Verhaltenstipps für Informanten des Schweizer Recherchenetzwerkes investigativ.ch

Journalisten des Recherchenetzwerkes investigativ.ch geben den Namen von Informanten nicht preis, auch nicht, wenn sie in einem Strafverfahren einvernommen werden. Dafür gibt es den Quellenschutz, der es Journalisten erlaubt, die Aussage zu verweigern. Doch noch wichtiger ist das Verhalten des Informanten selbst.

Wenn ein Informant einem Journalisten eine wichtige Information oder ein vertrauliches Dokument zukommen lässt, muss er sich von Anfang an richtig verhalten, denn Informanten, die Geheimnisse öffentlich machen, um Missstände anzuprangern (Whistleblower), sind gefährdet. Der Arbeitgeber kann ihnen grundlos kündigen, und wer ein Amts- oder Geschäftsgeheimnis öffentlich macht, macht sich strafbar, wenn er den Missstand nicht zuerst an den Arbeitgeber und allfällige interne oder externe Anlaufstellen gemeldet hat.

Deshalb müssen Sie sich zuallererst klar werden: Gehen Sie den Weg über den Arbeitgeber, allfällige interne oder externe Anlaufstellen für Whistleblower oder Behörden (zB. Staatsanwaltschaften) oder wenden Sie sich an die Medien, um den Missstand öffentlich zu machen? Es ist sinnvoll, diesen Entscheid grundsätzlich und zu Beginn zu fällen. Wenn Sie sich nämlich zuerst an den Arbeitgeber wenden, danach aber doch an die Medien, ist es für Arbeitgeber oder Strafverfolger oft einfach herauszufinden, wer den Missstand öffentlich gemacht hat.

Wenn Sie sich an Medien wenden, beachten Sie folgende fünf Punkte, bevor Sie mit einem Journalisten Kontakt aufnehmen

1. Zentral: Verschwiegenheit und Vorsicht

Die grösste Gefahr für Whistleblower sind die Whistleblower selbst. Viele Whistleblower mussten nur deshalb Nachteile wie Kündigung oder strafrechtliche Verurteilung auf sich nehmen, weil sie ihre Kritik und den Gang an die Öffentlichkeit an der Arbeitsstelle oder sonstwo rumerzählt haben. Deshalb: Erzählen Sie am besten niemandem von den Missständen und auch nicht von Ihrem Entscheid, an die Medien zu gelangen – weder Freunden noch Familienmitgliedern und schon gar nicht Arbeitskollegen.

2. Dokumentieren Sie sich und suchen Sie Verbündete, aber vorsichtig

Suchen Sie Belege, Dokumente und weitere Zeugen für Ihre Beobachtungen. Schreiben Sie auf, was Sie wann unternommen haben. Doch benutzen Sie keine Firmencomputer, kein Firmenmail oder Firmentelefon. Sonst hinterlassen Sie Spuren, die man gegen Sie verwenden kann. Auch wenn Sie Dokumente von internen Servern herunterladen, hinterlassen Sie Spuren. Machen Sie dies also zu Zeiten, die nicht auffällig sind, und achten Sie darauf, dass auch andere in diesen Zeiträumen auf die Dokumente zugreifen. Anonymisieren Sie Dokumente soweit möglich. Schwärzen Sie auch Ihren Namen. Löschen Sie die Metadaten von PDFs. Was das ist und wie man sie löscht, erfahren Sie zum Beispiel auf dieser Website (http://wiki.ubuntuusers.de/Metadaten). Schreiben Sie nichts Verdächtiges in Ihre Outlook-Agenda, schon gar nicht den Termin für ein Treffen mit dem Journalisten.

3. Den Namen bekannt geben oder anonym bleiben?

Der beste Schutz für Whistleblower ist die Anonymität. Ist der Name des Whistleblowers nicht bekannt, kann ihm nichts passieren. Die Anonymität hat aber auch Nachteile: Eine anonyme Meldung ist weniger glaubwürdig und Rückfragen sind nicht möglich. Oft können anonyme Meldungen nicht überprüft und deshalb journalistisch nicht verwertet werden. Bei einer anonymen Meldung riskieren Sie also, dass nichts passiert.

