Untersuchung der politischen Kommunikation extrem rechter Akteurinnen besonders interessant. Was und wie von rechtsextremen Instagrammerinnen in Instagram-Stories kommuniziert wird, versucht die nachfolgend berichtete Studie zu verdeutlichen.

Welche Accounts wurden betrachtet?

Aufgrund ihrer verstärkten Social-Media-Präsenz sowie Relevanz für extrem rechte Akteur*innen[3] dienten die Accounts von bekannten Mitgliedern der Jungen Alternative (JA)[4] sowie der AfD als Ausgangspunkt der Recherche. Weiterhin wurden die Abonnementlisten dieser Accounts manuell durchsucht und dadurch weitere relevante Accounts identifiziert und ergänzt. So entstand eine Liste von 17 Accounts.

Die Instagram-Stories wurden mit dem Tool *Instaloader* systematisch zweimal täglich erfasst[5] und gespeichert. Der Zeitraum der Datenerhebung betrug insgesamt 30 Tage und fand im April und Mai 2022 statt. Der finale Materialkorpus umfasst 879 Story-Postings und setzt sich primär aus den Dateiformaten Bild, Video sowie Text mit Bild und Video zusammen.

Wie wurden die Stories ausgewertet?

Die Untersuchung der Stories wurde entlang der folgenden Forschungsfragen durchgeführt. Übergreifend wurde zunächst die Frage gestellt, welche Inhalte werden auf der Plattform Instagram innerhalb der Storyfunktion durch extrem rechte Frauen kommuniziert. Diese wurde weiterhin in zwei Unterfragen gegliedert:

- Inwiefern handelt es sich um ein unpolitisches Posting, um ein Posting innerhalb der Grauzone oder um ein ‚direktes' politisch-ideologisches Posting?
- Welche narrativen Themenfelder werden innerhalb der Grauzone / ‚direkten' politisch-ideologischen Inhalte verbreitet?

Zur Beantwortung der Forschungsfragen wurde im Verlauf der Untersuchung zwischen drei Kommunikationsarten unterschieden, welche in einer ersten groben Kategorisierung des Materials identifiziert wurden: unpolitische Inhalte, eine Grauzone und direkte-politische Inhalte. Die Kategorie ‚unpolitisch' umfasste Beiträge, in welchen sich keine direkte oder subtile politisch-ideologische Botschaft erkennen ließen und daher im Weiteren eine untergeordnete Rolle spielen. Hierzu zählten beispielsweise Beiträge aus Alltag oder Freizeit. Der Bereich ‚Grauzone' beschrieb jene Beiträge, welche als ideologisch und/oder politisch bewertet, deren Inhalte allerdings über

3 Für die einzelnen Verflechtungen u.a. Bauer & Fiedler, 2021; Bundesministerium des Inneren, für Bau und Heimat, 2020; Fuchs & Middelhoff, 2019.

4 Pfahl-Traughber (2019) stuft die AfD als ein „rechtsextremistisches Projekt" ein, das einen „bedeutenden Bezugspunkt für den ganzen Rechtsextremismus" darstellt (S. 338).

5 Die technische Erhebung der Daten erfolgte mithilfe des Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) am (Social) Media Observatory (SMO).

subtile Strategien transportiert wurden. Sie erlauben keine klare Trennung zwischen unpolitischen und politisch-ideologischen Inhalten. Durch den hohen Interpretationsbedarf solcher Inhalte wurden diese nicht als ‚direkt' politisch-ideologisch gezählt. Im Kontrast zur Grauzone gehörten zur Kategorie der ‚direkten' politisch-ideologischen Inhalte solche Beiträge, welche politisch-ideologische Botschaften mittels eines klar kommunizierten Statements transportierten. Dies erfolgte durch die direkte Bezugnahme und Positionierung zu (aktuellen) Anliegen und Geschehnissen, welche in einen politisch-ideologischen Rahmen fielen und eine solche Motivation aufzeigten. Wertende Statements konnten sich in verbaler oder Textform, aber auch in nonverbaler Kommunikationsform, beispielsweise kommunikative Codes wie Emojis, erschließen. Die Einteilung der Story-Postings in die drei Typen ermöglichte es, die verschiedenen politisch-ideologischen Themen der ‚direkten' politisch-ideologischen Inhalte sowie die Grauzone zu betrachten. Visuelle Beispiele für die drei Kategorien zeigen die Story-Postings in Abbildung 2.

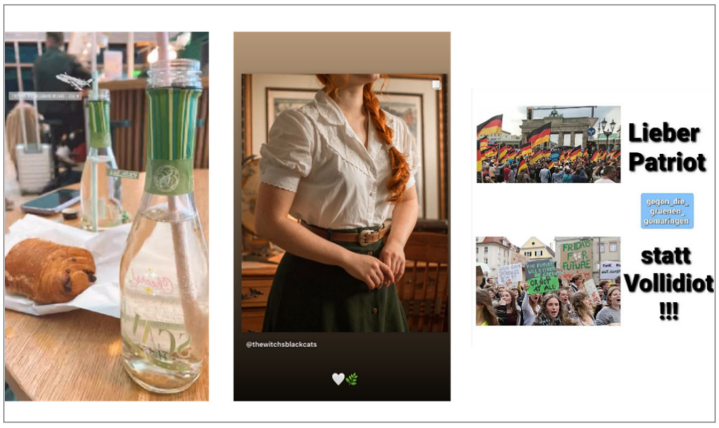


Abbildung 2 (v.l.n.r.) Kategorien ‚unpolitisch', ‚Grauzone', ‚direkte' politische Inhalte'.

Um die Story-Postings schließlich detaillierter zu analysieren, wurden deduktiv, also basierend auf allgemeinen Annahmen und Wissen, theorienthematische Kategorien gebildet. Teile des bereits bestehenden Forschungsstands[6] zu den Programmatiken, Ideologieelementen sowie (aktuell) kursierenden Narrativen des Spektrums der extremen Rechten wurden dazu ermittelt und zu übergreifenden thematischen Feldern (z.B. Regierungs- und Parteikritik, Antifeminismus) ausgearbeitet. Dabei entstanden 13 Kategorien, welche eine detaillierte Analyse der einzelnen Instagram-Stories der Kategorien ‚Grauzone' sowie ‚direkte' politische Inhalte erlaubte. Zum Themenfeld ‚Partei- und Regierungskritik' gehörten u.a. erkennbare rechtspopulistische Einstellungsmuster, wie etwa Thematisierung des Feindbildes der (Regierungs-) Parteien und darum kursierende Narrative (z.B. behauptete ‚Zensur der politischen Korrektheit' oder Referenz auf ‚politische Establishments'). Die Kategorie ‚Antifeminismus' umfasst beispielsweise u.a. Beiträge, welche regressive Geschlechterbilder proklamieren, den Feminismus und seine emanzipatorischen Errungenschaften diffamieren und die damit verbundene Implikationen von Sexualität und Familie delegitimieren. Marker für dieses Themenfeld sind ebenso kursierende Narrative um eine ‚demographischen Bedrohung durch Emanzipation' oder die Behauptung der ‚Gender-Ideologie' (siehe Abbildung 3).

Abbildung 3 Beispiel für ein Posting (April 2022) im Themenfeld Antifeminismus.

6 Vgl. hier u.a. die Arbeiten von Amadeu Antonio Stiftung, 2019; Baldauf et al., 2017; Fielitz & Marcks, 2019; Gümüş, 2020; Lang, 2020; Pfahl-Traughber, 2019; Salzborn, 2020; Sanders et al., 2019; Stöss, 2010.

Vor dem Hintergrund der identifizierten Subkategorien wurde das Material der übergeordneten Kategorien ‚Grauzone' sowie ‚direkte' politisch-ideologische Inhalte erneut bewertet und einem oder mehreren Themenfeldern, zugeordnet.

Welche Inhalte finden sich in den Instagram-Stories?

Durch die Aufteilung der Postings auf die drei definierten Kategorien (unpolitisch, Grauzone, ‚direkt' politisch-ideologisch) ließ sich ein erster Eindruck sowohl über das Ausmaß der politisch-ideologischen Postings im Gegensatz zu den unpolitischen als auch über die implizite (Grauzone) und explizite (‚direkte') Übermittlung politisch-ideologischer Inhalte gewinnen. Es zeigte sich, dass die politisch-ideologischen Instagram-Stories (53,98%) in der Gesamtbetrachtung gegenüber den unpolitischen Beiträgen überwogen (46,02%) (siehe Abbildung 4).

Unterteilte man in einem weiteren Schritt die politisch-ideologischen Inhalte in Grauzone und ‚direkte' politisch-ideologische Inhalte, wurde deutlich, dass letztere den weitaus größeren Teil ausmachten. So ließen sich nur 33 Beiträge der Grauzone zuordnen, 326 Beiträge vermittelten ‚direkte' politisch-ideologische Inhalte. Die zweite Forschungsfrage fragte, *welche* narrativen Themenfelder innerhalb der beiden Kategorien dominieren (siehe Abbildung 5).

