Privacy Paranoia: Wie die Erzählung einer Privatheitsparanoia Arme und Reiche scheidet

Anastassija Kostan

Zusammenfassung

Der *digital privacy divide* setzt gesellschaftlich marginalisierte Gruppen wie Ältere, Frauen*, Menschen mit Be_hinderung und einem niedrigen sozioökonomischen Status in verschiedener Weise Vulnerabilitäten in Bezug auf ihre digitale Privatheit aus. Der Beitrag präsentiert Ergebnisse einer explorativen Interviewstudie mit 17 als reich und 28 als arm geltenden Technologienutzer*innen. Erörtert wird, wie das Narrativ einer „Privacy Paranoia" die digitale Kluft zwischen Technologienutzer*innen mit einem hohem und niedrigem Einkommen vertieft, indem es ersteren dabei hilft, ihre privaten Daten umfassend zu schützen, während es letztere daran hindert, sich mit Fragen der digitalen Privatheit zu befassen, für sie befriedigende Schutzstrategien zu entwickeln und umzusetzen.

1. Einleitung

Digitale Privatheit wird zunehmend als ein zentrales Element sozialer Macht- und Ungleichheitsstrukturen aufgefasst (Sevignani 2016; Park 2021; Büchi u. a. 2021; Wäffler 2024). Die lange unter dem Label *privacy paradox* vorausgesetzte Responsibilisierung der*s einzelnen Technologienutzer:in für den Schutz der eigenen digitalen Privatheit geht zunehmend in systemischeren Perspektiven auf (Adjerid u. a. 2018). Diskutiert wird etwa, ob im „Überwachungskapitalismus" (Zuboff 2018; Voß 2020) die*der einzelne User:in überhaupt Verantwortung übernehmen *kann* für die eigene digitale Privatheit (Lamla/Ochs 2019) oder ob auch hier der vielbesprochene *digital divide* greift (Redmiles u. a. 2017; Frik u. a. 2022; Alhazmi u. a. 2022). Demnach gibt es mehrere Ebenen digitaler Ungleichheiten, eine sogenannte „digitale Kluft" zwischen Personengruppen hinsichtlich des Zugangs zu Alltagstechnologie, der Fähigkeiten mit dieser umzugehen und der durch

die Technologienutzung erzielten Ergebnisse und erlangten Auswirkungen (van Dijk 2017).

Neuerdings werden auch verschiedene Aspekte eines *online privacy divide* untersucht (Wang/Metzger 2024) und der Einfluss ‚klassischer' Ungleichheitskategorien wie des Geschlechts, Alters, von Be_hinderung und sozioökonomischem Status auf digitale Privatheit herausgearbeitet (Redmiles 2018; Epstein/Quinn 2020; Dutton u. a. 2022; Brand u. a. 2024), woran dieser Beitrag anknüpft.Anhand von Ergebnissen einer explorativen Interviewstudie mit 45 Technologienutzer:innen, die über ein so hohes bzw. niedriges monatliches Einkommen verfügen, dass sie gemessen an der OECD Nettoäquivalenzeinkommen Skala[1] als reich (n=17)[2] oder arm (n=28)[3] gelten, präsentiert dieser Beitrag einkommensrelevante Ungleichheiten in Bezug auf digitale Privatheit auf drei Ebenen: Auf der Ebene der Bedeutsamkeit, welche die Interviewten ihren privaten Daten zusprechen, des Grads ihrer Informiertheit über digitale Privatheit sowie auf der Ebene ihrer alltäglichen Privatheitspraktiken. Besonders deutlich hervor traten diese Ungleichheiten in der Art und Weise, wie die Interviewten das Narrativ einer „Privacy Paranoia" mobilisierten, um ihre Erfahrungen, Probleme und Strategien mit digitaler Privatheit zu rahmen und einzuordnen. Während den Interviewfragen aufgrund der Polysemie des Privatheitsbegriffs

1 „Nach der modifizierten OECD-Skala, die bei der Erhebung über Einkommen und Lebensbedingungen (EU-SILC) angewendet wird, erhält die erste erwachsene Person stets das Gewicht 1. Alle übrigen Haushaltsmitglieder von 14 Jahren und älter erhalten das Gewicht 0,5 und Kinder unter 14 Jahren das Gewicht 0,3. Ein Paar mit 2 Kindern unter 14 Jahren hätte daher bei einem verfügbaren Einkommen von 4500 Euro monatlich ein Äquivalenzeinkommen von 2142,86 Euro (4500/ (1,0+0,5+2*0,3) = 2142,86). Die wirtschaftliche Leistungsfähigkeit einer alleinlebenden Person mit einem Einkommen von 2142,86 Euro würde diesem Haushalt als gleichwertig angesehen werden" ((Netto-)Äquivalenzeinkommen, Statistisches Bundesamt: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Glossar/aequivalenzeinkommen_mz-silc.html, abgerufen am 12.12.2025).

2 „Reichtumsgrenzen dienen der Messung des Einkommensreichtums. In einem Haushalt, dessen Nettohaushaltseinkommen über der Reichtumsgrenze liegt, werden alle Haushaltsmitglieder als reich betrachtet. Oftmals wird die Grenze für den Einkommensreichtum bei 200 Prozent des mittleren bedarfsgewichteten Einkommens der Bevölkerung in Privathaushalten angesetzt" (WSI Verteilungsmonitor: Reichtumsgrenzen nach Haushaltstyp. https://www.wsi.de/de/reichtum-15099-reichtumsgrenzen-in-deutschland-15189.htm, abgerufen am 12.12.2025).

