www.vorratsdatenspeicherung.de

# STASI 2.0

Seit einiger Zeit werden verschiedene Bürgerrechte massiv eingeschränkt - meist mit der Begründung, dadurch könne eine effektivere Bekämpfung von Terrorismus und organisierter Kriminalität gewährleistet werden:

**Vorratsdatenspeicherung.** Am 18.04.2007 hat das Bundeskabinett den von Justizministerin Brigitte Zypries vorgelegten Gesetzesentwurf zur Vorratsdatenspeicherung beschlossen, der alle Anbieter von Kommunikationsdiensten (Telefon-, Internet-, Mailprovider usw.) dazu verpflichtet, verdachtsunabhängig künftig die gesamten Verkehrs- und Standortdaten ihrer Nutzer über mindestens sechs Monate für staatlichen Zugriff vorrätig zu halten. Dazu gehören alle besuchten Internetadressen (IPs), alle Mailkontakte sowie die Information, wann man von wo aus mit wem telefoniert hat.

**E-Pass.** Seit 01.11.2005 sind alle neuen deutschen Reisepässe mit einem RFID-Chip versehen. Auf diesem Chip werden neben den üblichen Passdaten auch ein biometrisch verwertbares Passfoto, eine Unterschriftenprobe sowie ab November 2007 zwei Fingerabdrücke digital gespeichert. Alle Daten sind aus meterweiter Entfernung per Funk auslesbar – auch mit selbstgebauten Geräten – und nicht ausreichend verschlüsselt. Ab 2008 soll dem E-Pass der mit biometrischen Daten versehene E-Personalausweis folgen.

**Online-Durchsuchungen.** Um dem Staat heimlichen Zugriff auf gespeicherte Daten (Kontakte, Korrespondenz, Chatlogs, Browserhistory) zu gewähren, können staatliche Ermittler über das Internet unbemerkt Spionagesoftware („Trojaner") auf Firmen- und Privatrechner einspielen. Am 25.04.2007 wurde bekannt, dass solche verdeckten Online-Durchsuchungen bereits seit 2005 auf Anordnung Otto Schilys durchgeführt werden, obwohl sie vom Grundgesetz und der Strafprozessordnung nicht gedeckt sind. In den Reihen der großen Koalition wird daher aktuell über eine Grundrechtsänderung zur „Schaffung einer gesetzlichen Grundlage" von Online-Durchsuchungen debattiert.

**Anti-Terror-Datei.** Das seit 31.10.2006 gültige „Gemeinsame-Dateien-Gesetz" dient als gesetzliche Grundlage zur Zusammenführung von über 100 Datenbanken verschiedenster staatlicher Institutionen, auf die nun die Polizei und Geheimdienste Zugriff haben. Dadurch wird der rechtsstaatliche Grundsatz der Trennung von Polizei und Geheimdiensten ausgehebelt: Die Polizei erhält Informationen, die von Geheimdiensten unter Missachtung rechtsstaatlicher Prinzipien beschafft wurden.

**Elektronische Gesundheitskarte.** Sie ist zwar keine Antiterrormaßnahme, aber – nicht zuletzt mangels ausgereifter IT-Sicherheit – dennoch eine Bedrohung für Datenschutz und Bürgerrechte: die bereits in der Testphase befindliche neue „Gesundheitstelematik". Ärztliche Verordnungen werden künftig als sog. „E-Rezepte" zentral gespeichert und können angeblich nur mittels eines digitalen Heilberufsausweises in Kombination mit der persönlichen Gesundheitskarte abgerufen werden. Die entsprechende zentrale Speicherung der lebenslangen Krankenakten aller Bürger ist vorgesehen.

