



# 2002/25 Thema

<https://shop.jungle.world/artikel/2002/25/deine-spuren-im-netz>

## Deine Spuren im Netz

Von **Lucien Maignret**

### **In Sevilla wird es auch um neue Überwachungsmaßnahmen gehen.**

Wenn die Gipfelstürmer nach Sevilla reisen, werden sie von der spanischen Polizei rundum überwacht. Während die Kollegen auf der Straße die EU-Gegner aus ganz Europa verkloppen, wird im Polizeipräsidium eine kleine, aber feine Einsatztruppe unter anderem Webseiten wie indymedia und rebellion.org durchforsten, um rechtzeitig über eventuell geplante Straftaten im Bilde zu sein.

Seit einigen Wochen schon schieben Polizeidienststellen aller EU-Länder Daten hin und her, die die Personalien von bekannten Demonstranten enthalten. Egal ob sie bereits durch Straftaten aufgefallen sind oder nicht. Wie bei früheren Gipfeltreffen wird auch diesmal wieder Demonstranten die Teilnahme an Protesten mit keinem anderen Argument verwehrt werden als dem, sie hätten dergleichen schon einmal getan.

Die technische Grundlage dafür bildet ein Netz aus immer mehr und immer dichter miteinander verwobenen Datenbanken der Polizei und der Geheimdienste, aber auch der Einwohnermeldeämter, Krankenversicherungen, Stromversorger und Kraftfahrzeug-Zulassungsstellen, aus dem in einer Art permanenter Rasterfahndung auffällige Subjekte herausdestilliert werden.

Eine wachsende Anzahl von europäischen Kontaktstellennetzen, die sich um den Begleitschutz von reisenden Politikerinnen, um Fußball-Hooligans, Drogenverdächtige oder eben um die Sicherheit bei Gipfeltreffen bemühen, soll dafür sorgen, dass jederzeit die richtige Information der richtigen Dienststelle vorliegt.

Das Schengen-Informationssystem (SIS) wird derzeit zur Zentralkomponente dieses europäischen polizeilichen Datenbanknetzes ausgebaut. Ursprünglich nur zur Speicherung von Daten im Zusammenhang mit Verbrechen vorgesehen, ist das SIS heute zu 85 Prozent mit Datensätzen abgelehnter Asylsuchender angefüllt. In Zeiten wachsender Abschottung und wachsenden Sicherheitswahns ist es nicht ausgeschlossen, dass politische Dissidenten wie Globalisierungs- und EU-Kritiker bald einen guten zweiten Platz belegen.

Die größte gegenwärtig denkbare Datenbank ist erst in Vorbereitung. Wer sich eines Telefons bedient, wer im Internet surft, faxt oder eine E-Mail schreibt, hinterlässt dabei eine Menge Spuren auf Rechnern, über die seine Daten geleitet werden. Diese Daten lassen nicht nur Rückschlüsse auf die Art, die Dauer und den Partner der Kommunikation zu. Darüber hinaus

kann auch der Aufenthaltsort der Benutzer von Mobiltelefonen - bei der neuen Generation UMTS sogar metergenau - bestimmt werden. Besuchte Webseiten gewähren Aufschluss über die politische Orientierung, die sexuellen Interessen, den Kontostand, die Kreditkartennummer und die Konsumgewohnheiten.

Weil diese Daten nur zum Verbindungsaufbau und allenfalls zur Rechnungsstellung gebraucht werden, wurden sie bislang gemäß der geltenden europäischen Datenschutzbestimmungen stets gelöscht. Ende Mai passierte jedoch eine Novelle der EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation das Europäische Parlament. Seither gilt, dass die Mitgliedstaaten die Telefongesellschaften und Internetprovider verpflichten können, solche Daten zu speichern, damit Polizei und Geheimdienste später zugreifen können.

Mithilfe von Data-Mining-Tools, wie sie bei Überwachungsbehörden schon im Einsatz sind und zum Beispiel bei der Rasterfahndung benutzt werden, lassen sich aus den Verkehrsdaten Interaktionsmuster wie diese erstellen: Gesucht wird ein schwuler Autonomer aus dem Raum Bielefeld, der sich am 3. Januar rund um Gorleben aufgehalten hat. Mit der Kombination mehrerer Datensätze lassen sich soziale Geflechte detailliert und diagrammartig darstellen.

