Kameras, Richtmikrofone, Smartphones & Geister

Überwachung und Paranoia

Emanzipatorische Überwachungskritik und direkte Aktion

Überwachung soll Freiräume eingrenzen und Verhalten normieren. Sie steht damit grundsätzlich der emanzipatorischen Idee von Selbstentfaltung im Wege. Das gilt unabhängig davon, wer mit welchem Ziel überwacht, kontrolliert. Auch „linke“ Ideen einer verstärkten Kontrolle (z.B. rechter Parteien, großer Konzerne, internationaler Finanztransfers oder bestimmter Straftätergruppen) sind in diesem Sinne immer antiemanzipatorisch, weil sie die Unterdrückung des gesellschaftlich (und damit herrschaftsförmig) als unerwünscht Stigmatisierten bedeuten würden.

Aktionstipps gegen Überwachung und Kontrolle über www.direct-action.tk

Eine emanzipatorische Kritik der Überwachung greift den Kern der Idee von Überwachung an — nämlich den Glauben, das Gute gegen das Böse von oben durchsetzen zu können. Es geht um das Prinzip von Überwachung, nicht um den konkreten Zweck. Normierung widerspricht der Selbstbestimmung — unabhängig davon, auf welche Norm Menschen getrimmt werden. Überwachung ist die Nachsorge dessen, was mit Pädagogik, Gesetzen und Diskursen an gewünschten Verhaltensweisen und an Moral in die Köpfe gebracht wird. Befreiung beinhaltet die Zerschlagung der Maschinerie, die dem Denken zunächst eine vorgegebene Richtung gibt und das Einhalten dann kontrolliert. Es gibt keine emanzipatorische Form der Überwachung.

Utopie einer kontroll- und straffreien Gesellschaft

Freiheit von Herrschaft kann es nur dort geben, wo Überwachung und Kontrolle fehlen. Denn Überwachung setzt voraus, dass welche da sind, die überwachen, und andere, die (potentiell) überwacht werden sollen. Die unterschiedlichen Möglichkeiten zerstören die Horizontalität zwischen den Menschen und zementieren das Gefälle von Macht. Dann aber entsteht Herrschaft, die dauerhafte Form (institutionalisierter) Machtunterschiede. Eine herrschaftsfreie Welt entsteht nur dann, wenn alle Formen organisierter unterschiedlicher Handlungsmöglichkeiten abgebaut werden. Das beinhaltet die Negation formaler Beschränkungen, ist aber mehr, nämlich das produktive Schaffen gleicher Möglichkeiten, da diese nicht von Natur aus bestehen. Welche dieser Handlungsmöglichkeiten Menschen in ihrem Leben nutzen, entscheiden sie. Dabei befinden sie sich immer in Kontakt mit anderen, handeln also als gesellschaftliche Wesen. Alle Beziehungen, das Eingehen oder Verweigern von Kooperation vollziehen sich aber ohne Zwang, d.h. in freier Vereinbarung.

Kritik an Machtverhältnissen und herrschaftsfreie Utopien unter www.herrschaft.tk

Überwachung und Kontrolle gibt es in einer herrschaftsfreien Gesellschaft folglich nicht. Aus der Sicht einer aktuell auch in linken Diskursen nach Sicherheit statt offenen Prozessen strebenden Denkkultur wirft das die Frage auf, wie mit Verhaltensweisen umgegangen wird, die Horizontalität zwischen Menschen durchbrechen und Gewalt- oder Machtverhältnisse wieder schaffen. Als Totschlagargumente gegen Utopien herrschaftsfreier Gesellschaft werden immer wieder Kinderschändis, Nazis oder Vergewaltigis genannt — oft fast wortgleich von radikal links bis NPD. Auch wenn solche Phrasen meist nicht auf eine analytische Debatte abzielen, steht hinter ihnen die sinnvolle Frage: Wie sieht der Umgang mit macht- und gewaltförmigem Verhalten in einer herrschaftsfreien Gesellschaft aus? Konsequent herrschaftskritisch gedacht lautet die Antwort: Es gibt kein Rezept, keine festlegbare Reaktion, weil diese wiederum eine Norm darstellen würde, die zur Durchsetzung Überwachung und Kontrolle bedürfte. Es gibt kein ‚Richtig und Falsch’, weil das die Existenz einer normsetzenden und damit privilegierten Instanz voraussetzt. Zudem sind privilegierte Handlungsmöglichkeiten nicht die Lösung, sondern die Ursache des Problems. Eine Vielzahl von Übergriffen, Unterwerfungen und Diskriminierungen basieren gerade auf der Existenz von Machtgefällen: Männer gegenüber Frauen, Deutsche gegenüber Nicht-Deutschen, sog. Erwachsene gegenüber sog. Minderjährigen, Menschen mit Bildungszertifikat gegen Menschen ohne Abschlüsse, Ärztis gegenüber Patientis, Reiche gegenüber Armen, Bewaffnete gegenüber Unbewaffneten, Amtsträgis gegenüber anderen, Betreuis gegenüber Betreuten usw. Gerade jene Institutionen, die zum Einhalten der Normen geschaffen wurden, sind die Orte exzessiver Gewaltanwendungen gegen Menschen: Gerichte, Polizei, Armeen, Arbeitsagenturen usw.

Die Alternative zur Normierung ist die direkte Einmischung und daraus entstehende Kommunikation zwischen Menschen. Sie ist horizontal, wenn alle Seiten gleiche Handlungsmöglichkeiten haben, also nicht eine Seite mit Sanktionen oder Strafe drohen kann. Damit entfällt die Steuerbarkeit über formale Mittel. Verlauf und Ausgang sind grundsätzlich offen. Genau das aber ist die Voraussetzung für eine möglichst hohe Wahrscheinlichkeit einer reflektierten, Veränderungen ermöglichenden Diskussion. Sanktionsbewehrte Wortgefechte hingegen führen zu aneinandergereihten Reden, die mit Kommunikation kaum noch etwas zu tun haben — Gerichtsprozesse sind das brillanteste Beispiel gestörter Kommunikation.