3 „Nach dem von der EU gesetzten Standard liegt die Armutsgrenze bei 60 Prozent des mittleren bedarfsgewichteten Einkommens der Bevölkerung in Privathaushalten" (WSI Verteilungsmonitor: Armutsgrenzen nach Haushaltstypen. https://www.wsi.de/de/armut-14596-armutsgrenzen-nach-haushaltsgroesse-15197.htm, abgerufen am 12.12.2025).

(Ochs 2019: 14; Pohle 2022: 24-25) absichtlich keine finite Definition von (digitaler) Privatheit zugrunde gelegt wurde, damit die Interviewten mit hohem und niedrigem Einkommen ihre eigenen Bilder und Auffassungen entfalten konnten, nutzten sie das Narrativ einer Privatheitsparanoia als eine Art Seismograph oder Gradmesser für die aus ihrer Sicht richtige Weise, mit digitaler Privatheit umzugehen und sich angemessen um ihre digitale Privatheit zu sorgen.[4] Ähnlich wie in aktuellen Mediendiskursen setzten sich die Interviewten mithilfe des „Privacy Paranoia" Narrativs damit auseinander, wann Sorgen um die digitale Privatheit angebracht sind und wann diese möglicherweise übertrieben ‚paranoid' sein könnten (etwa BBC News 2012; Forbes 2016) und positionierten sich im Rückgriff auf das „Privacy Paranoia" Narrativ auf einem Spektrum zwischen einer überzogenen Angst und einem naiv-nachsichtigen Verhältnis zu digitaler Privatheit.

Die verschiedenen Gebräuche des Narrativs der Interviewgruppe mit hohem und niedrigem Einkommen tragen – so das Argument dieses Beitrages – entscheidend zu einem digitalen *privacy divide* bei, vor allem im Hinblick auf die Konsequenzen und Ergebnisse ihres Umgangs mit Alltagstechnologie (vgl. Scheerder u. a. 2017; van Deursen u. a. 2017), welcher sich durch fundamental unterschiedliche Einstellungen und Haltungen äußert, die die Technologienutzer*innen mit niedrigem und hohem Einkommen unter Rückgriff auf das Narrativ einer Privatheitsparanioa einnehmen: So ist für die als arm geltende Nutzer*innengruppe die Haltung einer ‚antiparanoiden' oder ‚pragmatischen' Sorglosigkeit (vgl. Calmbach u. a. 2016: 195) charakteristisch, mit welcher sie die Tatsache beantworten, dass ihnen oft die finanziellen Mittel dazu fehlen, ihre digitale Privatheit in einem für sie befriedigenden Maße zu schützen. Dagegen richten sich die Interviewten mit hohem Einkommen nach dem Bild einer ‚abgeklärten' oder ‚vernünftigen' Paranoia aus (vgl. Paton-Simpson 2000). Diese äußert sich in deren Bemühen, möglichst immer und möglichst alles in ihrer Macht Stehende zum Schutz ihrer digitalen Privatheit zu unternehmen und dafür auch alle notwendigen Ressourcen zu mobilisieren.

4 Eine angemessene Haltung gegenüber der eigenen digitalen Privatheit und die richtige Privatheitspraxis im Alltag zu entwickeln, wurde häufig als eine Herausforderung beschrieben, welcher die Interviewten mit dem Narrativ der Privatheitsparanaoia begegneten. Zur sinnstiftenden Bedeutung von Narrativen im Umgang mit gesellschaftlichen Herausforderungen siehe Baader/Koch 2025.

2. Die Bedeutsamkeit privater Daten

Die Technologienutzer:innen mit niedrigem und hohem Einkommen messen ihren privaten Daten einen unterschiedlich wichtigen Stellenwert bei. Allein schon wegen der von ihnen genutzten Hardware stellen sich die Interviewten mit niedrigem Einkommen auf regelmäßigen Datenverlust ein. Ihre häufig gebraucht gekauften oder von Freund:innen und Verwandten übernommenen Geräte sind in der Regel so alt, dass sie nur unzuverlässig oder eingeschränkt funktionsfähig sind und jeden Moment schadhaft zu werden drohen. Die Interviewten finden sich damit ab, dass ihnen deshalb jederzeit wichtige und private Daten verloren gehen können, denn eine Reparatur oder ein Ersatz kommt aufgrund ihrer finanziellen Situation nicht infrage. P24 etwa beschreibt: „Also mir ist ein Rechner kaputtgegangen und ich hätte viel Geld dafür bezahlen müssen, die Daten wiederzuholen und dann waren sie weg" (P24). Dass Daten verloren gehen, gehört zu ihrem Alltag mit Technologie dazu, deshalb ist Datenverlust in dieser Gruppe nichts, das man fürchtet und zu verhindern sucht, sondern eher eine Realität, mit der man rechnet. Ihre Haltung einer ‚antiparanoiden' oder ‚pragmatischen' Sorglosigkeit äußert sich darin, dass sich die Interviewten mit der stets vorhandenen Möglichkeit des dauerhaften Datenverlusts einfach abfinden und berichten, es sei gar „nicht so schlimm" (P13), wenn ihre privaten Daten mal abhandenkommen. Sie „leben" dann „einfach weiter" (P14), ohne etwas Bestimmtes zu unternehmen, um die Daten zurück zu bekommen oder in Zukunft besser abzusichern.

