Dominique Strebel, Studienleiter MAZ und Co-Präsident investigativ.ch, dominique.strebel@maz.ch

Quellenschutz konkret

1. Informanten bereits vor dem ersten Kontakt mit den Medien schützen

Deshalb Postanschrift, public Key, Threema ID in öffentliches Register von investigativ.ch eintragen und in Xing, LinkedIn, Signatur etc. folgenden Eintrag machen:
«Hinweis für Informanten: Bitte lesen Sie vor dem ersten Kontakt das Infoblatt für Informanten (http://www.investigativ.ch/downloads/infoblatt-fuer-informanten.html) durch. Nehmen Sie nie per Büromail oder -telefon und nie per Handy, sondern am besten per Post (Name, Adresse) oder Telefon ab öffentlicher Telefonkabine mit mir Kontakt auf (Festnetznummer). Auch möglich ist ein verschlüsseltes Mail ab Privatcomputer über Tor-Browser (www.torproject.org). Mein public Key lautet: .... Dokumente bitte per Post zustellen – allenfalls auf USB-Stick.»

2. Informanten beim ersten Treffen umfassend checken und aufklären

a. Weshalb will der Informant an die Öffentlichkeit gelangen? Die Motive erlauben nicht nur einen Glaubwürdigkeitscheck, sondern zeigen auch mögliche Gefahren für den Informanten.
b. Abklären, ob der Informant überhaupt zu schützen ist: Wer weiss vom Missstand? Wer alles kann die Dokumente besitzen? Und mit wem hat der Informant über den Missstand bereits geredet? Besteht aus rechtlicher Sicht überhaupt Quellenschutz? (Bei 25 Delikten hat der Journalist nur ein eingeschränktes Zeugnis- und Editionsverweigerungsrecht vgl. Text in «Medienwoche» vom 21. Januar 2015: «Quellenschutz von Fall zu Fall»).
c. Empfehlung: Entweder intern melden – dann aber nicht an die Medien gelangen. Oder über die Missstände und den Gang an die Medien mit niemandem reden (auch nicht mit Ehemann/Ehefrau).
d. Dokumentation der Missstände: Nicht auf Geschäftscomputer, nichts ins Geschäfts-Outlook schreiben, Achtung beim Download von internen Dokumenten (wer alles hat Zugriff? Welche Sicherungen gibt es?). Keine Dokumente am Arbeitsplatz rumliegen lassen.
e. In Dokumenten immer Metadaten löschen und Name einschwärzen.
f. Kommunikationswege definieren (vgl. Beschrieb der Sicherheit im Infoblatt für Informanten).
g. Rechtliche Risiken von Whistleblowing:
    i. Eine Kündigung ist grundlos möglich. Falls ein Gericht eine Kündigung als missbräuchlich anerkennt, bekommt man nicht die Stelle zurück, sondern bestenfalls 6, in der Regel aber 2-4 Monatslöhne Entschädigung.
    ii. Amts-, Geschäfts- oder Bankgeheimnisverletzungen werden streng geahndet (der Rechtfertigungsgrund der Wahrung berechtigter Interessen greift kaum).
h. Quellenschutz: Nicht nur Journalisten sondern auch Informanten können das Editionsverweigerungsrecht in Anspruch nehmen: Sobald ein Polizist oder Staatsanwalt auftaucht sollte der Informant die Versiegelung von Computer, Dokumenten etc. verlangen.
i. Eine Stunde vor jedem Treffen Handys ausschalten, da der Ort, wo sie sich befinden, via Vorratsdatenspeicherung noch Monate danach nachverfolgt werden kann.
j. Allfällige Codewörter vereinbaren.

3. Verhaltenstipps für Journalisten

a. Falls Erstkontakt per unverschlüsseltes E-Mail geschah, antworten Sie per unverschlüsseltem Mail: «Es tut mir leid, ich kann Ihnen leider nicht helfen. Mit freundlichen Grüssen…»
b. Treffpunkt mit Informant sorgfältig aussuchen: Parkhaus? Öffentlicher Raum?
c. Handy mindestens eine Stunde vor dem Treffen ausschalten. Handy nicht für Kommunikation einsetzen.
d. In Extremfällen: Wichtige Informationen auf Zettel austauschen.
e. Für den Informanten immer Codenamen benutzen, auch in den eigenen Notizen.
f. Dokumente immer einschwärzen, Metadaten löschen.
g. Dokumente nur auf einem Computer anschauen und bearbeiten, der nicht fürs Internet benutzt wird.
h. Festplatte (und Handy) verschlüsseln. (Die im Betriebssystem vorhandene Variante reicht für einen angemessenen Grundschutz.)
i. Computer immer korrekt runterfahren und ausloggen. Bildschirm bei Nichtbenutzen sperren. Keine Passwörter speichern.
j. Keine Synchronisation von Daten in die Cloud und zum Hersteller des Betriebssystems/ Computers/ Smartphones.
k. Im Computer beim Löschen von Dokumenten immer «secure empty trash» wählen.
l. Keine Dokumente/Papiere am Arbeitsplatz rumliegen lassen.
m. Nach dem Treffen nächstes Treffen oder Codewort für nächstes Treffen vereinbaren.
n. Falls der Medienschaffende selbst Zwangsmassnahmen erleidet: Umfassenden Quellenschutz beanspruchen, Versiegelung von Computer, Dokumenten etc. verlangen.

Weiterführende Links/Literatur

- Infoblatt für Informanten von investigativ.ch: www.investigativ.ch/downloads/infoblatt-fuer-informanten.html
- Artikel in der «Medienwoche» vom 21. Januar 2015: «Quellenschutz von Fall zu Fall» (rechtliche Informationen über den Quellenschutz).