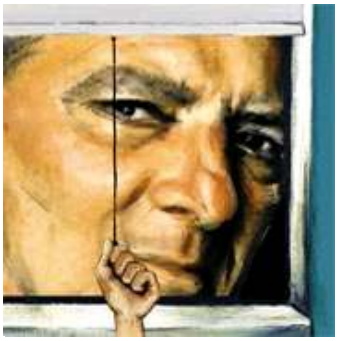
Technology Review

Ende des Wohlwollens

08.06.07
Infotech | Sicherheit

Von Gordon Bolduan

Technology Review 06/2007, Report



Wie ein Staatsfeind, Revoluzzer oder Agitator sieht Andreas Pfitzmann beileibe nicht aus: Der Seitenscheitel des 47-Jährigen ist akkurat gezogen, die Ränder sind sauber geschnitten. Tiefe Falten auf seiner Stirn zeugen von Nachdenklichkeit, ebenso wie die kurzen Pausen, die Pfitzmann stets einlegt, bevor er mit leiser Stimme eine Frage beantwortet. Sein Arbeitszimmer ist aufgeräumt, ein von seinem fünfjährigen Sohn gemaltes Blumenbild ziert die Wand. Bayrische Beamte aber beschimpfen Pfitzmann, Informatik-Professor an der TU Dresden, schon mal als "Förderer des Terrorismus". Und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde er im Mai 2005 als für den 9. Deutschen IT-Sicherheitskongress eingeplanter Referent kurzerhand wieder ausgeladen – mit einer für Pfitzmann fadenscheinigen Begründung.

Sein Vergehen: Als Leiter der Datenschutz- und Sicherheitsgruppe an der TU beschäftigt sich Pfitzmann seit vielen Jahren mit Dingen wie Kryptografie, Biometrie oder Anonymität im Internet. Lange Zeit war sein Sachverstand gefragt – den früheren Innenminister Otto Schily etwa konnte er nach eigener Erzählung noch von dem Vorhaben abbringen, staatliche Hintertüren für Krypto-Produkte vorzuschreiben. In der jüngeren Vergangenheit sind seine Überzeugungen aus der Mode geraten. Aber Pfitzmann erzählt weiter jedem, der es hören will, dass staatliche Überwachung und Bürgerrechte nicht zusammengehen: "Wer argumentiert, er braucht mehr Überwachung, um die Demokratie zu schützen, der hat Demokratie nicht verstanden." Er und viele andere Uni-Forscher aus seinem Dunstkreis arbeiten deshalb an Methoden, mit denen sich der grassierenden Kontrollwut des Staates – von dem sie letztlich bezahlt werden – technisch Einhalt gebieten lässt.

Seit Anfang der 80er-Jahre rüsten Innenpolitiker in Deutschland und Europa auf. Sie kämpfen gegen ein Feindbild, das im stetigen Wandel begriffen ist: Erst RAF, organisierte Kriminalität und dann Schleuserbanden, im neuen Jahrtausend heißen die Schreckgespenster Kinderpornografie und Terrorismus in jeder Form. Nach den Anschlägen vom 11. September 2001 verabschiedete der Bundestag die sogenannten Otto-Pakete – über 50 Änderungen aktueller Gesetze, angefangen vom Bundesverfassungsschutzgesetz bis zum Energiesicherungsgesetz: BKA, BND und militärischer Abschirmdienst erhalten mehr Befugnisse, das Asylverfahrensgesetz erlaubt nun die Aufzeichnung einer Stimmprobe, das Ausländerzentralregistergesetz den Online-Zugriff auf das Register, erweiterte Suchmöglichkeiten inklusive.

Und während das Kabinett noch an der gesetzlichen Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung feilt, prescht Innenminister Wolfgang Schäuble mit der Forderung nach Online-Durchsuchungen vor. Er setzte Pässe mit Speicherchips für biometrische Daten durch und will den Sicherheitsbehörden den Online-Zugriff auf gespeicherte Digital-Passfotos aller Bürger erlauben. "Terroristen wollten die Gesellschaft ändern, die Innenminister haben das geschafft", kommentiert Pfitzmann das trocken.