Darüber hinaus beeinflusst die Akzeptanz möglichen Datenverlusts auch ihre generelle Einstellung zu Alltagstechnologie, die, wie P25 beschreibt, von Bedenken und Skepsis geprägt ist: „Ich hatte auch schon Laptops, die so plötzlich kaputt waren, wo all meine Bilder und Daten weg waren. Und da ich halt solche Erfahrungen gemacht habe, möchte ich mich sozusagen nicht auf die Technik verlassen" (P25). Trotzdem wollen Technologienutzer:innen mit niedrigem Einkommen selbst für sie besonders wichtige und private Daten wie Finanzdaten nicht besser oder stärker als andere Datentypen schützen. Es gebe bei ihnen ohnehin nicht viel oder gar „nichts zu holen" (P5) – weder an „brisanten" (Finanz-)Informationen (P2) noch an Geldwerten. So äußern sie wiederholt die Überzeugung, kein attraktives Angriffsziel darzustellen. Weil sie es nicht für sehr wahrscheinlich halten, dass jemand Unbefugtes Interesse an ihren (Finanz-)Daten haben könnte, sorgen sie sich auch nicht besonders darum, diese zu schützen. Es ist vielen Interviewten aus dieser Gruppe lieber, sich wenigstens vorzumachen, sicher

zu sein (P1, P20) als „in so paranoide Verschwörungstheorien" abzudriften (P11). P11 etwa argumentiert: „Ich glaube, ich halte es einfach für sehr unwahrscheinlich, dass sich jemand letztlich wirklich für meine Daten jetzt interessieren könnte. Und deswegen bin ich da, glaube ich, so ein bisschen nachlässiger als andere Personen" (P11). Die Angst vor einer übermäßigen Privatheitsparanaoia überwiegt hier der Sorge vor potenziellen Angriffen und Datenverlust.

Dies hängt unter anderem damit zusammen, dass die Interviewten mit niedrigem Einkommen nicht abschließend für sich einschätzen können, welche Bedrohungsszenarien überzogen und welche realistisch sind oder aber auch bei welchen es sich schlicht um Falschinformation handelt. So wägt etwa P14 im Interview ab: „Ist es tatsächlich so, dass die Algorithmen manipulierbar sind, dass man dann quasi Content geteilt bekommt, der eben auch nicht wahr ist oder einen dann in eine gewisse Richtung lenkt? Und das klingt dann teilweise manchmal so ein bisschen paranoid oder quasi verschwörungslastig, aber das mit Cambridge Analytica z.B. war eben einfach die Wahrheit" (P14). Auch fällt es ihnen schwer, Erzählungen aus dem Bekannten- und Freundeskreis sinnvoll einzuordnen und zum Beispiel Übertreibungen als solche zu identifizieren und von echten Risiken abzugrenzen. P3 ist sich zum Beispiel unsicher: „Bei manchen [Freund:innen; AK] denke ich mir, ihr seid ein bisschen paranoid, aber auf der anderen Seite haben sie vielleicht auch einfach Recht" (P3). Ihr Unvermögen, tatsächlich existierende oder aus den Medien oder vom Hörensagen wahrgenommene Privatheitsrisiken richtig einzuschätzen übersetzen sie in die Absicht, sich während der Nutzung ihrer Alltagstechnologie nicht zu viele Gedanken um digitale Privatheit zu machen, obwohl ihnen eigentlich klar ist, dass sie gar nicht so recht wissen, ob und inwieweit diese Haltung Sinn macht und gut für sie ist. P9 beschreibt dies etwa folgendermaßen: „also, ich mache einfach alles, aber denke nicht so viel über die Konsequenzen nach. Ich habe nicht das Gefühl, dass die Konsequenzen schlimm wären. Aber ob das Gefühl richtig ist, keine Ahnung" (P9).

Die Interviewten mit hohem Einkommen hingegen bewerten grundsätzlich alle ihre Daten als sehr wichtig, privat und schutzwürdig. Fragen der Sicherheit und Privatheit beschränken sich in dieser Gruppe nicht auf das Digitale, sondern erstreckt sich ihr Bedürfnis nach Privatheit und Sicherheit über alle Lebensbereiche. P6 etwa zählt auf:

> Ich möchte ein sicheres Auto fahren, ich lege Daten sicher ab, ich verwende sichere Passwörter. [...] Ich prüfe regelmäßig meine Kreditkarten-

> abrechnung auf Unregelmäßigkeiten. Ich zahle sehr viel Geld an meinen Rechtsschutz und hoffe, dass ich in gewissen Punkten dort abgesichert bin. Wir haben das Haus mit zusätzlichen Schlössern abgesichert und haben es einbruchshemmend gemacht. (R6)

Die Haltung einer ‚abgeklärten' oder ‚vernünftigen' Paranoia in dieser Gruppe zeigt sich darin, dass sie auch die bestmögliche Sicherung und den größtmöglichen Schutz ihrer privaten Daten anstreben und dies durch eine ihrer Auffassung nach möglichst realistische Risikoabschätzung zu erreichen suchen. Sie akzeptieren die Tatsache, dass es reale Bedrohungen und Risiken gibt und sind sich bewusst, dass ihr Wissen notwendigerweise begrenzt ist und dass es keinen 100%-ige Sicherheit geben kann. So beschreibt etwa P9:

> Ich habe tatsächlich Bedenken, wenn jemand mein Smartphone finden sollte, ich verliere es oder er stiehlt es. Da ist es tatsächlich so, dass ich keine Ahnung habe, wie sicher Google wirklich ist. Ich gehe davon aus, dass man mein Smartphone sicherlich auslesen kann. Ich bin mir sicher, dass das Sicherheitsbehörden können. Wenn die das können, können das Akteure mit anderen Absichten wahrscheinlich auch. Davon muss ich ausgehen. (R9)

