



Fig. 1

## 1. Der V-Mann in der Tasche

Seid vorsichtig, aber nicht paranoid

Im Sinne dieses Mottos versucht dieser Vortrag, genug Hintergründe darzustellen, um euch eine informierte Entscheidung zu ermöglichen, wie ihr mit eurem Telefon umgehen wollt.

- GSM – ganz kurz
- Akkus raus? – Das Telefon als Wanze
- IMSI-Catcher und so
- Verkehrsdaten
- Fälle
- Was tun?

(vgl. Fig. 1)

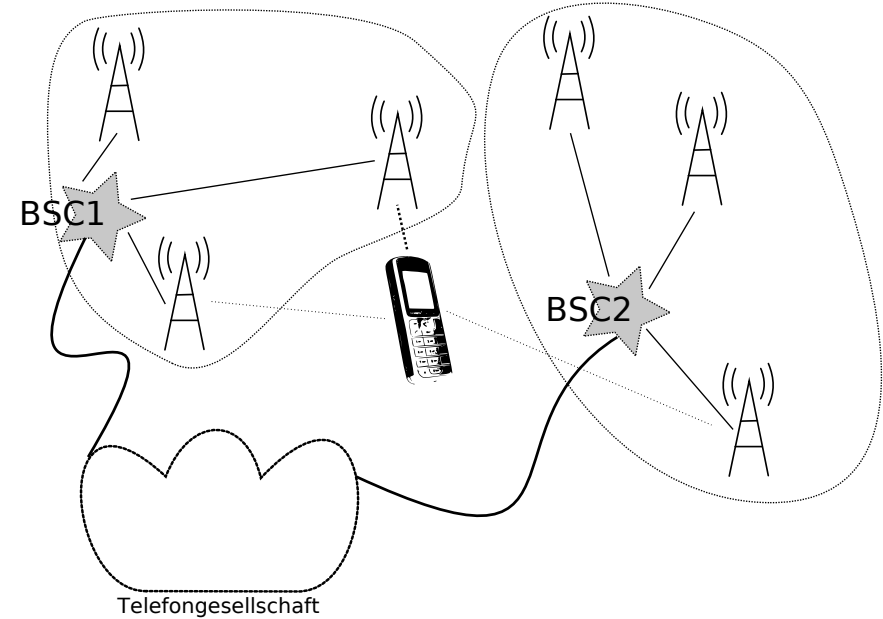


Fig. 2

## 2. GSM – ganz kurz

GSM steht für Global System for Mobile Communication und bezeichnet ein Regelwerk von rund 5000 Seiten, das vorschreibt, wie Mobiltelefone mit der Infrastruktur der Netzbetreiber und die einzelnen Komponenten dieser untereinander zu reden haben. Die üblichen Mobiltelefone in der BRD funktionieren nach diesem GSM-Standard. Neuere Telefone funken über den neueren UMTS-Standard. Logisch ändert sich für den nicht schrecklich viel, ein paar Details sind aber doch anders. Insbesondere verursachen UMTS-Telefone weitaus geringere elektromagnetische Störungen, was das Feststellen von Aktivität deutlich erschwert.

(vgl. Fig. 2)

SIM-Karte (IMSI) – damit ein Telefon funktioniert, braucht es eine Chipkarte namens Subscriber Identity Module. Es enthält neben etwas Speicher und kryptographischer Hardware die IMSI („Mobile Subscriber Identity“), eine weltweit eindeutige Zahl, die ausweist, an wen die Rechnung geht. Sie entspricht in etwa der Telefonnummer beim Festnetztelefon (i.d.R. gibt es eine 1:1-Entsprechung von IMSI und Telefonnummer). „Legal“ gekaufte IMSIs *sollen* mit der Identität der Ausweispapiere verbunden sein, aber nicht alle Telekoms nutzen die Kann-Bestimmung aus §95 (4) TKG.