4. Informieren Sie sich über Ihre Rechte und nehmen Sie diese wahr!

Informieren Sie sich als Whistleblower frühzeitig über Ihre Rechte. Der «Beobachter» hat eine Beratungsstelle für Whistelblower eingerichtet: +41(0)43 444 54 11, erreichbar jeweils werktags von 09:00 bis 13:00 Uhr. Sie erhalten aber auch rechtliche Beratung von Transparency International Schweiz: +41(0)31 382 50 45, werktags von 9 bis 12 Uhr.

Wichtig zu wissen: Verlangen Sie bei Hausdurchsuchung oder Beschlagnahme von Datenträgern und Dokumenten unbedingt sofort Versiegelung. Der Kontakt mit Journalisten sowie Dokumente, die Sie mit Journalisten ausgetauscht haben oder die den Kontakt belegen, fallen unter den Quellenschutz und müssen ausgesondert werden.

5. Vorsicht bereits beim ersten Kontakt mit dem Journalisten

Die Art, wie Sie mit einem Journalisten Kontakt aufnehmen, und wie Sie auch später mit ihm kommunizieren, ist entscheidend für Ihren Schutz.

Als Grundsätze gelten:

1. Kommunizieren Sie nie über Geschäftscomputer, Geschäftsmail oder Geschäftstelefon. Diese Daten werden vom Arbeitgeber und vom Staat gespeichert (Vorratsdatenspeicherung).

2. Analoger Kontakt (Brief oder Treffen, Hinterlegen von Dokumenten) ist sicherer als digitaler Kontakt (E-Mail oder Smartphone). Bei Treffen das Handy am besten zuhause lassen.

3. Kommunikation per Desktop-Computer ist besser als übers Smartphone.

4. Die Sicherheit der E-Mail-Kommunikation variiert stark von Mailprovider zu Mailprovider. Bei Bluewin.ch können Strafverfolgungsbehörden zB einfach Ihre Randdaten erheben (Swisscom untersteht als Provider dem einschlägigen Gesetz (BÜPF)), bei gmx.ch hingegen ist es schwieriger (der Provider hat seinen Sitz in Deutschland).

Das Recherchenetzwerk investigativ.ch empfiehlt eine erste Kontaktaufnahme per Post, notfalls per Telefon aus einer öffentlichen Telefonkabine oder per sorgfältig ausgewähltem Mailprovider (vgl. oben).

Wer sich technisch gut auskennt, fragt per verschlüsseltem Mail von privatem Computer über TOR-Browser einen Journalisten an (www.torproject.org – simple Handhabung). Post-Anschriften, Telefonnummern oder Public Keys von Recherche-Journalisten finden Sie im öffentlichen Mitgliederverzeichnis des Recherchenetzwerkes investigativ.ch.

Hier eine (nicht abschliessende) Liste von Kontaktformen mit Vor- und Nachteilen:

• **Per Post**

Der gute alte Brief ist noch immer eine sichere Form der Kommunikation. Wenn Sie ganz sicher gehen wollen, achten Sie darauf, dass Sie den Brief in Distanz zu Ihrem Wohn- und Arbeitsort einwerfen. Vergessen Sie nicht, im Brief die Art der weiteren Kommunikation zu definieren. Wenn Sie selbst der Post misstrauen, übermitteln Sie Dokumente am sichersten, indem sie diese dem Journalisten in den Briefkasten legen. Wenn Sie Daten zustellen wollen, die nur oder besser digital zu lesen sind, schicken Sie diese nicht per Mail – auch nicht verschlüsselt – (siehe weiter unten), sondern kopieren Sie die Daten auf einen USB-Stick und übermitteln Sie diesen direkt per Eigenzustellung oder über die Briefpost.