Sie sind wegen dieser Einschätzung auch der Meinung, alles in ihrer Macht Stehende zum Schutz ihrer privaten Daten beitragen zu müssen. Obwohl prinzipiell alle Daten privat und schützenswert für sie sind, lassen sie vor allem bei Finanzdaten eine „gesunde Vorsicht" (R10) walten und wollen keinerlei Aufmerksamkeit auf ihre Finanzen ziehen, weil ihnen dies potenziell schaden könnte. Selbst basale Informationen über ihre finanzielle Situation möchten die Interviewten mit hohem Einkommen für sich behalten: „Alles solche Dinge, wo ich der Meinung bin, dass das jetzt nicht unbedingt, ja, irgendwie von Dritten zugreifbar sein sollte, also alles, was so mit Finanzen zu tun hat, mit Steuern, mit Versicherungen und so weiter" (R13). Aus Sorge vor finanziellen oder Reputationsschäden teilen sie selbst mit engeren Freund:innen keine Informationen über ihr Geld und Vermögen (R8), geben Ehepartner:innen keinen Zugang zu Bankdaten (R14) und involvieren äußerstenfalls direkt Betroffene wie Erb:innen, Notar:innen (R3) und Steuerbehörden – und dies auch nur so weit wie unbedingt erforderlich – in ihre Finanzen. So möchte etwa R16 vermeiden, dass „die [alle anderen, AK] dann wissen, dass was bei uns zu holen wäre. Ich glaube, das wäre halt... Also wenn ich mir das vorstelle, wir sind wirklich von Hackern

angegriffen, jemand will irgendwie Ransomware-Angriff machen oder sowas. Und die sehen, wie viel Umsatz wir haben, dann wissen die natürlich auch, dass wir Umsatz in der Höhe haben" (R16). Finanzielle Angelegenheiten sowie Informationen über Besitztümer und Wertgegenstände möglichst privat zu halten, sich Sorgen darum zu machen, diese zu verlieren und sie deshalb besonders zu schützen, betrachten die Interviewten mit hohem Einkommen als völlig normal, vernünftig und angemessen. Dies ist Teil ihrer Haltung einer ‚abgeklärten' oder ‚vernünftigen' Privatheitsparanoia, die R9 folgengermaßen formuliert: „Ich glaube, dass ich mehr oder weniger, wie jeder andere Mensch, der eine Kreditkarte, EC-Karte oder ein paar Bankkonten besitzt, interessant für Kriminelle sein könnte" (R9).

3. Der Grad der Informiertheit

Die ‚abgeklärte' oder ‚vernünftige' Privatheitsparanoia äußert sich bei den als reich geltenden Technologienutzer*innen außerdem darin, dass sie stets neue Informationen heranziehen, die sie dazu befähigen sollen, auch ganz aktuelle und neu aufkommende Privatheitsrisiken ‚richtig' einzuschätzen, um ihre Schutzstrategien daran anzupassen. Viele Interviewte mit hohem Einkommen bezeichnen sich selbst als „technikaffin" (R6), „technologisch versiert" (R9) und stark „technologieinteressiert" (R1). Sie verfolgen technologische Entwicklungen ohnehin aktiv mit und informieren sich „gerne" (R10) und regelmäßig über neu auf dem Markt erscheinende Geräte, neue Software und kommende Softwareupdates. Dazu greifen sie auf für sie vertrauenswürdige Quellen und Medien zurück, für die sie teilweise bezahlen, oder haben Zeitschriften, Nachrichtenticker und Blogs abonniert, welche sie mit den neuesten Informationen versorgen. Sie konsultieren aber auch Handbücher und nehmen an Informationsveranstaltungen teil, wie etwa R11 ausführt: „Als ich mich das erste Mal über PGP-Verschlüsselung informieren wollte, gab es etwas, das war PGP für Dumme oder für Einsteiger oder Einsteigende. Ich weiß nicht, ich glaube, das war für Einsteiger. Es gibt diese Websites für alles, es gibt Workshops" (R11).

Auf dem Laufenden zu sein ist nicht nur wichtig für sie selbst, sondern teilen und diskutieren sie die neu erworbenen Informationen auch regelmäßig mit anderen: „Ich schaue Apple-Keynotes, ich schaue bei Microsoft, ob die etwas Neues ankündigen, wie zum Beispiel den Copiloten. Dann schaue ich mir an, was da los ist, um mitreden zu können" (R6). Gemeinsam mit anderen technologieinteressierten Kolleg*innen, Freund*innen

und Verwandten sprechen sie auch darüber, was für Sicherheitslücken sich bei ihnen gegebenenfalls schließen lassen, tauschen Informationen aus und helfen aber auch anderen: „Ich versuche, andere Leute darüber zu informieren, beziehungsweise zu beraten. Ich frage ab und zu nach, um mich weiter zu informieren oder ein bisschen gegen zu prüfen, was man von anderen noch mitnehmen und lernen und auch mitgeben kann" (R2). Zudem holen sich die Interviewten mit hohem Einkommen Rat von Personen, die sich auskennen und denen sie vertrauen: „Mein Schwager ist Informatiker. Ich habe mich mit ihm darüber ausgetauscht, was sicher ist, wie sicher es ist und was Sinn macht" (R7). Auf der Basis dieser Gespräche und der Informationen, die sie aus den Medien beziehen, können sie gut für sich einschätzen, ob sie ihre Daten in einem für ihre Zwecke ausreichenden Maße schützen oder ob und an welchen Stellen Nachholbedarf besteht. Außerdem fühlen sie sich auf Grundlage der ihnen verfügbaren Informationen und ihres über die Zeit angesammelten Wissens dazu befähigt, differenziert über allgemeine Sicherheitsrisiken nachzudenken und ihr persönliches Risiko dabei „realistisch" zu beurteilen (R1). Dadurch fühlen sich die Interviewten mit hohem Einkommen dazu befähigt, Falschinformationen von Berichten über echte Ereignisse zu unterscheiden.