**Zum Weiterrecherchieren:** Videoüberwachung, Wahlcomputer, §129a, Rasterfahndung, Großer Lauschangriff, Aufhebung des Bankgeheimnisses, Verwendung des Mautsystems zur Erstellung von Pkw-Autobahnbewegungsprofilen.

www.vorratsdatenspeicherung.de

STASI 2.0

Seit einiger Zeit werden verschiedene Bürgerrechte massiv eingeschränkt - meist mit der Begründung, dadurch könne eine effektivere Bekämpfung von Terrorismus und organisierter Kriminalität gewährleistet werden:

Vorratsdatenspeicherung. Am 18.04.2007 hat das Bundeskabinett den von Justizministerin Brigitte Zypries vorgelegten Gesetzesentwurf zur Vorratsdatenspeicherung beschlossen, der alle Anbieter von Kommunikationsdiensten (Telefon-, Internet-, Mailprovider usw.) dazu verpflichtet, verdachtsunabhängig künftig die gesamten Verkehrs- und Standortdaten ihrer Nutzer über mindestens sechs Monate für staatlichen Zugriff vorrätig zu halten. Dazu gehören alle besuchten Internetadressen (IPs), alle Mailkontakte sowie die Information, wann man von wo aus mit wem telefoniert hat.

E-Pass. Seit 01.11.2005 sind alle neuen deutschen Reisepässe mit einem RFID-Chip versehen. Auf diesem Chip werden neben den üblichen Passdaten auch ein biometrisch verwertbares Passfoto, eine Unterschriftenprobe sowie ab November 2007 zwei Fingerabdrücke digital gespeichert. Alle Daten sind aus meterweiter Entfernung per Funk auslesbar – auch mit selbstgebauten Geräten – und nicht ausreichend verschlüsselt. Ab 2008 soll dem E-Pass der mit biometrischen Daten versehene E-Personalausweis folgen.

Online-Durchsuchungen. Um dem Staat heimlichen Zugriff auf gespeicherte Daten (Kontakte, Korrespondenz, Chatlogs, Browserhistory) zu gewähren, können staatliche Ermittler über das Internet unbemerkt Spionagesoftware („Trojaner") auf Firmen- und Privatrechner einspielen. Am 25.04.2007 wurde bekannt, dass solche verdeckten Online-Durchsuchungen bereits seit 2005 auf Anordnung Otto Schilys durchgeführt werden, obwohl sie vom Grundgesetz und der Strafprozessordnung nicht gedeckt sind. In den Reihen der großen Koalition wird daher aktuell über eine Grundrechtsänderung zur „Schaffung einer gesetzlichen Grundlage" von Online-Durchsuchungen debattiert.

Anti-Terror-Datei. Das seit 31.10.2006 gültige „Gemeinsame-Dateien-Gesetz" dient als gesetzliche Grundlage zur Zusammenführung von über 100 Datenbanken verschiedenster staatlicher Institutionen, auf die nun die Polizei und Geheimdienste Zugriff haben. Dadurch wird der rechtsstaatliche Grundsatz der Trennung von Polizei und Geheimdiensten ausgehebelt: Die Polizei erhält Informationen, die von Geheimdiensten unter Missachtung rechtsstaatlicher Prinzipien beschafft wurden.

Elektronische Gesundheitskarte. Sie ist zwar keine Antiterrormaßnahme, aber – nicht zuletzt mangels ausgereifter IT-Sicherheit – dennoch eine Bedrohung für Datenschutz und Bürgerrechte: die bereits in der Testphase befindliche neue „Gesundheitstelematik". Ärztliche Verordnungen werden künftig als sog. „E-Rezepte" zentral gespeichert und können angeblich nur mittels eines digitalen Heilberufsausweises in Kombination mit der persönlichen Gesundheitskarte abgerufen werden. Die entsprechende zentrale Speicherung der lebenslangen Krankenakten aller Bürger ist vorgesehen.

Zum Weiterrecherchieren: Videoüberwachung, Wahlcomputer, §129a, Rasterfahndung, Großer Lauschangriff, Aufhebung des Bankgeheimnisses, Verwendung des Mautsystems zur Erstellung von Pkw-Autobahnbewegungsprofilen.

Warum solche Maßnahmen eine **große Gefahr Rechtsstaat und Bürgerrechte** darstellen, für die Bekämpfung von Terrorismus und Kriminalität aber sehr ineffektiv sind, soll hier am Beispiel der Vorratsdatenspeicherung diskutiert werden:

**Generalverdacht.** Alle Bürger werden ohne jeden Anlass wie Verdächtige behandelt, auch wenn keinerlei konkrete Hinweise auf eine Straftat bestehen.

