

Soziale Bewegungen im digitalen Tsunami

Tagung zu neuen digitalen Schnüffelwerkzeugen

4. Februar 2012, 11.00 – 19.00 Uhr

Südblock, Admiralstraße 1, 10999 Berlin-Kreuzberg



Vor fünf Jahren organisierten sich europäische Innenminister unter Rädelsführerschaft der deutschen EU-Präsidentschaft in einer sogenannten „Future Group“, um auf die Weichenstellungen für die Polizeiarbeit der Zukunft Einfluss zu nehmen. Schon damals wurde von „gewaltigen Informationsmengen, die für öffentliche Sicherheitsorganisationen nützlich sein können“ orakelt: Der erwartete „digitale Tsunami“ würde demnach verheißen, Milliarden elektronischer Geräte in Echtzeit zu verfolgen und Verhaltensmuster ihrer NutzerInnen analysieren zu können. Inzwischen wird diese digitale Aufrüstung zunehmend spürbar und erreicht auch Soziale Bewegungen. Denn die neuen kriminaltechnischen Werkzeuge finden in den behördlichen Beschaffungsabteilungen begeisterte Abnehmer. Die Aufstände in nordafrikanischen und arabischen Ländern zeigen, dass die Produkte der neuen Generation skrupellos auch an autoritäre Regierungen verkauft werden.

Ihr zunehmender Einsatz bewegt sich auch in Europa oftmals in einer rechtlichen Grauzone: Die Anwendungen liegen quer zur gegenwärtigen Gesetzgebung. Überkommene strafprozessuale und gefahrenabwehrrechtliche Eingriffsgrundlagen tragen den neuen erweiterten Datenerhebungs- und Verwendungsmöglichkeiten kaum angemessen Rechnung. Insbesondere der zunehmende Einsatz von Soft- und Hardware durch Polizeien und Geheimdienste weckt staatliche Begehrlichkeiten nach immer weiteren Datenmengen und vollzieht sich bislang ohne eine nennenswerte gesellschaftliche Auseinandersetzung:

Das Handy als polizeiliches Werkzeug zur Strafverfolgung und „Crowd Control“

Die Proteste gegen die Nazi-Aufmärsche in Dresden Anfang 2011 machten auf die polizeiliche Nutzung von Daten aus der **Funkzellenauswertung** (FZA) aufmerksam. Auf richterlichen Beschluss lieferten Provider Verkehrsdaten von Gesprächen oder SMS, darunter die Nummer beteiligter Anschlüsse, Beginn und Ende der Verbindung, IP-Adressen oder andere genutzte Dienste. Diese FZA tangierte die Rechte einer Vielzahl von Menschen, die offensichtlich nichts mit dem Ziel der Maßnahme zu tun hatten: In zwei Ermittlungsverfahren („Besonders schwerer Fall des Landfriedensbruchs“, „Bildung einer kriminellen Vereinigung“) wurden über eine Million Verbindungsdatensätze gespeichert und zu mehr als 40.000 Anschlüssen auch die zugehörigen AnschlussinhaberInnen ermittelt. Die so erlangten Daten nutzte die Staatsanwaltschaft zunächst auch für die zur Verfolgung geringfügiger Verstöße. Die in Ermittlerkreisen sogenannte **„telekommunikative Spurensuche“** kann aber auch **in Echtzeit** genutzt werden, wie es bereits 2009 über eine von Nokia Siemens Networks in den Iran gelieferte Plattform berichtet wurde: Die staatlichen Milizen registrierten, wenn sich auffällig viele Mobiltelefone in Funkzellen eingebucht hatten. Dadurch wurden Spontanversammlungen schnell ausfindig gemacht. Um auch inaktive Mobiltelefone ins Radar von Verfolgungsbehörden zu rücken, werden sogenannte **„Stille SMS“** versandt. Diese im Polizeijargon als „Ortungsimpulse“ bezeichneten SMS sind für die ausgeforschte Person unsichtbar. Mit diesem Trick zwingen die Polizeien und Geheimdienste die Provider, den Standort der Geräte bzw. Nutzer zu registrieren. Auf diese Weise verschickt allein die Polizei Nordrhein-Westfalens ebenso wie Schäubles Zollkriminalamt jährlich mehr als eine Viertelmillion „Stiller SMS“. Derart lokalisiert kann zur Ausforschung des/der Handy-Besitzers/Besitzerin ein sogenannter **„IMSI-Catcher“** eingesetzt werden. Dabei handelt es sich um eine mobile Überwachungseinheit, die gegenüber dem Telefon eine starke Funkzelle simuliert. Das Telefon bucht sich automatisch dort ein. Fortan können alle hierüber geführten Verbindungsdaten protokolliert oder Gespräche ohne Umweg in

Echtzeit mitgehört werden.