Die Interviewten mit niedrigem Einkommen haben dagegen nicht das Gefühl, dass Informationen über Datenschutz und digitale Privatheit ihnen Strategien bieten, die sie auch ernsthaft ergreifen können würden, wenngleich im Prinzip alle nötigen Informationen auch für sie verfügbar sind. Häufig sind die vorgeschlagenen Lösungen für sie ohnehin nicht finanziell aufbringbar, was dazu führt, dass sie lieber uninformiert bleiben, ehe sie sich mit Informationen auseinandersetzen, die sie ohnehin nicht in die Realität umsetzen können. So beschreibt etwa P26 ganz anschaulich: „Ich meine, Google spuckt ja auch alles aus. Aber dafür muss ich mich mit Dingen beschäftigen, die ich mir nicht leisten kann. Und das macht mich dann traurig und darum lasse ich das." (P26). Auch der Informationsgewinn selbst ist kostspielig, wie P18 beklagt: „Es gibt kaum noch Nachrichtenseiten, die ich jetzt gerne lese, dann sind viele Artikel müssen doch bezahlt werden. Und das war ja früher auch nicht anders, aber früher hat wenigstens im Café noch die Zeitung ausgelegen und da konntest du da noch mal in die Zeitung reingucken. Also so was zum Beispiel, dass so alles so wahnsinnig teuer ist und man zahlt schon mal fürs Internet und dann muss man halt, wenn man ohne Werbung oder beziehungsweise auch gewisse Artikel lesen will, dafür auch zahlen" (P18).

Darüber hinaus stellen auch zeitliche und mentale Kapazität eine entscheidende Barriere für die Interviewten mit niedrigem Einkommen dar, sich umfassend über Fragen digitaler Privatheit zu informieren. Sie geben an, durch ihren Alltag zu stark ausgelastet zu sein, sodass gar keine weiteren Kapazitäten mehr vorhanden sind, so etwa P20: „Ich glaube, ich habe in meinem Leben so viel Stress, dass ich bevorzuge, das einfach abzuschalten, darüber nicht nachzudenken. Ich habe einfach keine Zeit, mich damit zu beschäftigen, was mein Smartphone oder mein Laptop da macht" (P20). Auch P3 kommentiert: „Ich habe dann immer 100 andere Sachen zu tun und immer 300 andere Probleme, als mich jetzt damit zu beschäftigen" (P3). Weil sich viele außerdem nicht unmittelbar bedroht fühlen, sehen sie außerdem auch „nicht so die Notwendigkeit", sich im Detail über mögliche Angriffsszenarien und Datenschutz zu informieren (P13), was wiederum dazu führt, dass ihnen Gründe unbekannt bleiben, die sie womöglich dazu motivieren würden, sich intensiver damit auseinander zu setzen. Der niedrige Informationsgrad führt also dazu, dass sie auch keine „Ambition" verspüren, sich besser zu informieren, was den Kreislauf weiter schließt. P12 erläutert beispielsweise: „Also, wenn irgendjemand sagt, das ist superwichtig, du musst das dann unbedingt machen und sonst passiert das und das und das und die machen mit deinen Daten das alles. Also wenn es so schlimm wäre, dann müssten mir die Augen geöffnet werden und dann wäre die Hemmschwelle jetzt auch nicht so groß, da Zeit zu investieren" (P12). Gerade weil sie nicht genau wissen, was für Risiken es potenziell gibt und wie sie selbst von diesen betroffen sein würden, informieren sie sich auch nur wenig. Ihre Haltung der ‚pragmatischen', ‚antiparanoiden' Sorglosigkeit greift auch hier. So berichtet etwa P9: „Ich glaube, wenn ich einmal sehen würde, zu was man Zugriff hat, dann würde ich vielleicht meine Meinung ändern. Aber das müsste man mir auch erst einmal so vorzeigen. [...] Ich glaube, ich kenne auch oder verschließe auch die Augen vor den Konsequenzen. Vielleicht würde das etwas auswirken, wenn ich das wissen würde. Aber dadurch, dass ich nicht weiß, kann man auch gut die Augen verschließen" (P09). 4.Alltägliche Privatheitspraktiken

Der hohe Grad an Informiertheit bietet den Interviewten mit hohem Einkommen eine solide Grundlage für ihre alltäglichen Datenschutzpraktiken. Sie haben den Eindruck, alle verfügbaren Informationen gesammelt, bewertet, mit anderen diskutiert und im Rahmen ihrer Haltung der ‚abgeklärten' Privatheitsparanoia realistisch eingeschätzt zu haben, wie etwa R9 veranschaulicht: „Ich bin nicht so paranoid, dass ich kein natives Android benutzen würde. Es gibt ja unter Technikexperten viele Möglichkeiten, um

wesentlich mehr zu machen in der Hinsicht. Ich vertraue etwas darauf, dass ich als relativ durchschnittlicher Anwender, der kein Millionenvermögen besitzt, nicht zu der Zielgruppe organisierter Kriminalität gehöre" (R9). Auch hier fungiert das Motiv der ‚abgeklärten' oder ‚vernünftigen' Paranoia als Richtwert für das richtige, gut überlegte und ‚realistisch' begründete Maß an ergriffenen Sicherungs- und Schutzmaßnahmen, was den Interviewten ein hohes Sicherheitsgefühl gibt. R13 etwa berichtet:

