Informantenschutz first: Deutschlands Journalist:innen üben sich in digitaler Sicherheit

Überwachung, Cyberangriffe und Doxxing: Sensible Daten von Journalist:innen sind im digitalen Zeitalter großen Gefahren ausgesetzt. Zum Schutz ihrer Quellen, der eigenen Person und der Redaktionen bedarf es eines geschärften Problembewusstseins und wirksamer Prävention. Digitale Sicherheit gehört zu den wichtigen Kompetenzen im Journalismus der Gegenwart und Zukunft. Sie ist eine der Voraussetzungen, damit Journalismus seinen Beitrag zur freien und aufgeklärten Gesellschaft leisten kann. Wie aber steht es um diese Kompetenzen in deutschen Redaktionen?

Die Journalismusforschung hat sich seit Edward Snowden vermehrt mit digitaler Sicherheit und ubiquitären Überwachungsmöglichkeiten befasst (Bell & Owen 2017). Surveillance kann auch in funktionierenden Demokratien ein Problem für die journalistische Berufsausübung und deren Mandat für die Öffentlichkeit sein (Moßbrucker 2019). Organisationen, die sich mit Pressefreiheit beschäftigen, haben Guidelines zu digitaler Sicherheit zusammengestellt. Eine Metastudie (Berdan 2021) zeigt jedoch ein disparates Bild: Ein Übermaß an Informationen, Tools und teils widersprüchlichen Empfehlungen verwirrt eher, als dass sie helfen.

Die Forschung in diesem Bereich weist noch viele Lücken auf. Es haben sich zwei größere Diskurse herausgebildet: Einerseits werden mit Bezug vor allem auf die Surveillance Studies Abschreckungseffekte (so genannte *Chilling Effects*) durch Überwachung diskutiert, also mögliches Nicht-Handeln, Verschweigen oder eine Verhaltensänderung (Eide 2019). Andererseits wird im Rahmen von Cyber Security Studies diskutiert, wie Journalist:innen und Medienorganisationen technologisch auf die Gefahr einer Überwachung reagieren (Henrichsen 2020). Diesbezügliche Forschungsarbeiten mit Fokus auf den Journalismus in Deutschland gibt es nur wenige.

In unserer Studie untersuchen wir den Status Quo in Deutschland mit qualitativer und quantitativer Methodik anhand eines breit angelegten Samples. Basis der Untersuchung ist eine theoretisch gesteuerte Auswahl von 20 Medienhäusern, denen kostenfrei Workshops zum Thema angeboten wurden. Mit dabei sind öffentlich-rechtliche wie private und regionale wie überregionale Medien, Funkhäuser wie reine Onlineredaktionen. Zusätzlich wurden zwei Trainings für freie Journalist:innen organisiert, so dass eine aussagekräftigen Stichprobe von bis zu 264 Journalist:innen rekrutiert werden konnte.

In einem ersten Schritt füllen alle Teilnehmenden einen Online-Umfrage aus. Der Fragekatalog entstand literaturgeleitet sowie durch vorbereitende Experteninterviews. In einem zweiten Schritt wurden die Journalist:innen während des Trainings beobachtet und ihre Äußerungen protokolliert. Mit diesem Mix wird sichergestellt, dass auch Aspekte, die in der Literatur wenig oder keine Beachtung fanden, in die Studie einfließen.

Die Daten der Online-Umfrage werden deskriptiv statistisch ausgewertet und anhand von aus der Literatur abgeleiteten Hypothesen auf Korrelation getestet. Die Ergebnisse der Beobachtung werden transkribiert und per Inhaltsanalyse nach deduktiven und induktiven Kategorien ausgewertet.

Die ersten Ergebnisse aus der Umfrage zeigen ein eher diffuses und unspezifisches Problembewusstsein. Teilnehmende geben an, sich den Risiken in der digitalen Recherche bewusst zu sein, gleichzeitig fühlt sich ein Großteil in Bezug auf digitale Bedrohungen „eher unsicher“.

Die Arbeitgeber werden mit Intransparenz assoziiert. Die große Mehrheit der Befragten ist sich hinsichtlich der Maßnahmen des Arbeitgebers im Bereich digitale Sicherheit „unsicher“. Geäußert werden etwa Wünsche nach Weiterbildungen und praxisorientierteren IT-Abteilungen.

Der in der Literatur viel zitierte „chilling effect“ (Penney 2017) wird in den quantitativen Ergebnissen insbesondere in Bezug auf Dritte sichtbar. So geben Befragte häufig an, dass andere Journalist:innen

Dinge wohl nicht veröffentlichen, wenn sie sich bedroht fühlen. Auf sich selbst bezogen, glauben sie eher nicht, Recherchen zurückzuhalten. Im Gegenteil: Die Befragten geben relativ häufig an, wegen der digitalen Bedrohungslage neue Recherchen zu initiieren, neue Technologien anzuwenden und neue Kompetenzen zu erlernen. Diese Resultate bestärken kritische Stimmen aus den Surveillance Studies, die die pauschale Annahme von "chilling effects" kritisieren. Journalist:innen beschränken sich demnach nicht auf Schweigen und Verstecken, sondern können ihre Kompetenzen strategisch einsetzen und handlungsfähig bleiben. Das gilt im Idealfall auch für Fragen der physischen Sicherheit – etwa in der Lokalberichterstattung zu Rechtsextremismus.

Dafür braucht es jedoch angemessene digitale Kompetenzen, geeignete Infrastrukturen und praxisorientierte Handlungskonzepte. Diese zu identifizieren und konstruktiv zu entwickeln soll der nächste Schritt unseres Forschungsprojekts sein. Im Interesse von Transfer werden die Ergebnisse dialogisch in die beforschten Medienhäuser rückgespiegelt.

Bell, E. & Owen, T. (2017). *Journalism after Snowden: The future of the free press in the surveillance state*. *Columbia journalism review books*. Columbia University Press.

Berdan, K. (January, 2021). *An Evaluation of Online Security Guides for Journalists* (CLTC White paper Series). Berkeley.

Eide, E. (2019). Chilling Effects on Free Expression: Surveillance, Threats and Harassment. In *Making Transparency Possible* (S. 227–242). Cappelen Damm Akademisk/NOASP.

Henrichsen, J. R. (2020). Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism*, *8*(3), 328–346.

Moßbrucker, D. (2019). Digitaler Informantenschutz. In M. Schröder & A. Schwanebeck (Hrsg.), *Big Data - In den Fängen der Datenkraken* (S. 87–106). Nomos Verlagsgesellschaft mbH & Co. KG.

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, *6*(2).