Die Analyse zeigte, dass die Mehrheit der Inhalte regierungs- und parteikritisch geprägt waren (124 Beiträge). So wurde beispielsweise politisches Versagen im Umgang mit Asyl- und Migrationsfragen thematisiert oder die Aufhebung des Werbeverbots von Abtreibungen kritisiert. Deutlich vertreten waren auch Beiträge, die das Konstrukt Heimat und Tradition sowie Kultur positiv hervorhoben und/oder deren Erhalt forderten (93 Beiträge). Hierzu zählte beispielsweise die Befürwortung konservativer Geschlechter- und Familienbilder, als auch Beiträge aus den Themenfeldern Natur und Ökologie, welche als Identifikationssymbol von Heimat fungieren. In zahlreichen Story-Postings wurde zudem Kritik an politischen Gegner*innen geäußert. Diese enthielten personalisierte Kritik und/oder Diffamierung von Aktivist*innen, gesellschaftlichen (Personen-) Gruppen mit politisch-ideologischer Gegenposition und/oder (parteipolitischen) Einzelpersonen (78 Beiträge). Beispielsweise ließ sich diese Kategorie in Beiträgen mit Bezug auf die Grünen-Vorsitzende Ricarda Lang erkennen. Darin wurde sie als ‚grüne Tonne' beleidigt und ihr die politische Handlungsfähigkeit abgesprochen. Weitere Beispiele boten Story-Postings in denen missachtende Äußerungen gegenüber der Bewegung ‚Fridays for Future' und ihren Aktivist*innen getätigt wurden. Antifeministische Inhalte machten nach diesem (partei-)politisch orientiertem Schwerpunkt („Regierungs- & Parteikritik" sowie „Kritik an politischen Gegner*innen") den drittgrößten Anteil bezüglich politisch-ideologischer Feindbildkonstruktionen aus (für einen Überblick siehe Abbildung 5).

Unterschied man zwischen den politisch-ideologischen Beiträgen der Grauzone und den ‚direkten' politisch-ideologischen Beiträgen, wurde nicht nur ein Ungleichgewicht im Hinblick auf die Anzahl an Postings in diesen beiden Komplexen deutlich. Auch zeigte sich, dass die thematisierten Inhalte sich stark voneinander unterschieden (siehe

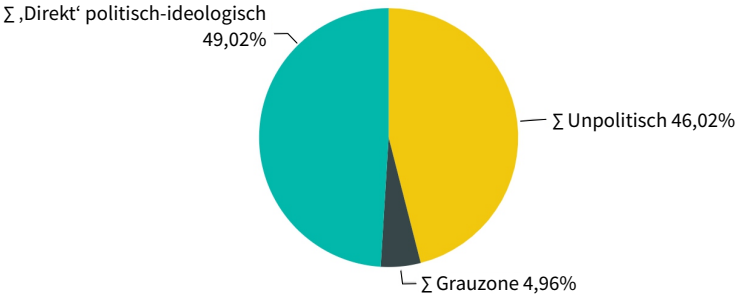


Abbildung 4 Verteilung der Instagram-Story-Postings auf die drei Kategorien.

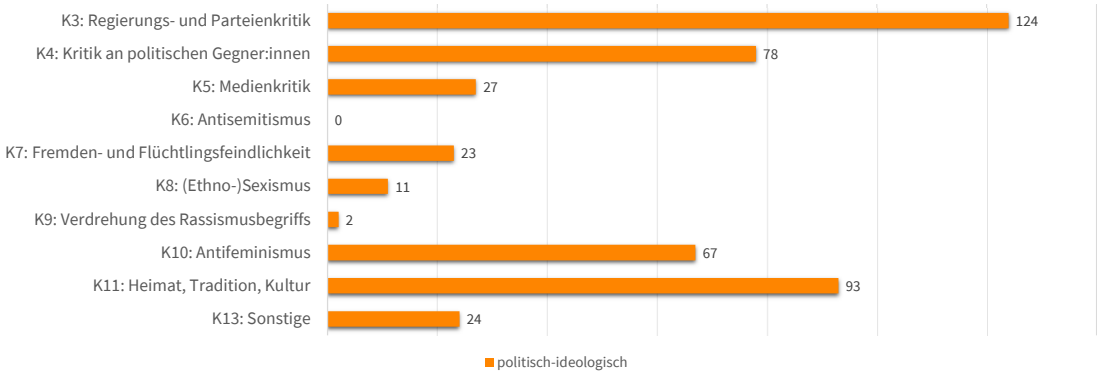
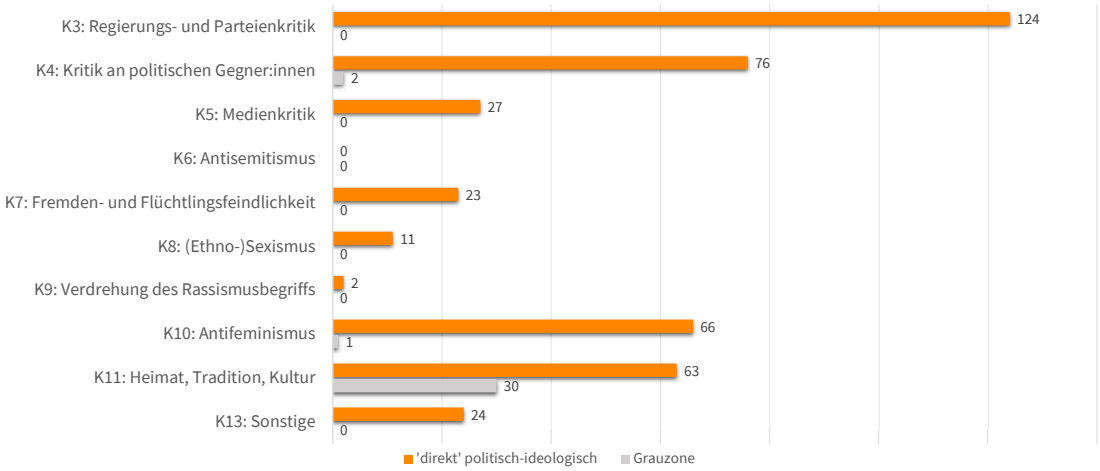


Abbildung 5 Verteilung der politisch-ideologischen Themenfelder insgesamt.



Anmerkung: Kategorie ‚(Partei-)Werbung' (K12) ausgeschlossen.

Abbildung 6 Verteilung der politisch-ideologischen Themenfelder auf die Kategorien ‚direkte' politisch-ideologische Inhalte vs. ‚Grauzone'.

‚Direkte' politisch-ideologische Inhalte dominieren die Story-Postings.

Abbildung 6). Während bei den ‚direkten' politisch-ideologisch vermittelten Inhalten, analog zum Gesamtergebnis, insbesondere das Themenfeld der ‚Regierungs- und Parteikritik' vorherrschte, wurden über suggestive, implizite Kommunikationsformen (Grauzone) nahezu keine Feindbildkonstruktionen, sondern fast ausschließlich Ideologievorstellungen rund um die Kategorie „Heimat, Tradition, Kultur" verbreitet.

Frauen in der extremen Rechten: Akteurinnen statt Nebenfiguren

Die Ergebnisse[7] stützen die Annahme, dass Frauen in der extremen Rechten nicht nur über inhärente Einstellungsmuster verfügen (u.a. Bitzan, 2016; Stöss, 2010), sondern auch die These, dass sie bei der unmittelbaren Streuung der ideologischen Konzepte eine aktive Rolle einnehmen und handlungsrelevant sind. Sie verbreiten aktiv explizite ideologische Inhalte

7 An dieser Stelle ist anzumerken, dass die Ergebnisse als erste, richtungsweisende Erkenntnisse zu verstehen sind. So gibt es keine Repräsentativitätsgarantie der Accountauswahl. Inhaltlich ergibt sich eine Limitation bezüglich der politisch-ideologischen Themenfelder.

über soziale Medien wie Instagram. Die Vermutung, dass innerhalb flüchtiger Medienformate – wie der schnelllebigen Story-Funktion – (kritische) Inhalte ungehemmter und unmittelbarer verbreitet werden, scheint sich darin widerzuspiegeln, dass politisch-ideologische Inhalte nicht nur auf eine vermeintlich harmlose und implizite Weise verbreitet wurden. Vielmehr sind es ‚direkte' politisch-ideologische Inhalte, die innerhalb der Story-Postings dominieren. Soweit sie nicht selbst als politische Akteurinnen – also Subjekte der Ideologisierung und Mobilisierung – sichtbar und als solche behandelt werden, verbleibt ihnen die Möglichkeit einer verhältnismäßig subtilen Verbreitung ihrer Inhalte. Diese Formen der Erweiterung ihres Tätigkeitsfeldes erfordern neue Umgangsweisen und eine verstärkte Sensibilisierung zivilgesellschaftlicher demokratischer Akteur*innen, um somit einer Verbreitung extremistischer Themen und Wertevorstellungen in die gesellschaftliche Mitte entgegenzuwirken.

Referenzen

Amadeu Antonio Stiftung (2014). *Overlooked and underrated: Women in right-wing extremist groups in Germany. Theoretical analysis and practical recommendations for state and civil society.* https://www.amadeu-antonio-stiftung.de/w/files/pdfs/fachstelle/140407_overlooked-and-underrated.-german-women-in-right-wing-extremist-groups.pdf

Amadeu Antonio Stiftung (Hg.) (2019). *Demokratie in Gefahr: Handlungsempfehlungen zum Umgang mit der AFD.*

Bainotti, L., Caliandro, A. & Gandini, A. (2020). From archive cultures to ephemeral content, and back: Studying Instagram Stories with digital methods. *New Media & Society, 23*(12), 3656–3676. https://doi.org/10.1177/1461444820960071

Baldauf, J., Dittrich, M., Hermann, M., Kollberg, B., Lüdecke, R. & Rathje, J. (2017). *Toxische Narrative: Monitoring rechts-alternativer Akteure.* Amadeu Antonio Stiftung.

Bauer, K. & Fiedler, M. (2021). *Die Methode AfD: Der Kampf der Rechten: im Parlament, auf der Strasse-und gegen sich selbst.* Klett Cotta.