Mit dem Verzicht auf Steuerung, die nur mit Überwachung und Kontrolle funktioniert, geht auch das Gefühl der Sicherheit verloren. Es bedeutet einen Wandel gesellschaftlicher Kultur, dieses als Gewinn zu sehen und das Prozesshafte herrschaftsfreier Gesellschaftlichkeit zu begreifen. Es geht schließlich darum, Horizontalität und gleiche Handlungsmöglichkeiten ständig zu erweitern. Direkte Intervention und Kommunikation können individuelles Machtverhalten überwinden. Formalisierte Kontrolle kann das nicht — Kameras, Abhöranlagen, Strafe und der daraufhin erneut einsetzende Prozess der Überwachung des Vollzugs verstärken die Neigung zu Gewalt und Machtanwendung.

Notwendigkeit einer Intervention

Überwachung und Kontrolle sind ein wichtiger Pfeiler institutionalisierter Herrschaft. Emanzipatorische Politik muss daher zum Ziel haben, (auch) diese Stütze einzureißen. Als materielle Form der Herrschaft haben Einrichtungen der Überwachung eine konkrete Form, gleichzeitig basieren sie aber auf einem Diskurs um gefühlte Kriminalität, Angst und geschürte Abneigungen. Beide bedürfen der politischen Intervention, d.h. konkrete Aktionen können die Überwachungsanlagen und -institutionen selbst sowie die Diskurse, auf denen ihre Akzeptanz basiert, attackieren.

Direkte Aktion

Die Spanne möglicher Handlungen ist breit. An dieser Stelle sollen solche Aktionsformen genannt werden, die direkt wir-

ken, also nicht als Appell an „Zuständige“, „Mächtige“ oder ähnliche Sphären daherkommen. Aus emanzipatorischer Sicht ist der Verzicht an das Appellative und Beratende im politischen Kampf wichtig, wenn dadurch die jeweils Mächtigen oder stellvertretend Handelnden (auch eigene Vorstände, SprecherInnen usw.) in ihrer Position legitimiert werden.

Direkte Aktion versucht, die Lage direkt zu verändern — also die materielle oder diskursive Ebene tatsächlich und ohne Umweg über Machtstrukturen zu beeinflussen. Sie unterscheidet sich damit von Lobbyarbeit, Massenpostkarten, Unterschriftensammlungen oder Beteiligung an Wahlen.

Neben der Unterscheidung in direkte Aktion und solche unter Legitimierung von privilegierten Sphären lassen sich Protest und Widerstand unterscheiden.

Und noch eine Unterscheidung: Direkte Aktion will die Köpfe erreichen. Und den Kopf benutzen. Das erste Ziel einer direkten Aktion ist die Schaffung eines „Erregungskorridors“ in der Gesellschaft: Aufmerksamkeit, Irritation, Freude oder Wut sind solche Formen. Wie das erreicht werden kann, ist vielfältig: Kommunikationsguerilla, verdecktes Theater, Blockade von Castor-Zügen, Sabotage, Internet-Hacken usw. Wo die Erregung entsteht, ist Platz für politische Positionen und Visionen. Aber auch deren Vermittlung will durchdacht sein, d.h. Ideen für kreative Vermittlungsformen sind nötig. Direkte Aktion besteht aus allen dreien: Die kreative, direkte Aktion, der entstehende Erregungskorridor und die politischen Positionen/Visionen.

Damit ist direkte Aktion mehr als Militanz oder Gewaltfreiheit. Es geht darum, eine gesellschaftliche Veränderung zu erreichen. Je nach Thema und Situation kann das mit verschiedenen Mitteln gehen. Aber immer ist die Überlegung wichtig, welche materielle und welche diskursive Veränderung dadurch erreicht wird.

Konkrete Beispiele

Im Folgenden sollen an einigen Beispielen Ideen benannt werden, wie kreativer Widerstand gegen Überwachung und Kontrolle aussehen kann.

Demaskierung

- Kameras überdeutlich kennzeichnen
  Ob sachbeschädigungsfrei mit Luftballons, Schildern u.ä. oder anders per Farbe — wenn die Menge an Kameras plötzlich in der Stadt deutlich sichtbar würde, könnte das Aufsehen erregen. Das gilt auch für andere Überwachungsanlagen.
- Überwachte Bereiche markieren
  Auch dieses ist sachbeschädigungsfrei mit Kreide, Absperrband oder Tüchern, aber auch (dann wohl eher nachts) mit Farbe möglich. Die überwachten Bereiche werden auf dem Boden sichtbar gemacht. Die Vermittlung kann z.B. durch Schilder oder Flugblätter erfolgen: „Sie betreten jetzt den überwachten Bereich. Bitte nicht mehr in der Nase popeln und hier keine Ausländer jagen“.

Sabotage

- Kameras funktionsunfähig machen
  Kabel durchtrennen (z.B. mit Teleskop-Obstbaumschere — achtet auf Stromisolierung!), Linse anmalen oder zukleben, Kamera wegdrehen oder zerstören
- Software hacken
- Bunte Postkarte u.ä. vor die Kamera hängen, so dass diese nur noch das filmt (das ist wahrscheinlich gar keine Straftat)

Subversion

Ein wichtiges Mittel der Subversion ist die Überidentifikation. Sie bedeutet, etwas zu demaskieren, in dem es übersteigert wiedergegeben, gespielt oder gestaltet wird. Das kann wirken, denn auch Repression ist zwar allgegenwärtig, aber mitunter verschleiert oder zur Normalität geworden. Sie ist dann kaum noch spürbar im Gang der Dinge. Überidentifikation, also die übertriebene Steigerung des Sicherheitswahns, kann Repressionsvorgänge oder die ständige Repression (Kontrolle, Zwänge usw.) ins Bewusstsein zerren und damit die Aufmerksamkeit für Kritik schaffen.

- Kameragottesdienst
  Gießen, 28.12.2002: Die eigens dafür gegründete „Initiative Sicheres Gießen“ veranstaltete einen „Gottesdienst“ für mehr Kameras. Die Rund-um-Kamera am Marktplatz war Ziel der Prozession, Gebete und Choräle wurden vorgetragen — vom „Kamera unser“ bis zum „Kamerabekenntnis“. Als die Polizei auftauchte, wurden die Beamtis als Prophetis des Sicherheitsgottes bejubelt und angebetet. Entnervt verschwanden sie wieder, die Prozession aber wurde dadurch nur frecher und wiederholte den gesamten Kameragottesdienst im örtlichen Karstadt unter einer der dortigen Überwachungsanlagen. Ein dritter Auftritt folgte im Hauptbahnhof. Am nächsten Tag berichtete das sonntägliche Anzeigenblatt mit Foto von der Aktion — ganz ernst, das Gelächter über den dummen Redakteur war groß. Der Kameragottesdienst wurde inzwischen einige Male nachgespielt — z.B. in Frankfurt im Verlauf der Wahnmache im April 2003 und in Hamburg während des Jugendumweltkongresses Ostern 2002 (Berichte standen auf Indymedia).