• **Digitale Briefkästen von Redaktionen und SecureDrop**

Einzelne Redaktionen haben digitale Briefkästen eingerichtet, über die Sie Daten hochladen und Nachrichten mitteilen können, ohne dass Sie Spuren hinterlassen (vgl. etwa www.sichermelden.ch). Auch internationale Medien bieten solche digitalen Briefkästen an (basierend auf SecureDrop). Die Liste dieser Redaktionen findet sich hier https://securedrop.org/directory .

Für Strafverfolger kann zwar nicht nachvollzogen werden, *was* Sie an diesen digitalen Briefkästen gemacht haben, aber *dass* Sie ihn besucht haben. Zwar können Sie die Auswertung dieses Kontakts untersagen, da er unter Quellenschutz fällt, doch gegenüber Nachrichtendiensten ist diese Garantie wertlos und auch gegenüber Strafverfolgern ist sie fehleranfällig, da Sie nicht sicher sein können, dass Zwangsmassnahmengerichte sie aussondern. Deshalb wird empfohlen, solche digitalen Briefkästen nur über den TOR-Browser zu besuchen (www.torproject.org). Dann kann auch die Tatsache, dass sie den Briefkasten besucht haben, von Dritten nicht nachverfolgt werden.

• **Kontaktformular auf der Redaktionsseite / Webformular auf der persönlichen Website eines Journalisten**

Kontaktformulare sind meist sicherer als Mails, da sie weniger Spuren hinterlassen. Es kann aber nicht ausgeschlossen werden, dass die Nachricht dennoch per Mail zur Redaktion weitergesendet wird. Das Formular muss zudem per https (also verschlüsselt) angeboten werden. Natürlich kann der Besuch des Kontaktformulars von der Redaktion selbst, aber auch von Strafverfolgern rückverfolgt werden, da Ihre IP-Adresse Sie identifizierbar macht. Die IP-Adresse ist eine Zahlenreihe, die Sie auf jeder Website hinterlassen, die Sie besuchen und die sie und Ihren Standort mit hunderprozentiger Präzision identifiziert. Deshalb wird empfohlen, solche Kontaktformulare nur über den TOR-Browser zu besuchen und die Nachricht zu verschlüsseln (siehe „Verschlüsseltes Mail" weiter unten). Dann kann auch die Tatsache, dass sie die Website besucht haben, von Dritten nicht nachverfolgt und der Inhalt nur vom Empfänger gelesen werden.

• **Telefonieren von einer öffentlichen Telefonkabine aus**

Telefonieren hinterlässt weniger Spuren als mailen. Über Fixnet telefonieren ist besser als über Mobiltelefon. Brauchen Sie aber weder ihren Geschäfts- noch ihren privaten Anschluss, sondern benutzen Sie eine öffentliche Telefonkabine.

• **Nachricht über SMS**

Das Senden einer Nachricht über SMS ist so unsicher wie ein Anruf vom Smartphone. Strafverfolger können die Randdaten (Wer hat wem wann eine SMS geschickt und von wo nach wo?) auswerten, Nachrichtendienste die Nachrichten mitlesen. Zudem bleibt die

SMS im Smartphone gespeichert, wenn Sie sie nicht aktiv löschen. Zwar können Sie bei einer allfälligen Beschlagnahmung des Smartphones die Versiegelung und das Aussondern der Kontakte mit Medienschaffenden verlangen (Quellenschutz), doch gestehen Sie damit auch ein, solche Kontakte gehabt zu haben.

• **Nachricht über WhatsApp**

WhatsApp bietet mittlerweile Ende-zu-Ende-Verschlüsselung. Allerdings muss davon ausgegangen werden, dass die Metadaten (wer kommuniziert wann mit wem) vom Anbieter gespeichert werden und Strafverfolgungsbehörden und Geheimdiensten (mindestens auf Anfrage) zur Verfügung gestellt werden.