Telefon (IMEI) – auch Telefone haben eine Nummer, die IMEI („Mobile Equipment Identity“; wenn ihr neugierig seid: \*#06# zeigt sie an). Mit ihr könnten gestohlene Mobiltelefone gesperrt werden, doch wurde das höchstens ausnahmsweise gemacht. Mittlerweile wird sie regelmäßig mitgespeichert, so dass nicht nur NutzerInnen, sondern auch Geräte identifiziert werden können.

Provider wollen IMEIs derzeit fürs Aussperren patentverletzender Telefone nutzen, die Polizei ist noch eher zurückhaltend, weil sie nicht wissen, was sie damit machen sollen.

Netz – viele Antennen (in etwa die „Zellen“ des Netzes), verbunden durch Kabel oder Funkstrecken. Wenn das Telefon eine Verbindung hat, kontrolliert immer eine davon das Telefon. Das Telefon meldet die Feldstärken der benachbarten Antennen; auf dieser Basis entscheidet das Netz, ob es das Telefon an eine andere Antenne weiterleitet („Handover“; das ist bei UMTS anders, da kann ein Telefon von mehreren Masten gleichzeitig bedient werden).

Ist das Telefon nicht am Telefonieren und wird auch nicht bewegt, meldet es sich nur selten zum PLU (Periodic Location Update, zwischen 30 Minuten und 12 Stunden). Das Telefon sucht sich dann selbst die Antenne („Zelle“), die es für gut hält. Die Zellen haben eine Größe zwischen wenigen 100 Metern und ca. 25 Kilometern und dabei häufig die Geometrie von großzügigen Tortenstücken.

Provider – die einzelnen Antennen (auch „Base Transceiver Station“ BTS) sind zunächst mit einem lokalen Rechner verbunden, dem BSC („Base Station Controller“), und der wiederum mit einer Zwischen-Verwaltungseinheit, dem Mobile Service Center MSC, meist per Kabel, bei geizigen Providern auch per Funkstrecke verbunden.

Typischerweise bilden alle Antennen, die an einem BSC hängen, eine „Location Area“ (LA; zur Not können da auch mehrere BSC zusammengeschaltet sein). Wichtig ist das, weil das Netz von einem idlenden Gerät die Position nur bis auf eine LA genau weiß (und die sind in Nordbayern auch mal 100 km groß). Andererseits kann das Netz ein Telefon jederzeit pagen und so die Position wieder auf mindestens eine Antenne genau bestimmen.

Das MSC ist auch der Übergabepunkt in die anderen Netze. Dort steht die Abhörausrüstung.

Beim Provider sehen verschiedene Computer nach, ob ein Telefon dieses Netz benutzen darf, an wen die Rechnung geht usw. Der Provider weiß, in welcher LA ihr seid, wer ihr seid, er speichert eure SMS, wenn euer Telefon nicht erreichbar ist usw.

Ein Telefon kann (im Groben) aus, idle oder dedicated sein. Es ist „idle“, wenn es keine Verbindung hat; dass macht es nur PLUs und location updates, wenn es feststellt, dass es eine location area wechselt. Das Netz weiß dann nur die location area, in der das Telefon ist. Es ist „dedicated“, wenn ein Gespräch geführt oder eine SMS übertragen wird. Dann weiß das Netz die Zelle, in der das Telefon ist, und dank des „timing advance“ (das ist ungefähr die Laufzeit von Licht zwischen der Antenne und dem Gerät) auch, wie weit es von der Antenne entfernt ist. Tatsächlich weiß es auch noch, wie stark die Signale von anderen Antennen am Telefon ankommen, womit evtl. eine noch genauere Ortsbestimmung möglich wäre. Wegen dieses Informationsvorteils ist die „stille SMS“ so interessant für die Repressionsbehörden.

Die Situation bei datenbasierten Diensten (z.B. GPRS) ist nochmal komplizierter; z.B. eine Lokalisierung von Geräten, die immer in GPRS eingebucht sind, genauer als bei Telefonen im idle mode, aber weniger genau als bei Telefonen im dedicated mode.