Vielfach laufen die Informationen in Lagezentren zusammen. Diese sogenannten „**Monitoring Centers**“ zur Visualisierung eingehender Informationen sollen den Behörden ein umfassendes Lagebild verschaffen und die Entscheidungsfindung und Führungsfähigkeit verbessern. Die Systeme sollen aber zunehmend miniaturisiert werden, um sie auch ad hoc für „Konferenzen, Großanlässe, Demonstrationen oder Entführungen“ nutzen zu können. Hierzu finanzieren EU-Mitgliedstaaten ebenso wie die Europäische Union (EU) **Forschungsprogramme**, um eine „automatische Aufdeckung von Bedrohungen“ zu befördern.

Mathematik gegen Dissens – Computergestützte Repression

Neben der üblichen polizeilichen Fallbearbeitung und Vorgangsverwaltung wird etwa **Ermittlungssoftware** eingesetzt, um Beziehungen in Datensätzen zu finden. Aufgebohrt mit „Zusatzmodulen“ kann die Software auf weitere Datenbanken zugreifen oder GPS-Überwachung einbinden. Die Software-Industrie verkauft Produkte zum „**Data Mining**“, die einen Mehrwert aus bislang unstrukturierter Information besorgen sollen. Laut Anbietern verwalten die Anwendungen Texte und Audio-Mitschnitte, Videos, Emails, Bewegungsprofile oder Handy-Ortungsdaten. Doch damit nicht genug: Auf zahlreichen Verkaufsmessen werden statistische Verfahren auch für die Polizeiarbeit beworben, die mittels „vorausschauender Analyse“ Kriminalitätsmuster erkennen und sogar Straftaten vorhersehen wollen. Einer der Marktführer bezeichnet die versuchte Vorhersage als „Evolution in der Verbrechensbekämpfung“.

Auch das Internet wird längst mit allerlei Anwendungen ausgeforscht.

Telekommunikationsanbieter sind zur Zusammenarbeit mit Verfolgungsbehörden verpflichtet und müssen technische Standards für „**Lawful Interception**“ (etwa „behördliches Abhören“) einhalten. Je nach Lage der Bürgerrechte setzen Regierungen Anwendungen zur „**Deep packet inspection**“ (DPI) ein, die den Internetverkehr nach Suchbegriffen filtern können. Weil immer mehr NutzerInnen ihre Kommunikation verschlüsseln (auch der Verkehr von Internettelefonie via Skype ist codiert), infiltrieren Polizeien und Geheimdienste die genutzten Rechner direkt. Diese behördlichen Hackerangriffe unterscheiden offiziell zwischen „**Quellen-Telekommunikationsüberwachung**“ und „**Online-Durchsuchung**“ – eine Trennung, deren Machbarkeit von AktivistInnen grundlegend in Frage gestellt wird. Die Überwachung des Nutzerverhaltens im Internet bleibt indes nicht auf den eigenen Rechner beschränkt.

Soziale Netzwerke, also Twitter, Facebook, Google+ oder StudiVZ müssen

Verfolgungsbehörden ebenfalls auf richterliche Anordnung Daten herausgeben. Auch in öffentlichen Blogs und Chaträumen kann nach Auffälligkeiten, Interessen von Gruppen, Trends oder anderen Aussagen über Beziehungen zwischen Personen und Vorgängen gesucht werden. Zahlreiche Studien belegen den Wert dieser „**Open Source Intelligence**“ (OSINT). Demnach können Beziehungen unter Personen vollständig aufgedeckt werden, wenn nur acht Prozent der Gruppe ausgeforscht werden.

Digitaler Selbstschutz, Rechtsschutz, Online-Petition? Gegenstrategien in den Wogen des „digitalen Tsunami“

Die beschriebenen Entwicklungen erfordern ein Umdenken nicht nur bei AktivistInnen. Auch RechtsanwältInnen, Antirepressionsgruppen und Bürgerrechtsorganisationen müssen sich den neuen digitalen Kriminaltechniken stellen. Die Skandale um die Nutzung von Funkzellenauswertung oder Staatstrojanern machen deutlich, dass die Technologien durch die gegenwärtige Rechtslage nur unzureichend erfasst und beschränkt werden. Die munteren Exporte entsprechender Hard- und Software werfen zudem weitgehende bürgerrechtliche und demokratietheoretische Fragen auf.