Niederknien und beten zur Kamera: Die Aktion in Gießen (Bericht links). Angemeldet wurde sie von der selbstgegründeten Initiative Sicheres Gießen (ISG).

- Aufkleber inflationieren
  Ebenfalls Gießen, Landtagswahl 2003: Auf Wahlplakaten werden nicht nur subversive Veränderungen vorgenommen, sondern zusätzlich klebt ein kleiner Zettel mit der Aufschrift „Dieses Plakat wird videoüberwacht! Keine Chance für Chaoten“ als freche Satire auf den veränderten Ständern.
- Alles filmen
  Als Sicherheitsdienst dekoriert mit einer (eventuell unsinnig großen) Kamera alles aufzeichnen. Dabei ständig von mehr Sicherheit reden oder Umfragen parallel durchführen, ob sich die Menschen jetzt schon besser fühlen. Variante: Ganz viele Kameras bzw. Attrappen aufbauen.
- Fakes
  „Fake“ steht für Fälschung z.B. behördlicher Schreiben. In Gießen wurde 2003 allen Anwohnis am Marktplatz ein Schreiben zugeleitet, dass die Innenaufnahmen aus ihren Wohnungen, die die Überwachungskamera aufgezeichnet hat, jetzt gelöscht werden sollen. Das Schreiben trug den Briefkopf des Polizeipräsidiums Mittelhessen. Es war gefälscht und musste dementiert werden.
  Hohe Kunst des Fakes: Auch das Dementi faken.
- Anträge für mehr Überwachung
  Absurde Unterschriftensammlungen, Anträge usw. — eventuell dafür eine Bürgerinitiative/-wehr für mehr Sicherheit gründen und ständig mit skurrilen Vorschlägen die Sicherheitspolitiken der Parteien unterstützen.
  Ähnlich: Seltsame Statistiken veröffentlichen, z.B. dass

Reader „Selbstorganisierung“
Leben ohne Geld, unabhängig aktiv sein.
A4, 56 S., 6 €

quadratisch.praktisch. theoriestark: Die Reihe mit Einführungen in emanzipatorisches Denken
Ja ca. 64 S., 3,- €. Zum Beispiel die Titel:
Herrschaft
Offene Räume
Konsumkritik-Kritik
Den Kopf entlasten?

Im Namen des Flummiballs
Skurrile Geschichten aus der Justiz. Ein Lesebuch. 72 S., 3,- €

blauäugige Menschen oder solche mit Weisheitszähnen häufiger straffällig werden und deshalb schärfer zu überwachen sind usw.

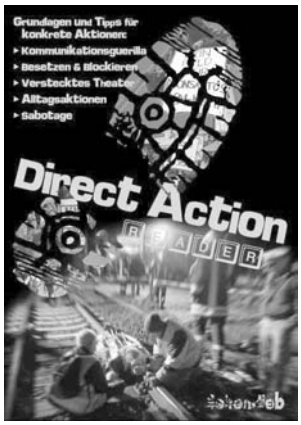
Achtung bei aller Subversion: Es ist unglaublich, was alles geglaubt wird. Das kann dann nach hinten losgehen. Gute Planung ist einerseits wichtig, andererseits aber auch die schnelle Reaktion, d.h. eine Aktion zu erweitern oder durch eine weitere Handlung neu auszurichten, wenn es nicht so läuft, wie erwünscht.

Verstecktes und sonstiges Straßentheater

Durch theatralische Darstellung lassen sich Themen und Positionen transportieren. Eine spezielle Form ist das versteckte Theater. Dabei wird eine Szene gespielt (als fester Ablauf oder mit Improvisationen, d.h. dem spontanen Reagieren auf die sich entwickelnde Situation), aber den Umstehenden wird das nicht als Inszenierung erkennbar. So können interessante Situationen im Alltag entwickelt werden.

- Kontrolle aufgrund Kamera
  Eine uniformierte Person (oder zwei) sprechen eine Person an und behaupten, die sei auf einer Videokamera bei irgendwas gefilmt worden — einfach irgendeiner absurden Handlung. Eine andere Person (auch von der Theatergruppe) mischt sich scheinbar als Unbeteiligte ein ... und wenn es gut läuft, entsteht dann auch mit Umstehenden eine Dialogsituation.

Mehr Tipps für kreative Aktionen im Direct-Action-Reader — bestellen oder Download über www.aktionsversand.tk.



Gegenöffentlichkeit

Neben solchen Aktionen können eigene Zeitungen, Videomagazine, Kinostreifen, Internetplattformen usw. Diskurse beeinflussen.

Kreative Antirepression

Wenn Polizei oder gar Gerichte auftreten, ist es oft vorbei mit der Aktion. Doch das muss nicht sein — ganz im Gegenteil: Kreative Antirepression will Menschen zu Akteuris machen und die weit verbreitete Ohnmacht durchbrechen. Es geht darum, Repression anzugreifen, zu demaskieren und lächerlich zu machen. Ziel ist es, offensive Strategien gegen Repression aller Art zu entwickeln und Mut zu machen, sich dieser immer wieder subversiv und kreativ entgegen zu stellen und eigene Ideen zu entwickeln. Das kann z.B. bedeuten, Repression bei der Planung von Aktionen mitzudenken und — als wäre sie Teil eines Theaterstücks — vorab einzubauen. Dabei geht es nicht darum, die Gegenseite militärisch zu schlagen, d.h. darauf zu hoffen, durch zahlenmäßige Überlegenheit auch mal eine Polizeikette zu durchbrechen. In dieser Logik kann Staatlichkeit mit ihren fast unendlichen materiellen und personellen Ressourcen nur gewinnen. Spannender ist es, subversiv zu denken: Wie kann Repression gegen sich selbst gewendet, ins Leere laufen gelassen oder für andere Zwecke verwendet werden? Gegenüber hierarchischen (Polizei-)Apparaten sind Frechheit, Überraschung & Wendigkeit das „Gegengift“.

Foto der „Demo der Sprachlosen“ in München auf Seite 6.

Foto unten: MarsTV im Einsatz an einer Polizeitruppe.