Im GSM-Netz weist sich nur das Telefon gegenüber dem Netz aus (Schlüssel auf der SIM-Karte), das Netz aber nicht gegenüber dem Telefon. Das ermöglicht Angriffe wie IMSI-Catcher. UMTS hat daraus gelernt und schreibt beiderseitige Authentifizierung vor (kann aber auf GSM zurückfallen).

### 3. Vorneweg: Lauschangriff

Mobiltelefone können ihre Umgebung abhören:

1. Indem sie ohne klingeln abheben oder
2. indem sie die Umgebungsgeräusche aufzeichnen und später übertragen

Fall (1) ist leicht zu diagnostizieren und fällt leicht auf – das Telefon ist „abgehoben“, es stört Verstärker, Monitore usw.

Fall (2) ist weit schwieriger zu diagnostizieren. Dazu kommt, dass für grenzwertig verständliche Sprache größenordnungsmäßig 1 MiB/Stunde reichen – ein modernes Telefon könnte so über Monate ununterbrochen mitschneiden, was gesagt wird.

Das Anschalten eines abgeschalteten Telefons durch „Fernbefehl“ ist *nicht* möglich und wird es nie sein.

Allerdings könnten richtig fiese Leute modernen Telefonen beibringen, sich ausgeschaltet zu stellen, aber noch zu laufen. Dazu ist denkbar, dass Telefone so programmiert werden, dass sie sich zu einem bestimmten Zeitpunkt selbst einschalten. Solche Befürchtungen sind ein Grund für die Empfehlung, den Akku zu entfernen, wenn mensch „sicher“ sein will. Der andere ist, dass der Akku des Telefons auch eine unabhängige Wanze versorgen könnte, wenn die Polizei viel Zeit hatte mit dem Telefon.

Die Bundesregierung hat 2008 gesagt, das BKA habe sowas nicht eingesetzt. Über Landespolizeien und Geheimdienste hat sie nichts gesagt, aber es erscheint insgesamt unwahrscheinlich, dass sich diese so viel Mühe geben; alle diskutierten Optionen sind jeweils auf einzelne Telefone zuzuschneiden und auch dann nicht ganz trivial umzusetzen.

Insofern ist das Telefon als Billig-Wanze eher ein untergeordnetes Problem.

Rechtsgrundlage wäre §100c StPO („großer Lauschangriff“) oder §23 PolG BaWü. Ersteres geht bei „besonders schweren Straftaten“ (wozu natürlich die 129er-Familie gehört), letzteres zur Abwehr einer Gefahr für den Staat oder die Gesundheit einer Person. Es braucht in der Regel einer richterlichen Anordnung, außer, wenn das Ziel nur die Eigensicherung ist.

Dabei sind große Lauschangriffe nach StPO selten (niedrig zweistellig pro Jahr).

### 4. Lawful Interception

Die Daten auf dem Weg zwischen Antenne und Telefon sind verschlüsselt und normalerweise schwer zu knacken. Abhörschnittstelle ist daher das MSC; dort ist es einfach.

Allein die Polizeien in der BRD haben 2007 in 4800 Verfahren abgehört, davon vielleicht etwa 300 aus dem weiteren Politbereich. Schätzungen gehen von gegen 30000 betroffenen Anschlüssen, davon 20000 Mobiltelefonen, und in die Millionen gehenden Gesprächen aus, harte Zahlen sind nicht verfügbar.

**Abhilfe:** Mobiltelefone und Festnetz unterscheiden sich hier nicht – nichts Vertrauliches am Telefon.

Rechtsgrundlagen sind §100a/b StPO. Das heißt, dass bisher Abhören zur „Gefahrenabwehr“ (jedenfalls in Baden-Württemberg) nicht geregelt ist. Abhören nach StPO geht natürlich nach Familie 129, aber auch nach zahlreichen anderen Tatbeständen, etwa Anstiftung zu Ungehorsam und dergleichen.