> Ja, also ich, ich habe, sagen wir mal so, ich habe ein recht gutes Gefühl, dass das, was möglich ist, dass ich das gemacht habe und dass es für meine Belange oder Schutzbedarf eigentlich so weit reicht. Also für das, was man so privat machen kann, glaube ich, bin ich ganz gut aufgestellt. (R13)

Dazu gehört es für die Interviewten mit hohem Einkommen präventive Maßnahmen auf Basis ihrer umfassenden Informiertheit und ‚realistischen' Einschätzung zu ergreifen, wie P14 angibt: „Ich tue im Vorfeld alles, was ich weiß, muss man sagen. Ich weiß ja auch nicht alles. Aber da, wo ich weiß, ich sollte und muss mich schützen, da tue ich mein Möglichstes, um das zu tun" (R14). Zum Beispiel haben viele „so etwas Ähnliches wie eine Worst-Case-Vorbereitung" für den Fall eines Angriffs (R6), oder sie sichern sich schon im Vorfeld durch verschiedene Strategien ab, um es gar nicht erst zu einem Angriff oder Datenverlust kommen zu lassen: „Ich habe großen Respekt davor und habe mir in der Vergangenheit dazu Gedanken gemacht. Bestimmte Daten habe ich auf mehreren Instanzen, auf Festplatten oder auch online verfügbar. Falls etwas wäre, habe ich eine Absicherung" (R2).

Zu deren Strategien gehört es nicht nur, regelmäßig Backups auf mehreren Geräten zu machen: „Mindestens einmal im Monat mache ich eine Sicherheitskopie von meinem Desktop, an dem ich immer arbeite, und übertrage die Daten auf meinen Stick und vom Stick auf den Laptop. Ich habe drei Sicherheitskopien" (R4). Auch bezahlen sie für „Schutz-Software" (R15) und nutzen neben Backup-Hardware noch zusätzliche Cloud Services, denen sie vertrauen und für die sie ebenfalls extra zahlen (R1; R8). Einige Interviewte mit hohem Einkommen haben sogar eine eigene Cloud eingerichtet (R2).

Da es ohnehin zu ihrem Alltag gehört, neue Geräte, Anwendungen und Apps auszuprobieren, mit Technologie „herumzuexperimentieren" (R6) oder „herumzuspielen" (R1), sehen sie es auch weniger als eine lästige Pflicht und mehr als eine willkommene, spielerische Herausforderung an, eine möglichst tragfähige Sicherheitsinfrastruktur aufzubauen und diese

aufrecht zu erhalten. Sie fühlen sich in ihren Schutzpraktiken und Sicherheitsmechanismen bestätigt, so lange kein Angriff stattfindet oder etwas Unerwünschtes passiert. P14 beschreibt zum Beispiel: „ich merke aber natürlich nur dann, dass es funktioniert hat, wenn ich nicht angegriffen werde. Wenn ich also nicht beklaut werde, wenn ich nicht bloßgestellt werde. Das ist bis jetzt noch nicht passiert, kann aber jederzeit passieren. Braucht man sich ja nichts vormachen. Ja, die absolute Sicherheit gibt es halt nicht. Ich fühle mich aber, wie gesagt, dadurch, dass ich im Vorfeld mir Gedanken gemacht habe und meine Möglichkeiten ausschöpfe, fühle ich mich doch relativ sicher" (R14).

Ähnlich geben auch die Interviewten mit niedrigem Einkommen an, in Vergangenheit eher wenig Situationen erlebt zu haben, in denen sie sich unsicher oder bedroht gefühlt hatten. Diesen vorgeblichen[5] Mangel an negativen Erfahrungen werten sie allerdings nicht im Sinne einer Bestätigung dafür, dass sie ihre privaten Daten im Großen und Ganzen angemessen schützen und dabei vieles ‚richtig' machen. Vielmehr ist er ein Anlass, untätig zu bleiben. Die Interviewten mit niedrigem Einkommen berichten, dass sie sich so lange sicher fühlen werden, bis einmal etwas passiert. Ansonsten nehmen sie keine Notwendigkeit wahr, aktiv zu werden. Diese Facette ihrer ‚antiparanoiden' und ‚pragmatischen' Sorglosigkeit beschreibt P13 treffend: „Ich denke mir, wenn es so weit kommen würde, dann würde ich vielleicht anders darüber denken. Aber dadurch, dass ich halt bis jetzt keine negativen Erfahrungen hatte und auch positiv bin, dass es so bleibt, habe ich nicht so das Gefühl, dass mich das stört" (P13).

Entsprechend haben die Interviewten mit niedrigem Einkommen auch „keine besonderen Sicherheitsmechanismen" (P2). Allerdings nicht allein, weil sie keine erkennbaren Probleme wahrnehmen, sondern auch, weil sie sich oft selbst rudimentäre Schutz- und Sicherungsmaßnahmen finanziell nicht leisten können. Selbst basaler Virenschutz kann eine Belastung darstellen, wie etwa P28 berichtet: „Wenn man vollen Schutz haben möchte, muss man da ja auch wieder ein Virenschutz Programm oder sowas installieren. Das kostet dann wieder extra" (P28). Auch P12 berichtet aus Geldmangel keinen VPN-Server mehr zu nutzen, obwohl dieser einst Teil von dessen Sicherungspraxis war: „Ich hatte mal VPN und so weiter. Damit