- Beispiel: Auf das Verbot sämtlicher politischer Demonstrationen während der NATO-Sicherheitskonferenz in München (2001) reagierte eine Gruppe mit der „Demo der Sprachlosen“ — mit leeren Transparenten, leeren Flugblättern und zugeklebten Mündern wurde das Verbot auf Meinungsäußerung sehr gewitzt angegriffen.
- Clowns Army und Mars-TV (www.projektwerkstatt.de/marstv) sind zwei theatralische Formen, Autorität zu hinterfragen und zu demaskieren.

Ideen schmieden, Üben, Loslegen

Die Qualität entsteht auch durch Übung: In Workshops und Trainings kann über direkte Aktionen geredet und an konkreten Beispielen geübt werden, wie Langeweile und Wirkungslosigkeit politischer Arbeit überwunden werden kann.

Zur Unterstützung können dienen:

- Trainings zu Direct Action und kreativer Antirepression: Schulungen mit Einführungsteil, Übungen und Rollenspielen können helfen, den Zugang zu solchen Aktionsformen zu finden. Referentis und Themen auf www.vortragsangebote.tk
- Aktionstipps im Internet über www.direct-action.tk und www.antirepression.tk
- Rechtstipps: www.prozesstipps.tk und www.laienverteidigung.tk
- Aktionstipps in Broschüren oder als Download über www.aktionsversand.tk

Tipps und Tricks gegen die Überwachungsindustrie

Nicht jede*r weiß über den weit verbreiteten Datendiebstahl Bescheid, ob erlaubt oder verboten. Dabei sind die vielen Verstöße gegen das Recht auf Privatsphäre und Redefreiheit, die wie ein Vorgeschmack auf den Überwachungsstaat aus dem Roman „1984“ wirken, schon lange bekannt. Aber die zahlreichen Warnungen vor dem „Gläsernen Bürger“ werden in der BigBrotherSelbstdarstellungsgesellschaft kaum noch ernstgenommen. Daher sollte mensch versuchen sich mit den Mitteln, die jede*m selbst zur Verfügung stehen, gegen die zunehmende Kontrolle der staatlichen und privaten Überwachungswirtschaft wehren.

Denn: Wer will schon ständig verdächtigt und ausspioniert werden?

Die Überwachung ist - von der direkten sozialen Kontrolle mal abgesehen - technisch sehr weit vorangeschritten. So gibt es sichtbare und unsichtbare Überwachungskameras im privaten und öffentlichen Bereich, die die Bewegung von Menschen aufzeichnen und auswerten. Mittlerweile muss mensch auch davon ausgehen, dass die Kameras automatische Gesichtserkennung besitzen. Es ist zwar 2017 noch in der Entwicklungsphase, Kameras mit solcher Technik auszustatten, aber wir sollten es besser schon einplanen, dass dies kurz vor der Einführung ist. Zudem zeichnen immer mehr Kameras den Ton auf, belauschen also die Vorübergehenden. Außerdem werden mit Hilfe von Computern alle möglichen privaten Daten (Kontobewegungen, Adressen, eMails) ausspioniert und von verschiedenen Behörden und Firmen gesammelt. Der Einzelhandel will zusätzlich zu Kundenkarten demnächst flächendeckend alle Produkte mit Funk-Etiketten (RFID-Chips) registrieren bzw. ausstatten. Dieselbe Technik ist in allen neuen Europäischen Reisepässen und Personalausweisen verbaut. Auch die elektronische Gesundheitskarte ermöglicht es Patientendaten zu sammeln. Bislang (2017) gibt es aber zum Glück noch keine zentrale Infrastruktur, wo diese Daten gesammelt gespeichert werden. Auch Handys bieten ein weites Feld der drahtlosen Kontrollmöglichkeiten. Ebenso alle Gespräche und Nachrichten im Festnetz oder Internet.

Hier soll es nun aber vor allem um die vielfältigen Gegenmaßnahmen gehen, die den Alltag anonymer und damit sicherer machen. Gegen all die Terror-Panik und Angstmache hilft es manchmal, die Möglichkeiten der Überwachungswirtschaft zu kennen. Nur so ist es möglich auf die sich überall ausbreitende Kontrollgesellschaft zu reagieren, ohne dabei in unbegründete Paranoia zu verfallen.

Handy und Telefonieren

Das Mobiltelefon ist heute ein weit verbreitetes Mittel der Kommunikation. Überall quatschen und tratschen die Leute, wie es ihnen gefällt. Dass sie dabei meist unwichtige, aber dennoch private Details öffentlich ausposaunen, ist den meisten völlig egal. Wen es dennoch stört, dass jede Gesprächsverbindung und der Standort, bzw. die Bewegungsrichtung des Anrufenden, von den Betreiberfirmen aufgezeichnet wird, der*die sollte sich nach einer Alternative umschauen.

Erstmal gibt es zwei „eindeutige Daten“ an einem Handy: eine eindeutige Kennung des Handys, die sogenannte IMEI, und die der SIM-Karte. Beide Daten werden selbstverständlich immer verschickt. Deswegen macht es keinen großen Sinn eine neue SIM-Karte in sein altes Handy zu stecken, da durch die Kennung des Handys beide SIM-Karten verknüpft werden können. Doch auch Bewegungsprofile eines Handys können schon genug verraten, um darauf zu schließen, wem das Handy gehört. Und mensch sollte klar sein, dass die Mobilfunkbetreiber die Bewegungsdaten auch immer speichern und nutzen, vorgeblich um ihre Netze besser auszubauen. Eine Callcentermitarbeiterin eines Mobilfunkanbieters erzählte, dass die sofort sehen, woher Menschen anrufen, des weiteren sehen sie die komplette History, wo sich die SIM-Karte aufgehalten hat. Jedoch waren die Callcentermitarbeiterinnen angewiesen dieses Wissen den Kunden gegenüber zu verheimlichen. Es ist auch mittlerweile ein Standardverfahren, dass Behörden zu allen möglichen Anlässen eine Funkzellenabfrage beantragen. Funkzellenabfrage bezeichnet den Begriff, dass die Behörden eine Liste von allen eingebuchten Handys in der Funkzelle bekommen. Außerdem können Handys auch ausgeschaltet weiter mithören und senden, wenn sie illegal - also von fremder Hand/außen — aktiviert werden.

Smartphones sind erstmal nicht anders zu behandeln als Handys. Jedoch ermöglicht das „Smart“ in Smartphones noch mehr Überwachungsmöglichkeiten, weil mehr Daten anfallen, die benutzt werden können Besitzer*innen auszuspionieren. Die Betriebssysteme für Smartphones sind sogar zusätzlich von bekannten Datenkraken wie Google und Apple hergestellt, die bekannt dafür sind ihre Benutzer*innen auszuspionieren.

