Friedemann Vogel

Identifizierung und Authentifizierung in digitalen Diskursen

1 Einleitung

Identifizierung und Authentifizierung, Wiedererkennen und Zugangskontrolle zählen zu den anthropologischen Grundprinzipien sozialer Selbstregulation. Auf dieser in Vogel (2020a) entwickelten These aufbauend geht der vorliegende Beitrag der Frage nach, wie sich die damit verbundenen zeichenvermittelten Praktiken im Kontext digitaler Kommunikationsmedien gestalten, welche Effekte sie für die diskursive Reproduktion von Wissen und Herrschaftsstrukturen haben können und welche methodischen Herausforderungen sich daraus für die wissenschaftliche Untersuchung von digitalen Diskursen ergeben. Um die globale Relevanz dieses Themas zu umreißen, beginne ich aber mit einem kurzen Exkurs zur jüngeren Geschichte der (Verfassungs-)Rechtsdogmatik, einer Domäne, der sich DiskursanalytikerInnen (leider) bislang nur selten zuwenden:

Im Jahr 2008 entwickelte das Bundesverfassungsgericht in einem viel beachteten Urteil das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) weiter und deklarierte das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (BVerfGE 120: 274; in den Medien wurde es oft verkürzt als *Computergrundrecht* bezeichnet). Das Urteil stärkte alle Menschen der Bundesrepublik Deutschland in ihrem grundrechtlich verbrieften Anspruch, auch in der ungleich leichter zugänglichen digitalen Welt nicht leichtfertig Gegenstand von Überwachung oder Ausforschung durch staatliche oder auch private Akteure zu werden. Anlass zu diesem Urteil waren Klagen gegen die Novellierung von Polizeigesetzen, die – so die Begründung der staatlichen Behörden – analog zur physischen Hausdurchsuchung (§ 102ff. StPO) in besonderen Fällen auch eine „Online-Durchsuchung“ (von KritikerInnen oft als „Staatstrojaner“ kritisiert), also eine digitale und vor allem verdeckte Ausforschung von personenbezogenen Computersystemen wie Personal Computer, Smartphones u.ä. zulassen sollten.[1] Das *Computergrundrecht* erneuerte auch das 1983 im sog. „Volkszählungsurteil“ (BVerfGE 65: 1) entwickelte „Grundrecht auf informationelle Selbstbestimmung“, dem Recht des/der Einzelnen darüber zu entscheiden, welche personenbezogenen Informationen dem Staat zugänglich werden sollten. Der Staat sollte damals in Form von BeamtInnen nicht un-

1 Zur rechtslinguistisch rekapitulierten Diskursgeschichte um die Entwicklung der Online-Durchsuchung vgl. Vogel (2012).

https://doi.org/10.1515/9783110721447-010

gefragt von Tür zu Tür gehen und verschiedene Personendaten erheben und auswerten. Diese „jüngeren“ Meilensteine des Datenschutzes, der in der Zwischenzeit durch eine Ausweitung von Ermittlungsbefugnissen teilweise normativ[2] und praktisch[3] erheblich ausgehöhlt wurde und wird, sind letztlich motiviert durch die Erfahrungen mit dem Dritten Reich, einem Regime, dessen globale Macht maßgeblich durch eine total(itär)e und bürokratisch durchorganisierte Identifizierung und Kontrolle aller Individuen und sozialer Netzwerke beruhte und dem Millionen verfolgter Menschen zum Opfer fielen. Der langen Geschichte der bürokratisch geformten Verfolgung in totalitären Herrschaftssystemen gegenüber steht die moderne digital(isiert)e Welt des 21. Jahrhunderts, die nicht nur Behörden, ressourcenstarken Unternehmen und spezialisierten IT-Kriminellen, sondern auch dem/der ‚OttonormalbürgerIn‘ völlig neue und vor allem niedrigschwellige Techniken und Praktiken der medialen, zeit- und raumübergreifenden Selbst- und Fremdauthentifizierung erlaubt.

Im Folgenden werde ich zunächst den Begriff der Authentifizierung als einen Oberbegriff für den Zusammenhang von Identifizierung und Ressourcenkontrolle erläutern (Abschnitt 2) und im Anschluss anhand von Beispielen der Frage nachgehen, wie sich Authentifizierungspraktiken in digital(isiert)en Diskursen ausformen und welche Effekte sie auf die diskursiven Verhältnisse selbst – also auf die (Re)Produktion von kollektivem Wissen und gesellschaftlicher Asymmetrien – haben können (Abschnitt 3). Im letzten Abschnitt fasse ich resultativ zusammen, welche methodischen Implikationen die veränderten Authentifizierungspraktiken im digitalen Raum für Diskursanalysen mit sich bringen (Abschnitt 4).

2 Authentifizierung: Praktiken der Identifizierung und Zugangskontrolle

Ausgangspunkt einer Theorie der Authentifizierungspraktiken ist die These, dass sich im Grunde alle Aktivitäten menschlicher Interaktion anthropologisch auf zwei elementare Grundprinzipien zurückführen lassen, nämlich der Identi-

2 Die verdeckte Online-Durchsuchung ist trotz massiver Grundrechtsbedenken heute in zahlreichen Polizeigesetzen und seit 2017 sogar in der Strafprozessordnung (§ 100b StPO) verankert.

3 Es ist ein offenes Geheimnis, dass etwa der Richtervorbehalt – also der Einsatz von grundrechtsverletzenden Maßnahmen nur nach richterlicher Anordnung – in der Praxis aus verschiedenen Gründen oftmals keine wirksame Kontrollinstanz darstellt (vgl. etwa Brüning 2006).

fizierung und der Zugangskontrolle. Der Ansatz schließt an Ansätze der Sozialsemiotik und Positionierungstheorie (etwa Lacoste et al. 2014 und Spitzmüller et al. 2017) sowie an die Praxeologie und Lebensstilstudien Bourdieus (2005) an. Im Fokus steht dabei ein prozessuales, dynamisches Verständnis von sozialer Selbst- und Fremdverortung, das Begriffe wie „Identität" oder „Authentizität" als Praktiken der wechselseitigen, kommunikativen Aushandlung von sozialen Positionen und ihren Geltungsansprüchen in Interaktionen oder transsituativ konstituierten Diskursen reformuliert. Dieses Verständnis manifestiert sich insb. in soziolinguistischen und gesprächsanalytischen Arbeiten seit der Jahrtausendwende auch terminologisch in der Wendung „from authenticity to authentication" (Bucholtz 2003: 407). Bourdieu zeigt in seinen Studien schon deutlich früher – zwar sprachsensibilisiert (Bourdieu & Beister 2005), jedoch alle Modi sozialer Repräsentationsformen einbeziehend –, wie soziale (Gruppen-)Positionen durch von den Gesellschaftsmitgliedern objektivierbare Lebensstile reproduziert werden. Im Vordergrund stehen jedoch nicht die symbolischen Repräsentationen, Zeichen und Praktiken von Personen und Gruppen selbst, sie sind vielmehr analytisches Vehikel zur Entwicklung einer praxeologisch fundierten Sozialtheorie und zum Verständnis der Reproduktion gesellschaftlicher Klassen und ihrer Kämpfe um Kapital.