Bitzan, R. (2016). Geschlechterkonstruktionen und Geschlechterverhältnisse in der extremen Rechten. In F. Virchow, M. Langebach & A. Häusler (Hg.), *Handbuch Rechtsextremismus* (S. 325–374). Springer VS. https://doi.org/10.1007/978-3-531-19085-3_12

Bundesministerium des Inneren, für Bau und Heimat. (2020). *Verfassungsschutzbericht 2020.*

CORRECTIV (2020, 7. Oktober). *Kein Filter für Rechts.* Abgerufen am 03.01.2023, von https://correctiv.org/topstories/2020/10/06/kein-filter-fuer-rechts-instagram-rechtsextremismus-daten-so-sindwir-vorgegangen/#daten-daten-daten-so-sind-wir-vorgegangen

Counter Extremism Project (CEP) (2020). MUSIK, KAMPFSPORT, GELD UND GEWALT: TRIEBFEDERN DER BEWEGUNG. In Counter Extremism Project (CEP) (Hg.), *Gewaltorientierter Rechtsextremismus und Terrorismus – Transnationale Konnektivität, Definitionen, Vorfälle, Strukturen und Gegenmaßnahmen* (S. 22–30). https://www.counterextremism.com/sites/default/files/CEP-Studie_Gewaltorientierte

Eagly, A. H. & Mladinic, A. (1989). Gender Stereotypes and Attitudes Toward Women and Men. *Personality and Social Psychology Bulletin, 15*(4), 543–558. https://doi.org/10.1177/0146167289154008

Eckes, T. (2008). Geschlechterstereotype: Von Rollen, Identitäten und Vorurteilen. In R. Becker & B. Kortendiek (Hg.), *Handbuch Frauen- und Geschlechterforschung* (S. 171–182). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531- 919720_20

Fielitz, M. & Marcks, H. (2019). *Digital fascism: Challenges for the open society in times of social media.* Institute for Peace Research and Security Policy at the University of Hamburg. https://escholarship.org/uc/item/87w5c5gp

Fuchs, C. & Middelhoff, P. (2019). *Das Netzwerk der neuen Rechten: Wer sie lenkt, wer sie finanziert und wie sie die Gesellschaft verändern.* Rowohlt.

Hölig, S., Hasebrink, U. & Behre, J. (2021). Reuters Institute Digital News Report 2021: Ergebnisse für Deutschland. *Arbeitspapiere des Hans-Bredow-Instituts.* https://doi.org/10.21241/SSOAR.73637

Jaschke, H.-G. (2001). *Rechtsextremismus und Fremdenfeindlichkeit: Begriffe, Positionen, Praxisfelder* (2. Aufl.). Westdeutscher Verlag. https://doi.org/10.1007/978-3-322- 80839-4

Lang, J. (2020). Zwischen Tradition und Moderne: Frauen in neuen rechten Gruppierungen. In O. Decker & E. Brähler (Hg.), *Autoritäre Dynamiken: Alte Ressentiments – Neue Radikalität: Leipziger Autoritarismus Studie 2020* (S. 341–352). Psychosozial-Verlag.

Lehnert, E. (2015). Fazit. In Amadeu Antonio Stiftung (Hg.), *Rechtsextreme Frauen – übersehen und unterschätzt Analysen und Handlungsempfehlungen* (S. 66–67). https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2014/05/rechtsextreme_frauen_internet.pdf

Lehnert, E. (2021). Die Relevanz von Gender im modernen Rechtsextremismus – rechtsextreme Frauen*

in NRW. In Amadeu Antonio Stiftung (Hg.), *Weiblich, bewegt, extrem rechts Frauen, Rechtspopulismus und Rechtsextremismus in Nordrhein-Westfalen* (S. 18–21). https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2021/07/RexNRW-Netz.pdf

Pfahl-Traughber, A. (2019). *Rechtsextremismus in Deutschland: Eine kritische Bestandsaufnahme*. Springer VS.

Radvan H. & Voigtländer, H. (2015). Wie werden (rechtsextreme) Frauen wahrgenommen? Ein Blick in die Geschichte. In Amadeu Antonio Stiftung (Hg.), *Rechtsextreme Frauen – übersehen und unterschätzt: Analysen und Handlungsempfehlungen* (S. 10–17). Amadeu Antonio Stiftung. Fachstelle Gender und Rechtsextremismus. https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2014/05/rechtsextreme_frauen_internet.pdf

Rau, J., Kero, S., Hofmann, V., Dinar, C. & Heldt, A. P. (2022). *Rechtsextreme Online- Kommunikation in Krisenzeiten: Herausforderungen und Interventionsmöglichkeiten aus Sicht der Rechtsextremismus- und Platform-Governance-Forschung*. https://doi.org/10.21241/SSOAR.78072

Salzborn, S. (2020). *Rechtsextremismus: Erscheinungsformen und Erklärungsansätze* (4., aktualisierte und erweiterte Aufl.). Nomos.

Sanders, E., Berg, A. O. & Goetz, J. (2019). *Frauen*rechte und Frauen*hass: Antifeminismus und die Ethnisierung von Gewalt.* Verbrecher Verlag.

Statista (2021, November). *Frauenanteil im Bundestag nach Fraktionen 2021*. Abgerufen am 05.01.2023, von https://de.statista.com/statistik/daten/studie/1063172/umfrage/frauenanteil-imbundestag-nach-fraktionen-in-deutschland/

Stöss, R. (2010). *Rechtsextremismus im Wandel* (3., aktualisierte Aufl., Neuaufl.). Friedrich-Ebert-Stiftung, Forum Berlin.

Trültzsch, L. (2019). Frauen in der rechtsextremen Szene – Strategien geschlechts-spezifischer Selbstermächtigung und politische Instrumentalisierung von Frauen im Rechtsextremismus. In K. Ketelhut & D. Lau (Hg.), *Gender, Wissen, Vermittlung: Geschlechterwissen im Kontext von Bildungsinstitutionen und sozialen Bewegungen* (S. 133–148). Springer VS. https://doi.org/10.1007/978-3-658-27700-0_8

Zick, A., Küpper, B. & Berghan, W. (2019). *Verlorene Mitte - feindselige Zustände: Rechtsextreme Einstellungen in Deutschland 2018/19* (F. Schröter, Hg.). Dietz.

Sandra Kero

Center for Advanced Internet Studies (CAIS)

E-Mail sandra.kero@cais-research.de

Sandra Kero ist Medienwissenschaftlerin und arbeitet als Referentin für Wissenschaftskommunikation im Rahmen des Projekts Meinungsmonitor Künstliche Intelligenz am Center for Advanced Internet Studies (CAIS). Sie forscht zu (rechtsextremer) Online-Kommunikation und beschäftigt sich mit digitalen Medien und deren Infrastrukturen sowie Medieninhaltsforschung. Zuvor war sie am (Social) Media Observatory des Leibniz-Institut für Medienforschung | Hans-Bredow-Institut tätig.

doi: 10.15464/easy.2023.11

Periods in the Public Eye

Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications

Annika Deubel & Pauline Heger

Period tracking apps allow for tracking and monitoring various aspects of reproductive health, making them a convenient and popular choice for personal tracking. However, concerns have been raised regarding the data-sharing practices of such apps. Against this background, the study at hand investigated the perceived privacy risks of period trackers and connection to knowledge about data sharing practices among German users. Exploratory analyses reveal that users who actively use period trackers have a lower risk perception than those who have discontinued the use. Additionally, perceived knowledge of data sharing practices of period trackers shows a negative relation with risk perception.

Perioden-Tracking-Apps sind für viele Menschen ein beliebtes Mittel für die Überwachung verschiedener Aspekte der reproduktiven Gesundheit. Gleichzeitig gibt es jedoch zahlreiche Bedenken hinsichtlich der Datenweitergabepraktiken solcher Apps. Die vorliegende Studie untersucht die wahrgenommenen Datenschutzrisiken von Perioden-Trackern sowie die Rolle von Wissen über Datenweitergabepraktiken unter deutschen Nutzenden. Die explorativen Analysen zeigen, dass Nutzende, die Perioden-Tracker aktiv verwenden, eine geringere Risikowahrnehmung haben als solche, die die Verwendung eingestellt haben. Darüber hinaus steht das wahrgenommene domänenspezifische Wissen über den Umgang mit Daten von Perioden-Trackern in einem negativen Zusammenhang mit der Risikowahrnehmung.

Keywords: perceived privacy risk, mobile health, period trackers

The accelerated global diffusion of information and communications technology (ICT) has led to a significant increase in the use of mHealth, i.e., the use of mobile apps for healthcare. While such applications can be useful for many purposes and users, at the same time, the discussion surrounding the sharing of healthcare data has been a prevalent issue in recent years (Schnall et al., 2015; Schroeder et al., 2022). The recent significant changes in the legislation regulating abortions in the United States intensified these discussions. The loss of federal protection for abortion rights by the Supreme Court's decision to overturn Roe v. Wade in the US has sparked serious data privacy concerns over the abuse of medical records as well as information generated from a person's online activity worldwide (Somberg, 2022). One main concern is that reproductive health information collected by such apps may be used to infer whether someone is seeking an abortion. Even prior to this, concerns have been voiced worldwide about the quantity of data and metadata gathered and traded to third parties by most reproductive health apps (Alfawzan et al.,

2022). How perceptions of privacy risks may have changed in particular after the legislative changes regarding abortions within the US is, however, still unclear.

In the study we present in this article, we investigated how users perceive the privacy risks associated with data sharing via period trackers, particularly in light of these recent political developments. We especially look at the role of knowledge about data privacy and usage patterns regarding other mHealth apps, on the condition of being active users or having used period trackers in the past.

mHealth Usage and Period Trackers

Mobile Health (mHealth) refers to the use of mobile-enabled applications for collecting and providing health care information (Azhar & Dhillon, 2018). These applications offer the potential for users to continuously monitor and promote their health and well-being, detect issues early, or have an improved access to healthcare (Papageorgiou et al., 2018). One type of mHealth applications are period tracking apps, which have become increasingly popular over the years. As a subgroup of mHealth applications, they allow users to track and analyse their menstrual cycles and other related factors, such as birth control (Levy & Romo-Avilés, 2019). At present, over 200 million individuals worldwide are estimated to use period trackers (Healy, 2021).