Auch muss sich Mensch davon verabschieden, dass es Festnetztelefonie gibt, also ein vom Internet getrenntes Telefonnetz. Denn seit einigen Jahren rüsten die Telefonanbieter alle Anschlüsse auf VOIP (Voice over IP, also Internettelefonie; das eingesetzte Protokoll heißt SIP) Anschlüsse um. Dadurch gibt es kein getrenntes Telefonnetz mehr. Das heißt nicht, dass die Überwachungsmöglichkeiten durch diese Umstellungen stark gestiegen sind. Es können zwar ein paar mehr Server der Verbindung lauschen, jedoch konnten das die relevanten Stellen sowieso auch davor.

Was kann mensch also tun? Ein anonymes Prepaid-Handy gibt es auf dem grauen Markt und in manach einschlägigem Laden, damit weiß der Mobilfunkanbieter nicht wem das Telefon gehört. Desweiteren gibt es in fast allen Städten öffentliche Telefone und Callshops, und die sind meist sogar preisgünstiger. Also: Besser immer genügend Bargeld dabei haben. Der Versand von SMS ist über das Festnetz bzw. Internet natürlich etwas umständlicher, aber ohnehin werden SMS demnächst für die Behörden gespeichert — zur Terrorabwehr versteht sich. Die goldene Regel im Umgang mit Handys: Akku raus, einfach das Handy zu Hause lassen oder das Handy auch mal auf Reisen schicken und einfach ohne Handy agieren.

Die Free Software Foundation Europe stellt auf der Internetseite https://fsfe.org/campaigns/android/android.de.html vor wie mensch wieder Kontrolle über sein Smartphone erlangt.

Da es sich bei Telefonie wieder „nur“ um Internetverbindungen geht, können wir dieselben Maßnahmen treffen um anonym und sicher zu kommunizieren, wie beim normalen Surfen. Also TOR für die Anonymisierung und starke Verschlüsselung, damit der Inhalt verschlüsselt ist. Das Verschlüsselungsprotokoll für Telefonie heißt ZRTP und MIKEY. Mit der starken Verschlüsselung bekommen die Behörden nur noch Metadaten, also wer wen wann angerufen hat, bzw. welche IP Adresse wen angerufen hat, aber keinen Inhalt mehr. Als sichere Alternative zu Skype und Festnetztelefonie ist hier RING (https://ring.cx/en) zu empfehlen, was verschlüsselte Telefonie anbietet. Damit auch diese Metadaten nicht anfallen müssen wir „nur“ noch die verschlüsselte Verbindung über TOR schicken. Leider hat RING bislang noch keinen Tor Support, also keine Anonymität, sie sind aber dabei das zu implementieren (2017).

Allen Ernstes hatte der Deutsche Bundestag obige Werbung geschaltet.

Internet

Durch die Benutzung des Internets fallen viele Daten an, die staatliche wie private Stellen mit Eifer speichern. So hat jede*r Internetteilnehmer*in eine eindeutige IP-Adresse, die an alle möglichen Stellen weitergeleitet wird. Des Weiteren senden Internetbrowser im Normalfall eine ganze Reihe von Daten (installierte Plugins, installierte Schriftarten, Auflösung des Bildschirms, ...), mit denen der Browser weltweit eindeutig wird und es möglich ist, auch bei einem geteilten Internetanschluss einzelne Benutzer zu identifizieren. Kommerzielle Produkte, wie der MS-Internet-Explorer, sind unzuverlässig, weil ihr Programmcode nicht bekannt ist. Außerdem treten immer wieder dramatische Sicherheitslücken auf und die Anbieter legen einen zweifelhaften Umgang mit der Behebung der Probleme an den Tag. Aber auch ohne dass die Benutzis irgendetwas machen, laufen im Hintergrund Dienste, die auf das Internet zugreifen, um zum Beispiel nach Updates zu suchen. Die meisten kostenlosen Mailpostfächer nehmen es mit der Sicherheit und Anonymität ihrer Kunden nicht besonders ernst. So verschicken diese Emails zwischen den Servern unverschlüsselt, manche schnüffeln sogar in fremder Post nach Stichwörtern und Internetlinks. Beim aktuellen Windows kann die ständige Durchsuchung des Computers nicht mehr abgeschaltet werden. In den AGB's steht sogar, dass Microsoft sich das Recht vorbehält, Daten zu löschen, die nicht ihren Richtlinien entsprechen.

Angesichts des Überwachungswahns war das eine ziemlich dreiste Darstellung. Die Parodie unten war dann auch ein naheliegendes Fakes aus Politgruppen.

Wer sich frei und unerkannt im Internet bewegen will, ist im Internet-Café gut aufgehoben. Ohne persönliche Zugangsdaten und für wenig Geld kann mensch dort die anonyme Meinungsfreiheit genießen. Allerdings haben einige Inhaber zusätzlich zu den Webcams auch Überwachungskameras eingebaut. Mensch sollte darauf achten, dass die Verbindung zu Internet und Online-Diensten verschlüsselt ist, so dass nur du und der Empfänger der Kommunikation (Server) die Daten lesen können und die Daten nicht auf dem Weg manipuliert werden können. Zu erkennen am HTTPS am Anfang.

Hingewiesen sei noch auf Kinderspielzeug mit Internetverbindung wie die Puppe Cayla, die deswegen im Februar 2017 verboten wurde. Solches Spielzeug stellt eine permanente Überwachung oder zumindest die Gefahr dar.

Um wirklich anonym zu surfen, kommt mensch nicht um die Anoymisierungssoftware TOR herum. TOR versteckt dabei die eigene IP-Adresse, so dass selbst der Server nicht mehr sagen kann, welche Benutzer*in ihn besucht hat. Das Tor-BrowserBundle ist sehr einfach überall zu installieren (https://www.torproject.org/projects/torbrowser.html.en) und ist ein Browser mit TOR Unterstützung. TOR ist jedoch kein Allheilmittel. Wenn zum Beispiel in einer TOR-Session sich in irgendeinen Dienst eingeloggt wird, weiß der Server natürlich wieder wer du bist. Gefährlich wird das bei sowas wie Facebook und den bekannten „Daumen hoch“ Buttons auf anderen Seiten. Durch das Einloggen bei Facebook und das ansurfen einer anderen Seite mit „Damen hoch“ Button, kann Facebook die Verbindung nachvollziehen und dich auch als Besucher*in der anderen Seite identifizieren. Das kannst du verhindern, indem du den TOR-Browser zwischen verschieden Aktivitäten schließt.