Insbesondere ein Projekt seiner Gruppe, das sich über fünf Jahre hinweg über 960000 Euro Fördermittel aus dem Wirtschaftsministerium freuen durfte, sorgt für Zündstoff: AN.ON, das eine technische Infrastruktur schafft, mit der Internet-Surfer ihre Datenspuren im Web zuverlässig verwischen können. AN.ON verschleiert, was das Internet in seiner Transportschicht (TCP/IP) normalerweise gern preisgibt: Wer kommuniziert mit wem. Surfen die Anwender über AN.ON, kann ein Internet Service Provider weder erkennen, welche Seiten seine Kunden aufsuchen, noch ein Server-Betreiber abspeichern, von welchen IP-Adressen aus Inhalte abgerufen werden.

Dazu schützt ein Netzwerk aus zwischengeschalteten Servern, Mixe genannt, die

Kommunikationsbeziehungen zwischen Sender und Empfänger. Vereinfacht gleicht ein Mix einem Postamt, das Briefe sammelt, deren aktuelle Umschläge abstreift und alle Nachrichten zum gleichen Zeitpunkt in gleich aussehenden neuen Umschlägen weiterschickt. Die Unordnung in der Masse, das gleiche Aussehen und der Umschlag machen die einzelnen Nachrichten anonym. Dadurch wird es einem Überwacher unmöglich, einen Zusammenhang zwischen eintreffenden und das Amt verlassenden Nachrichten herzustellen.

Besuch vom BKA

Damit sie gegen falsche Freunde gewappnet sind, werden die Daten zudem durch mehrere Mixe nacheinander geleitet – solange auch nur ein wirklich vertrauenswürdiger darunter ist, bleibt das "Wer mit wem" geheim. Die AN.ON-Mixe werden von unabhängigen Organisationen wie der TU Dresden, der FU Berlin, dem Chaos Computer Club und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) betrieben. Um sie zu nutzen, muss der Anwender nur die in der Programmiersprache Java geschriebene Software JAP (Java Anon Proxy) auf seinem Rechner installieren. JAP verschlüsselt die Anfragen vom Webbrowser, sodass sie ohne Aufdeckungsgefahr von einem Mix zum anderen weitergereicht werden können, und nimmt die Antworten auf dem gleichen Wege entgegen. Das macht es selbst dem mächtigen Angreifer Staat nahezu unmöglich, den Weg der Daten zu verfolgen.

Doch damit geben sich die Behörden längst nicht mehr zufrieden. Bis Mitte des Jahres 2003 ließen sie Pfitzmann und Kollegen gewähren, dann aber erhielt er am 31. August während eines Urlaubs einen unschönen Anruf: Am Apparat war der Direktor seines Instituts an der TU – in seinem Wohnzimmer standen Beamte des BKA und bedrängten ihn zur Herausgabe von AN.ON-Daten. Um eine Durchsuchung des Institutes zu verhindern, gaben die Wissenschaftler die gewünschten Daten heraus; wenige Wochen später stellt das Landesgericht Frankfurt auf Antrag des ULD klar, dass die BKA-Beamten rechtswidrig gehandelt hätten. Bis heute melden sich Sicherheitsbehörden jeden Monat vier- bis fünfmal und bitten Pfitzmann um die Preisgabe bestimmter Verbindungen – ein Ansinnen, das er routinemäßig an die Juristen im ULD weiterleitet. "So ist das Leben", kommentiert der Professor gelassen.

Er setzt die BKA-Anfragen in Relation zu rund 100000 AN.ON-Anwendern und JAP-Downloads in Millionenhöhe: "So wie unsere Gesellschaft momentan aussieht, stellt ein Anonymisierungsdienst keine Bedrohung für sie dar. Es gibt noch genug andere Möglichkeiten, den Bösen auf die Schliche zu kommen."

Trotzdem fordern Politiker immer wieder die Abschaltung von AN.ON, zuletzt im Sommer 2006, nachdem Kofferbomben in Zügen nach Koblenz und Dortmund gefunden worden waren. Pfitzmann argumentiert dagegen: Die Balance der Interessen sei durch die technische Entwicklung – billiges Aufzeichnen und Auswerten – und neue Gesetze schon zu weit in Richtung Überwachungsstaat hin verschoben worden. "Was in Deutschland völlig fehlt, ist eine Diskussion über die Verbrechen ermöglichende Wirkung von Überwachung", kritisiert der Forscher. Gehört wird er nicht mehr: Das Bundeskabinett hat Mitte April den Gesetzesentwurf zur Neuregelung der Telekommunikationsüberwachung abgesegnet. Darin ist vorgesehen, dass künftig auch Anonymisierungsdienste wie AN.ON Verbindungsdaten auf Vorrat speichern sollen. Genau das hatten die Forscher bereits in der Entwurfsphase ausgeschlossen – nicht nur wegen der erhöhten Betriebskosten, sondern vor allem wegen der Missbrauchsgefahr im Falle von unerkannten Sicherheitslücken.