Der hier vertretene Ansatz setzt nun genau diese Zeichen und Praktiken der sozialen Selbst- und Fremdkategorisierung ins Zentrum der Untersuchung und fragt nach den historischen, kulturellen, modalen wie medialen Realisierungsmustern und ihren situativen wie transsituativen Funktionen. Vor diesem Hintergrund verstehe ich hier unter „Authentifizierung" (oftmals ritualisierte) kommunikative Praktiken und anthropologisch gedachte Kulturtechniken,

> die den Zweck haben, erstens den oder die Sprecher [bzw. Kommunikanten, FV] zu identifizieren – das heißt als ‚Den- oder Dieselben' mit bestimmten Eigenschaften wiederzuerkennen und kontinuierlich zu verifizieren; und zweitens in Abhängigkeit von dieser Identifizierung Zugangsrechte bei der ökonomischen, sozialen, kulturellen und symbolischen Ressourcenverteilung einzuräumen oder zu verwehren (Authentisierung und Autorisierung). (Vogel 2020a: 49)

Der Begriff der „Identifizierung" verweist auf alle Formen, Muster und Verfahren der Hervorbringung, Rezeption und Löschung reziproker Sichtbarkeit von sozialer Zugehörigkeit. Damit gemeint sind erstens automatisierte Prozesse unseres Wahrnehmungsapparates und dessen Fähigkeit, durch inferenzbasierte Verarbeitung von Sinneseindrücken die uns so begegnende Welt und ihre Wesen als Elemente sozialer Kategorien einordnen zu können; wie etwa verändern sich auf Identifizierung zielende Praktiken, wenn Bestandteile der Perzeption (z. B. partielle oder dauerhafte Blindheit, Gehörverlust, oder auch Beeinträchtigung des Geruchssinns) oder Kognition (z. B. Gedächtnisverlust) blockiert werden? Die

automatischen perzeptuell-kognitiven Prozesse werden zweitens überformt durch unterschiedliche Kulturtechniken, die das Individuum als Teil von bestimmten Gruppen markieren und wiedererkennbar machen. Diese Kulturtechniken können unterschiedlich komplex ausfallen, verschiedene Zeichenmodalitäten und Medien einbeziehen, zeitlich und räumlich strukturiert sein usw. Identifizierung kann komplett oder teilweise fehlschlagen und muss dann durch kompensierende Praktiken ‚repariert' werden. Beispiele ließen sich vielfältig anführen. In der Linguistik wurden Praktiken der Identifizierung etwa gesprächsanalytisch beim Telefon untersucht (Schegloff 1979; Lindström 1994), einem Kommunikationsmedium, bei dem die Interaktanten sich durch auditive ‚Stimmproben', Benennungen, Nachfragen oder durch das Explizitmachen und Spiegeln von gemeinsamen Kommunikationserfahrungen gegenseitig ausweisen. Bei einem anderen markanten Beispiel – der forensischen Linguistik (Fobbe 2011) – werden vielfach Annahmen der Varietätenlinguistik zu gruppensprachlichen Sozialmarkern gezielt als ‚Raster' eingesetzt, um bei der kriminologischen Einordnung von AutorInnen (z. B. von Erpresserbriefen) oder SprecherInnen (z. B. Morddrohung auf Tonband) zu unterstützen. Beide Beispiele zeigen jedoch nur bei näherem Hinsehen, dass es nicht allein um Identifizierung von Personen oder Gruppen geht. Identifizierung und kontinuierliche gegenseitige Verifizierung am Telefon ist mit der Frage verbunden, welche Information (schon beginnend mit der Stimmprobe nach Abnahme des Hörers) als Auszug meiner sozialsemiotisch lesbaren Körperrepräsentation ich bereit bin, dem anderen Ende der Leitung zur Wahrnehmung zu überlassen. Die forensische Identifizierung von Sprecher/SchreiberInnen erschöpft sich ebenso nicht in der erfolgreichen oder erfolglosen Einordnung; vielmehr dient das Verfahren dazu, die ggf. betroffenen Personen vom Zugang zu bestimmten Ressourcen abzuschneiden oder bestehende Ressourcen umzuverteilen (partieller Rechteentzug, Inhaftierung, Bußgeld, Entschädigungszahlungen usw.). Mit anderen Worten: Identifizierung als elementare Aufgabe menschlicher Kommunikation macht nur Sinn, wenn man sie mit der ebenso anthropologischen Aufgabe der Ressourcenverteilung und also der Ressourcenzugangskontrolle innerhalb von sozialen Kollektiven verknüpft sieht.

Der Begriff der „Authentifizierung" versucht genau diesem Zusammenhang gerecht zu werden, indem er die vielfach in der Forschung aufgeworfene Frage nach (der sozialsemiotischen und medialen Konstruktion von) „Identität(en)" und „Authentizität" stets verbindet mit der Frage danach, in welche sozialhistorisch situierten, gesellschaftlichen Kontrollmechanismen diese Identitäts- und Authentizitätskonstrukte eingebunden sind. Entlang dieser beiden konstitutiven Prinzipien von Authentifizierungspraktiken lassen sich weitere strukturelle Unterscheidungen treffen:

– **Authentifizierungszeichen** an sich: alle sinnlich wahrnehmbaren Formen und Strukturmuster, die innerhalb eines sozialen Kollektivs und dessen

kollektiven Gedächtnisses eine Identifizierung (Abgrenzung) des so selbst- oder fremdmarkierten Individuums bzw. Teilkollektivs erlauben und damit zugleich auch das abgrenzende Kollektiv semiotisch reproduzieren.

- **Praktiken zur Produktion, Instanziierung und Distribution von Authentifizierungszeichen**, also Verfahren und Praktiken, die eine beliebige wahrnehmbare Form mit einer Signal- bzw. Stigmatisierungsfunktion verknüpft, die im kollektiven Gedächtnis (d. h. auch mit zeitlich, lokal, sozial usw. beschränkter Gültigkeit) verankert und in unmittelbarer Interaktion zwischen Kommunikanten durch Antizipation reziprok wirksam werden: z. B. die erkennbare Deformation des Körpers (Schandmale wie Schlitzohr, Brandzeichen, Gravierungen) und das Bekanntmachen durch mündliche Weitergabe; die private Herstellung, massenmediale Verbreitung (d. h. diskursive Reproduktion) und markenrechtlich verankerte Mode; das staatlich-institutionell bewehrte Gestalten, amtliche Verteilen und Erklären (z. B. in der Schule) von Personalausweisen oder Aufenthaltsgenehmigungen usw. An den Beispielen ist schnell ersichtlich, dass die Produktion und Distribution von Authentifizierungszeichen nicht lediglich eine Frage der materiellen Herstellung ist, sondern vor allem die epistemische Frage, wie das notwendige Wissen über die zugangssteuernde Funktion von ausgewählten Zeichen (und das schließt auch Wissen über Erkennbarkeit, Abgrenzung gegenüber falschen Duplikaten usw. mit ein) in den Zielkollektiven verteilt werden kann. Oft, aber nicht immer wird darum mit dem Wissen um die Signal- bzw. Stigmatisierungsfunktion eines Zeichens zugleich auch das Wissen um die Ressource vermittelt, zu deren Zugangs- oder Verteilungskontrolle das Authentifizierungszeichen dient. So finden sich etwa auf Führerscheinen sprachliche und ikonische Zeichen, die das zugangsberechtigte Bewegungsmittel illustrieren, und auf Beförderungsscheinen (Bus- oder Bahnticket) stehen üblicherweise Angaben zur Geltungszeit und zum Geltungsraum, in dem uns die Ressource ‚Mobilität' zur Verfügung steht.
- **Praktiken der Authentifizierungsblockade und Löschung von (gültigen) Authentifizierungszeichen**: Wie schon eingangs kurz angedeutet, sind (grund-)rechtlich verankerte Datenschutzansprüche nichts anderes als eine kulturtechnische Antwort auf die Gefahr einer ungewollten, verdeckten Identifizierung und Zugangskontrolle (d. h. meist Ressourcenverwehrung und sozialer Ausschluss). Was in den öffentlichen und privaten Diskursen des 21. Jahrhundert heute oft übersehen wird: an der Frage eines effektiven Datenschutzes entscheidet sich letztlich der soziale und demokratische Rechtsstaat. Da staatlicher Schutz vor ungewollter Authentifizierung weder früher noch heute de facto immer greift, finden sich zahlreiche Praktiken, die eine Identifizierung durch Dritte verhindern sollen: Pseudonymisierung durch Chiffren in Kontaktanzeigen; Maskierungen auf

Demonstrationen; Versuch der Verschleierung von Autorschaft durch Imitation fremdstigmatisierender Varietätsmerkmale in Erpresserbriefen usw. Schließlich müssen Authentifizierungszeichen regelmäßig für ungültig erklärt, also aus dem kollektiven Gedächtnis gelöscht bzw. im Sinne der Transkriptivitätstheorie (Jäger 2003) überschrieben werden: situativ etwa durch „Entwertung" (z. B. Einreißen, Stempeln) einer Eintrittskarte; durch Einziehung eines Reisepasses; oder durch das Ausstellen eines Totenscheins (der nichts anderes ist als die amtliche/öffentliche Feststellung der Ungültigkeit eines einem Individuum zurechenbaren Körper(zeichen)s) und das Verteilen der Todesnachricht früher mündlich durch Totenfrauen (Stöhr 2015) und später durch Todesanzeigen in Zeitungen.