To investigate the use of period tracking apps and associated perceptions of privacy risks, we conducted an online survey among individuals who are or have been using such apps. A total of 146 participants took part in the survey which was fielded between November 28th and December 19th, 2022. Regarding general usage, 82.2% of participants (i.e., 120 individuals) stated that they actively used period trackers at the time of their response. Figure 1 shows the reasons why active users are currently using a period tracker. Out of these, the majority (93.3%) use the app for tracking their menstrual cycle, while over half of them (58.3%) also want to better understand their cycle. Other reasons were predicting premenstrual syndrome (PMS), symptoms of endometriosis or using the app to have better control over their fertility. 17.8% (i.e., 26 participants) in our sample have used period trackers in the past but have stopped to do so. Figure 2 displays the reasons for discontinuing the use of period trackers. 38.5% of the respondents stated that the app was no longer needed, while 8 (30.7%) stopped using the app due to data privacy reasons. Out of the 7 people who specified

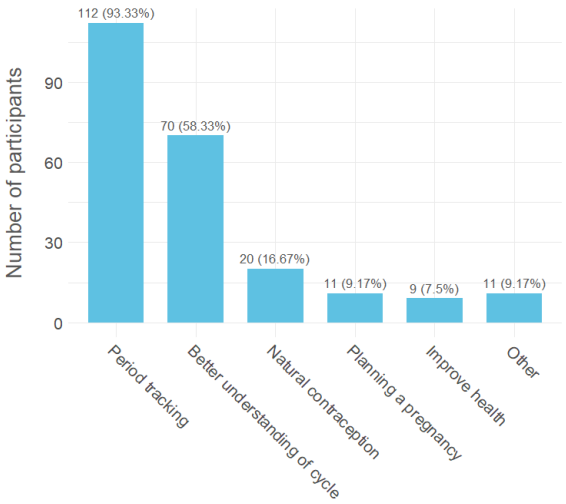


Figure 1 Reasons for using period trackers.

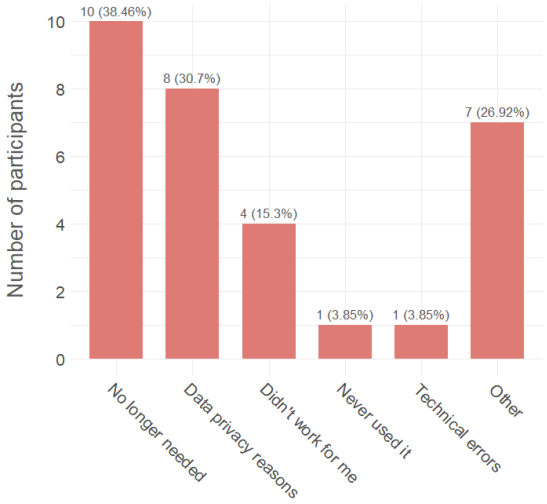


Figure 2 Reasons for discontinuing period trackers.

other reasons, all stated that they currently do not have their period (due to contraception or pregnancy).

Data Privacy Issues and Information Sharing

Despite their potential benefits, the collection, storage, and sharing of personal health data by these digital apps also raise privacy concerns. While the sharing of user data collected through health apps is a common practice, it is currently largely unregulated. For example, in 2022, a study looking at online cancer patient communities found that sensitive health data was funneled through cross-site tracking to Facebook, where it was used for marketing purposes (Downing & Perakslis, 2022). Further, previous research has shown that popular period trackers have significant shortcomings in terms of data privacy, sharing, and security standards. They also fail to comply with regulations of the EU General Data Protection Regulation (GDPR) (Alfawzan et al., 2022). Additionally, a general unease has been expressed about the amount of data and metadata collected and and sold to third parties by most period trackers (Alfawzan et al., 2022). Even before the aforementioned debate surrounding the overturn of Roe v. Wade, data security professionals have warned about the vast amounts of data that these apps collect and sell to third parties, such as Facebook, or even law enforcement agencies, on a large scale (Borges et al., 2018; Mozilla Foundation, n.d.).

Data security professionals have warned about the vast amounts of data that these apps collect and sell to third parties.

Period Trackers and Perceived Privacy Risk

Regardless of these findings, existing research provides an unclear picture of how users *perceive* these issues. On the one hand, some researchers have highlighted a lack of concern among app users when it comes to data privacy and the sharing of personal information. For example, Hohmann-Marriott (2021) found that many users had not given much thought to these issues, deeming them largely unimportant. In a similar vein, a study from the UK showed that particularly among "digital natives", there is a sense of indifference toward data privacy (Broad et al., 2022). Participants saw the sharing of personal data and companies' access to it as standard procedure. On the other hand, research has found that the actual intention to use mHealth applications, such as period trackers, may be heavily influenced by an individual's perceived risks associated with data disclosure, i.e. the belief that the use of mHealth applications may lead to abuse of personal information (Deng et al., 2018).

In that regard, when assessing risk perception in relation to mHealth, *perceived privacy* risk seems especially relevant. Perceived privacy risk refers to the extent to which an individual believes personal information abuse or privacy harm may occur because of mHealth application use (Klaver et al., 2021, p. 2). According to Bhatia & Breaux (2018), there are seven privacy harms leading to perceived privacy risk (see Table 1).

Previous research has found that people are less likely to perceive privacy risks when they are associated with specific benefits, such as lifestyle improvements (Park et al., 2019). This means that individuals who see a great benefit in using mHealth technology are less likely to see privacy risks than those who do not see any benefits.

Table 1 Privacy Harms as in Perceived Privacy Risk.

Appropriation	The feeling of personal information being used unexpectedly
Distortion	The feeling that others are using or sharing inaccurate, misleading, or incomplete information about the user
Induced Disclosure	The feeling of pressure to reveal personal information to others
Insecurity	The feeling that lapses in security aimed at protecting your personal information exist
Surveillance	The feeling of being tracked or monitored
Unanticipated Revelation	The feeling that user information is being revealed or exposed
Unwanted Restriction	The feeling of being unable to access or control personal information

What Did We Find in Our Study?

We measured perceived privacy risk by using the framework of Bhatia and Breaux (2018). Specifically, we asked the participants to what extent they experience the respective privacy harm when using period tracking apps on a scale from 1 to 5.

Overall, our results show a relatively low risk perception in our sample. With 1 being the lowest and 5 the highest value, the participants stated an average perceived privacy risk of *2.3*. Considering the different privacy harms, the feeling of pressure to reveal personal information (*Induced Disclosure*) as well as the feeling of being tracked and monitored (*Surveillance*) were the least prominent. In contrast, users felt more strongly that lapses in security aimed at protecting personal information (*Insecurity*) may exist and that they are unable to access or control their personal information (*Unwanted Restriction*). Although this was not part of our research objectives, we found significant differences between active and past users. Overall, participants who stopped using period trackers reported a 20% higher perceived privacy risk than those who are currently using period trackers.[1] When looking at the reasons why participants had decided to discontinue using the tracking apps, 30.8% stated they stopped due to data privacy reasons. This is in line with previous mHealth research showing that the intention to use depends – among other things – on how individuals perceive privacy risks (Azhar & Dhillon, 2018).

Other studies also demonstrated that when perceived privacy risks are low, they are likely outweighed by the benefits provided by the app (Bhatia & Breaux, 2018; Park et al., 2019). In our case, most active users value being able to track their period as well as better understand their menstrual cycle, especially in relation to co-occurring conditions, such as PMS or endometriosis. This could also be an explanation for higher risk perception in those who do not use the apps anymore since the benefits when using the app could most likely not outweigh the perceived privacy risks anymore.

The Role of Knowledge

Studies on risk perception indicate that having domain-specific knowledge about risks can significantly improve one's ability to evaluate potential hazards. This means that when faced with a potential risk, experts and non-experts tend to approach the situation differently (Siegrist & Árvai, 2020). Experts already possess the required knowledge to make accurate risk assessments, whereas non-experts typically have a more general understanding of the situation, which can lead to an inadequate perception of the risk involved. According to Larsen et al. (2022), more knowledge or

1 We calculated a Wilcoxon rank sum test with $W = 790$, $p < 0.01$, $r = 0.33$.

even awareness of privacy issues can thereby manifest in a lower risk perception regarding data sharing. Others argue that users with the necessary knowledge about data sharing practices may be more likely to tolerate the potential misuse of personal information (Schroeder et al., 2022). In online privacy literacy research, it has also been suggested that users may lack the knowledge to behave in ways that can mitigate the perceived risk (Masur et al., 2017). Overall, there is a scientific argument for knowledge playing a role in shaping our perception of risk. However, there is no consensus on how it specifically influences this perception. In the framework established by Masur et al. (2017), knowledge about online privacy is defined by four pillars, which can be seen in Figure 3.

Individuals with higher perceived knowledge tend to have a lower risk perception.

For our study, we used the online privacy scale (OPLIS), which is a questionnaire based on the four pillars shown below. This questionnaire captures the knowledge about privacy and data protection regarding online applications. As the questionnaire does not specifically measure knowledge for our domain and no validated scale for knowledge about data privacy and information sharing in mHealth/period tracking apps exists yet, we included five questions for *perceived* knowledge specifically for period trackers.

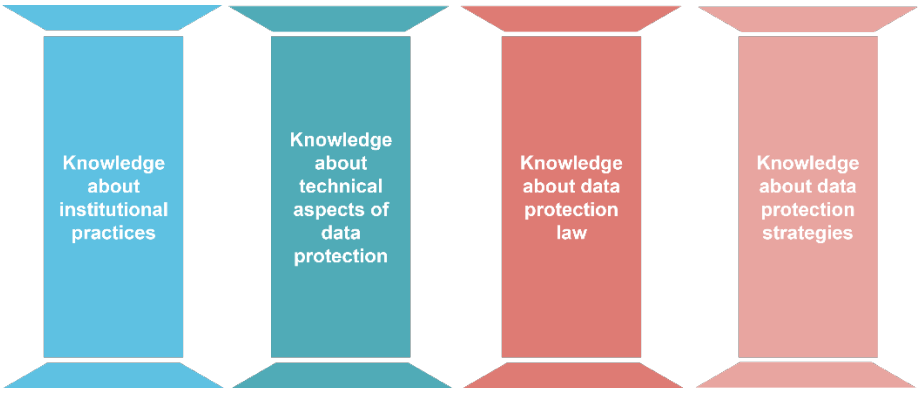


Figure 3 Knowledge of online privacy based on OPLIS (Masur et al., 2017).

