Buchrezension

kommunikation.medien
Open-Access-Journal
für den wissenschaftlichen Nachwuchs
ISSN 2227-7277
Nr. 9/2018
http://eplus.uni-salzburg.at/JKM
DOI: 10.25598/JKM/2018-9.18

Welchering, Peter/Kloiber, Manfred (2017): Informantenschutz. Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation. Wiesbaden: Springer, 146 S., 22,99 €
ISBN: 978-3-658-08718-0

Martin Oberbichler

Über journalistische Praktiken wurde in den letzten Jahren viel geschrieben. Vor allem durch neue Methoden und Möglichkeiten, die Onlinemedien bieten, änderten sich Arbeitsweisen. Rasche Informationsbeschaffung, Überprüfung vorhandener Quellen und das schnelle Publizieren stehen hierbei im Vordergrund. Dass diese Veränderungen den Journalismus prägten und zugleich auch veränderten, haben nicht nur Peter Welchering und Manfred Kloiber erkannt. In ihrem an die Praxis angelehnten Werk aus dem Jahr 2017 halten sie die ethischen, rechtlichen und technischen Veränderungen der letzten Jahre fest und geben einen Einblick in die journalistische Praxis und den Informantenschutz. Vor allem die technischen Aspekte rund um die Themen Verschlüsselungen und Sicherheit, die sich durch das Internet ergeben, spielen in diesem Werk eine entscheidende Rolle.

Gleich im ersten Kapitel des Buches („Die tägliche Datenspur“, S. 1-8) zeigen die Autoren, dass sich Journalisten und Journalistinnen zum Teil nicht bewusst sind, im täglichen Gebrauch des Internets Datenspuren zu hinterlassen und welche Folgen dies haben kann. Fehlende Sensibilität sowie mangelndes Wissen über Programme im Hintergrund von speziellen Dienstleistern werfen die Autoren Journalisten und Journalistinnen bei der Recherche von Themen vor (S. 7f.). Des Weiteren nennen sie Beispiele für Datenspeicherung und Überwachungen unterschiedlicher Anwendungen und Geräte im Alltag: der Wecker am Smartphone, Kameras an öffentlichen Orten, Suchmaschinen im Internet bis hin zu intelligenten Stromzählern und der Mikrowelle.

In Kapitel zwei („Grundlagen des Informantenschutzes“, S. 9-24) geht es um die Grundlagen des Informantenschutzes und somit die rechtlichen Aspekte. Dabei werden wichtige Rechtsgrundlagen erklärt, wie etwa die Bedeutung des Informantenschutzes, der Presse- und Rundfunkfreiheit oder die Haftung des Informanten bzw. der Informantin. Die Autoren stellen von vornherein klar, dass Journalisten und Journalistinnen genauso wie Whistleblower unverzichtbar als Wächter der Demokratie sind (S. 10) und schreiben des Weiteren dem Informantenschutz einen hohen Stellenwert zu. Die medienethische Begründung des Informantenschutzes erklären die Autoren insofern, als dass Journalisten und Journalistinnen auf Whistleblower angewiesen sind, um eine umfassende Berichterstattung über sensible Vorgänge zu gewähren (S. 21).

Mit einem anschaulichen Beispiel zur Recherche sowie den damit verbundenen Datenspuren beginnt Kapitel drei („Datenspuren bei der Recherche und ihre Analyse“, S. 25-30): Die Finanzierung der elektronischen Personalausweise in Deutschland aus dem Jahr 2006 wird von den Autoren genannt. Dabei handelte es sich um einen Vorschlag vonseiten des Innenministeriums, neben demografischen Daten auch biometrische Werte wie Fingerprints oder Iris-Scans im Personalausweis zu speichern. Dieses aus ihrer eigenen Praxis bekannte Beispiel wird als Best Practice-Beispiel verwendet, um zu zeigen, mit welchem Vorgehen eine ordentliche Recherche erfolgen kann. Verdeckte Recherche, technische Komponenten, der Schutz des Informanten mittels Einmal-Telefonnummern oder die Kontaktaufnahme mit dem Bundesministerium prägten die Vorgehensweise der Autoren zu ordentlichen Recherchevorgängen bei sensiblen Themen.

Kapitel vier („Informanten im Netz schützen“, S. 31-42) gibt dem Leser bzw. der Leserin einen Einblick in den Schutz von Informanten und Informantinnen im Netz. Dieser zum Teil sehr technisch und mit Fachausdrücken geprägte Abschnitt wird jedoch mit Beispielen aus der Praxis erläutert. Unter anderem wird das Vorgehen der NSA (National Security Agency) geschildert. Wichtige Bausteine des Schutzes der eigenen Informanten bzw. Informantinnen sind unter anderem getarnte Mail-Adressen, der erfolgreiche und sichere Erstkontakt sowie die Vereinbarung von Treffen mittels verschlüsselter Symbole in GIFs oder ähnlichen Formaten (S. 33-35).

Ein weiterer sehr technischer Abschnitt findet sich in Kapitel fünf („Der PC und seine verräterischen Spuren“, S. 43-56). Hier werden die Problematiken des Computers in Bezug auf die Sicherheit eines möglichen Zugriffes beschrieben und welche Spuren damit hinterlassen werden können. Primär werden hierbei temporäre Dateien genannt, die von Programmen zum Teil automatisch erzeugt werden. Eines der wichtigsten Tools, Dateien vor verräterischen Metadaten zu schützen, ist der PDF-Creator. Dieser erstellt keine genaue Kopie der Datei, sondern erzeugt eine PDF-Datei mit dem Abbild des Ausdrucks (S. 47).

