Freiheit stirbt mit Sicherheit

Terror lässt sich durch die Speicherung von Verbindungsdaten nicht aufhalten.

Die Vorratsdatenspeicherung im Auge. Eine Analyse von ROLAND SPITZLINGER.

Je unsicherer das Selbst, desto gigantischer seine Investitionen in Sicherheit", schreibt der deutsche Philosoph und Pädagoge Andreas Tenzer. Doch nicht nur Individuen reagieren auf Bedrohung instinktiv mit erhöhtem Schutzbedürfnis, auch Staaten und supranationale Organisationen beherrschen diesen Reflex. Unter die Räder kommen dabei zunehmend verfassungsmäßig verbürgte Freiheiten, wie die jüngste EG-Richtlinie über die Vorratsdatenspeicherung zeigt.

Salut Big Brother

Unter dem Eindruck der Terroranschläge von London und Madrid verabschiedete die Europäische Union in der Rekordzeit von drei Monaten am 15. März 2006 eine Richtlinie, der zufolge sämtliche EU-Bürger in Zukunft präventiv überwacht werden sollen (siehe Infokasten). Im Gegensatz zur derzeitigen Regelung, wonach staatliche Institutionen nur bei gierung an, die sich von Beginn an für eine möglichst umfassende Überwachung einsetzten. Innenminister Günther Platter etwa verlangt nun den Zugriff auf die Daten nicht nur zur Bekämpfung terroristischer Aktivitäten, sondern auch bereits zur Aufklärung all jener Vergehen, die mit mehr als einem Jahr Freiheitsentzug bestraft werden. In Schweden soll es Telekommunikationsunternehmen ermöglicht werden, die gesammelten Daten kommerziell zu verwerten. Unternehmen wären damit in der Lage, noch detailliertere Kundenprofile zu erstellen und ihre Werbeaktivitäten entsprechend darauf abzustimmen.

Liberté passé

Frankreich wiederum weitete die Datenspeicherpflicht bereits auf sämtliche Anbieter von Kommunikationsdiensten aus. Damit sind nun auch Fast-Food-Ketten, Hotels, gemeinnützige Organisationen und Privatpersonen, die Kampf gegen den Terrorismus zu suchen ist. Mittlerweile beherrschen vorwiegend wirtschaftliche Interessen das Feld. Doch sind diese die Aufgabe grundlegender Freiheiten wert?

Datenschützer und Menschenrechtsorganisationen kritisieren die Richtlinie hart und verweisen auf deren Unvereinbarkeit mit der völkerrechtlich verbindlichen Europäischen Menschenrechtskonvention. Darin heißt es unter Artikel acht: „Jede Person hat das Recht auf Achtung des Familienlebens, ihrer Wohnung und ihrer Korrespondenz." Nach einhelliger Meinung von Rechtsexperten wie etwa dem Europäischen Zentrum für E-Commerce und Internetrecht muss ein derart starker Eingriff, wie sie die EU-Richtlinie darstellt, wohlbegründet und verhältnismäßig sein. Sie ist daher nur gerechtfertigt, wenn dadurch „schwere Straftaten" verhindert werden können. Eben diese Bedingung ist jedoch nicht erfüllt.

Tatsächlich kann die Vorratsebenso wenig gedacht, wie die lückenlose Überwachung öffentlicher Telefonzellen. Fügt man die Möglichkeit der Manipulation einer Kommunikationsverbindung unbedarfter Bürger hinzu, so steht eines fest: Für Kriminelle wird es trotz strenger Überwachung auch weiterhin sehr einfach sein, eine Entdeckung zu verhindern. Selbstmordattentäter dürfte die Tatsache, dass Polizeibeamte ihre Verbindungsdaten postum analysieren ohnehin nicht von ihren Vorhaben abbringen. Das Ergebnis wird der Aussage des Präsidenten des Dachverbands europäischer Polizeigewerkschafter sehr nahe kommen: „Ein enormer Aufwand mit wenig mehr Wirkung auf Kriminelle und Terroristen, als sie etwas zu verärgern."