Im Folgenden möchte ich anhand von Beispielen diskutieren, welche Folgen digital (isiert)e Diskurse für Authentifizierungspraktiken haben (können) und umgekehrt wie neue bzw. durch ihre digitale Prozessierung veränderte Authentifizierungspraktiken ihrerseits zur Strukturierung von öffentlichen Diskursen beitragen.

3 Authentifizierung im digitalen Raum

Das auch im Alltag gebräuchliche Konzept der „Authentizität", also die Frage, wer oder was denn „echt" sei, hat sich durch digitale (bzw. hier konkreter: internetbasierte) Diskurse teilweise grundlegend verändert. Grund sind vor allem die veränderten semiotischen und medientechnischen Ressourcen, die konfligierenden Akteuren zur Konstitution von Selbst- und Fremdbildern sowie zur Konstruktion von Wahrheit(sansprüchen) zur Verfügung stehen. Die veränderten Bedingungen sorgten in der Anfangszeit sozialer Medien zunächst für Euphorie mit Blick auf die Möglichkeit des freieren, spielerisch erprobbaren Rollentausches (quasi ‚digitales Kleidertauschen'). Mit zunehmender Übernahme von Plattformen als Grundlage digitaler Diskursoperationen durch wirtschaftlich-profitorientierte, staatlich-behördliche sowie kriminelle Aktivitäten ist diese Euphorie nicht gänzlich, aber doch in Teilen der öffentlichen Debatte der Vorstellung von einer eher dystopischen Welt der Flames, des Mobbings, der Fake News und Diskursmanipulation gewichen, einer Dystopie, die sich erst durch die Möglichkeit, sich (aus Sicht von Betroffenen) drohender Authentifizierung und damit normalisierender (Selbst-)Kontrolle entziehen zu können, habe entfalten können. Das ist so nicht ganz richtig, aber auch nicht ganz falsch. Tatsächlich ist aus der Gemengelage ein komplexes, hier nur im Ansatz nachzeichenbares Geflecht kon- und divergierender sozialer wie auch medientechnisch sedimentierter (algorithmisierter) Authentifizierungspraktiken hervorgegangen, mit denen die kon-

kurrierenden Gruppen den Zugang zu Ressourcen (weiterhin) zu kontrollieren versuchen. Die Folgen bzw. Effekte dieser Entwicklung, so hier die These, sind aber zunehmende Fragmentierung, Polarisierung und „Abkühlung" sozialer Beziehungen in bzw. Rückzug aus digitalen Diskursen.

3.1 Semiotische und mediale Ressourcen digitaler Authentifizierung

Authentifizierungspraktiken konstituieren sich im digitalen, zumal computergestützten und internetbasierten Raum unter anderen Bedingungen als im ‚analogen' Raum. Der wichtigste Grund hierfür ist meines Erachtens die Möglichkeit, mithilfe medienvermittelter (räumlicher) Distanzkommunikation die habituell geprägten, in den Körper (als Hexis) physisch eingeschriebenen Authentifizierungsmerkmale[4] in Form, Umfang und Geltungskraft zu relativieren oder gar weitestgehend zu neutralisieren. Dies beginnt mit der Abwesenheit bzw. gezielten Abblendung bestimmter Zeichenmodalitäten je nach medienhistorischem und kommunikativem Setting (z. B. meist fehlender olfaktorischer, haptischer usw. Modus; Nutzung schriftbasierter Kommunikation oder bewusstes Abschalten der Webcam in einer Videokonferenz) bis hin zur Möglichkeit, einzelne Modi mithilfe niedrigschwelliger Software (Text-, Bild- und Videobearbeitung) zu manipulieren[5]. Textbausteine lassen sich etwa aus anderen Plattformen kopieren (ohne dass der Vorgang des Kopierens offensichtlich würde) und als die eigenen einsetzen; viele soziale Medien befördern den kreativen Umgang mit Userprofilen und Avataren; Deepfake-Videos lassen sich schon mithilfe einfacher Apps realisieren usw. Selbst der in der analogen Welt zumindest teilweise fixierte Personenname lässt sich in der internetbasierten Kommunikation mithilfe freier (Nick-) Namenswahl weitestgehend umgehen. Mit der Beschreibung dieser Unterschiede zwischen analogem und digitalem Raum soll mitnichten eine Bewertung erfolgen – die internetbasierten bzw. generell medienvermittelten Authentisierungsmög-

4 „Es scheint durchaus, als würden die mit bestimmten sozialen Verhältnissen gegebenen Konditionierungsprozesse das Verhältnis zur sozialen Welt in ein dauerhaftes und allgemeines Verhältnis zum eigenen Leib festschreiben – in eine ganz bestimmte Weise, seinen Körper zu halten und zu bewegen, ihn vorzuzeigen, ihm Platz zu schaffen, kurz: ihm soziales Profil zu verleihen. Die körperliche Hexis, eine Grunddimension des sozialen Orientierungssinns, stellt eine praktische Weise der Erfahrung und Äußerung des eigenen gesellschaftlichen Stellenwerts dar [...]" (Bourdieu 2005: 739).

5 Den Ausdruck „Manipulation" verwendet ich deskriptiv im Sinne der ‚strategisch geleiteten manuell-händischen Veränderung'.

lichkeiten und Selbst-Konstruktionen sind nicht besser oder schlechter als die ‚analogen', körper- und raumgebundenen Realisierungsmöglichkeiten, sie sind einfach nur anders und das hat Folgen für die Geltungskraft sämtlicher Erscheinungsformen von Authentifizierungszeichen: Mit zunehmender Verbreitung von (passiven oder auch aktiven) Kenntnissen über die Manipulierbarkeit von Text, Ton, Bild, Bewegtbild wird der Wahrheitsanspruch dieser Modi verändert.

Die Abstinenz von physischen Authentifizierungszeichen und/oder die Manipulierbarkeit im digitalen Medium hat entsprechend natürlich Folgen für die Praktiken der Kontrolle zugangsbeschränkter Ressourcen. Ein Fingerabdruck als Authentifizierungszeichen ist am Smartphone nur solange zuverlässig, bis der Chaos Computer Club illustriert, wie man sich damit als Wolfgang Schäuble ausweisen kann.[6] Die Möglichkeit selbst für technisch Unversierte, sich im digitalen Raum jederzeit mehrfach gebrauchte Authentifizierungszeichen anzueignen, sie selbst zu konstruieren, zu adaptieren oder zu kopieren, provoziert insbesondere organisationelle Akteure zur Entwicklung immer neuer Techniken zur Identifizierung (3.2). Aber auch für PrivatanwenderInnen ist digitale Identifizierung zumindest heute keine Hürde mehr: Nie war es leichter, dem/der NachbarIn mithilfe von Google 3D-Maps in den Garten zu sehen; nie war es leichter selbst für Internet-Novizen, mit wenigen Klicks via Google oder Facebook höchstpersönliche Informationen über eine Zielperson oder -gruppe zusammenzutragen und aus dem sich daraus ergebenden Wahrnehmungsprofil Entscheidungen über deren Ressourcenzugang abzuleiten. Es ist ein offenes Geheimnis, dass ArbeitgeberInnen sich regelmäßig über Internetrecherchen schlau machen, um ihre BewerberInnen schon bei erster Aktendurchsicht und noch vor dem Bewerbungsgespräch – bei dem ggf. Informationen auch historisch-situativ kontextualisiert werden – näher einordnen zu können[7].

Dieses Beispiel verweist schließlich noch auf ein weiteres medientechnisches Dispositiv im digitalen Raum: nämlich die Resistenz einmal eingebrachter Zeichen gegen Löschung. Wenngleich heute eine Binsenweisheit („Das Netz vergisst nie!"), hat diese Tatsache bislang nur zu wenig Umdenken beim Umgang mit personenbezogenen Daten im digital-öffentlichen Raum geführt. Wer (noch) nicht von Mobbing, imageschädigendem Identitätsklau o. ä. direkt oder im engeren Freundes- und Familienkreis betroffen war, unterschätzt in der

6 Siehe etwa der CCC 2008: https://www.ccc.de/updates/2008/schaubles-finger?language=de (01.05.2021).

7 Vgl. etwa den Metadiskurs dazu: https://arbeitgeber.careerbuilder.de/news/arbeitgeber-ueberpruefen-social-media-profile-von-bewerbern (26.05.2021) und die damit verbundene juristische Auseinandersetzung (https://www.lto.de/recht/hintergruende/h/bewerbung-facebook-check-arbeitgeber-background, 26.05.2021).