• **Nachricht über Threema, Wire, Signal oder Telegram**

Threema ist ein (Schweizer) Nachrichtendienst, der die gesamte Kommunikation automatisch verschlüsselt. Sie ist als App für iphone oder für Android für wenig Geld erhältlich. Der Inhalt ist für Aussenstehende somit nicht lesbar. Doch können Strafverfolgungsbehörden via Randdaten aus der Vorratsdatenspeicherung nachvollziehen, an wen Sie wann eine Nachricht geschrieben haben. Kontaktaufnahme mit Journalisten dürfen Strafverfolgungsbehörden wegen des Quellenschutzes grundsätzlich nicht einsehen, doch ist das Aussondern solcher Mails fehleranfällig. Einige Journalisten machen ihre Threema ID öffentlich. Wire, Signal oder Telegram sind vergleichbare (ausländische) Dienste.

• **Nachricht über Skype**

Skype ist heute nicht mehr viel sicherer als ein normales Telefongespräch. Skype hat sich verpflichtet, mit Strafverfolgungsbehörden und Nachrichtendiensten zusammenzuarbeiten.

• **Privates Mail von privatem Computer oder Internetcafé**

Bei E-Mail ist die Wahl des Mailproviders wichtig. Ansonsten kann ebenso gut eine Postkarte verschickt werden. Sowohl Absender und Adressat wie auch der Inhalt können mitgelesen werden. Strafverfolgungsbehörden können via Vorratsdaten nur die Randdaten (also etwa Absender und Adressat, Datum und Zeit der Kommunikation) einsehen. Zudem ist ihnen selbst dies bei einer Kommunikation mit Journalisten untersagt. Doch ist das Aussondern solcher Mails fehleranfällig. Ein privates Mail von einem privaten Computer hat aber den Vorteil, dass der Arbeitgeber auf keinen Fall darauf zugreifen kann. Zwar darf der Arbeitgeber auch als privat gekennzeichnete Mails auf dem Server am Arbeitsplatz nicht lesen, doch ist die Tatsache einer Kontaktnahme mit einem Journalisten belegbar. Zudem kann eine Kündigung grundlos erfolgen und das kann auch aufgrund einer (verbotenen) Auswertung privater Mails geschehen. Als Mailprovider, die Wert auf Sicherheit legen, können zum Beispiel posteo.de oder mailbox.org empfohlen werden. Diese lassen sich auch einfach mit GnuPG/Mailvelope kombinieren (siehe unten).

• **Verschlüsseltes Mail von privatem Computer aus**

Falls Sie per Mail kommunizieren wollen, verschlüsseln Sie die Kommunikation mit einem gängigen Verschlüsselungsprogramm (zB. GnuPG, resp. OpenPGP, GPG, Mailvelope). Einige Journalisten machen ihren Public Key öffentlich zugänglich (vgl. öffentliches Mitgliederverzeichnis auf www.investigativ.ch). So kann der Inhalt von Drittpersonen nicht gelesen werden. Aber es bleibt via Vorratsdaten für Strafverfolgungsbehörden erkennbar, wer wem wann ein Mail geschickt hat. Kontaktaufnahme mit Journalisten dürfen Strafverfolgungsbehörden wegen des Quellenschutzes grundsätzlich nicht einsehen, doch ist das Aussondern solcher Mails fehleranfällig. Die Software kann auch

verwendet werden, um Dateien oder Texte zu verschlüsseln, die dann via Kontaktformular versendet werden können (siehe weiter oben).

- **Kontakt via TOR-Browser**

Wer einen Journalisten kontaktieren will und mit der PGP-Verschlüsselung überfordert ist, kann einen TOR-Browser herunter laden und installieren (www.torproject.org). Das ist viel einfacher, als man sich es vorstellt. Bei einem Mail-Anbieter eine Adresse registrieren (auf einen fiktiven Namen) und von dieser Adresse aus mit dem Journalisten Kontakt aufnehmen. Damit taucht der Name des Informanten nirgendwo in den Randdaten auf, ebenso wenig seine IP-Nummer. Bei mailbox.org lassen sich zusätzlich per «Guard-Sicherheit» PGP-verschlüsselte Mails versenden.

Eine gute Übersicht über diese und weitere Tools finden Sie hier (https://www.digitale-gesellschaft.ch/?p=8383)

Kire/ds, 10. 11. 2016