**Harmlose Verkehrsdaten?** Die Internet-Verbindungsdaten liefern präzise Informationen darüber, wie sich ein Nutzer im Netz bewegt und geben somit Aufschluss über seine Interessen, Vorlieben und Meinungen. Aus den Telefon-Verkehrsdaten ist zu erkennen, wer mit wem einen sehr engen, einen eher flüchtigen oder gar keinen Kontakt hat. Damit lässt sich ein Modell des sozialen Netzes der gesamten Bevölkerung bilden. Bei Mobiltelefonen wird zusätzlich der Standort registriert, an dem das Telefonat geführt oder die SMS gesendet oder empfangen wurde. Diese Daten sind also alles andere als harmlos – sie können als Grundlage zur Erstellung von Persönlichkeits- und Bewegungsprofilen jedes einzelnen Einwohners der Bundesrepublik dienen.

**Analysemethoden digitaler Daten.** Die Hoffnung, der Staat könne mit der Auswertung dieser Fülle an Daten überfordert sein, ist leider vollkommen unbegründet. Schon heute gibt es sehr ausgereifte Verfahren, die unter Anwendung von Methoden der künstlichen Intelligenz (Data-Mining) eine sehr tiefgehende, vollständig automatisierte semantische Analyse großer Datenmengen gestatten.

**Unumkehrbarkeit und Tragweite.** Informationen, die man einmal in die Hände eines Anderen gegeben hat, lassen sich nicht wieder einfordern – dieser Schritt kann nicht rückgängig gemacht werden, die ordnungsgemäße Löschung von Daten ist nicht überprüfbar. Wer weiß aber, welcher gravierende Nachteil in zehn Jahren aus einer jetzt bedenkenlos preisgegebenen Information entstehen kann? Rechtssysteme sind nicht unveränderlich, und was heute harmlos erscheint, kann dann zu höheren Krankenkassenbeiträgen, dem Verlust der Arbeitsstelle oder zu Schlimmerem führen.

**Unwirksam.** Schon mit verhältnismäßig geringen finanziellen Mitteln und basalem technischem Wissen kann jeder Kleinkriminelle die Wirkung der Vorratsdatenspeicherung vollständig aushebeln. Die Vorratsdatenspeicherung trifft also jeden unbedarften Bürger, der vor derlei Aufwand zurückschreckt – nicht aber den Personenkreis, gegen den sie sich eigentlich richtet: Das organisierte Verbrechen.

## Kann ich für meine Grundrechte eintreten – als Einzelner?

**Ja – und du bist nicht allein. Du kannst zum Beispiel aktiv werden, indem...**

- du mit Freunden z.B. über die Gefahren der Vorratsdatenspeicherung sprichst.
- du einer Bürgerrechtsorganisation wie der Humanistischen Union, dem FoeBuD, dem FifF, dem netzwek neue medien, der Deutschen Vereinigung für Datenschutz oder dem Chaos Computer Club beitrittst und/oder deren Arbeit ehrenamtlich oder finanziell unterstützt. Eine Liste gibt's hier: **www.freiheit-statt-angst.de**
- du von den Rechten, die uns bislang zustehen, Gebrauch machst und ihre Wahrung durch Verwendung technischer Mittel wie Verschlüsselung (GnuPG) oder Anonymisierung (JAP, TOR) sicherstellst: **de.wikipedia.org/wiki/Enigmail**
- du dich an der Verfassungsbeschwerde des Arbeitskreis Vorratsdatenspeicherung beteiligst. Das kostet einmalig 55 Cent Porto, macht kaum Mühe, setzt aber ein klares Zeichen, dass du – wie viele andere – mit Überwachungsmaßnahmen dieser Art nicht einverstanden bist: **www.vorratsdatenspeicherung.de**

Warum solche Maßnahmen eine **große Gefahr Rechtsstaat und Bürgerrechte** darstellen, für die Bekämpfung von Terrorismus und Kriminalität aber sehr ineffektiv sind, soll hier am Beispiel der Vorratsdatenspeicherung diskutiert werden:

**Generalverdacht.** Alle Bürger werden ohne jeden Anlass wie Verdächtige behandelt, auch wenn keinerlei konkrete Hinweise auf eine Straftat bestehen.