Regel die systematische, plattform- und medienübergreifende Sammlung und aggregierende Verdatung von personenbezogenen Informationen in riesigen Datenarchiven und deren Weiterverwendung im Zweifel bis über den Tod hinaus.

Für die Konstruktion von Personen- und Gruppenprofilen und damit die Konstitution von Authentifizierungszeichen bedeutet die Löschungsresistenz vor allem eine Tendenz zur Dehistorisierung, also temporal-situativer Kontextabstraktion (siehe auch 3.3 und 4). Mit anderen Worten: Selbst- und fremdgruppenbezogene attributive Zeichen, die ihre Gültigkeit in unterschiedlichen sozialhistorischen Momenten hatten und Teil verschiedener situativer Authentisierungsversuche waren, werden bei einer späteren Autorisierungsprüfung in einen Zusammenhang miteinander gebracht. Besonders problematisch ist dieser Umstand vor allem bei rein algorithmisierten, automatisierten Authentifizierungsprozeduren, deren Ergebnis auf statistischen (Kurz-)Schlüssen basieren und im Zweifel immer gegen etwaige Risiken entscheiden (etwa bei Versicherungen, Kreditinstituten u.ä.). Aber auch googelnde ArbeitgeberInnen differenzieren qualitativ nicht immer, irgendetwas bleibt immer hängen.

3.2 Praktiken digitaler Authentifizierung

Welche Folgen haben die veränderten semiotischen und medialen Konstitutionsbedingungen für Authentifizierungspraktiken im digitalen Raum? Zunächst erlaubt der digitale Raum heute (noch) mit vergleichsweise geringen Voraussetzungen, nicht nur das eigene Selbstbild zu variieren, durch Anpassung von Profilinhalten Attribute (und damit assoziierte Erwartungen) zu verstärken oder zu unterdrücken, oder jenseits der Körper-Befangenheit gleich (und zugleich) gänzlich unterschiedliche Rollen einzunehmen und Authentifizierungspraktiken aus der nicht-digitalen Welt spielerisch zu erproben. Spielerische Erprobung ist dabei sowohl im übertragenen Sinne (als generelles Austesten: z. B. mit einer potentiell älteren oder anders-/gleichgeschlechtlichen Person im Chat zu flirten) als auch wörtlich gemeint im Sinne der Game Studies: Natürlich können manche Rollenbilder (‚mal wie ein Ritter sein' oder ‚wie ein Höhlenmensch hausen') durch ein lebendiges Vorstellungsvermögen und einen geschickten, kreativen Umgang mit Maskierungstechniken (Kostüme, Schminke etc.) in Rollenspielen (Games) kohärent inszeniert werden. Im Unterschied zu Rollenspielen in computergestützten Games bleibt das Gestaltungsspektrum aber ungleich kleiner. An die Stelle körperlicher Dispositive treten allerdings plattformspezifische Gestaltungsgrenzen: im Community-Bereich der Wikipedia etwa dominieren schriftsprachliche Praktiken der Selbst- und Fremdreferenzierung, die zudem von der Wiki-Technologie (Versionierung, Vernetzung, administrative Rollen und Aufgaben usw.) gerahmt werden (Vogel

2016). In dreidimensional virtualisierten Gestaltungswelten – z. B. World of Warcraft 3 (Stertkamp 2017 und Collister 2014) oder Second Life (Frohwein et al. 2008) – treten dagegen auch multimodale Formen der Avatargestaltung und sozialsemiotischen Gruppenkontrolle in den Vordergrund. Oft werden bei der Verhandlung von Selbst- und Fremdgruppe soziale Kommunikationshandlungen verknüpft mit algorithmisch produzierten, messbaren Einheiten: In der Wikipedia – vereinfacht formuliert – definieren sich legitime Insider über eine hohe Anzahl an Artikelbearbeitungen (Edits); in World of Warcraft und anderen MMORPGs[8] sind es Erfahrungsstufen und andere Punkteskalen, die einem den Zugang zu bestimmten Gruppen („Gilden") erleichtern oder erschweren. Dies führt mich zu einem zweiten Punkt:

Wir finden allerorten – sowohl innerhalb digitaler Medien als auch außerhalb – eine Zunahme an automatischen Authentifizierungsprozeduren, also solchen Praktiken, die einen Großteil der Identifizierungs- und Zugangskontrollpraktiken an Sensoren- und Verdatungstechnologien delegiert haben bzw., kulturanthropologisch gedacht, die in diesen Technologien selbst aufgegangen sind. Dies gilt nicht nur für die automatische Verbindungsherstellung zwischen Endgeräten und Internetnetzwerk (z. B. über einen WLAN-Router, dessen Zugangssicherheitsschlüssel in der Regel zuvor einmalig durch soziale, kommunikative Aktivitäten erfahren und eingegeben werden müssen) oder einfache Passwortabfragen beim Zugang zu Inhalten sozialer Medien nach vorheriger manueller Registrierung und Schlüsselhinterlegung. Wenn es – wie im Falle des mittlerweile eingestellten Start-Ups „Precire" – möglich erscheint (das heißt mitnichten, dass es auch funktionieren würde, sondern nur *dass* es eingesetzt wird), dass anstelle von Aktenarbeit und Personalgespräch ein Algorithmus lediglich auf Basis eines aufgezeichneten Bot-Interviews und mithilfe maschinellen Lernens die eignungsdiagnostische Personalauswahl betreibt, dann wird McLuhans Diktum „the Medium is the message" (McLuhan et al. 2014 [1967]) gleich in zweifacher Hinsicht virulent: Nicht nur wird Sprachgebrauch im Verdatungsprozess dekontextualisiert zum vermeintlich neutralen Medium kognitiver Eigenschaften und damit zum sprachlichen „Fingerabdruck" simplifiziert[9], die Maschine soll die Arbeit menschlicher Selektionsleistung und sozialer Kontrolle auch verlängern, verstärken, ersetzen. Treibende Kräfte für eine Zunahme an Authentifizierungsprozeduren sind – so zumindest vorläufige Beobachtungen – meistens Rationalisierungs-, d. h. Kostenreduktionserwägungen und/oder die Hoffnung, damit Sicherheitsrisiken

8 Das Akronym steht für "Massive Multiplayer Online Role-Playing Game" (Online-Rollenspiele).
9 https://www.consulting.de/hintergruende/fachartikel/einzelansicht/fingerabdruck-fuer-die-sprache/ vom 29.03.2017 (02.05.2021); vgl. dagegen die kritischen Beiträge von Joachim Scharloth in seinem Blog „surveillance and security" (http://www.security-informatics.de/blog/?cat=22, 26.05.2021).

verringern zu können. Besonders deutlich tritt das zu Tage, wo menschliche KommunikationspartnerInnen ausschließlich eine Gatekeeper-Funktion (‚Türsteher'-Funktion) und/oder wiederkehrende Aufgaben (Beratung, Dateneingabe, Überweisungen u.ä.) erfüllen und dann durch technische Anlagen (z. B. Pin-basierte Zugangskontrolle zu Ressourcen via Automat, Kundenonlineportal oder Chatbot) ersetzt werden.