Doch es gibt Möglichkeiten des Widerstands gegen die technokratischen polizeilichen Allmachtsphantasien. Betroffene wehren sich im Rahmen des Individualrechtsschutzes und skandalisieren die Ermittlungsmethoden und den mangelnden Grundrechtsschutz. Bürgerrechtsgruppen kritisieren die unverhältnismäßigen Datensammlungen, die eine

Bevölkerung unter Generalverdacht und die Unschuldsvermutung damit auf den Kopf stellen. Auf Kampagnenebene wird die Forderung artikuliert, den Quellcode polizeilicher und geheimdienstlicher Überwachungssoftware offenzulegen – insbesondere bei Data-Mining-Programmen oder „vorhersagender Analyse“.

Zumindest in deutschen aktivistischen Kreisen hat sich eine kritische Haltung in der Nutzung elektronischer Kommunikation herumgesprochen. Viele nutzen längst Dienste linker Internetanbieter, Email-Verschlüsselung oder die Absicherung eigener Rechner durch freie Betriebssysteme.

Jedoch geht es nicht allein um eine technische Antwort auf den neuen digitalen Ermittlungseifer.

Auf der Tagung wollen wir die verschiedenen Aspekte des „digitalen Tsunami“ erörtern. Nach der Darstellung ihrer technischen Funktionsweisen wollen wir uns der Frage widmen, was diese Entwicklungen für eine vorwärtsgewandte Antirepressionsarbeit und Netzpolitik von AktivistInnen, RechtsanwältInnen und BürgerrechtlerInnen bedeutet.

PROGRAMM

11.00 – 13.00 Uhr

Podium 1: Das Handy als polizeiliches Werkzeug zur Strafverfolgung und „Crowd Control“

- * Funkzellenauswertung zur Strafverfolgung in Dresden (Peer Stolle, Rechtsanwalt)
 - * Aufspüren von DemonstrantInnen in Echtzeit im Iran (Erich Moechel, Internetreporter)
 - * Die Verwaltung des digitalen Tsunami: Die Rolle der EU-Sicherheitsforschung (Eric Töpfer, Statewatch/ CILIP)
- Moderation: N.N.

14.00 – 16.00 Uhr

Podium 2: Mathematik gegen Dissens – Computergestützte Repression

- * Deep packet inspection und Vorratsdaten (Ralf Bendrath, Wissenschaftlicher Mitarbeiter von Jan Philipp Albrecht, MdEP/ Grüne)
 - * Ermittlungssoftware, Data Mining, voraussagende Analyse (Matthias Monroy, Journalist, Gipfelsoli)
 - * Polizeiliche Ermittlungen in Sozialen Netzwerken (Rena Tangens, Foebud)
- Moderation: Arbeitskreis Vorratsdatenspeicherung Münster

16.30 – 19.00 Uhr

Was tun: Digitaler Selbstschutz, Rechtsschutz, Online-Petition? Gegenstrategien in den Wogen des „digitalen Tsunami“

- * Alternative Provider und digitaler Selbstschutz (NADIR, angefragt)
- * Die Kampagne gegen Vorratsdatenspeicherung: Ein Modell für zukünftige Initiativen? (Katharina Nocun, Arbeitskreis Vorratsdatenspeicherung)
- * Wer macht eigentlich Netzpolitik? (Sandra Mamitzsch, Digitale Gesellschaft e.V.)
- * Mit Recht und Gesetz gegen ausufernde digitale Kriminaltechnik? (Thilo Weichert, Landesbeauftragter für den Datenschutz Schleswig-Holstein)
- * Aus dem Arsenal der polizeilichen Beschaffungsabteilung: Was da ist, wird auch benutzt

(Josephine Fischer, Initiativgruppe „Sachsens Demokratie“, Dresden)
Moderation: N.N.

**Die Tagung beginnt um 11.00 Uhr im Südblock, Admiralstraße 1, 10999 Berlin
(U-Bahn 8, Kottbusser Tor)
Die Teilnahme ist kostenfrei.
Auf Twitter: #RAV42**

Veranstalter: Republikanischer Anwältinnen- und Anwälteverein e.V., Zeitschrift Bürgerrechte & Polizei/ CILIP, Arbeitskreis Vorratsdatenspeicherung, Komitee für Grundrechte und Demokratie e.V., data:recollective, Kritische Jurist_innen der FU

Mit freundlicher Unterstützung der Holtfort-Stiftung.