**Harmlose Verkehrsdaten?** Die Internet-Verbindungsdaten liefern präzise Informationen darüber, wie sich ein Nutzer im Netz bewegt und geben somit Aufschluss über seine Interessen, Vorlieben und Meinungen. Aus den Telefon-Verkehrsdaten ist zu erkennen, wer mit wem einen sehr engen, einen eher flüchtigen oder gar keinen Kontakt hat. Damit lässt sich ein Modell des sozialen Netzes der gesamten Bevölkerung bilden. Bei Mobiltelefonen wird zusätzlich der Standort registriert, an dem das Telefonat geführt oder die SMS gesendet oder empfangen wurde. Diese Daten sind also alles andere als harmlos – sie können als Grundlage zur Erstellung von Persönlichkeits- und Bewegungsprofilen jedes einzelnen Einwohners der Bundesrepublik dienen.

**Analysemethoden digitaler Daten.** Die Hoffnung, der Staat könne mit der Auswertung dieser Fülle an Daten überfordert sein, ist leider vollkommen unbegründet. Schon heute gibt es sehr ausgereifte Verfahren, die unter Anwendung von Methoden der künstlichen Intelligenz (Data-Mining) eine sehr tiefgehende, vollständig automatisierte semantische Analyse großer Datenmengen gestatten.

**Unumkehrbarkeit und Tragweite.** Informationen, die man einmal in die Hände eines Anderen gegeben hat, lassen sich nicht wieder einfordern – dieser Schritt kann nicht rückgängig gemacht werden, die ordnungsgemäße Löschung von Daten ist nicht überprüfbar. Wer weiß aber, welcher gravierende Nachteil in zehn Jahren aus einer jetzt bedenkenlos preisgegebenen Information entstehen kann? Rechtssysteme sind nicht unveränderlich, und was heute harmlos erscheint, kann dann zu höheren Krankenkassenbeiträgen, dem Verlust der Arbeitsstelle oder zu Schlimmerem führen.

**Unwirksam.** Schon mit verhältnismäßig geringen finanziellen Mitteln und basalem technischem Wissen kann jeder Kleinkriminelle die Wirkung der Vorratsdatenspeicherung vollständig aushebeln. Die Vorratsdatenspeicherung trifft also jeden unbedarften Bürger, der vor derlei Aufwand zurückschreckt – nicht aber den Personenkreis, gegen den sie sich eigentlich richtet: Das organisierte Verbrechen.

## Kann ich für meine Grundrechte eintreten – als Einzelner?

**Ja – und du bist nicht allein. Du kannst zum Beispiel aktiv werden, indem...**

- du mit Freunden z.B. über die Gefahren der Vorratsdatenspeicherung sprichst.
- du einer Bürgerrechtsorganisation wie der Humanistischen Union, dem FoeBuD, dem FifF, dem netzwek neue medien, der Deutschen Vereinigung für Datenschutz oder dem Chaos Computer Club beitrittst und/oder deren Arbeit ehrenamtlich oder finanziell unterstützt. Eine Liste gibt's hier: **www.freiheit-statt-angst.de**
- du von den Rechten, die uns bislang zustehen, Gebrauch machst und ihre Wahrung durch Verwendung technischer Mittel wie Verschlüsselung (GnuPG) oder Anonymisierung (JAP, TOR) sicherstellst: **de.wikipedia.org/wiki/Enigmail**
- du dich an der Verfassungsbeschwerde des Arbeitskreis Vorratsdatenspeicherung beteiligst. Das kostet einmalig 55 Cent Porto, macht kaum Mühe, setzt aber ein klares Zeichen, dass du – wie viele andere – mit Überwachungsmaßnahmen dieser Art nicht einverstanden bist: **www.vorratsdatenspeicherung.de**