Das Bedürfnis, das individuelle oder gruppenbezogene Selbstbild in digitalen Diskursen durch strategische Zeichenoperationen zu prägen und unerwünschte Authentifizierung (gar über die Grenzen der digitalen Diskurswelt hinweg) zu vermeiden, steht zunehmend im Konflikt mit einer auf kalkulierbare Identifizierung und Selektion angewiesenen Ökonomie und (auch rechts-) staatlichen Verwaltung von Gesellschaft. Entsprechend suchen Ökonomie und Verwaltung kontinuierlich nach technischen oder auch rechtlichen (d. h. sanktionsbewehrten) Wegen, eine Verknüpfung zwischen körpergebundenen und digitalen Selbstrepräsentationen, oder aber zumindest eine crossmediale Beziehung zwischen verschiedenen sozialsemiotischen Repräsentationen innerhalb digital (isiert)er Diskurse herstellen zu können. Die Privatwirtschaft arbeitet mit komplexen, oft verdeckten Tracking-Verfahren, um User-Verhalten auch über verschiedene Plattformen und Endgeräte hinweg einem Benutzerprofil zuordnen und daraus weitreichende Rückschlüsse auf Interessen, Bedürfnisse oder Ängste der beobachteten Akteure ziehen zu können (Roesner et al. 2012, Mayer & Mitchell 2012 und Arp et al. 2017). Regierungen führen zunehmend Befugnisse in ihre Rechtsordnungen ein, vergleichbare Deanonymisierungstechnologien für Strafverfolgungs- sowie auch präventive Überwachungszwecke einsetzen zu können. Gruppen, die sich dagegen der Verteidigung von Persönlichkeitsrechten im digitalen Raum verschrieben haben (IT-Sicherheitsforschung, Hacking-Kultur u.ä.), entwickeln kontinuierlich neue Verfahren, um das individualisierte Nachverfolgen von Datenströmen und sozialsemiotischen Spuren im Netz zu blockieren oder zumindest bis zur Unrentabilität zu verschleiern und zu stören. Erfolgreich sind diese technischen Lösungsansätze allerdings nur in Kombination mit einer manuellen Selbstkontrolle, das heißt eine disziplinierte datenseitige Anonymisierung bis hin zur ‚digitalen Enthaltsamkeit', Abmeldung oder gar nicht erst Nutzung von öffentlichen sozialen Medien (wie Facebook u.ä.)[10].

Doch nicht nur staatliche, wirtschaftliche und kriminelle Identifizierung und Selektion prägen den öffentlichen (Meta-)Diskurs. Vielleicht sogar noch stärker in der Diskussion sind Praktiken des privaten Ausforschens im digitalen

10 Zur Mediengeschichte des Identifizierens bzw. Registrierens und gegenläufiger Praktiken vgl. Gießmann (2020).

Abb. 1: Metadiskurs und Ratgeber zur Identifizierung von falschen LiebhaberInnen im Netz (hier: Techbook: https://www.techbook.de/apps/so-erkennen-sie-ein-fake-profil-bei-tinder vom 07.08.2020; 02.05.2021).

Raum, sei es das Sammeln und ggf. pejorative Rekontextualisieren von Informationen über unliebsame Nachbarn, Schulkameraden oder politische Gegner, oder sei es das Nachverfolgen digitaler Aktivitäten von Idolen zum Zwecke der Annäherung –; die technische wie soziale Hemmschwelle für solcherlei Praktiken ist durch die Möglichkeit ihrer Verschleierung und damit dem Entzug vor sozialer Sanktionierung kontinuierlich gesunken. Auf der anderen Seite steht ebenso oft die Verunsicherung über die Zuverlässigkeit von im digitalen Raum (insb. Dating-Apps und -plattformen) angebandelten sozialen Beziehungen, eine Frage, zu der sich wiederum ein Metadiskurs zur Identifizierung von Dating-Bots, Heiratsschwindlern und falschen Administratoren (Spam, Phishing-Mails u.ä.) entwickelt hat (vgl. Abb. 1).

3.3 Diskurseffekte digital(isiert)er Authentifizierungspraktiken

Welche weitergehenden Diskurseffekte lassen sich infolge digitaler Authentifizierungspraktiken beobachten? Eine kohärente empirische Forschungsbasis gibt es als Antwort auf diese Frage bislang nicht. Gleichwohl können Beobachtungen aus bisherigen Metadiskursen mögliche Ansätze liefern:

- Die multiplen Möglichkeiten der Identifizierung und daraus resultierende Gefahr einer sozialen Kontrolle können nicht nur bei technisch-informierten Akteuren oder von Sanktionserfahrungen direkt betroffenen Gruppen zu verstärkter „Selbstzensur" in digitalen Diskursen führen. Denkbar ist durchaus auch eine kontinuierliche, in gewisser Weise schleichende Passivierung, ein allgemeiner Rückzug breiterer gesellschaftlicher Gruppen aus digitalen Diskursen bzw. eine Zunahme an (der Demonstration von) konformistischen Haltungen in öffentlichen Debatten. Dieser zuweilen als „social cooling" oder „Klickangst"[11] bezeichnete Effekt wird abgeleitet aus Erfahrungen mit historischen staatlichen Kontroll- und Überwachungssystemen und ist eine durchaus plausible und ernstzunehmende Gefahr für eine demokratische Diskurskultur (vgl. etwa die eindringliche, den Effekt explizit auf drohende Selektion beziehende Kampagnenseite: https://www.socialcooling.com, 02.05.2021).
- Umgekehrt lässt sich in digitalen Diskursen aber auch eine zunehmende Verrohung beobachten, das heißt eine polarisierende, teilweise aggressivere, weniger Face-Work betreibende Interaktion vor allem in sozialen Medien (Vogel 2020b und 2018). Ob diese Tatsache auch schon für nicht-digitale Diskurse galt und jetzt nur lediglich sensibler in der Öffentlichkeit wahrgenommen und diskutiert wird, steht auf einem anderen Blatt, entscheidend ist die leichtere Sichtbarkeit dieser Interaktionsmodi. Mein Eindruck ist dabei, dass die Hemmschwelle sowohl für herabsetzende Stigmatisierungs- und Ausgrenzungspraktiken in den letzten 10 Jahren online sukzessive abgenommen hat, ohne dass es sich bei den Agierenden durchgehend um einen rechtsnationalistischen, gewaltbereiten Mob handelte (dies überraschte zum Beispiel auch die Grünen-Politikerin Renate Künast, die ihre Online-Angreifer in der analog-physischen Welt konfrontierte und dabei zuweilen auf für sie durchschnittliche Sozialmilieus stieß). Grund hierfür kann dann nur sein, dass die Gefahr von Identifizierung und Anschlusssanktionen nicht bewusst ist (die Akteure sich also in anonymisierter Sicherheit wägen, vgl. Kaspar 2017) oder aber ein Stück weit in Kauf genommen wird.
- Tatsächlich ist die Nachverfolgbarkeit und sanktionsbewehrte Einhegung verbaler Angriffe und Herabsetzungen auf digitalen Plattformen zuweilen technisch (Verschleierungstechnologien) wie rechtlich voraussetzungsreich. Unter anderem diese Tatsache befördert in regelmäßigen Abständen Forderungen nach einer stärkeren Regulierung von digitalen Diskursen, etwa durch Haftbarmachung von Plattformbetreibern (etwa mit dem Netzwerkdurchsetzungs-

11 Vgl. https://www.heise.de/newsticker/meldung/34C3-Daten-kontra-Freiheit-3928458.html (02.05.2021).

gesetz 2017), erweiterten staatlichen Ermittlungs- und Eingriffsbefugnissen und/oder eine Pflicht aller BürgerInnen zur Deanonymisierung (Fahnenwörter aus jüngerer Zeit sind etwa *Klarnamenpflicht* oder *digitales Vermummungsverbot* u.ä.).

– Demokratietheorie und Partizipationsbewegungen feierten in der frühen Internet- und Web 2.0-Ära der 1990er und 2020er Jahre die neuen, globalen Freiheiten zur sozialen Vernetzung und politischen Artikulation jenseits der großen medialen Gatekeeper. Politische und ökonomische Eliten haben die daraus resultierende Gefahr für etablierte Machtstrukturen alsbald erkannt, zuweilen auch durch Beobachtung erfolgreicher internetgestützter Herrschaftsumbrüche (z. B. im sog. „Arabischen Frühling"; Baringhorst 2009 und Rilling 1998). Generell deutet daher vieles darauf hin, die digital repräsentierten sozialen (Diskurs-)Praktiken immer stärker mit außer-digitalen Repräsentationsformen zu verknüpfen, ‚Online-Identitäten' also mit ‚Offline-Identitäten' identifizier- und damit kontrollierbar(er) zu machen. Die Verfolgung von Hate-Speech, Kinderpornographie oder Extremismus wird hierfür regelmäßig als (auch moralisch aufgeladener) Topos ins Feld geführt. Nicht alles aber, was aus kriminalistischer Sicht nützlich wäre, ist in demokratietheoretischer Perspektive auch angemessen.