## 5. IMSI-Catcher

Der IMSI-Catcher simuliert für eine kleine Umgebung einen starken Funkmast eines Netzes. Die Telefone denken, sie hätten sich bewegt und versuchen einen Location Update. Daraufhin kann der Catcher dem Telefon IMSI und IMEI entlocken. Neuere IMSI-Catcher können auch *ein* Gespräch nach außen weitergeben und derweil abhören.

Ansonsten sorgt ein IMSI-Catcher dafür, dass alle Telefone, die auf dem Netz eingebucht sind, für einige Minuten nicht funktionieren (weil er ja keine echte BTS ist); laufende Gespräche werden aber nicht unterbrochen, Telefone im dedicated mode suchen sie ja die Antennen nicht selbst.. Die Weiterleitung („Man-in-the-middle attack“) geht auch nur dann leicht, wenn sich das Telefon auf unverschlüsselte Übertragung zwingen lässt (das tun sie wohl alle). Abhören ist aber für die Behörden eher langweilig, weil sie das einfacher über den Provider tun können.

Zweck: (1) Sehen, ob ein Telefon in einem Haus ist, etwa zur Ergreifung von Flüchtlingen. (2) Bestimmung von IMEI und IMSI, die eine observierte Person mit sich führt.

**Abhilfe:** Telefon ausschalten. Da während eines Gesprächs das Netz und nicht das Telefon über die verwendeten Basisstationen entscheidet, ist man während eines Gesprächs immun gegen IMSI-Catcher. Alternativ könnte man ein UMTS-Telefon verwenden und ihm den fallback auf GSM verbieten; inzwischen soll es aber auch dafür Geräte geben, die ähnlich einem IMSI-Catcher funktionieren. Details sind dazu nicht zu bekommen.

Rechtsgrundlage: §100i StPO oder §23a (6) PolG BaWü Nach StPO kann der IMSI-Catcher eingesetzt werden, wenn man abhören dürfte, oder wenn die Polizei behauptet, anders nicht weiterzukommen. Die Polizei muss idR ein Gericht fragen. Beim Einsatz zur Gefahrenabwehr erlaubt sich die Polizei den IMSI-Catcher selbst.

## 6. Verkehrsdaten

Verkehrsdaten sind in §96 TKG definiert:

- Kennung der verbundenen Anschlüsse und ggf. weiterer beteiligter Anschlüsse
- IMEI und IMSI der beteiligten Geräte
- „Standortdaten“ (etwa Funkzellen)
- Anfang und Ende der Verbindung, Dienst, ggf. Datenmenge
- „sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten“

Es gibt noch weitere Bestimmungen dazu, z.B. im derzeit ausgesetzten §113a TKG (Vorratsdatenspeicherung), in §3 TKG oder §100g StPO – das ist vor allem Folge der immer hektischer eingeführten Kontroll- und Überwachungsgesetze; sogar das Internet-Zensurgesetz („Zugangser-schwerung“) hat hier eingegriffen.

Die Vorratsdatenspeicherung verlangte, diese Daten 6 Monate vorzuhalten.

Die tatsächlichen Speicherfristen variieren derzeit je nach Provider. Eine Übersicht der Polizei von 2011 zeigt folgendes Bild:

- D1 30 Tage mit Geodaten, 180 Tage Verbindungen
- D2 30 Tage mit Geodaten, 180 Tage Verbindungen
- E-Plus 92 Tage mit Geodaten
- O2 7 Tage mit Geodaten, 30 Tage Verbindungen

Vermutlich ließen sich diese Speicherfristen vielfach anfechten, da sie, vor allem im Prepaid- und Flatrate-Bereich kaum erkennbaren Zielen dienen. Eine derzeit in Beratung befindliche Novelle des Telekommunikationsgesetzes wird den Telekoms aber spezielle Speicherrechte einräumen (wenn nicht ein Aufstand diese Regelung rausschießt, womit aber nicht zu rechnen ist).