What Did We Find?

The knowledge regarding online privacy was surprisingly high among our participants. Interestingly, however, and unlike what previous findings show, our results did not reveal a significant relationship between online privacy literacy and perceived privacy risk. Instead, we found a relationship between perceived domain-specific knowledge and perceived privacy risk, which is visualized in Figure 4. The findings show that individuals with higher perceived knowledge tend to have a lower risk perception. In addition, our results indicate that individuals who discontinued using period trackers have a higher overall risk perception.

Both user groups (active & past) achieved similar results for online data privacy literacy. With an average of 14.54, the respondents overall performed better than 67% of the population according to the findings by Masur et al. (2017). However, while online privacy literacy was not related to risk perception, we found that this was the case for *perceived domain-specific knowledge*. In particular, the more users thought they knew about the data privacy practices of period trackers, the lower their privacy risk perception. Our findings, thus, conform with one of the previous narratives in related research: It can be argued that the majority of regular users are aware of data-sharing practices, but have grown accustomed to those and view them as a normal aspect of using the app (Broad et al., 2022; Hohmann-Marriott, 2021), which may lead to a lower risk perception (Larsen et al., 2022).

This also corresponds with findings on the so-called "privacy paradox": Despite being aware of privacy risks on the internet, many users willingly provide personal information in exchange for goods and personalized services

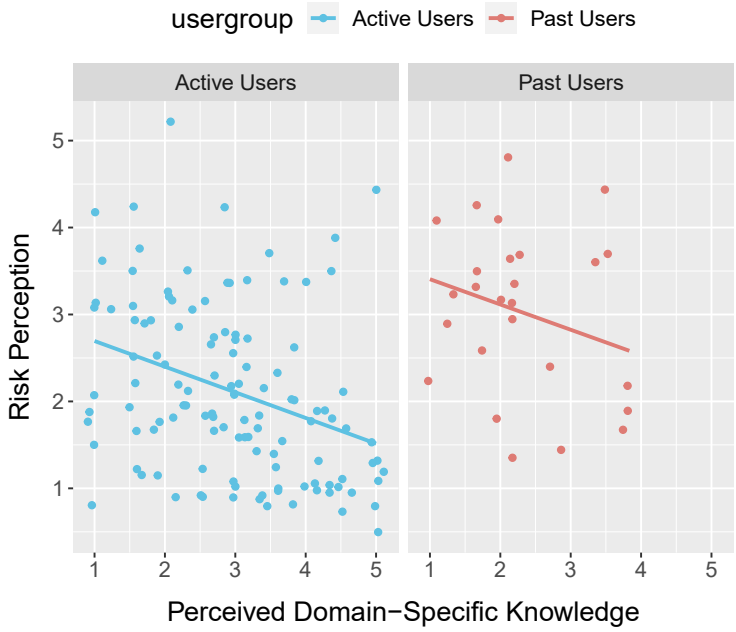


Figure 4 Scatter plot for the relationship between the variables risk perception and perceived domain-specific knowledge. We performed a linear regression analysis and the resulting model explained 15% of the variance in the outcome variable ($R^2 = 0.15$). It should be noted that the sample size for the groups is extremely unbalanced as we did not specifically set out to identify group differences between active and past users.

(Bhatia & Breaux, 2018). We suggest that further research about the privacy paradox regarding period tracking apps is necessary to understand the full picture. In that regard, a comparison between European countries and the US could, for example, reveal differences as to how local laws (e.g., the legal landscape surrounding abortion rights) can affect trade-offs between benefits and risks while using period trackers.

What Could Further Research Look Like?

The limitations of this study are essential to consider when interpreting the findings, as they cannot be generalized. First and foremost, our survey was conducted in German. The personal data of German citizens is protected by the GDPR, so users may have a lower perception of data sharing risks since they know that their data is protected – at least to some degree. In the future, comparative studies with, e.g., the US may, hence, be informative. Further, it should be noted that with measuring *perceived* domain-specific knowledge, our results cannot provide information about whether the perception of knowledge or the actual knowledge of data sharing in period trackers was responsible for the correlation with risk perception. This would be interesting to further disentangle in future research. The type of apps that respondents were using may also play an essential role. In our study, the most commonly used period tracker was *Clue* with 27.4%. According to the Mozilla Foundation (n.d.), *Clue* is based in Germany, and its data use is governed by the European GDPR. However, nearly 20% used *Flo*, which attracted negative attention by sharing sensitive data with Facebook without prior disclosure (Gupta & Singer, 2021). Flo Health Inc., the company behind Flo App was founded in Belarus with current headquarters in England and USA (*Flo App, Inc.*, n.d.; Khidekel, 2018). The relationship between different data privacy regulations of individual apps and perceived risk could be explored in further research.

Key Messages

Our study found that active users of period trackers have a relatively low perception of risks concerning data privacy and information sharing, while those who have stopped using such apps perceive the risks to be significantly higher. Our findings, thus, align with previous studies in mHealth research which have shown that the actual intention to use an app can be related to how individuals perceive privacy risks. Additionally, perceived domain-specific knowledge was associated with lower risk perception in our study.

In terms of practical implications for users, our results suggest that it is important for individuals to consider the data privacy and sharing practices of different companies when choosing a period tracker. This is particularly crucial in light of recent changes to laws surrounding reproductive rights in several countries, including the US, and to ensure the protection of personal privacy. The study by the Mozilla Foundation (n.d.) highlights clear distinctions between different apps in terms of their data sharing practices and privacy regulations, and this is something that users should consider when deciding on an app.

References

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, data sharing, and data security policies of women's mHealth apps: Scoping review and content analysis. *JMIR MHealth and UHealth, 10*(5), e33735. https://doi.org/10.2196/33735

Azhar, F., & Dhillon, J. S. (2018). An investigation of factors influencing the intention to use mHealth apps for self-care. *International Journal of Business Information Systems, 29*, 59. https://doi.org/10.1504/IJBIS.2018.094005

Bhatia, J., & Breaux, T. D. (2018). Empirical measurement of perceived privacy risk. *ACM Transactions on Computer-Human Interaction, 25*(6), 34:1-34:47. https://doi.org/10.1145/3267808

Borges, A. L. V., Moreau, C., Burke, A., Santos, O. A. dos, & Chofakian, C. B. (2018). Women's reproductive health knowledge, attitudes and practices in relation to the Zika virus outbreak in northeast Brazil. *PLOS ONE, 13*(1), e0190024. https://doi.org/10.1371/journal.pone.0190024

Broad, A., Biswakarma, R., & Harper, J. C. (2022). A survey of women's experiences of using period tracker applications: Attitudes, ovulation prediction and how the accuracy of the app in predicting period start dates affects their feelings and behaviours. *Women's Health, 18*. https://doi.org/10.1177/17455057221095246

Deng, Z., Hong, Z., Ren, C., Zhang, W., & Xiang, F. (2018). What predicts patients' adoption intention toward mHealth services in China: Empirical study. *JMIR MHealth and UHealth, 6*(8), e9316. https://doi.org/10.2196/mhealth.9316

Downing, A., & Perakslis, E. (2022). Health advertising on Facebook: Privacy and policy considerations. *Patterns, 3*(9), 100561. https://doi.org/10.1016/j.patter.2022.100561

Flo App, Inc. (n.d.). Flo.health - #1 mobiles Produkt für die weibliche Gesundheit. Retrieved June 12, 2023, from https://flo.health/de/kontakt

Gupta, A. H., & Singer, N. (2021, January 28). Your app knows you got your period. Guess who it told? *The New York Times.* https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html

Healy, R. L. (2021). Zuckerberg, get out of my uterus! An examination of fertility apps, data-sharing and remaking the female body as a digitalized reproductive subject. *Journal of Gender Studies, 30*(4), 406–416. https://doi.org/10.1080/09589236.2020.1845628

Hohmann-Marriott, B. (2021). Periods as powerful data: User understandings of menstrual app data and information. *New Media & Society.* https://doi.org/10.1177/14614448211040245

Khidekel, Marina. (2018, June 25). *The race to hack your period is on*. ELLE. https://www.elle.com/beauty/health-fitness/a21272099/clue-period-app/

Klaver, N. S., van de Klundert, J., van den Broek, R. J. G. M., & Askari, M. (2021). Relationship between perceived risks of using mHealth applications and the intention to use them among older adults in the Netherlands: Cross-sectional study. *JMIR MHealth and UHealth, 9*(8), e26845. https://doi.org/10.2196/26845

Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research, 3*, 100065. https://doi.org/10.1016/j.martra.2022.100065

Levy, J., & Romo-Avilés, N. (2019). "A good little tool to get to know yourself a bit better": A qualitative study on users' experiences of app-supported menstrual tracking in Europe. *BMC Public Health, 19*(1), 1213. https://doi.org/10.1186/s12889-019-7549-8

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskom-

petenzskala (OPLIS). *Diagnostica, 63*(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

Mozilla Foundation. (n.d.). **Privacy not included: A buyer's guide for connected products*. https://foundation.mozilla.org/en/privacynotincluded/

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access, 6*, 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries, 29*(1), 31–43. https://doi.org/10.1002/hfm.20750

Schnall, R., Higgins, T., Brown, W., Carballo-Dieguez, A., & Bakken, S. (2015). Trust, perceived risk, perceived ease of use and perceived usefulness as factors related to mHealth technology use. *Studies in Health Technology and Informatics, 216*, 467–471.