Jedoch ist es auch das Betriebssystem selber, was sich und dich verraten kann, durch z.B. die Updatesuche oder duch eine Reihe von schlechten Standardeinstellungen. Tails (https://tails.boum.org) ist ein Betriebssystem, was genau diese Lücke füllt und sehr einfach zu benutzen ist. Es wird einfach auf einem USB-Stick (oder CDROM) installiert. TAILS wird von einer Gruppe entwickelt, die versucht eine sehr hohe Sicherheit rauszuholen und trotzdem dabei be-

Mehr Infos gibt es bei: ccc.de | cilip.de | foebud.org | gulii.com | safercity.de | stop1984.com

Bemerkung

Diese Texte stammen aus verschiedenen Quellen. Wie groß die Gefahr ist, abgehört zu werden, ist umstritten. Zwischen Leichtsinn und Selbstinszenierung als überwachter Mensch (zwecks besserer Eigendarstellung der Wichtigkeit) ist alles alltäglich. Wo, bei welchen konkreten Aktionen und wieweit auch im Alltag vorsichtig agiert wird, muss jedi selbst entscheiden. Dafür nützlich ist, Wissen über die technischen Möglichkeiten zu haben. Gleichzeitig aber sollte auch klar sein: Überwachung ist personalintensiv. Die Polizei kann nicht alles sehen, kontrollieren, auswerten. Kreativer Umgang und Willen zur Aktionsfähigkeit sind sinnvoller als die Angststarre vor der Überwachungsmaschinerie. Sie soll verunsichern — zumindest das sollte ihr nicht gelingen!

nutzbar zu bleiben. So läuft jede Verbindung ins Netz über TOR und TAILS bringt alles mit, was mensch normalerweise erwartet: Browser, Emailclient, Chatprogramm und alles ist so eingerichtet, dass für Nutzer*innen eine sehr gute Sicherheit gegeben ist. Zumal TAILS monatlich aktualisiert wird, so dass auch auf neue Angriffe auf die Anonymität schnell reagiert werden kann.

Die meisten bekannten großen Mailanbieter sollten nicht benutzt werden, wie Gmail, Outlook, GMX, WEB.de, Yandex or Hushmail. Zu empfehlen dagegen Anbieter die Wert auf Sicherheit legen: Posteo, MyKolab, riseup, mailbox.org.

Die sicherste Art der privaten Kommunikation ist natürlich, eine starke Verschlüsselung zu benutzten. Gute Kryptographie mit gegenseitig austauschbaren Schlüsseln bietet Pretty Good Privacy (PGP) für Email an. Zu empfehlen vor allem die freie Implementation von GnuPG.org.

Wer sich im Internet frei bewegen will, braucht einen passenden Browser. Bei freien Browsern wie Chromium oder Mozilla/Firefox kann der komplette Quellcode eingesehen werden, was es Sicherheitsforscher*innen einfacher macht Fehler zu finden und diese zu lösen. Ein sicheres Programm kann deswegen nur aus freier Software bestehen. Zum erweiterten Schutz der Privatsphäre sollte das AddOn „uBlock origin“ oder „Privacy Badger“ installiert werden. Damit lassen sich Tracker, Werbung und Integration in soziale Netzwerke effektiv blockieren. Nebenbei spart mensch Traffic. „AdBlockPlus“ ist nicht zu empfehlen, da es einem privatwirtschaftlichen Unternehmen gehört und zu vermuten steht, dass die Privatsphäre der User nicht geachtet wird. Den eigenen Browser auf Sicherheitsmängel überprüfen geht bei Heise.de. Auch bei kai.jksjena.de gibt es jede Menge aktuelle Infos über schädliche Software (Viren, Trojaner) oder Falschmeldungen (wie auch bei Hoaxinfo.de). Für andere Programme außerhalb des Browsers, kann mensch einfach schauen was TAILS anbietet, mit deren Programmauswahl ist mensch eigentlich gut beraten.

Da starke Verschlüsselung für Behörden für die Überwachung ein echtes Problem ist, versuchen diese darauf zu reagieren und entwickeln z.B. den sogenannten Bundestrojaner. Schadsoftware, die auf Rechner eingeschleust wird um Daten bevor sie verschlüsselt werden abzugreifen. Dieser Trojaner muss aber irgendwie auf deinen Rechner, dagegen hilft vor allem Festplattenverschlüsselung (auch aus anderen Gründen gut) die normalen Maßnahmen gegen Viren und Trojaner: Keine unbekannten Anhänge öffnen, nicht irgendwas aus dem Internet installieren etc.

Virenschutzprogramme helfen nicht, schließlich können sich Behörden mit den Herstellern der Programme zusammen setzten und erklären, dass der Bundestrojaner ein gutmütiges Programm ist.

Geld

Heutzutage ist Onlinebanking ähnlich sicher, wie der Gang zum Schalter. Wenn dazu ein sicherer Browser (Tor-Browser) verwendet wird fallen bei beiden Vorgängen gleich viele Daten an. Die Gefahr, dass Kontodaten in falsche Hände geraten ist natürlich vorhanden, aber mit gesundem Menschenverstand zu vermeiden. Alle Zahlungen von Magnetkarten (EC, VISA, Master) werden natürlich auch abgespeichert. Nach dem Aufweichen des Bankgeheimnisses stehen sie nun neben dem Kreditinstitut auch zahlreichen Polizei- und Geheimdienstbehörden offen. Mit der Verbreitung von bargeldlosem Zahlungsverkehr werden außerdem Menschen aus dem Alltag ausgeschlossen, die aus wirtschaftlichen oder anderen Gründen nur mit Bargeld zahlen, wie viele Wohnungslose oder Menschen ohne Papiere. Mit dem Vorwand der Verhinderung von Geldwäsche wird aber Bargeld auch heute sehr viel stärker überwacht. Die Seriennummern, die ausgegeben werden, werden gespeichert und da die meisten Läden ihr Bargeld täglich zu Banken bringen, kann der Lebenslauf eines einzelnen Geldscheines verfolgt werden.