Andererseits *scheinen* KundInnen von Resellern nicht in den Verkehrsdatensilos der großen Provider gespeichert zu werden (also z.B. Simyo nicht bei E-Plus), und es scheint, dass speziell Prepaid-Anbieter weniger speichern. Da ist allerdings noch Recherchearbeit nötig.

## 7. Bestandsdaten

Das sind Name, Adresse, Telefonnummer, IMSI, IMEI usw., die zu einem „Anschluss“ gehören.

Verkehrsdaten kommen idR quasi pseudonymisiert, also mit Rufnummer oder IP-Adresse. Übersetzung in Namen nach §112/113 TKG.

Die Bundesnetzagentur kann in den Gesamtdaten auch mit Wildcards suchen und reicht die Fähigkeit an u.a. Polizei (zu Strafverfolgung und Gefahrenabwehr) durch. Die Abfrage erfolgt automatisiert ohne Prüfung oder Anordnung (es gibt aber ein Protokoll).

Nach §113 TKG: u.a. Auskunft zu PUK für „Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.“

## 8. Zugriff auf Verkehrsdaten

Die Polizei fordert Verkehrsdaten unter Angabe einer „räumlich und zeitlich hinreichend bestimmte[n] Bezeichnung“ an (§100g/h StPO, §23a PolG BaWü). Dabei verlangt das PolG noch die Angabe von Telefonnummern („individualisierte FZA“; das ist bei StPO auch für „mittels einer Endeinrichtung“ begangenen oder geplanten Straftaten vorgesehen), während die StPO bei „schwerwiegenden Straftaten“ nur Raumzeit fordert.

Damit kann die Polizei während der Speicherfrist und auch live:

- für 30 bis 180 Tage sehen, mit wem ihr telefoniert (habt)
- für 7 bis 92 Tage grob sehen, wo ihr seid (wart)

Voraussetzung: Verkehrsdaten müssen entstanden sein.

Nebenbei: §23a (7) PolG BaWü erlaubt der Polizei auch, eure Gespräche zu unterberechnen oder zu unterbinden.

## 9. Stille SMS

Verkehrsdaten lassen sich auch ohne Kommunikation von eurer Seite erzeugen. Zur Wartungs- und Diagnosezwecken kann der Provider einem Telefon ein SMS-Äquivalent schicken, das das Telefon kurz dedicated macht: „stille SMS“.

2009 hat die Polizei NRW 320000 davon verschickt.

Ausgeschaltete Telefone können nicht dedicated werden und sind daher immun gegen stille SMS.

## 10. Fälle

Der sächsische LfD hat eine schöne Übersicht über gerichtliche Entscheidungen zur FZA gemacht:

- Magedburg, Banküberfall, 2005. LG Magdeburg verbietet FZA über einige Funkzellen in der Stadtmitte Magdeburgs für eine Stunde, weil „Mobilfunkverkehr von tatunbeteiligten Dritten in erheblichem Umfang“ zu erwarten war und mithin ein in Abwägung mit dem Banküberfall zu großer Eingriff in Grundrechte stattfinden würde. Außerdem zweifelte das Gericht daran, dass die Täter telefoniert haben.
- Oldenburg, Holzklotz-Fall, 2008. Jemand hat Autos dick und wirft Holzklotze von einer Autobahnbrücke. LG Oldenburg findet FZA in 29 Funkzellen von 17 bis 23 Uhr zur Aufklärung „noch“ rechtmäßig. Das Gericht fand plausibel, dass der Täter ein Telefon dabei hatte, und der Vorwurf war Mord. Das Gericht hat nochmal die Mär von den harmlosen Verbindungsdaten (ggü. Gesprächsinhalten) nachgebetet.
- Rostock, Kupferdiebstahl, 2007. Jemand hat eine Windkraftanlage ruiniert, indem er Kupfer geklaut hat. LG Rostock hat eine bereits abgenickte FZA kassiert, weil die Polizei nicht vorher probiert hat, ohne FZA aufzuklären (Antrag kam 2 Tage nach der Tat, und offensichtlich waren nicht mal Altmethallhändler gefragt worden). Ob FZA sonst ok gewesen wäre, wollte das Gericht nicht entscheiden.
- Stade, Raubüberfälle auf Privatwohnungen, 2005. Es ging um die Ermittlung unbekannter Täter, das Gericht hat die FZA abgelehnt, u.a., weil keine Tatsachen dafür sprachen, dass die Täter telefoniert hatten. Das LG Stade hat auch nochmal betont, Verbindungsdaten unterlägen dem uneingeschränkten Schutz von GG Art. 10, und drum müssten die Begründungen besonders gut sein.
- Köln, Telefonkauf mit Falschgeld, 2003. Hier wollte die Polizei drei Monate rückwirkend alle Verbindungen, an denen die (vier) per IMEI identifizierten Telefone teilgenommen hatten, haben. Das AG Köln hat die Maßnahme abgewiesen, weil eine Geräteüberwachung gesetzlich nicht vorgesehen ist.
- Rottweil, Diebstahl, 2004. Zwischen 4:30 und 5 Uhr trümmern Leute mit einem Gullydeckel eine Schaufensterscheibe ein und klauen aus einem Telefonladen Geld und Karten. Das LG Rottweil stimmt einer FZA zu, weil um die frühe Uhrzeit wohl nicht viele Unbeteiligte betroffen seien und es das Verbrechen ausreichend schwer fanden.