Schroeder, T., Haug, M., & Gewald, H. (2022). Data privacy concerns using mHealth apps and smart speakers: Comparative interview study among mature adults. *JMIR Formative Research, 6*(6), e28025. https://doi.org/10.2196/28025

Siegrist, M., & Árvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk Analysis, 40*(S1), 2191–2206. https://doi.org/10.1111/risa.13599

Somberg, T. (2022). *Living in a Post-Roe V. Wade world: Can your period tracker app data be used against you? - Exclusive*. Women. https://www.women.com/1242703/can-your-period-tracker-app-data-be-used-against-you/

Annika Deubel

Center for Advanced Internet Studies (CAIS)

E-Mail: annika.deubel@cais-research.de

Annika Deubel is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany. In her research, she focuses on health information on social media. She is generally interested in computational methods and digital behavioural data.

Pauline Heger

Center for Advanced Internet Studies (CAIS)

E-Mail: pauline.heger@cais-research.de

Pauline Heger is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany, with a background in communication science. Her research focuses on social diffusion of innovation, sustainable technologies, and HCI.

doi: 10.15464/easy.2023.12

Making Sense of the Big Data Mess

Why Interdisciplinarity Matters in Smart Cities

Niklas Frechen, Pauline Heger, Christoph Bieber & Mennatullah Hendawy

Smart cities use vast amounts of (big) data, often creating what we call an urban "data mess". In this article, we show the ***diversity and complexity of data*** *that make up this mess and outline examples of urban data processing. Furthermore, we point out problems with the sector-specific perspective that is usually taken when dealing with smart cities. We argue that a collective way of dealing with data across sectors and disciplines needs to be found. To achieve that, we advocate for* ***more interdisciplinary cooperation*** *between different disciplines and stakeholder groups. The Pandemic Recovery Dashboard of the City of Los Angeles gives a first impression of how this could work. We aim to show that approaching data in smart cities from an interdisciplinary angle may help deal with the data mess in smart cities – both for researchers and city developers.*

„Smart Cities" stützen sich auf große Datenmengen („Big Data") – wobei die unterschiedlichen Daten häufig in ungeordneter Form vorliegen (engl.: „data mess"). Im Beitrag widmen wir uns dieser ***Diversität im städtischen Datenbestand*** *und skizzieren Beispiele urbaner Datenverarbeitung. Dabei verweisen wir auf Probleme und Herausforderungen einer engen, an einzelne Bereiche gebundenen Datennutzung: Aus unserer Sicht fehlt bislang ein gemeinschaftlicher, sektorübergreifender Ansatz zum Umgang mit Smart-City-Daten. Aus diesem Grund sind* ***mehr interdisziplinäre Kooperationen*** *erforderlich, d.h. die Zusammenarbeit unterschiedlicher Disziplinen und Stakeholder-Gruppen. Das Pandemic Recovery Dashboard der Stadt Los Angeles gibt einen ersten Eindruck davon, wie urbane Daten erfolgreich genutzt werden können. Wir argumentieren dafür, dass Daten in Smart Cities am besten in ganzheitlicher Perspektive bearbeitet und der städtische Datendschungel so übersichtlicher gestaltet werden kann – für Wissenschaft und Praxis.*

Keywords: smart city, interdisciplinarity, big data, urban data, civic tech

Cities have been of scholarly interest for a long time and lots of metaphors have been used to describe the urban scenery: cities have been conceived as organisms, as nature, as machines, as theatres, or as a form of memory. More recently, the increasing use of technology and the collection of data has brought about ideas of the city as a computer, an intelligent machine, or even a cyborg. In urban planning and city politics, the term "smart city" has become increasingly popular to describe this view.

The multi-faceted landscape of smart city projects all over the world is an interesting field not only for city planners but also for the growing number of people living in cities as well as for scholars from various disciplines being confronted with new objects for research. This

article deals with a key element of modern city life: the collection, storage, and processing of many kinds of data to improve cities in various regards. The basic idea focuses on improving knowledge about what determines the life of city dwellers. As modern cities have grown into complex structures, many different sources provide data that can be tracked, stored, and processed – but in the first place, they create a complex and confusing mass of unstructured material. This situation holds lots of challenges for city administrations and politics as well as for researchers. Modernization of long-standing organizational structures is needed as well as expanding interdisciplinary efforts in data and city management.

What is a Smart City?

Software studies scholar Rob Kitchin defines a smart city as "one that can be monitored, managed, and regulated in real-time using ICT infrastructure and ubiquitous computing" (Kitchin, 2014, p. 132). Put simply, cities often qualify for being called "smart" when they use digital technology, such as security cameras, pollution sensors, traffic meters, or other specialized devices, to collect different sorts of data (see the following section). These data are used further, especially for processes of urban policymaking, e.g., for city officials' decisions about what services in terms of health, transportation and security will be offered to citizens. In most cases, plans for making a city smart (called *smart city strategies*) form the next step in a long history of city modernization. The overarching goal of many of these strategies is to use data-based technologies to improve the quality of life for their residents (Al Nuaimi et al., 2015).

When we look at the smart city strategies published by different city governments[1], we

> ***Cities are often called "smart" when they use digital technology to collect different sorts of data.***

notice that there are often specific visions the smart city tries to provide, indicating a certain "sense" as per Kitchin's (2014) words. Sometimes, these visions are called *smart city narratives* – which can be understood as a "story" a city wants to tell during the process of digital urban modernization. In Germany, for example, depending on the respective emphasis of the smart city strategy in place, we notice that promoted visions include *traffic-smart* cities (cf. Hamburg), *energy-* or *climate-smart* cities (cf. Paderborn), and sometimes *administration-smart* cities (cf. Nuremberg). As shown in Figure 1, certain narratives are closely related to certain applications and hence require specific kinds of data (e.g., traffic and transportation data would be very relevant for traffic-smart cities), as we will show in this article. Overall, while narratives, goals, progress, and implementation already differ greatly between smart city projects, there is even more variety when it comes to the kinds of data that are used and needed in these projects. In the next section, we elaborate on these different kinds of data.

What Kind of (Big) Data do Smart Cities Use or Produce?

Data is an essential part of smart city projects (e.g., Kitchin & Dodge, 2011). In a general sense, data refers to (collections of) many different pieces of information about something. However, there can be different ways in which this information is represented in terms of meaning, format (e.g., in numeric form, text-

1 Usually, cities accompany their measures with extensive documentation and strategy papers, outlining the basic goals of smart city activities. These are often publicly available on the cities' websites (e.g., for Los Angeles, Barcelona, and Bochum, to name a few).

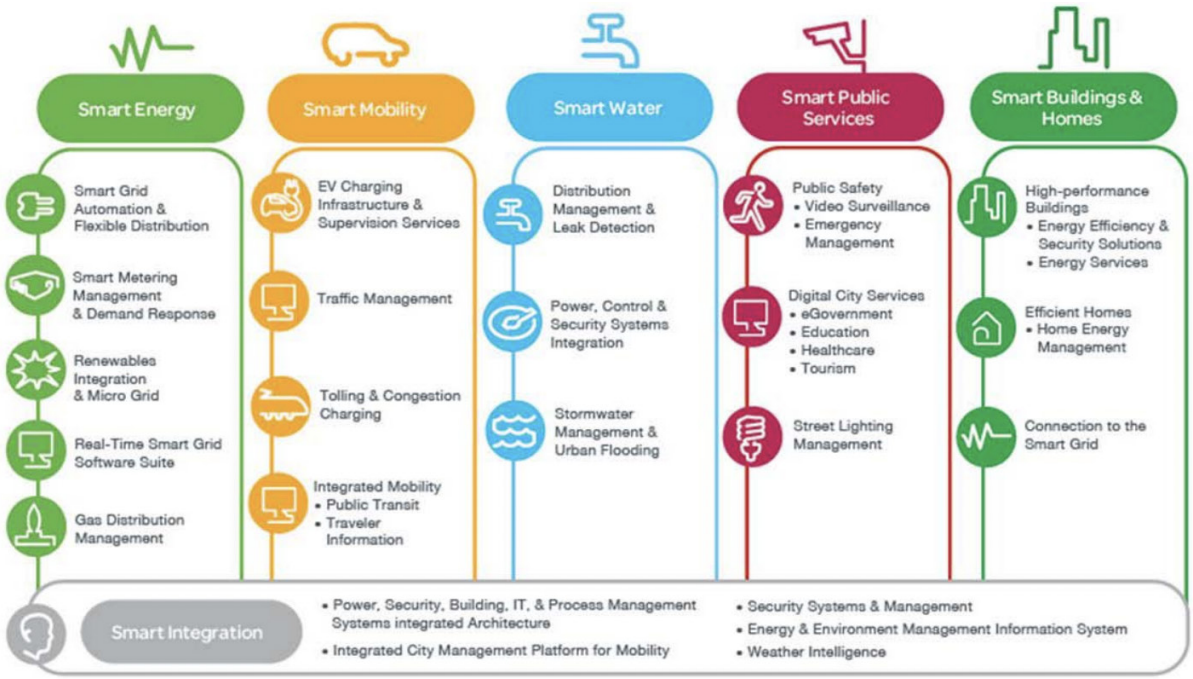


Figure 1 Smart City Services and Solutions. Image Source: Aoun, 2013, p. 9.

based, or otherwise), what units of measurement are used, and how the data is stored and processed. Additionally, the sources of the data themselves can vary greatly. As the data discussed here is produced by all technology implemented in cities, the amount and variety of data are extremely high. In other words: smart city data is big data.