Trotzdem empfiehlt es sich, möglichst viel mit Bargeld zu bezahlen. Zum Beispiel, die Fahrkarten für Bahnreisen entweder mit Bargeld zu bezahlen (auch an Automaten möglich) oder nur mit dem Geldchip, der auf vielen Geldkarten die virtuelle Währung speichert. Aber da Geldkarten (Guthabenkarten) auch Seriennummern haben, sind sie nicht völlig anonym.

Eine ganz neue Methode, anonym Geld zu transferieren, bieten die sogenannten Cryptowährungen z.B. Bitcoin. Da dort ein Konto nur eine Nummer ist und jede*r mehrere Konten erstellen kann, gibt es von außen keine Zuordnung, wer im Besitz eines Kontos ist. Es gibt auch schon ein paar Bitcoinbankautomaten, an denen Bitcoins in einer anderen Währung ausbezahlt werden können. Aber Achtung, jede Kontobewegung in Bitcoin kann nachvollzogen werden. Das heißt wenn irgendwie darauf geschlossen werden kann, dass dir ein Bitcoinkonto gehört, kann auch jede Kontobewegung nachvollzogen werden. Die Sicherheit bei Bitcoin besteht also darin, dass mensch beliebig viele Konten haben kann und die Zuordnung von Kontonummer zu Kontoinhaber*in nicht vorhanden ist.

RFID

Ein weiterer neugieriger Computerchip ist auf dem Vormarsch in unseren Alltag: die RadioFrequenzIdentifizierung (RFID). Der riesige Handelskonzern Metro mit seinen Kaufhäusern (Extra, Kaufland, Mediamarkt, Praktiker, Real, Reno, Saturn) hat bei der Einführung dieser Funketiketten eine Vorreiterrolle eingenommen. Gemeinsam mit anderen Firmen ist Metro an einem Verbund zur Erprobung dieser unsichtbaren Kontrolltechnologie beteiligt. Auch Philips benutzt schon diese auf mehrere Zentimeter drahtlos übertragende Produkterkennung für seine Waren, ebenso wie Texas Instruments, Infineon und Intel. Die hauchdünnen Funksender befinden sich zudem in Etiketten von Tchibo und Benetton, ebenso wie auf Gilette-Klingen, Pantene-Shampoo und Philadelphia-Käse. Auch auf einigen CD-Rohlingen und in der BahnCard 100 wird RFID schon benutzt. Der Vorteil für Industrie und Handel liegt dabei in der kontaktlosen Erkennung der einzelnen Produkte, die bisher nur über den allgemeinen Strichcode mit einem Laserscanner automatisch lesbar waren. Außerdem enthält jeder RFID-Aufkleber eine über Funk lesbare, einmalige Produktnummer, die den Weg jeder einzelnen Ware von der Produktion bis ins Verkaufsregal nachvollziehbar macht. Die Kundschaft hingegen wird mit dem Versprechen auf bargeldloses Einkaufen ohne Warteschlange gelockt, denn letztlich reicht es nun, einen Warenkorb durch die Funkschranke zu schieben. Kassenpersonal wird eingespart, das Geld direkt von der Kundenkarte abgebucht. Wessen Kundenkarten sich gerade im Geschäft befinden, erkennt der Radioempfänger ebenfalls, denn in zahlreichen der Plastik-Rabattkarten (PayBack) ist heute schon ein solcher RFID-Chip eingebaut. Computer können so in Kaufhäusern die Kaufgewohnheiten ausspionieren und der Kundschaft gezielte Werbung nach Hause schicken.

Auch ist es nicht garantiert, dass diese passiven Funkchips nach dem Bezahlen nie mehr weitersenden können. Einer weiteren kommerziellen Ausgrenzung von Leuten, denen die entsprechende Kaufkraft für Markenprodukte fehlt, ist damit der Weg geebnet, da Firmen das Kaufverhalten einzelner Kunde*innen nachvollziehen können. So träumen große Handelsketten schon davon, personalisierte Preise und zugeschnittene Angebote pro Kund*in anbieten zu können. Wem es nicht passt, dass die Firmen ungefragt die Kundenkarte ausspionieren, der kann diese Produkte entweder von vornherein ablehnen oder aber diese Plastikwanzen in Metall abgeschirmt verpacken (Visitenkartendose oder dicke Alufolie/Kühltüte/Rettungsdecke). Damit kann das auf 13,56 MHz gesendete Radiosignal nicht zu dem Passivsender durchdringen und zurückgeschickt werden. Der Foebud (https://foebud.de) bietet auch einen RFID-Scanner-Detector an, der anzeigt, wenn irgendwo RFID Sender angeschaltet ist. Wer einen versteckten RFID-Chip findet, der meist beim einfa-

chen Durchleuchten erkennbar ist, kann ihn bei stoprfid@foebud.org melden und damit öffentlich machen. Kenne deinen Feind ...

Perso & Reisepass

In neuen EU-Reisepässen und Personalausweisen ist ein solcher RFID-Chip eingebaut, auf dem neben der persönlichen Daten auch die biometrischen Merkmale (Körpergröße und Gesichtsformen) abrufbar gespeichert sind. Damit sollen Passkontrollen an Flughäfen erleichtert werden. Allerdings weiß mensch nie so genau, wo und von wem diese Daten aus dem Chip abgefragt werden.

Schließlich ist die Funkerkennung eine relativ leicht nachzubauende Technik, die in der Wirtschaft immer mehr eingesetzt wird. Gegen diese Überwachungstechnologie regt sich natürlich auch Widerstand (siehe z.B. DerGrosseBruder.org). Dass die RFID-Chips in der Mikrowelle zerstört werden können, stimmt zwar, aber das führt meist auch zur Zerstörung des umgebenden Stoffes. Das Durchbohren und Zerstechen des dünnen Blechchips hilft allerdings ebenso gut, wie gründliches Zerkratzen und Zerschneiden. Das gilt auch für die meisten anderen Datenträger (CDs, DVDs, Festplatten), die mensch unbrauchbar machen möchte. Der Foebud bietet einen sogenannte RFID-Zapper an, der wie die Mikrowelle durch Kurzschluss den Chip dauerhaft zerstört, jedoch mit deutlich weniger Energie, so dass dabei kein verräterisches Brandloch hinterlassen wird.

Gegenmaßnahmen bei Wanzen, Richtmikrofonen und Co.

„Wanzen“ heißen die immer kleiner werdenden Minisender, die zu verstecken mit der durch modernste Technik schrumpfenden Baugröße immer einfacher wird.