Aus diesen Überlegungen heraus möchte ich im abschließenden vierten Teil andiskutieren, welchen methodischen Herausforderungen sich Analysen digitaler Diskurse stellen müssen, wenn sie der Rolle von Authentifizierungspraktiken nachgehen und/oder den möglichen Gefahren von ungewollter Authentifizierung infolge eigener Forschungsergebnisse Rechnung tragen möchten.

4 Methodische Implikationen für die Untersuchung digitaler Diskurse

Die zuvor kursorisch genannten Bedingungen und Effekte von Authentifizierungspraktiken im durch digitale Medien geprägten Sozialraum haben verschiedene Implikationen für die Untersuchung digitaler Diskurse generell sowie ebendieser Praktiken im Besonderen:

(1) Forschungsethische Aspekte zur Vermeidung von Deanonymisierung

Allem voran stellt sich die Frage nach einem datenschutzsensiblen Umgang mit erhobenen bzw. aggregierten Informationen und (der Publikation von) wissenschaftlichen Erkenntnissen in zugespitzter Weise. Nicht nur der Zugang und damit die leichte(re) Objektivierbarkeit von direkt personenbezogen Daten (z. B. Erhebung und Auswertung von durch die User selbst erstellten Personenprofilen in den Metaangaben von Twitter, YouTube oder Facebook), auch das Sammeln und Auswerten unterschiedlicher sprachlicher Ressourcen selbst in streng pseudonymisierter Form können oftmals eine nachträgliche Identifizierung der davon betroffenen Personen und Gruppen nicht verhindern. Das gilt zum einen für einzelne Informationen und sprachliche Belege, die (zumal digital) publiziert schnell mithilfe von Suchmaschinen personenbezogen dekodiert werden können; das gilt zum anderen für größere Datensammlungen (sprachliche Primär- wie auch anonymisierte Metadaten in Korpora), die aus sich heraus und/oder in Kombination mit anderen frei zugänglichen bzw. erwerbbaren Datensammlungen durch eine aggregierende Auswertung eine Deanonymisierung und damit eine spätere (ungewollte) Authentifizierung ermöglichen. Aufgrund der Tatsache, dass viele Daten noch Jahre oder Jahrzehnte später in digitalen Medien leicht auffindbar sind und/oder früher oder später in Datenarchive eingehen, ergeben sich durch (digitale wie auch digitalisierte) Diskursanalysen so Verfolgungs- und Ausschlussrisiken für Personen und Gruppen, die selbst bei sorgfältiger Einbeziehung aktueller Authentifizierungstechniken zum Zeitpunkt der Analyse nicht hinreichend absehbar sein können.

Die einzige Möglichkeit, diese Risiken zu minimieren, ist im Zweifel der generelle Verzicht auf Publikation von größeren Datenmengen wie kompromittierbaren Einzelbelegen. Damit allerdings wird nicht nur die Replikation der Ergebnisse erschwert (wenn nicht unmöglich gemacht), auch Forschung insgesamt wird ineffizient, weil zuvor kostspielig aufgesetzte Korpora kaum nachnutzbar sind und also immer wieder aufs Neue produziert werden müssen. Alternativ kann die Publikation von Forschungsdaten systematisch beschränkt werden, zum Beispiel:

- in Form einer qualitativen, durch das Forschungsergebnis geleiteten Auswahl von Texten (kontrollierte Samples), die das beobachtete Phänomen prototypisch repräsentieren (im Sinne der Repräsentanz, nicht der statistischen Repräsentativität);

- als randomisierte Datenrekompositionen, d. h. die nachträgliche Erzeugung und Publikation eines Datenformats, das ursprüngliche Satz- und Textgrenzen und damit letztlich Kohärenzstrukturen verwischt (weitreichende Schlüsse werden damit erheblich erschwert);
- in Form von Datenaggregierungen, das heißt Veröffentlichung nur von kotext-isolierten Ausdrucks-Frequenzdaten, aus denen die Originaltexte nicht wiederhergestellt werden können (vgl. etwa das CAL^{2}Lab, das diesen Weg zur Vermeidung urheberrechtlicher Probleme gewählt hat[12]).

Auch eine Publikation dezidiert im nicht-digitalen Raum (nur Printveröffentlichung) ist eine Möglichkeit zur Vermeidung von Deanonymisierung: Denn oftmals genügt es schon, die eigenen Daten in eine Form zu bringen, die für eine automatisierte Weiterverwertung etwa für ökonomische, kriminelle oder staatliche Verfolgungszwecke einen nicht-vertretbaren Aufwand erforderte. Das gleiche gilt nicht nur für Analysedaten, sondern auch für etwaige Algorithmen, die zur Datenverarbeitung, analytischen Profilbildung oder zum Nachvollzug ethnomethodischer Profilbildungsverfahren entwickelt und eingesetzt werden. Anders als bei Beobachtungsdaten ist im Falle von Algorithmen eine Publikation z. B. in Form von Programmcode der Nicht-Veröffentlichung m. E. regelmäßig vorzuziehen. Nur so kann die Debatte auch über sicherheitstechnische Gegenmaßnahmen informiert und in einem emanzipatorischen Sinne vorangebracht werden.

Zur Orientierung bei all diesen Fragen können Ethikcodices sicherlich hilfreich sein; eine fallspezifische Risikenantizipation ist aber im Grunde nur realistisch im Rahmen von interdisziplinär aufgestellten Sicherheitsaudits (Ethikkommissionen, die die aktuelle Diskurslage sowohl medientechnologisch als auch semiotisch-kommunikativ einzuordnen wissen). In extremen Fällen könnte auch der einzige Ausweg die Nicht-Objektivierbarkeit mancher verdateter Untersuchungsgegenstände sein, also der Verzicht auf bestimmte Forschungsvorhaben.

(2) Forschungspraktische Aspekte bei der Analyse von Authentifizierungspraktiken

Neben der forschungsethischen Frage nach der Gewährleistung eines effektiven Persönlichkeitsschutzes gegenüber späterer, ungewollter Identifizierung stellen sich für die Analyse von Authentifizierungspraktiken in digitalen Diskursen ihrerseits weitere Herausforderungen:

12 https://cal2lab.diskurslinguistik.net (28.05.2021).

Will man den Verfahren und Praktiken des kommunikativen Identifizierens und Zugangskontrollierens analytisch gerecht werden, reicht es in der Regel nicht, sich allein auf die im digitalen Raum beobachtbaren Datenspuren zu konzentrieren. Vielmehr muss regelmäßig durch triangulierende Verfahren (v. a. durch Einbezug digitaler wie ‚analoger' Ethnographie: längerfristige Beobachtungen und auch Befragungen) eruiert werden, welche Anteile von Authentifizierungspraktiken originär im digitalen Kommunikationsraum und welche Anteile außerhalb digitaler Medien konstitutiv sind. Dabei ist auch zu berücksichtigen, dass manche (Teil-)Praktiken innerhalb digitaler Medien über verschiedene Plattformen verteilt strukturiert sein können (Ketten von Authentifizierungspraktiken). Denn was organisationelle Player im großen Stil vermögen, ist ‚im Kleinen' individuell möglich: etwa die Deanonymisierung von Akteursprofilen in der Wikipedia durch Verfolgung und Kontextualisierung über Nickname (Vogel & Jacob 2014) oder andere Textspuren auf verschiedenen Plattformen (Foren, Twitter usw.). Das Erfassen der Komplexität solcher Praktiken ist essentiell, will man sie angemessen verstehen und bereits bestehende mögliche Risiken in der öffentlichen Kommunikation antizipieren. Dabei reicht es in der Regel nicht, die Analyse allein auf die kommunikativen Zeichen selbst zu fokussieren, sondern es bedarf auch einer intensiven Auseinandersetzung mit der medientechnischen Funktionsweise der verschiedenen Plattformen und Algorithmen. Ein Beispiel: Als *Checkuser*-Abfrage (abgekürzt: *CU*)[13] bezeichnet man in der Wikipedia-Community das Verfahren, mit Hilfe administrativer Sonderrechte die IP-Adresse(n) eines User-Profils abzufragen und damit zum Beispiel verschiedene Benutzerprofile einem Internetanschluss und über diese Behelfsbrücke einer Person zuzuordnen, sie also – in der Regel zu Sanktionszwecken (Aussperrung) – zu deanonymisieren. Diese Anfragen kommen zum Einsatz, wenn der Vorwurf im Raum steht, Schreibrechte in der Wikipedia missbräuchlich zu nutzen (Werbung, Propaganda, Manipulation von Diskussionsverläufen u.ä.). Checkuser-Abfragen stellen damit einen starken Eingriff in die Integrität von Wikipedia-Benutzern dar und stehen meist am Ende einer längeren Kette von algorithmisch gestützten Identifizierungspraktiken. Will man diese Zusammenhänge verstehen, ist es notwendig, diese Algorithmen zumindest im Ansatz nachzuvollziehen: die Funktionslogik von Wikis (bzw. Mediawikis im Besonderen), des Internet-Protokolls (IP), die Rolle automatischer Datenverarbeitungsprozesse (in der Wikipedia spielen „Bots" eine große Rolle bei der automatischen Verdatung, intertextuellen Verknüpfung, Kategorisierung usw.[14]).