Big data is often distinguished from regular data by its characteristics of *volume*, *velocity*, and *variety*, commonly referred to as the "3 Vs". These categories were introduced by Laney in 2001 as a framework for defining what constitutes big data. Volume refers to the massive amounts of data generated, velocity to the speed at which it is accumulated, and variety to the diversity of the data collected (Laney, 2001). While some of the big data is produced by humans both directly (e.g., election results, participation data) and indirectly (e.g., platform usage data collected by providers), there is also "data produced by objects", which derives from sensors, cameras, RFID tags, or Wi-Fi signals (Flyverbom & Madsen, 2015, pp. 124, 131). In a "mobility-smart" city, for example, this can include data from pollution sensors on busy roads, or the passenger data from public transport. By comparison, in an "energy-smart" city, this can include data from smart grids, or feed-in data from private solar power systems. Data produced by objects is an important driver of data collection and processing by administrative or other actors and also fuels the data resources of smart city projects.

Within the masses of data that a smart city creates (and needs), one can distinguish between various *data sectors* that smart cities attempt to develop (e.g., smart mobility, smart administration, smart energy, etc.). Until today, we have observed that data in smart cities has usually been dealt with from a sector-specific perspective, both by researchers and smart city planners. These sectors, in turn, involve many different *data types,* such as environmental data, geographic data, traffic data, data from politics and administration, and statistical data. An illustration of this sector-based approach and the associated data types is shown in Figure 2. The division into data sectors is usually also reflected in the structure of city governments and institutional divi-

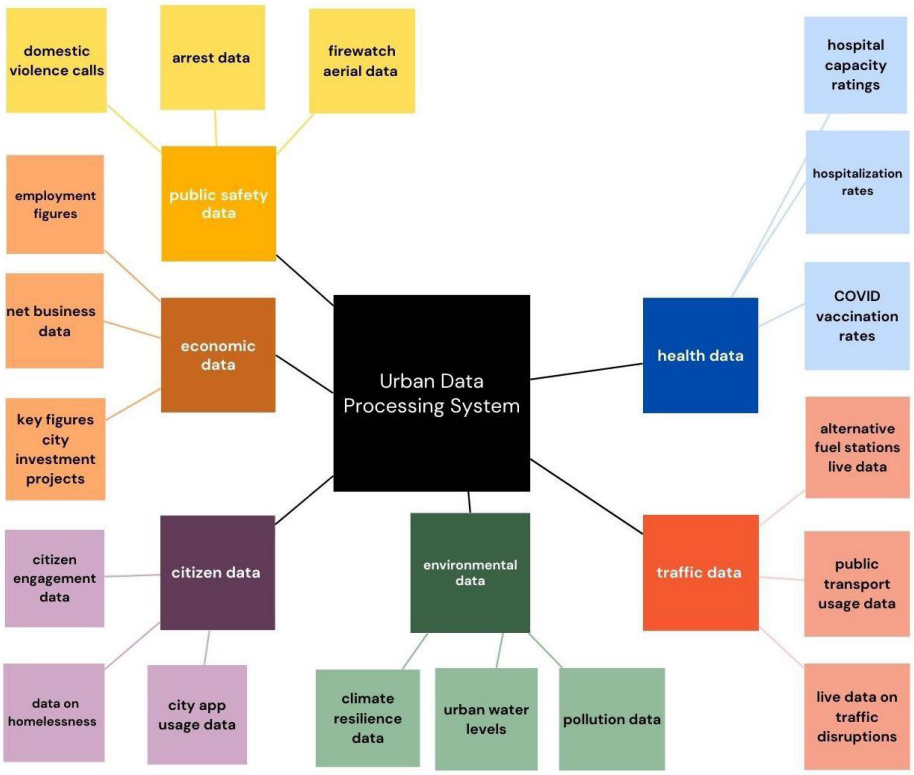


Figure 2 Exemplary presentation of different data sectors and corresponding data types produced in smart cities (developed by the authors).

sions (cf. Bundesministerium des Innern und für Heimat, 2012). Thus, data sectors are often directly connected to specific policy domains. The scope and priority of these domains (and of the associated data sectors) depend on the chosen narrative of the city.

Even though generating data in smart cities may be common practice by now, using it can be challenging. To be ready for interpretation by experts, researchers, or policymakers, these masses of data must be processed—which means *integrating* and *aggregating* the data and combining it with already existing data (Bischof et al., 2014). Integrating data means bringing together data from different sources, such as different sensors or cameras, into a single system or platform. Aggregating data, on the other hand, means summarizing or combining data into a more manageable form. This can, for example, mean grouping data based on specific criteria, such as time periods, geographic regions, or demographics.

However, processing the different sorts of data for city management and decision-making is only the first step in a complex challenge. In the next section, we show that the variety of sectors and types of big data involved creates many problems and thus results in what we call an urban "data mess" in smart cities – which cannot be dealt with from one single perspective.

What is the Problem With Disciplinarity When Looking at Smart City Data?

A symptom of the data mess is that big city data is often not used effectively (Hashem et al., 2016). This can lead to insufficient policy making, like a city recording traffic data, but failing to use it to improve traffic light circuits. While investigating such failures, researchers find that tackling the 3 Vs is often unsuccessful. Smart city data comes in huge volumes and is also varied in terms of type (e.g., traffic, weather, noise, and pollution data), source

(e.g., different types of sensors, meters, etc.), and quality. Furthermore, such data is produced in different velocities, which range on a scale from static (only ever updated manually) to dynamic (continuously and automatically updated), can be provided in differing measurement units or formats, and may differ in structure (Osman, 2019; Bischof et al., 2014).

In addition to these challenges, the often fragmented structure of city governments with its many boards, departments, commissions, and bureaus leads to a large number of data silos that have to be re-connected within the structure of a citywide data catalog.[2] Examples of this problem can be seen in city-based data repositories, often called *urban data platforms,* where streams from different data sectors are collected and oftentimes only loosely structured by several non-standardized topics, categories, or formats[3]. Due to the diverse set of stakeholders involved in city politics, data-related expertise often remains scattered. There often is no exchange across *disciplines* (i.e., areas of expertise, such as sociology, politics, environmental studies, computer science, biology, etc.) due to a certain historical preference for *disciplinarity*, meaning a focus on a specific order of knowledge (discipline), where people share a common language, specific theories, and methods and, in turn, a focused and thus limited scope.

Within the context of big data and smart cities, this means that somebody trained in data science, for example, could have the expertise to handle environmental data from a technical point of view but would need the domain expertise of meteorologists, environmental engineers, and others to interpret these data. In turn, for acting upon the insights gained, there would be a need to interact with politicians and/or citizens to put the data to beneficial use. Also, some interactions between different issues (e.g., environmental problems arising from economic issues) might not be visible if only looked at from one specific disciplinary viewpoint. Thus, cooperation between several different disciplines is necessary to cover all the experience, interests, and skills needed to gain a complete overview (and to know what to do with it). Otherwise, urban innovations, interventions, and scientific studies will be limited to a small fraction of the technological, social, and political issues that arise from current narratives of smart city development.

How Can Interdisciplinarity Help to Deal With the Data Mess?

Interdisciplinarity, understood as the integration of methods and knowledge from various disciplines by combining different approaches (Stember, 1991), is an important lead for understanding the diversity of data and the complexity of smart cities. By bringing in diverse experts, more complex situations and challenges, such as the management of urban data, can be tackled (Lemos & Morehouse, 2005).

To assemble an adequately interdisciplinary team that can make sense of a city's data mess, a potential approach is to map the different data types that a smart city needs and/or produces and start from there to identify the expertise needed to effectively develop the project. In this regard, an overview as presented in Figure 2 can be a starting point that shows that some of the necessary experts can come from various disciplines, such as public safety, public health, data science, traffic management, environmental studies, social sciences, etc. An additional asset in covering diverse backgrounds and views for navigating smart city projects can be interdisciplinary persons whose backgrounds already lie at the intersection of disciplines, such as computational planning, feminist geography, and

2 The Los Angeles strategy, for example, envisions the central data repository as the "LA Data Lake" (Ross, 2020, p. 24).

3 These catalogs can provide an (incomplete) overview. Many cities or regional networks develop their own versions of open data access points (two examples: City of Los Angeles: https://data.lacity.org, Ruhr region: https://opendata.ruhr).

> ***Cooperation between several different disciplines is necessary to cover all the experience, interests, and skills needed to gain a complete overview.***

philosophy of technology, for example.

The most important argument for getting people with different backgrounds to work together is that smart cities can only be completely understood when seen from a *socio-technical* perspective. Smart cities cannot be seen from a purely technical standpoint, but also need to be looked at from a social one – cities are social spaces that are inhabited by (inherently social) human beings, after all. The technical view might focus on the practical implementation of new technologies, such as sensors or transportation schemes. Meanwhile, the social view includes the needs and challenges of the city's inhabitants, potential (non-technical) solutions, and the effects that new technologies have on citizens. To see both sides, smart city developers and researchers need to assemble teams that include experts from both social and technical sciences, e.g., from sociology, philosophy, psychology, political science, urban planning, engineering, economics, computer science, and others. For an interdisciplinary project, it is crucial to create a space for dialogue and collaboration among experts from different sides. That way, smart city development can, for example, produce technical solutions for social problems (cf. Trencher, 2019).

Finally, smart city research and development should include the interaction with city decision-makers (i.e., city officials; for implementing changes in practice) as well as the perspectives of the general public (i.e., citizens; for feedback and information). This very broad concept of interdisciplinarity includes different skills and expertise in a cooperative and socio-technical view by assembling diverse teams in line with the different kinds of data as well as bringing in political decision-makers and involving the general public.

One illustrative example for the implementation of interdisciplinary cooperation in smart city contexts is a recent project from the city of Los Angeles that was created during the COVID-19 pandemic, which we will present in the next section.