Im Folgenden ist zusammengestellt, durch welcher Art von Lauschangriffen die Privatsphäre des Bürgers oder das Chefzimmer eines Unternehmens heutzutage gefährdet werden und wie man sich dagegen zur Wehr setzen kann.

Minisender

FUNKTION: Versteckte, getarnte Raummikrofone übertragen Gespräche über Funk. Reichweite 20 m bis 3 km. Energieversorgung meist über Batterie, aber auch über Strom- und Telefonnetz oder Solarzellen.

VERSTECK: Die winzigen elektronischen Bauteile von Streichholzschachtelgröße können in jedem Hohlraum stecken, in abgehängten Decken, Böden, Möbeln, Elektrogeräten, Zimmerpflanzen.

AUFWAND: Die Montage geht schnell und ist kinderleicht. Einfache Wanzen sind ab 300 Euro zu haben.

TÄTER: Jeder, der Zugang zum Chefzimmer hat. Mitarbeiter, Besucher, Putzfrauen, Handwerker, Monteure.

ABWEHR: Wanzenaufspürgeräte ab 300 Euro. Tagessatz von Profis für elektronisches „Großreinemachen“ (Sweeping) 1.000 bis 5.000 Euro. Mit Profigeräten wie dem X Sweeper von Optoelectronics (Vertrieb u.a. TelCorn, Siegen) lassen sich versteckte Minisender leicht aufspüren (Test in RADIOSCANNER 3/2003).

Mini-Tonbandgeräte

FUNKTION: Die Winzlinge zeichnen Sprache auf. Ein Tonbändchen in Scheckkartengröße nimmt drei Stunden lang auf, selbst das allerkleinste Gerät in einem Kugelschreiber schafft 30 Minuten.

VERSTECK: Fast immer bringen Besucher die Tonbänder mit. Die Geräte werden entweder am Körper getragen, in Aktenkoffern oder anderen Konferenzutensilien eingebaut.

AUFWAND: Jeder Laie kann die Mini-Tonbänder einsetzen. Ein Gerät in Scheckkartengröße kostet um 300 Euro.

TÄTER: Besucher, die das vertraulich gesprochene Wort heimlich dokumentieren wollen.

ABWEHR: Schwierig. Durch das geringe Magnetfeld des Löschkopfs elektronisch kaum zu orten. Tonbanddetektoren bringen wenig. Notfalls Gepäck röntgen, Metalldetektoren einsetzen.

Körperschallmikrofone

FUNKTION: Der Lauscher nutzt z.B. einen Heizkörper oder die ganze Wand wie ein Mikrofon. Schallwellen versetzen den Körper in Schwingungen, die das Gerät auffängt, verstärkt, filtert und hörbar macht.

VERSTECK: Der Lauscher sitzt unbehelligt im angrenzenden Raum. Beliebte Lauschstellen sind auch Versorgungsschächte, die vertikal durch alle Etagen führen.

AUFWAND: Spitzengeräte liefern erstaunliche Hörqualität, Preis ab 1.000 E. Leistungsschwächere Geräte ab 500 Euro.

TÄTER: Jeder, der Zugang zum Nachbarraum hat. Funktioniert auch durch die Glasscheibe. Betriebsinterne oder betriebsfremde Täter.

ABWEHR: Rauschgeneratoren machen das Belauschen von Körperschall unmöglich, sind aber teuer. Rauschgeneratoren für einen kleinen Raum kosten um 500 Euro.

Drahtfunk

FUNKTION: Funktioniert innerhalb des Gebäudes. Der Langwellensender nutzt die 220-VoltStromleitung als Antenne und bezieht den Strom aus dem Netz.

VERSTECK: An Elektrogeräte gebunden. Fast immer tauschen die Täter vorhandene gegen präparierte Geräte aus. Sehr beliebt: Einbau in handelsübliche Mehrfachsteckdosen.

AUFWAND: Wie bei Wanzen wird ein zusätzliches Empfangssystem benötigt. Das System kostet um die 500 Euro.

TÄTER: Besucher, Monteure, Mitarbeiter. Der Empfang kann nur im Gebäude stattfinden.

ABWEHR: Netzverrauschung durch Rauschgeneratoren oder Einbau von Netzfiltern. Letztere filtern die Langwellen (zu übertragende Sprache) heraus und verhindern so das Auffangen.

Verdrahtete Raummikrofone

FUNKTION: Die klassische Stasi-Wanze wird oft schon bei der Errichtung eines Gebäudes fest installiert. Gespräche werden von einer festen Abhörstation im Haus belauscht

VERSTECK: Diese Raummikrofone finden sich vor allem in Deckenverkleidungen und Mauerhohlräumen.

AUFWAND: Nur mit hohem Aufwand machbar, aber dann unbegrenzte Betriebs- und Nutzungszeit.

TÄTER: Profi-Lauscher in Botschaften und Auslandsvertretungen, Hotels und Konferenzzentren.

ABWEHR: Extrem aufwendig. Abhören durch Rauschgeneratoren erschweren. Ausweichen ins Freie nur sinnvoll, wenn niemand in Sichtweite elektronisch mithören kann.

Richtmikrofone

FUNKTION: Der Schall wird durch ein Parabolrichtmikrofon eingefangen. Die Schallwellen werden wie beim Körperschall einige 1.000fach verstärkt, gefiltert und wiedergegeben.

VERSTECK: Der Lauscher lauert im Freien ca. 30 bis 100 m in direkter Sicht vom geöffneten oder gekippten Fenster des Chefzimmers.

AUFWAND: Technisch wie finanziell gering. Leistungsfähige Geräte kosten rund 500 Euro.

TÄTER: Jeder kommt in Frage.

ABWEHR: Wichtige Gespräche nicht im Freien in Sichtweite anderer Personen führen. In Chef und Besprechungsräumen Fenster geschlossen halten. Bezugsquellen: Anbieter von Sicherheits- und Abhörtechnik, Spionageläden.

Ergänzender Hinweis: Generell sollte bei sensiblen Gesprächsthemen am Telefon, an sensiblen Orten oder bei Verdacht einer Observierung nicht allzu offen gesprochen werden. Vorher vereinbarte Schlüsselwörter können dabei helfen, z.B. wenn eine Aktionsvorbereitung als Planung für eine Radtour abläuft. Vor allem genaue Orte, Zeitpunkte usw. sollten nicht klar in Verbindung mit einer Aktionsidee benannt werden. Zudem müssen sie nicht bei jedem neuen Gespräch wiederholt werden.