13 https://de.wikipedia.org/wiki/Wikipedia:Checkuser (28.05.2021).
14 https://de.wikipedia.org/wiki/Wikipedia:Bots (28.05.2021).

Für ein Verständnis von Algorithmen (auch unbekannten bzw. nicht offensichtlichen Programmen) ist es in der Regel notwendig oder zumindest hilfreich, rudimentäre Programmierkenntnisse zu besitzen und/oder die betroffenen Medien selbst aktiv, explorativ bzw. teilnehmend-beobachtend auszutesten. Solche digitalethnographischen Verfahren bringen zumal in einer verdeckten Form wiederum neue, auch ethische Fragen mit sich, denn sie stellen natürlich einen Eingriff ins Feld dar, der – es geht hier schließlich um das Ausforschen von (Zugangs-)Kontrollpraktiken! – auch zum Ausschluss aus dem Feld führen kann (Androutsopoulos 2008; zu Risiken verdeckter Ethnographie unter Türstehern vgl. Calvey 2018). Hier ist also besondere Behutsamkeit bei der Feld-Annäherung gefragt. Zum Studium von (zumindest frei verfügbaren) Medientechnologien ist es schließlich auch möglich, die jeweiligen Plattformprogramme in einer lokalen „Sandbox", also auf einem separaten Rechnersystem zu installieren und dort geschützt auszutesten. Im Falle der Wikipedia etwa ist es möglich, das gesamte System des Mediawikis (inkl. Plugins und auch Daten) in einer lokalen Umgebung zu reproduzieren.

Zur angemessenen Einordnung ethnomethodischer Authentifizierungspraktiken gehört schließlich auch, die hierfür zu erhebenden digitalen Daten in ihrem jeweiligen historischen Erscheinungskontext adäquat einzuordnen: Nicht immer sind sozialsemiotische Spuren mit zuverlässigen Zeitangaben verknüpft, so dass die Analyse ahistorisch zu verflachen droht – eine Gefahr, die generell bei quantifizierender Auswertung leicht unterschätzt wird. So können etwa über die Wikipedia-API oder mithilfe von Foren-Crawlern leicht User-bezogene Sprach- und Textprofile erzeugt und anschließend korpuslinguistisch ausgewertet werden; mit Blick auf Authentifizierungspraktiken der User ist dabei allerdings problematisch, wenn sich über die Zeit oft wandelnde sprachliche Selbstpositionierungen zu einem abstrakten Profil aggregiert werden.

5 Fazit und Ausblick

Der vorliegende Beitrag geht den besonderen sozialsemiotischen Konstitutionsbedingungen von Praktiken des Identifizierens und der Ressourcen-Zugangskontrolle (Authentifizierungspraktiken) in digitalen Diskursen nach und diskutiert damit verbundene methodische Implikationen, will man Authentifizierung in der digital (isiert)en Welt forschend nachspüren. Im Ergebnis ergibt sich das Bild einer Diskurswelt, die durch immer weiter zunehmende automatische wie auch semi-automatische Verdatung allen menschlichen Tuns und Lassens ihre Akteure einer kontinuierlichen (Selbst-)Kontrolle ausliefern könnte. Im Raum steht dann die allgegenwärtige und latente Gefahr, dass wir als Individuen jederzeit und allerorten

Gegenstand (d. h. auch im verfassungsrechtlichen Sinne: „Objekt") einer verdeckten Fremd-Identifizierung und potentiellen Ressourcenverwehrung ausgesetzt sind. Plattform- und sogar Endgeräte-übergreifendes Tracking hebeln Praktiken des Sich-Unsichtbar-Machens (Authentifizierungsblockaden: Anonymisierung, Maskierung u.ä.) aus und in der dehistorisierenden Aggregation von personenbezogenen Daten droht der Mensch mangels Löschung zum kontextabstrahierten, einmal kategorisierten (stigmatisierten) „Profil" zu sklerotisieren. Die möglichen Folgen für demokratische Gesellschaften könnten vor allem in Staatskrisen verheerend sein, wenn größere Bevölkerungsteile beginnen, ihre digitalen Profile zu pflegen, allgegenwärtige Kontrolle antizipierend, normalisierend, massenkonform. Soweit sind wir noch nicht – aber auch jetzt schon trifft es in westlichen Kulturen (ohnehin bereits) benachteiligte Gruppen, wenn etwa Schätz-Algorithmen des „Predictive Policing" oder automatischer Gesichtserkennung in den USA vor allem Dunkelhäutige ohne jeden Anlass als potentielle Verbrecher diskriminieren und löschungsresistent in handlungsleitenden Listen abspeichern (vgl. Belina 2020 und Meyer 2021: 20 ff.). Und während ich diese abschließenden Zeilen noch formuliere, veröffentlicht die DFG ein Informationspapier mit dem Titel „Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage"[15], in dem der Ausschuss für Wissenschaftliche Bibliotheken und Informationssysteme der DFG warnt:

> Seit einiger Zeit verändern die großen wissenschaftlichen Verlage ihr Geschäftsmodell grundlegend mit erheblichen Auswirkungen auf die Wissenschaften: Die Aggregation und die Weiterverwendung bzw. der Weiterverkauf von Nutzerspuren werden relevante Aspekte der Verlagstätigkeit. Verlage verstehen sich jetzt teilweise ausdrücklich als Unternehmen für Informationsanalysen. Das Geschäftsmodell der Verlage wandelt sich damit von Content Providern hin zu einem Data Analytics Business. Dabei werden die Daten von Wissenschaftlerinnen und Wissenschaftlern (das heißt personalisierte Profile, Zugriffs- und Nutzungsdaten, Verweildauern bei Informationsquellen usw.) bei der Nutzung von Informationsdiensten wie z. B. der Literaturrecherche getrackt, das heißt festgehalten und gespeichert. Wissenschaftstracking erfolgt durch ein Ensemble an Werkzeugen, die vom Nachverfolgen von Seitenbesuchen über Authentifizierungssysteme bis zu detaillierten Echtzeitdaten über das Informationsverhalten von Einzelnen und Institutionen reichen. [...] Diese Entwicklung kann möglicherweise erheblich in die datenschutzrechtlich grundsätzlich gewährleistete Anonymität der Wissenschaftlerinnen und Wissenschaftler eingreifen und wissenschaftliche Institutionen zu Mitverantwortlichen für die Verletzung des Rechts auf informationelle Selbstbestimmung machen. Das Datentracking leistet potenziell auch dem Datenmissbrauch und der Wissenschaftsspionage Vorschub

15 https://www.dfg.de/download/pdf/foerderung/programme/lis/datentracking_papier_de.pdf, erschienen am 20.05.2021 (28.05.2021).

> und kann zur persönlichen Diskriminierung von Wissenschaftlerinnen und Wissenschaftlern führen. […] Der Skalierung der Wissenschaftsnachverfolgung dienen Trojaner, die Bibliotheken im Zusammenhang mit Rabatten für andere Leistungen angeboten werden. Die in den Bibliotheken zu installierende Zusatzsoftware sammelt biometrische Daten wie Tippgeschwindigkeit oder Art der Mausbewegung, um auf diese Weise Nutzer trotz des Einsatzes von Proxy-Servern und VPN-Tunneln personalisieren zu können. Die von Elsevier und Springer Nature gegründete Scholarly Networks Security Initiative (SNSI) dient diesem Zweck und argumentiert auch in Verbindung mit Firmen wie PSI damit, mit solcher Zusatzsoftware Nutzerinnen und Nutzer von „Schattenbibliotheken" identifizieren und rechtlich verfolgen zu können. Diese Trojaner hebeln die Sicherheit von Hochschulnetzen aus und setzen die Hochschulen potenziell Angriffen aller Art aus. (DFG 2021: 3 ff.)