Adieu absolute Sicherheit

Doch wenn eine lückenlose Überwachung die Sicherheit nicht erhöht und darüber hinaus einer offenen Gesellschaft zutiefst wi-

DIE FAKTEN

Der EU-Richtlinie 2006/24/EG zufolge müssen die EU-Mitgliedsstaaten Telekommunikationsunternehmen dazu verpflichten, die Verbindungsdaten ihrer Kunden für mindestens sechs Monate zu speichern. Die Daten geben Aufschluss darüber, wer wann mit wem und von welchem Ort aus kommuniziert hat, sei es per Telefon, Handy, E-Mail oder Internet. Der Inhalt eines Telefonats bzw. eines E-Mails soll nicht erfasst werden. Die Richtlinie muss von den EU-Mitgliedsstaaten bis zum 15. September 2007 umgesetzt werden, darf allerdings für die Dienste Internetzugang, Internet-Telefonie und E-Mail bis zum 15. März 2009 aufgeschoben werden.

Die von der Richtlinie betroffenen Telekommunikationsanbieter befürchten hohe zusätzliche Kosten, die laut aktuellem Gesetzesentwurf nicht abge-

konkretem und fundiertem Verdacht in die Persönlichkeitsrechte der Bürger eingreifen dürfen, steht bei erfolgreicher Umsetzung der Richtlinie in die nationale Gesetzgebung der EU-Mitgliedsstaaten die gesamte EU-Bevölkerung unter Generalverdacht. Das Verhältnis zwischen Staat und Bürger wäre nicht mehr durch grundsätzliches Vertrauen, sondern durch Misstrauen geprägt.

Wurde die europäische Öffentlichkeit zunächst mit dem Argument der terroristischen Bedrohung von der Notwendigkeit der Vorratsdatenspeicherung überzeugt, so gehen die aktuellen Entwürfe der Nationalstaaten zum Teil weit über die vom EU-Parlament ursprünglich genehmigte Regelung hinaus. Tatsächlich nähern sie sich den Vorschlägen der britischen und dänischen Regierung, welche alle Unternehmen, die einen öffentlichen Zugang zum Internet anbieten, gezwungen, die Verbindungsdaten zu protokollieren. Der aktuelle dänische Entwurf verpflichtet die Unternehmen sogar zur Speicherung des Ursprungs, der Zeit und des Ziels jedes einzelnen Datenpaketes. Durch die Maßnahme dürften die Kosten der Überwachung weiter steigen. Zudem kommt die Regelung einer vollständigen Aufhebung des Kommunikations-Geheimnisses sehr nahe. In Deutschland kämpft wiederum die Musikindustrie um den Zugriff auf die Verbindungsdaten, wäre sie damit doch in der Lage, auch kleinere Urheberrechtsverletzungen effektiv zu bekämpfen.

Die Beispiele zeigen, dass der ursprüngliche Grund für die Aufgabe grundlegender persönlicher Freiheiten längst nicht mehr im datenspeicherung leicht umgangen werden. Die Verwendung von Wertkartenhandys oder die Nutzung von E-Mail-Anbietern mit Firmensitz außerhalb der Europäischen Union ist dafür vollkommen ausreichend. Darüber hinaus bieten sich Telefongespräche über das Internet an, da sie technisch äußerst schwer zu überwachen sind. Personen, die völlig sichergehen möchten, können ihre E-Mails zudem jederzeit von privaten Mailservern aus verschicken, sich über anonyme WLAN-Hotspots (öffentlich zugängliche Funknetze) in das Internet einwählen oder den Mailverkehr über das nächstgelegene Internetcafé abwickeln. An eine vollständige Überwachung auch nichtkommerzieller Telekommunikationsanbieter ist laut Justizministerin Maria Berger schließlich in Österreich dernspricht, dann müssen sich der Staat und die Bürger vom Ideal einer absoluten Sicherheit verabschieden. Stärkere Überwachung führt in so einem Szenario lediglich zu weniger Freiheit, verstärkter Kampf gegen den Terror wird zum Kampf gegen die Bürger selbst. Richard Johnson, Diplomat im 18. Jahrhundert, wies auf die Gefahren einer solchen Entwicklung hin: „Diejenigen, die ihre Freiheit zugunsten der Sicherheit aufgeben, werden am Ende keines von beiden haben – und verdienen es auch nicht.“ Dramatischer brachte es Aristoteles vor über 2000 Jahren auf den Punkt: „Wer Sicherheit der Freiheit vorzieht, ist zu Recht ein Sklave.“ Wie weit es tatsächlich kommt, wird die Zukunft weisen.