In Kapitel sechs („Surfen ohne Spuren“, S. 57-76) widmen sich die Autoren dem richtigen Surfen im Internet. Welchering und Kloiber sind auch in diesem Abschnitt wieder darauf bedacht, den Fokus auf die technische Komponente zu richten. Als grundlegendes Werkzeug von Journalisten und Journalistinnen nennen sie öffentliche Computer in Verbindung mit sogenannten Einmal-Browsern, um eine sichere Recherche zu betreiben (S. 58). Zusätzlich raten die Autoren, Datenschutz-Einstellungen von Browsern zu beachten oder den Verschleierungsdienst TOR (The Onion Router) zu verwenden (S. 61 -65).
Ein ähnliches Vorgehen bei der Recherche gibt es auch in Kapitel sieben („Mail verschlüsseln“, S. 77-92). Beim richtigen Verschlüsseln von Mails spielen für die Autoren abermals zahlreiche technische Komponenten eine entscheidende Rolle. Sie streichen etwa den Einsatz von Thunderbird heraus, um eine brauchbare Zertifizierung bei Mails zu erhalten (S. 83). Ein zentraler Aspekt dieses Kapitels ist die asymmetrische Verschlüsselung. Diese Form der Verschlüsselung weist zwei verschiedene Schlüssel auf: den öffentlichen und den geheimen Schlüssel (S. 80). Die Autoren beschreiben diese Anwendung im Detail.
Die folgenden drei Kapitel (acht bis zehn) behandeln das Thema Informantenschutz und die sichere Kommunikation zwischen Journalisten bzw. Journalistinnen und Informanten bzw. Informantinnen. Dabei gehen die Autoren kurz auf den grundlegenden IT-Schutz ein. Dabei nennen sie zahlreiche Methoden, Daten zu schützen und zu speichern, verweisen auf den Gebrauch von externen Rechnern in Serverräumen und warnen vor tragbaren Geräten (S. 93). Auch nicht-elektronische Methoden des Informantenschutzes sollen eine (fast) sichere Kommunikation ermöglichen. Ein solches Beispiel sind etwa Postkarten (S. 109). Im digitalen Bereich sollten zudem wieder Verschlüsselungen verwendet werden - die Autoren nennen hier Truecrypt (S. 110). Um im Anschluss einen sicheren Datenaustausch bzw. ein sicheres Treffen mit den Informanten bzw. Informantinnen zu ermöglichen, verwendeten die Autoren Verschlüsselungssoftwares oder ließen Umschläge mit einer Nachricht an der Rezeption des Hotels der Informanten und Informantinnen (S. 121).
Im letzten Kapitel („Quo vadis, Informantenschutz?“, S. 133-146) fassen die Autoren verschiedene Möglichkeiten des Informantenschutzes zusammen und geben einen Ausblick auf mögliche Entwicklungen und aktuelle Thematiken in dem Bereich des Informantenschutzes.

Grundsätzlich ist das Buch als Zusammenfassung praktischer Methoden der Informationsbeschaffung anzusehen. Dies ist nicht nur an der praktischen Auslegung, sondern auch an den genannten Beispielen deutlich zu erkennen. Es vermittelt einen Überblick über die Gefährdungsgrundlagen und die entsprechenden Schutzmaßnahmen und Abwehrmethoden möglicher Überwachungen und Sicherheitslücken. Hervorzuheben sind die darin genannten Beispiele aus der Praxis der beiden Autoren, die sich etwa mit der Finanzierung der elektronischen

Personalausweise in Deutschland oder der Kontaktaufnahme mit der Organisation Anonymous beschäftigen.
Kritisch zu betrachten ist jedoch der Nutzen für die Kommunikationswissenschaft bzw. die zu bestimmende Zielgruppe. Klar ersichtlich ist die technische Komponente, die in allen Kapiteln des Werks im Mittelpunkt steht und die im Titel erwähnte technische Praxis erkennen lässt. Die zum Teil zu sehr ins Detail gehende Erklärung unterschiedlicher Verschlüsselungs-Techniken bzw. von Möglichkeiten der sicheren Informationsbeschaffung ist nur für technisch Versierte verständlich. Die Autoren versuchen jedoch mit zahlreichen Beispielen die Komplexität zu reduzieren und somit auch all jenen einen Eindruck zu vermitteln, die nicht auf demselben technischen Niveau agieren. Für alle, die sich nur grundsätzlich über journalistische Praktiken des Informantenschutzes informieren wollen, ist dieses Werk mitunter ein zu praktisch ausgelegter und zu komplexer Einstieg in diese Thematik.

Kurzbiografie des Autors

Martin Oberbichler, BA, ist 27 Jahre alt und absolviert das Masterstudium Kommunikationswissenschaft an der Universität Salzburg. Während dem Studium war Martin Oberbichler bei zahlreichen Medienunternehmen im Redaktionsbereich tätig und arbeitet derzeit als Contentmanager eines Online-Reiseanbieters.
Kontakt: Martin.Oberbichler@stud.sbg.ac.at