Example: Making Sense of Pandemic Data in Los Angeles

The case of Los Angeles is instructive, as the city made use of a broad array of accessible data to inform decision-makers while developing strategies to overcome the challenges of the COVID-19 pandemic and the resulting shutdown of large parts of the city. By pooling data from various sectors, the *Los Angeles Data Team* created a *Pandemic Recovery Dashboard* with datasets from four categories regarded central for a swift recovery from the crisis: COVID, crime, economy, and homelessness[4]. Figure 3 displays the extraction of pandemic-related datasets from the LA data catalog.

Los Angeles' *Pandemic Recovery Dashboard* shows a multi-domain approach seeking to integrate a diverse set of data and the accompanying expertise. To combine the information, domain-specific expertise had to be connected across several data sectors. The backbone was the cooperation of the Los Angeles Department of City Planning and the Information Technology Agency. Setting up a repository for city data (*Open Data Portal*) and a public platform for geospatial data (*GeoHub)* improved cooperation across administrative sections. Directly working under the mayor[5], the *Los Angeles Innovation Team* developed new ideas, infrastructures, and processes for civic design. Ideation sessions hosted by the team brought together civil servants from different departments, elected officials, and external partners like designers, urban planners, and

4 The dashboard data is published at https://data.lacity.org/stories/s/afkw-g9zz (accessed January 23, 2023).

5 The *Los Angeles Innovation Team* served under mayor Eric Garcetti (2013-2022) as an example for modernizing urban politics. The unit was not continued under the new mayor Karen Bass.

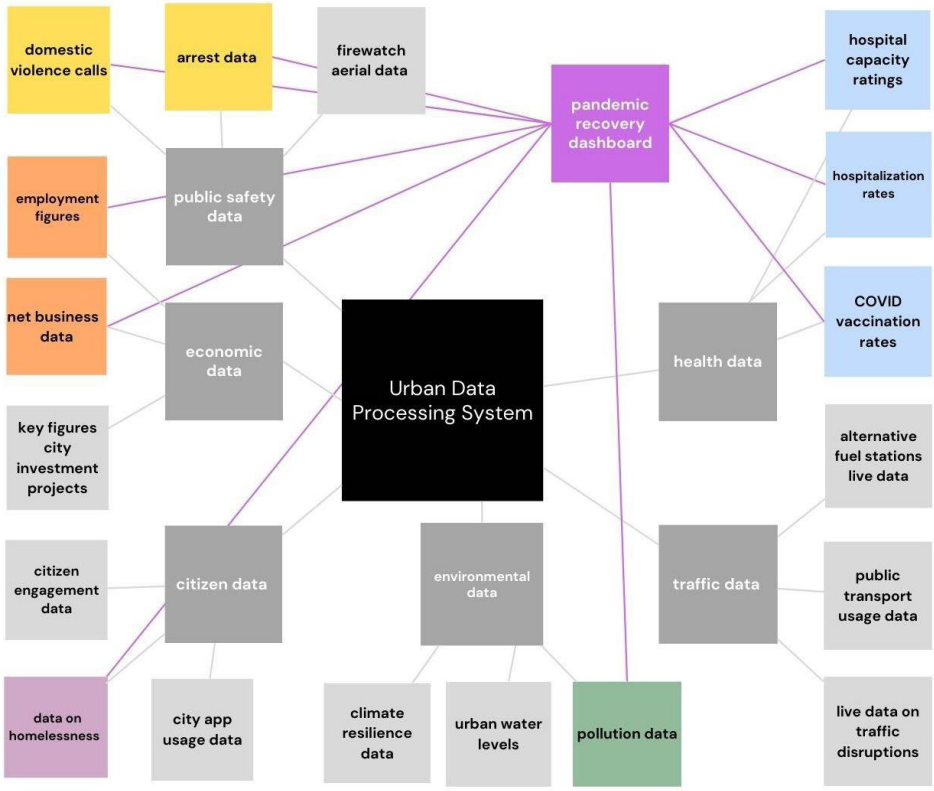


Figure 3 Sources for the Pandemic Recovery Dashboard within the Los Angeles Data Catalog (developed by the authors). Extracted data is shown in colors.

software developers. Among other projects, the team was responsible for the Daily *Los Angeles COVID-19 Data Summary* by connecting various sources from the city government with material from departments of the surrounding Los Angeles county structures. By using forms of online storytelling, Los Angeles' digital COVID-19 response connected the administrative efforts to the broader public. Publishing data-driven articles about crime trends in the city (Zhong et al. 2022) or a "story map" on the efficiency of the rental assistance program (Alcazar & Zavala, 2021) emphasized the possibilities of interdisciplinary cooperation. Nevertheless, projects like the *Pandemic Recovery Dashboard* remain somewhat incomplete by not making use of all the datasets available due to limited resources or the experimental status of new, inter-divisional teams.

Cooperation Beats Data Mess

In this article, we have argued that interdisciplinary cooperation should be a main approach both when studying smart cities and when developing them in practice – and that it could be helpful to shift the public debate about smart cities towards a more socio-technical perspective. Bringing in the expertise of diverse disciplines to the creation and study of smart cities allows for a better understanding and utilization of the data gathered in urban environments. Future research should explore how interdisciplinary cooperation can be effectively achieved to deal with the smart cities' data mess and how interdisciplinary cooperation in smart cities can be related to policy and practical implications. As of now, we conclude that interdisciplinary cooperation has the potential to benefit everyone involved in the process of handling the "big data mess" of smart cities – be it researchers, city planners, or city residents.

References

Alcazar, I., & Zavala, S. (2021, August 16). *ERAP evaluation. Evaluation phase 1 of the Emergency Rental Assistance Program*. Los Angeles Department of Housing. Retrieved August 31, 2023, from https://storymaps.arcgis.com/stories/0c59272161634bc69f3e0dd077fcf41b

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications, 6*(1). https://doi.org/10.1186/s13174-015-0041-5

Aoun, C. (2013). *The smart city cornerstone: Urban efficiency. Schneider Electric White Paper.*

Bischof, S., Karapantelakis, A., Nechifor, C.-S., Sheth, A. P., Mileo, A., & Barnaghi, P. (2014). *Semantic modeling of smart city data.*

Bundesministerium des Innern und für Heimat (2012). *Open government data Deutschland*. BMI.

Flyverbom, M., & Madsen, A. K. (2015). Sorting data out: Unpacking big data value chains and algorithmic knowledge production. In F. Süssenguth (Ed.), *Die Gesellschaft der Daten: Über die digitale Transformation der sozialen Ordnung* (pp. 123–144). Transcript.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management, 36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Kitchin, R. (2014). Making sense of smart cities: Addressing present shortcomings. *Cambridge Journal of Regions, Economy, and Society, 8*(1), 131–136. https://doi.org/10.1093/cjres/rsu027

Kitchin, R., & Dodge, M. (2011). *Code/Space: Software and everyday life*. MIT Press.

Laney, D. (2001). *3D data management: Controlling data volume, velocity, and variety*. Meta Group.

Lemos, M. C., & Morehouse, B. J. (2005). The co-production of science and policy in integrated climate assessments. *Global Environmental Change, 15*(1), 57–68. https://doi.org/10.1016/j.gloenvcha.2004.09.004

Osman, A. M. S. (2019). A novel big data analytics framework for smart cities. *Future Generation Computer Systems, 91*, 620–633. https://doi.org/10.1016/j.future.2018.06.046

Ross, T. (2020). *SmartLA 2028. Technology for a better Los Angeles*. Los Angeles. https://ita.lacity.org/sites/g/files/wph1626/files/2021-05/SmartLA2028%20-%20Smart%20City%20Strategy.pdf

Stember, M. (1991). Advancing the social sciences through the interdisciplinary enterprise. *The Social Science Journal, 28*(1), 1–14. https://doi.org/10.1016/0362-3319(91)90040-B

Trencher, G. (2019). Towards the smart city 2.0: Empirical evidence of using smartness as a tool for tackling social challenges. *Technological Forecasting and Social Change, 142*, 117–128. https://doi.org/10.1016/j.techfore.2018.07.033

Zhong, J., Gui H., Kotamreddy, H., Lew, A., Sherzai, A. (2022, October 4): A data-driven exploration of crime trends in Los Angeles. *DataLA*. https://medium.com/datala/a-data-driven-exploration-of-crime-trends-in-los-angeles-6124c2980eda

Niklas Frechen

Center for Advanced Internet Studies (CAIS)

E-Mail niklas.frechen@cais-research.de

Niklas Frechen is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany. He has a background in cognitive psychology and linguistics and is currently focusing on the need for analog in a digitalized world.

Pauline Heger

Center for Advanced Internet Studies (CAIS)

E-Mail pauline.heger@cais-research.de

Pauline Heger is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany, with a background in communication science. Her research focuses on social diffusion of innovation, sustainable technologies, and HCI.

Christoph Bieber

Center for Advanced Internet Studies (CAIS)

E-Mail christoph.bieber@cais-research.de

Christoph Bieber is a research professor at the Center for Advanced Internet Studies (CAIS) and a political scientist at the University of Duisburg-Essen. He leads the research program Digital Democratic Innovations.

Mennatullah Hendawy

Center for Advanced Internet Studies (CAIS)

E-Mail mennatullah.hendawy@cais-research.de

Mennatullah Hendawy is an interdisciplinary urban planner working on cities and technology towards equity and sustainability. She is a Postdoc at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany, and an Assistant Professor at Ain Shams University in Cairo, Egypt.

Published by

GESIS – Leibniz Institute for the Social Sciences
Knowledge Exchange & Outreach (KEO)
Unter Sachsenhausen 6-8
50667 Cologne
easy@gesis.org · www.gesis.org/easy

***easy* Editors**

Dr. Johannes Breuer, Dr. Philip Jost Janßen,
Dr. Lydia Repke, Dr. Sophie Zervos

Editorial Office

Dr. Philip Jost Janßen (Team Publications)
Dr. Sophie Zervos (Team CommuniCation & Transfer)

Layout

Bettina Zacharias

GESIS is member of the Leibniz Association

ISSN 2749-2850 (Online)