Der Autor ist freier Journalist.

golten werden sollen. Alleine in Österreich gibt es zwölf bis 14 Millionen Telefonanschlüsse, mit bis zu 40 Milliarden Anrufen pro Jahr. Die geplante Überwachung würde alleine bei der Telekom Austria nach Eigenangaben einen Aufwand von 4,5 Millionen Euro verursachen. Das europäische Parlament geht für jedes größere Telekommunikationsunternehmen sogar von geschätzten einmaligen Kosten von 180 Millionen Euro, sowie von jährlichen Betriebskosten von 50 Millionen Euro aus. Damit würde sich, sofern die Kosten an die Kunden weitergegeben werden, die Telefon-, Handy- und Internetnutzung für die Konsumenten um 15–20 Prozent verteuern.

Roland Spitzlinger

„Nur die Dummen werden erwischt“

HANS G. ZEGER, Obmann der ARGE Daten, über Grundrechte im Bereich des Datenschutzes.


GEORG LEMBERGH

Die Furche: *Wird die EU durch die Vorratsdatenspeicherung sicherer?*

Hans G. Zeger: Nein, man erwischt nur die paar Dummen, die es nicht geschafft haben, einige Vorkehrungen zu treffen.

Die Furche: *Wie steht's mit der Terrorismusbekämpfung?*

Zeger: Den Terrorismus wird das überhaupt nicht tangieren. Die Verbrecher können diese Datenspeicherung sehr gut unterlaufen, und gerade terroristische Netzwerke verwenden andere Kommunikationswege wie Botendienste, mündliche Weitergaben usw. Für bestimmte Daten und Delikte riskieren diese Menschen ihr Leben, denen ist egal, ob sie nach der Tat ausgeforscht werden. Ein Punkt ist auch die Datenmenge. Wenn ein Terroranschlag stattgefunden hat, müssen viele Ressourcen aufgewendet werden, um in der Unmenge an Daten zu suchen, wenn überhaupt klar ist, wonach man sucht. Diese Ressourcen wären in der klassischen Verbrechensbekämpfung viel besser aufgehoben.

Die Furche: *Zu welcher Art von Gesellschaft führt dieser Wunsch nach absoluter Sicherheit?*

Zeger: Er führt zu einer fundamentalistischen Gesellschaft. Wir erfüllen die Wünsche jener, die angeblich bekämpft werden. Es kommt zu einem Paradigmenwechsel. Der Grundsatz der Verfassung, dass jeder Bürger unbehelligt leben darf, so lange er sich nichts zuschulden kommen lässt, und erst auf Verdacht ermittelt wird, gilt nicht mehr. Zunächst wird alles gespeichert und später definiert, welche Handlung unbescholten ist und welche nicht.

Die Furche: *Die Informations-Beschaffung wird schwierig werden?*

Zeger: So ist es, Beamte, Offizielle und dergleichen werden sich hüten, in den Dunstkreis zu geraten, sie hätten Informationen weitergegeben. Im vorauseilendem Gehorsam werden sie alles daran setzen, nicht erreichbar zu sein.

Die Furche: *Ist dieses absurde Sicherheitsbedürfnis ein Import?*

Zeger: Der Vergleich mit anderen Ländern ist schwer, weil fundamentale Dinge anders sind. Die Überwachung hat sich in den USA extrem verschärft, aber in erster Linie richtet sie sich gegen Ausländer. Die Vorratsdatenspeicherung, wie sie die USA in Europa fordert, ist in den Vereinigten Staaten nicht durchsetzbar.

Die Furche: *Besteht noch eine Chance, dass die Richtlinie kippt?*

Zeger: Man könnte den Passus, dass keine Daten aufgezeichnet werden dürfen, die auf den Inhalt rückschließen lassen, streng auslegen. Damit könnte man Nummern von NGOs, Redaktionen, Anwälten, Steuerberatern und ähnliche von der Speicherung ausnehmen. Dann würde nichts mehr übrig bleiben. Oder man ruft den Europäischen Gerichtshof für Menschenrechte an, weil die Richtlinie entgegen der Europäischen Menschenrechtskonvention verabschiedet wurde.

Das Gespräch führte Thomas Meickl.