5 Interessanterweise können viele Interviewte mit niedrigem Einkommen auf Nachfrage dann doch von Situationen berichten, in denen sie relativ hohen finanziellen Schaden genommen haben oder persönliche Bedrohungen durch das Publikwerden ihrer privaten Daten erfahren hatten, worauf in diesem Beitrag aus Platzgründen allerdings nicht weiter eingegangen wird.

ich nicht getracked werden kann und damit meine IP nicht freigegeben wird und so weiter. Also ich habe es mittlerweile nicht mehr, weil es mir zu teuer ist“ (P12). Ähnlich gibt P26 an: „einfach mal eine neue Grafikkarte, das kann man nicht eben stemmen. Und wenn man sich die Preise anguckt, dann will man das auch nicht“ (P26). Danach befragt, was sie im Falle eines Angriffs oder einer heiklen Situation tun würden, antworten sie, dass sie erst dann nach passenden Informationen suchen würden, um ad-hoc auf die Situation zu reagieren. P6 etwa erklärt:

> Es kommt drauf an, wenn jetzt mal PayPal irgendwie rausgefunden wird oder so was. Da würde ich schon so ein bisschen mehr recherchieren, was ich dann zu tun hätte, aber auch alles dann erst, wenn es passiert ist. Jetzt habe ich keine wirkliche Ahnung, erst wenn was Schlimmes passiert ist, dann werde ich mich damit befassen. (P6)

Die ‚antiparanoide‘ Sorglosigkeit der Interviewten mit niedrigen Einkommen kann also auch als Antwort auf die aus finanziellen Gründen für sie unerreichbaren Schutzmöglichkeiten gewertet werden, was der Responsibilisierung einzelner Technologienutzer*innen widerspricht.

5. Schlusskommentar

Der *privacy divide* zwischen Technologienutzer:innen mit hohem und niedrigem Einkommen vertieft sich mit den im Beitrag herausgearbeiteten unterschiedlichen Verwendungen des Narrativs einer Privatheitsparanoia, welche auf die Bedeutsamkeit privater Daten, den Grad der Informiertheit und die alltäglichen Privatheitspraktiken einwirken. Das präsentierte Interviewmaterial zeigt, wie Technologienutzer:innen mit hohem Einkommen unter Rückgriff auf das Privatheitsparanoia-Narrativ mit der Haltung einer ‚abgeklärten‘ und ‚vernünftigen‘ Paranoia den eigenen Daten einen hohen Wert zusprechen, sich umfassend mit Fragen der digitalen Privatheit auseinandersetzen und regelmäßig über Sicherheitsrisiken und Schutzstrategien informieren - und darauf aufbauend vergleichsweise umfassende Privatheitspraktiken in ihrem Alltag verankern. Dagegen spricht die Interviewtengruppe mit niedrigem Einkommen im Sinne einer ‚antiparanoiden‘ oder ‚pragmatischen‘ Sorglosigkeit ihren privaten Daten vergleichsweise wenig Wert zu, legitimiert dadurch ihren vergleichsweise geringen Grad an Informiertheit und ihre teils bewusst mangelhaft belassenen Privatheitspraktiken. Deutlich wird hier, wie sehr sich die materiellen Bedingungen

der Technologienutzer:innen auf ihre digitale Privatheit auswirken. Datenschutzansätze, die auf individuelles Handeln und die Responsibilisierung einzelner Nutzer:innen ausgerichtet sind, kommen dabei an ihre Grenzen. Sie müssen noch weiter um systemischere Analysen verschiedener Ungleichheitsebenen und deren Auswirkungen auf digitale Privatheit ergänzt und erweitert werden.

Literatur

Alhazmi, Hamoud; Imran, Ahmed und Alsheikh, Mohammad Abu (2022): How do socio-demographic patterns define digital privacy divide? *IEEE Access* 10, S. 11296-11307.

Adjerid, Idris; Peer, Eyal und Acquisti, Alessandro (2018): Beyond the Privacy Paradox. *MIS Quarterly,* 42(2), S. 465-488.

Baader, Maike Sophia und Koch, Sandra (2025): Über die Macht von Narrativen in krisenhaften Zeiten und gesellschaftlichen Transformationen. In: Sturm, Tanja; Tervooren, Anja; Schmidt, Melanie; Bärmig, Sven; Grunau, Sabrina; Thaler, Isabel; Ritter, Michael und Wrana, Daniel (Hrsg.): *Krisen und Transformationen: Anschlüsse an den 29. Kongress der Deutschen Gesellschaft für Erziehungswissenschaft.* Opladen: Budrich, S. 55-66.

Brand, Tilman; Herrera-Espejel, Paula; Muellmann, Saskia; Wiersing, Rebekka und Busse, Heide (2024): Social Inequality in the Context of Digital Health Applications: Digital Divides in Access, Use, Effectiveness, and Privacy. *Bundesgesundheitsblatt, Gesundheitsforschung, Gesundheitsschutz*, 67(3), S. 268-276.

Büchi, Moritz; Festic, Noemi; Just, Natascha und Latzer, Michael (2021): Digital Inequalities in Online Privacy Protection: Effects of Age, Education and Gender. In: Hargittai, Eszter (Hrsg.): *Handbook of Digital Inequality.* Edward Elgar Publishing, S. 296-310.

Calmbach, Marc; Borgstedt, Silke; Borchard, Inga; Thomas, Peter Martin und Flaig, Bodo Berthold (2016): Digitale Medien und digitales Lernen. In: Wie ticken Jugendliche 2016? Wiesbaden: Springer.

Dutton, William H.; Blank, Grant und Karpauskaitė, Eglė (2022): A Digital Privacy Divide: How Privacy Concerns Reinforce Inequalities Online.