Aber: Die meisten Maßnahmen kommen gar nicht vor richtige Gerichte, die Ermittlungs- oder Amtsgerichte lehnen fast keine Anträge der StA ab (die nicht selten die Anträge gleich auf dem Briefpapier der Gerichte schreiben), so dass die Kasuistik nur selten wirklich hilft.

Plus: Meist ignorierte Benachrichtigungspflichten bei Abhören, Observation, Verkehrsdatenabfrage, IMSI-Catchen. Zwar ist seit der letzten StPO-Reform irgendwann die nächsthöhere Instanz einzuschalten, aber auch die findet offenbar in aller Regel, die Betroffenen könnten nicht ohne Gefährdung von „schutzwürdigen Belangen“ oder des Untersuchungszwecks unterrichtet werden, oder sie könnten ohnehin kein Interesse an einer Benachrichtigung haben, weil die Rechtsverletzung nur unerheblich war.

Schließlich ist eine Anfechtung der Schnüffelei angesichts des schieren Ausmaßes praktisch nicht möglich. Zumal gibt es für die Täter keine Konsequenzen aus rechtswidrig durchgeführten Überwachungen.

Daher: Rechtsschutz ist normalerweise FDGO-Fiktion.

## 11. Zwei Verfahren in Dresden

Im Gefolge der Anti-Nazi-Aktionen vom 13. und 19.2.2011 kam es in Sachsen zu einigen Skandalverfahren mit massenhaften Verkehrsdatenabfragen. Auch nach einer recht scharfen Rüge des LfD machten die Polizeibehörden munter weiter.

(1) 129-Prozess des LKA: 5 FZAen rund um den 13. und 19.2., darunter eine über 48 Stunden und eine über 12 Stunden für die ganze Dresdener Südvorstadt. Das Gericht hat eine Anordnung abgezeichnet, die die StA vorher unverändert von der Polizei übernommen hat. Zur Zeit der LfD-Untersuchung waren das 896972 Datensätze mit 257858 Rufnummern, die zu 40732 Bestandsdatenabfragen führten. Zum 7.11.2011 hatte das LKA 923167 Verkehrs-Records und daraus 54782 Namen.

Irre Aussagen des sächsischen Innenministeriums: Es seien zu nicht relevanten Verkehrsdaten keine Bestandsdaten erhoben worden – also sollen alle 40000 Namen was mit der kriminellen Organisation zu tun haben. Auch behauptet das Ministerium, aus den Verkehrsdaten sei nicht ersichtlich, wer mit wem geredet hat – entweder haben diese Leute überhaupt keinen Schimmer, was sie tun, oder sie sind unglaublich frech.