Pfitzmann schüttelt den Kopf, seine Haare stehen inzwischen kreuz und quer: "Die Technik ist von vornherein so gebaut, dass sie mit solch einer Situation fertig wird", sagt er und prophezeit: "Kriminelle werden nun peinlich genau darauf achten, dass einer der Knoten in einem Land steht, wo keine Vorratsdatenspeicherung existiert." Mit dem verdächtigen Datenverkehr würden sich dann auch gleich Sicherheitsdienstleister aus den anonymitätsunfreundlichen Ländern verabschieden – die Vorratsdatenspeicherung in der EU und in den USA würde damit völlig ausgehebelt.

Ein Ausweichkandidat für internationalen anonymen Datenverkehr spannt sein Netz bereits heute über 1300 Knoten zwischen rund 30 Ländern. Selbst JAP-Anwender können auf den Dienst zugreifen, dessen Abkürzung TOR für "The Second Generation of Onion Routing" steht. Zwiebel (onion) führt er im Namen, weil Datenpakete dabei mit mehreren Kryptografie-Schichten geschützt sind, die eine nach der anderen beim Passieren der eingeschalteten Zwischenstationen abgezogen werden. Das macht es nur bei vollem Zugriff auf sämtliche Stationen möglich, ein Datenpaket zum Absender zurückzuverfolgen. Onion Routing wurde wie AN.ON ursprünglich mit öffentlichen Geldern finanziert: Die Grundlagen stammen aus einem

Forschungsprojekt der US-Marine.

Der entscheidende Faktor für die kontinuierliche Existenz von Anonymisierungsnetzwerken wie TOR liegt jedoch nicht in der Kombination aus aktiver Entwicklergemeinde und vertrauenswürdiger Open-Source-Software: Entscheidend ist der freie Zugang zur Infrastruktur des Internets. "Darin lag meine Motivation. Im Internet hatte ich die Möglichkeit, die Dinge unmittelbar selbst zu bauen", erklärt Hannes Federrath, ehemaliger Projektleiter von AN.ON. Zuvor hatte er bei Pfitzmann über vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen promoviert. "Im Mobilfunk kann ich als Wissenschaftler ohne Hilfe des Netzbetreibers niemals meinen Entwurf in einen Prototypen umsetzen", erklärt der 37-jährige Informatiker, heute Professor an der Universität Regensburg. Auch Federrath sieht sich nicht als Rebell – mit seinem faltenlosen Gesicht und den sympathisch lächelnden braunen Augen erfüllt er eher das Bild eines dynamischen Dozenten.

Fahnden am Computer

Federrath ist in der DDR aufgewachsen und kennt staatlichen Kontrolldrang aus eigener Anschauung. Vor seinem Studium absolvierte er eine Lehre zum Elektronik-Facharbeiter und entdeckte im Ausbildungsbetrieb einen stark abgesicherten Raum – "es war klar, wofür die vollautomatischen Kassettendecks mit sehr langsam laufenden Motoren und hochwertigen Tonköpfen gedacht waren". Und auch in der heutigen Bundesrepublik hatte Federrath schon direkten Kontakt mit der neugierigen Staatsmacht, wie er berichtet: Schon zweimal hätten ihn Vertreter von deutschen Geheimdiensten für eine Zusammenarbeit gewinnen wollen – einmal in seinem Büro und einmal nach einem Vortrag.

Das Abhören von Funknetzen ist heute beinahe alltäglich. Mit den sogenannten IMSI-Catchern nutzen staatliche Angreifer Sicherheitslücken im GSM-Standard und ermitteln die netzinternen Rufnummern aller Nutzer in einer bestimmten Funkzelle. "Sie verdächtigen einen, überwachen aber alle", empört sich Federrath. Nach Angaben der Bundesnetzagentur haben deutsche Gerichte im vergangenen Jahr 35816 Anordnungen zur Überwachung von Handys erlassen. Federrath sitzt in seinem Büro, der ehemaligen Hausmeisterwohnung der Universität Regensburg, wo er mittlerweile den Lehrstuhl für Management der Informationssicherheit innehat. Direkt im Raum nebenan programmieren seine Studenten, der Zugang zu den Räumen ist mittels Fingerabdruck-Scanner und Kartenleser gesichert.