Dergleichen wurde in den USA mit den Attentätern vom 11. September praktiziert - auf einer wesentlich schmaleren Datengrundlage, als sie jeder einzelne europäische Bürger mit großer Wahrscheinlichkeit demnächst hinterlassen wird. Dass die Kommunikationsinhalte von der Speicherung zunächst ausgenommen sein sollen, ist da fast egal.

Deutschland, schon jetzt Weltrekordhalter in der Telefonüberwachung, ist vorgeprescht und hat als erster EU-Staat ein Gesetz auf den Weg gebracht, das sich die neuen Vollmachten zunutze macht. Der Entwurf des Bundesrates für ein »Gesetz zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen« erklärt kurzerhand alle Bürger zu potenziellen Kindervergewaltigern. Dem Entwurf zufolge sollen alle Verkehrsdaten der konventionellen elektronischen und der Internet-Kommunikation gespeichert werden.

Dass eine solche Verschärfung mit dem Verdacht des Kindesmissbrauchs begründet wird, ist seit langem üblich. Die Ausweitung auf einen ganzen Katalog von anderen Straftaten ist dabei gewissermaßen bereits mitgedacht. Hat man die Daten erst einmal, kann man sie gebrauchen, wie man will.

Der Entwurf harret derzeit einer Stellungnahme der Bundesregierung, um dann vom Bundestag verabschiedet zu werden. Die Regierung wird wohl kaum etwas zu mäkeln haben, denn er erteilt ihr weitreichende Vollmachten. Das Gesetz soll keine Regelungen enthalten, welche Daten von wem und wie lange zu speichern sind. Das darf die Regierung per Verordnung festlegen.

In einigen europäischen Ländern, so in Belgien und Frankreich, werden die Verbindungsdaten bislang sechs Monate lang gespeichert, was vordergründig mit Abrechnungsnotwendigkeiten und der Rechtsklarheit in Streitfällen über Telekomrechnungen begründet wird. Andere Länder - auch solche, von denen man es nicht vermuten würde - sind momentan noch liberaler.

Spaniens konservative Regierung musste in der vorigen Woche nach Protesten von Internet-Nutzern und -Providern ein Gesetzesvorhaben zurückziehen, das die Speicherung der Verbindungsdaten für zwölf Monate ermöglicht hätte. In Großbritannien hingegen will das

Unterhaus in dieser Woche über eine Verschärfung des Regulation of Investigatory Powers Act (Ripa) debattieren.

Nach diesem zwei Jahre alten Gesetz können Polizei- und Geheimdienststellen jederzeit von den Telefongesellschaften und den Internet Providern Informationen über einzelne Kunden abfragen. Provider beschwerten sich, das Gesetz werde zu »Fischzügen« missbraucht, was eine unerträglich hohe Zahl von Anfragen zur Folge habe. Darauf reagiert die Regierung nicht, indem sie Anfragemöglichkeiten einschränkt, sondern zahlreichen weiteren Behörden das Recht gibt, Anfragen zu stellen.

Nicht nur die veränderte Gesetzeslage beim Datenschutz dürfte die Regierungen derjenigen Länder, in denen heute noch nicht gespeichert wird, zu der Überlegung bewegen, den nationalen Sicherheitshütern diese Investigationsmöglichkeit zu verschaffen. Zudem arbeitet ein Team beim Europäischen Rat an einem Gesetzesentwurf, nach dem die Verbindungsdatenspeicherung in der ganzen EU verbindlich vorgeschrieben werden soll.

Auch dieser Entwurf wird wohl die Möglichkeit enthalten, solche Daten über Staatsgrenzen hinweg abzufragen. Dann könnte Spanien vor dem nächsten Großereignis gleich eine europaweite Anfrage stellen, welche verdächtigen Subjekte sich derzeit auf die Grenzen der iberischen Halbinsel zubewegen, um sie dort festzusetzen. Die Aufstandsbekämpfungseinheiten der Guardia Civil müssten nur in kleiner Besetzung anrücken. Da sage noch einer, die moderne Kommunikationstechnologie mache mehr Arbeit, als sie einspart.