Diese Entwicklung ist alarmierend. Sie zeigt, wie notwendig eine versierte Beschäftigung der Diskursforschung mit Authentifizierungspraktiken im digitalen Raum ist, und wie sensibel die Forschungspraxis ihrerseits mit dem Umgang eigener Datensammlungen verfahren muss.

Literatur

Androutsopoulos, Jannis. 2008. Potentials and Limitations of Discourse-Centred Online Ethnography. *Language@Internet*, http://nbn-resolving.de/urn:nbn:de:0009-7-16100. (3 October, 2017).

Arp, Daniel, Erwin Quiring, Christian Wressnegger & Konrad Rieck. 2017. Privacy Threats through Ultrasonic Side Channels on Mobile Devices. *2017 IEEE European Symposium on Security and Privacy (EuroS&P), Security and Privacy (EuroS&P), 2017 IEEE European Symposium on, EUROS-P*.

Ausschuss für Wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft (DFG). 2021. Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage, https://www.dfg.de/download/pdf/foerderung/programme/lis/datentracking_papier_de.pdf (14 February, 2022).

Baringhorst, Sigrid. 2009. Politischer Protest im Netz – Möglichkeiten und Grenzen der Mobilisierung transnationaler Öffentlichkeit im Zeichen digitaler Kommunikation. *Politische Vierteljahreszeitschrift* 42. 609–635.

Belina, Bernd. 2020. Predictive Policing: dubioses Geschäftsmodell und diskriminierende Tendenzen. In Felix Bode & Kai Seidensticker (eds.), *Predictive Policing. Eine Bestandsaufnahme für den deutschsprachigen Raum*, 15–20. Frankfurt (Main): Verlag für Polizeiwissenschaft.

Bourdieu, Pierre. 2005. *Die feinen Unterschiede: Kritik der gesellschaftlichen Urteilskraft*. Frankfurt am Main: Suhrkamp.

Bourdieu, Pierre & Hella Beister. 2005. *Was heißt sprechen?: Zur Ökonomie des sprachlichen Tausches*, 2nd edn. Wien: Braumüller.

Brüning, Janique. 2006. Der Richtervorbehalt – ein zahnloser Tiger?: Über die verfassungsrechtliche Notwendigkeit des Richtervorbehalts und seine Ineffizienz in der Praxis. *Zeitschrift für Internationale Strafrechtsdogmatik* (1). 29–35.

Bucholtz, Mary. 2003. Sociolinguistic nostalgia and the authentication of identity. *Journal of Sociolinguistics* 7(3). 398–416.

Calvey, David. 2018. The everyday world of bouncers: A rehabilitated role for covert ethnography. *Qualitative Research* 25(1). 146879411876978.

Collister, Lauren B. 2014. Surveillance and Community: Language Policing and Empowerment in a World of Warcraft Guild. *Surveillance & Society* 12, http://d-scholarship.pitt.edu/22515/.

Fobbe, Eilika. 2011. *Forensische Linguistik: Eine Einführung* (Narr-Studienbücher). Tübingen: Narr.

Frohwein, Stefan, Christof Goldhammer & Anna Eggers. 2008. Sprache und Kommunikation in Second Life. http://www.mediensprache.net/archiv/pubs/4074.pdf. (5 September, 2016.)

Gießmann, Sebastian. 2020. *Identifizieren: Theorie und Geschichte einer Medienpraktik* (WORKING PAPER SERIES | NO. 17 | SEPTEMBER 2020). Universitätsbibliothek Siegen.

Jäger, Ludwig. 2003. Transkription – zu einem medialen Verfahren an den Schnittstellen des kulturellen Gedächtnisses. http://www.inst.at/trans/15Nr/06_2/jaeger15.htm. (5 October, 2012.)

Kaspar, Kai. 2017. Hassreden im Internet – Ein besonderes Phänomen computervermittelter Kommunikation? In Kai Kaspar, Lars Gräßer & Aycha Riffi (eds.), *Online Hate Speech: Perspektiven auf eine neue Form des Hasses* (Schriftenreihe zur digitalen Gesellschaft NRWBand 4), 63–70. Düsseldorf, München: Kopaed.

Lacoste, Véronique, Jakob Leimgruber & Thiemo Breyer (eds.). 2014. *Indexing Authenticity: Sociolinguistic Perspectives* (linguae & litterae 39). Berlin: De Gruyter.

Lindström, Anna. 1994. Identification and Recognition in Swedish Telephone Conversation Openings. *Language in Society* 23(2). 231–252.

Mayer, Jonathan R. & John C. Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. 413–427.

McLuhan, Marshall, Quentin Fiore & Jerome Agel. 2014 [1967]. *Das Medium ist die Massage: Ein Inventar medialer Effekte*, 3rd edn. (Tropen-Sachbuch). Stuttgart: Tropen.

Meyer, Roland. 2021. *Gesichtserkennung: Vernetzte Bilder, körperlose Masken* (Digitale Bildkulturen). Berlin: Verlag Klaus Wagenbach.

Rilling, Rainer. 1998. Marktvermittelt oder selbstorganisiert?: Zu den Strukturen von Ungleichheit im Netz. In Claus Leggewie & Christa Maar (eds.), *Internet & Politik: Von der Zuschauer- zur Beteiligungsdemokratie?*, 366–380. Köln: Bollmann.

Roesner, Franziska, Tadayoshi Kohno & David Wetherall. 2012. Detecting and Defending Against Third-Party Tracking on the Web. 155–168.

Schegloff, Emanuel A. 1979. Identification and recognition in telephone conversation openings. In George Psathas (ed.), *Everyday language: Studies in ethnomethodology*, 23–78. New York, NY: Irvington.

Spitzmüller, Jürgen, Christian Bendl & Mi-Cha Flubacher. 2017. Soziale Positionierung: Praxis und Praktik. Einführung in das Themenheft. *Wiener Linguistische Gazette* (81). 1–18.

Stertkamp, Wolf. 2017. *Sprache und Kommunikation in Online-Computerspielen*. Gießen: Justus-Liebig-Universität Dissertation.

Stöhr, Anna. 2015. *Die Todesanzeige im Wandel: Gattungsspezifische Analyse eines Kommunikationsmittels*. Diplomica Verlag GmbH.

Vogel, Friedemann. 2012. *Linguistik rechtlicher Normgenese: Theorie der Rechtsnormdiskursivität am Beispiel der Online-Durchsuchung* (Sprache und Wissen 9). Berlin [u. a.]: De Gruyter.

Vogel, Friedemann. 2016. Konflikte in der Internetkommunikation. In Friedemann Vogel, Janine Luth & Stefaniya Ptashnyk (eds.), *Linguistische Zugänge zu Konflikten in europäischen Sprachräumen. Korpus – Pragmatik – kontrovers*, 165–200. Heidelberg: Winter.

Vogel, Friedemann. 2018. Jenseits des Sagbaren – Zum stigmatisierenden und ausgrenzenden Gebrauch des Ausdrucks Verschwörungstheorie in der deutschsprachigen Wikipedia. *Aptum. Zeitschrift für Sprachkritik und Sprachkultur* 14(3). 259–288.

Vogel, Friedemann. 2020a. Authentifizierung – Grundlagen einer Theorie zu sozialsymbolischen Praktiken der Identifizierung und Zugangskontrolle. *Linguistik online* 105(5). 43–67.

Vogel, Friedemann. 2020b. „Wenn Virologen alle paar Tage ihre Meinung ändern, müssen wir in der Politik dagegenhalten“: Thesen zur politischen Sprache und (strategischen) Kommunikation im Pandemie-Krisendiskurs. *Sprachreport* 36, https://ids-pub.bsz-bw.de/frontdoor/deliver/index/docId/10043/file/Vogel_Thesen_zur_politischen_Sprache_und_Kommunikation_im_Krisendiskurs_2020.pdf. (27 October, 2020.)

Vogel, Friedemann & Katharina Jacob. 2014. Sprachkritik im Internet: Aushandlungsprozesse und Spracheinstellungen auf den Diskussionsseiten der deutschsprachigen Wikipedia. *Aptum* (1). 1–32.