Auch das LKA hatte keinen Plan. Ihre Ermittlungsstrategie bestand darin, bei der „kleinsten Funkzelle“ anzufangen und immer größere Funkzellen zu bearbeiten. Unklar bleibt, was sie in ihrer Arbeit gemacht haben oder welchen Sinn – über schlichten Terror und offenen Hass auf AntifaschistInnen hinaus – dieser Murks hätte haben sollen.

Im Rahmen des 129er-Verfahrens wurde auch der IMSI-Catcher auf zwei bekannte Karten losgelassen, also seine Lokalisierungsfunktion genutzt.

(2) Landfriedensbruch, „Soko 19/2“: 14 „Tatorte“ mit recht genauen Zeiten. Die PD Dresden hatte recht schnell 138630 Datensätze von 65645 Anschlüssen, aus denen 379 Personen für Bestandsdatenabfrage ermittelt wurden. Zum 7.11.2011 153266 Datensätze aus Verkehrsdaten, 445 aus Bestandsdaten. Was genau die Polizei gemacht hat, um 99.5% der Anschlüsse als unverdächtig zu identifizieren, ist unklar. Vermutlich haben sie einfach ein paar Knöpfe auf ihrer Software („eFAS“) gedrückt, und was die tun, ist Geschäftsgeheimnis der privaten Hersteller.

Die Daten wurden auch für 45 Verfahren wg. Versammlungsgesetz verwendet. Das war dann selbst der Staatsanwaltschaft zu viel, und sie hat die Polizei gebeten, das doch zu lassen. Auch hat die Polizei wohl Daten in Verfahren wegen Verwendung von Kennzeichen, Sachbeschädigung und Beleidigung eingesetzt, was der LfD beanstandet hat. Das LKA hat dann noch seine Datensätze aus (1) an die Soko 19/2 gegeben. Dafür hat der LfD dann eine Rüge ausgesprochen. Die „Gewalttaten“ der Anti-Nazi-AktivistInnen identifiziert der LfD aber durchaus als Anlassstraf-taten. Er baut bei seiner Kritik leider vor allem Zeugnisverweigerungsrechte und Religionsfreiheit.

Absurditäten am Rande: Die PD Dresden hat behauptet, sie habe nicht vorhersehen können, dass so viele Daten zurückkommen. Sie hat auch von „mehrere[n] tausend potenziell als Tatverdächtige in Frage kommende[n] Personen“ schwadroniert. Klasse auch die Behauptung, „die Heimlichkeit einer verdeckten polizeilichen Maßnahme und ein unmittelbar einhergehender Einschüchterungseffekt“ gingen nicht zusammen. Ganz offensichtlich haben die Leute in Dresden nur sehr vage Vorstellungen von dem, was dieser Staat seinen BürgerInnen für ihre Gefolgschaft anbietet.

## 12. Was tun?

Fazit: Das Mobiltelefon ist auch ohne weitere staatliche Intervention eine permanente Datenerfassungsmaschine. Wenn ihr es im laufenden Zustand irgendwohin mitnehmt, kann die Staatsgewalt für eine ganze Weile auf Zellengröße genau nachvollziehen, dass ihr dort wart. Analog sind alle eure Kontakte nachvollziehbar. Mit anderen Worten sind die Verkehrsdaten angesichts ihres reichlichen Vorhandenseins mittlerweile weit dramatischer als die auch schon weit verbreitete Gesprächsüberwachung.

„Wer sein Telefon einschaltet, braucht eigentlich die Batterie auch nicht rauszutun.“

Dennoch: Es ist keine schlechte Idee, Prepaid-Karten zu kaufen und dabei falsche Personalien anzugeben – vielfach geht das.

**Aber:** Letztlich ist das nur politisch anzugehen. Überwachungsparagrafen (z.B. §§100ff StPO) müssen weg, weitere Befugnisse der Polizei verhindert, Gesetze zur politischen Verfolgung (z.B. §§129ff StGB) abgeschafft werden.

Schafft Rote Hilfe (oder sowas ähnliches)