Epstein, Dmitry und Quinn, Kelly (2020): Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, 6(2).

Frik, Alisa; Kim, Julian; Sanchez, Joshua Rafael und Ma, Joanne (2022): Users' expectations about and use of smartphone privacy and security settings. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (S. 1-24).

Meier, Yannick und Bol, Nadine (2025): Unequal experiences, unequal outcomes? Digital inequalities in experiencing online benefits and privacy harms, mistrust, and self-inhibiting behaviors. *Journal of Computer-Mediated Communication*, 30(5).

Ochs, Carsten (2019): Teilhabebeschränkungen und Erfahrungsspielräume: eine negative Akteur-Netzwerk-Theorie der Privatheit. In: *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*. Stuttgart: JB Metzler, S. 13-31.

Park, Yong Jin (2021): Why privacy matters to digital inequality. In: *Handbook of digital inequality*. Edward Elgar Publishing, S. 284-295

Paton-Simpson, Elizabeth (2000): Privacy and the reasonable paranoid: The protection of privacy in public places. *University of Toronto Law Journal*, 50(3), S. 305-346.

Pohle, Jörg (2022): Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In: Verbraucherzentrale NRW e. V. (Hrsg.). Paper zur Vortragsreihe „Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung". Eine Online-Vortragsreihe der Verbraucherzentrale NRW e.V..

Redmiles, Elissa M.; Kross, Sean und Mazurek, Michelle L. (2017): Where is the digital divide? A survey of Security, Privacy, and Socioeconomics. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, S. 931-936.

Redmiles, Elissa (2018): Net Benefits: Digital Inequities in Social Capital, Privacy Preservation, and Digital Parenting Practices of U.S. Social Media Users. *Proceedings of the International AAAI Conference on Web and Social Media*, 12(1).

Rogers, Everett M. (2001): The digital divide. *Convergence*, 7(4), S. 96-111.

Scheerder, Anique; Van Deursen, Alexander und Van Dijk, Jan (2017): Determinants of Internet skills, uses and outcomes. A systematic review of the second-and third-level digital divide. *Telematics and Informatics*, 34(8), S. 1607-1624.

Sevignani, Sebastian (2016): Krise der Privatheit: Zur Dialektik von Privatheit und Überwachung im informationellen Kapitalismus. In: *Kritische Öffentlichkeiten-Öffentlichkeiten in der Kritik*. Wiesbaden: Springer, S. 237-254.

Van Deursen, Alexander; Helsper, Ellen; Eynon, Rebecca und Van Dijk, Jan (2017): The compoundness and sequentiality of digital inequality. *International Journal of Communication*, 11, S. 452-473.

Van Dijk, Jan und Hacker, Kenneth (2003): The Digital Divide as a Complex and Dynamic Phenomenon. *The Information Society*, 19(4), S. 315-326.

Van Dijk, Jan (2017): Afterword: The state of digital divide theory. In: *Theorizing digital Divides*. Routledge, S. 199-206.

Voß, G. Günter (2020): *Der arbeitende Nutzer: über den Rohstoff des Überwachungskapitalismus*. Frankfurt a.M.: Campus.

Wäffler, Benigna (2024): Who cares privacy? Erschütterte Privatheit. *Ethik und Gesellschaft*, 2.

Wang, Laurent H. und Metzger, Miriam J. (2024): The Online Privacy Divide: Testing Resource and Identity Explanations for Racial/Ethnic Differences in Privacy Concerns and Privacy Management Behaviors on Social Media. Communication Research.

Wei, Miranda; Mink, Jaron; Eiger, Yael; Kohno, Tadayoshi; Redmiles, Elissa M. und Roesner, Franziska (2024): SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. *Proceedings of the 33rd USENIX Security Symposium*, S. 7011-7030.

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt a.M.: Campus Verlag.

Online Ressourcen

Statistisches Bundesamt: (Netto-)Äquivalenzeinkommen. https://www.destatis.de/DE/Themen/GesellschaftUmwelt/Einkommen-Konsum-Lebensbedingungen/Glossar/aequivalenzeinkommen_mz-silc.html, abgerufen am 12.12.2025.

WSI Verteilungsmonitor: Armutsgrenzen nach Haushaltstypen. https://www.wsi.de/de/armut-14596-armutsgrenzen-nach-haushaltsgroesse-15197.htm, abgerufen am 12.12.2025.

WSI Verteilungsmonitor: Reichtumsgrenzen nach Haushaltstyp. https://www.wsi.de/de/reichtum-15099-reichtumsgrenzen-in-deutschland-15189.htm, abgerufen am 12.12.2025.

BBC News: Internet Privacy. Genuine Concerns or Paranoia? Beitrag vom 25. März 2012, https://www.bbc.com/news/business-17369659, abgerufen am 7.3.2026.

Forbes Opinion: Privacy Paranoia: Is Your Smartphone Spying On You? Beitrag vom 5. Juli 2016, https://www.forbes.com/sites/omribenshahar/2016/07/05/privacy-paranoia-is-your-smartphone-spying-on-you/, abgerufen am 7.3.2026.

Über die Autorin

Dr. Anastassija Kostan
ist Soziologin und Philosophin, derzeit Postdoc in der Abteilung für Soziologie mit den Schwerpunkten Innovation und Digitalisierung an der Johannes Kepler Universität Linz. Sie arbeitet zu Sozial- und Gesellschaftstheorien der Privatheit mit besonderem Fokus auf digitale Ungleichheiten und erforscht in der Technologieentwicklung wirksame Vorstellungen und Narrative von Diversität. E-Mail: anastassija.kostan@jku.at.