Auf der Eingangstür klebt der Aufkleber "Coding is not a crime" von der amerikanischen Bürgerrechtlerorganisation Electronic Frontier Foundation (EFF), auf dem Serverschrank dahinter der Sticker des Chaos Computer Clubs "Schnüffeln verboten". Federrath will nach eigener Aussage auf keinen Fall die Aufklärung schwerer Straftaten behindern. Seine Überzeugung lautet aber nach wie vor: "Wenn schon, dann müssen diese Maßnahmen so teuer sein, dass es damit völlig indiskutabel ist, eine Massenüberwachung zu praktizieren."

Der Trend aber geht in die andere Richtung: Aller Voraussicht nach wird auch den Mobilfunkanbietern die Vorratsdatenspeicherung über sechs Monate vorgeschrieben werden. Dabei muss der Benutzer nicht einmal telefonieren – sobald das Handy eingeschaltet ist, meldet es sich beim Netzbetreiber an, teilt ihm Identität des Nutzers, Handy-Seriennummer und Daten zum aktuellen Standort mit. Letzterer Datensatz ist besonders brisant, da damit nach dem "Wer spricht wann mit wem" auch das "Wo" bequem vom Computer der Polizei aus einsehbar wird. Das erlaubt nicht nur die Lokalisierung des Nutzers zu einem bestimmten Zeitpunkt, sondern auch das Erstellen kompletter Bewegungsprofile über die gesamte Speicherungsdauer.

Um die Erreichbarkeit sicherzustellen, dem Nutzer aber dennoch die Kontrolle über seine Daten wiederzugeben, schlug Federrath den Netzbetreibern in seiner Dresdner Zeit "Temporäre Pseudonyme" vor: Anstatt jeden Ortswechsel in der Datenbank des Netzbetreibers mit der eindeutigen Rufnummer zu verknüpfen, sollte jeder Ort unter einer neuen Zufallszahl gespeichert werden. Das würde Bewegungsprofile verhindern, da die Information "Pseudonym X gehört zu Person A" den Betreibern nicht bekannt wäre und zusätzlich nach einer bestimmten Zeit auch noch verfallen würde. Bei einem eingehenden Anruf sollte der Netzbetreiber das aktuelle Pseudonym über zwischengeschaltete Mixe ermitteln.

Keine Überraschung: Die Betreiber haben Federraths Konzept nicht verwirklicht. Misstrauischen Mobilfunkkunden empfiehlt er daher eine Lowtech-Lösung: "Lassen Sie das Handy aus, solange es geht. Wenn Sie telefonieren, dann mit UMTS. Da ist die Verschlüsselung besser." Plötzlich schimmern die

Augen des Jung-Professors kurz auf: "Für UMTS ist auch der IMSI-Catcher schwerer zu realisieren", fügt er spitzbübisch hinzu.

Überwachungsparadies auf Erden

Das Wissen aus seinen früheren Arbeiten fließt in die aktuelle Forschung von Federraths Gruppe an sogenannten Vehicular Ad Hoc Networks (VANETS) ein – Funknetzwerke, die sich dynamisch zwischen Fahrzeugen bilden. Sie sollen in erster Linie zur Verkehrssicherheit beitragen, indem jedes Auto Daten über Geschwindigkeit, Position oder Straßenzustand mit den anderen austauscht und so in jedem Fahrzeug ein Überblick über die momentane Verkehrssituation entsteht.

Dass dabei auch die Datenschutz-Interessen aller Beteiligten gewahrt bleiben und gleichzeitig eine Strafverfolgung ohne automatisierte Überwachung möglich ist, will Federrath mit einer ausgefeilten Sicherheitsarchitektur sicherstellen. Noch vor wenigen Jahren hätte er für diese Berücksichtigung von Datenschutz-Interessen bei einer neuen Technologie wohl mit Wohlwollen aus der Politik rechnen können. Doch damit ist es vorbei: Federrath macht nach eigener Aussage zunehmend die Beobachtung, dass sich weniger Forschungsgelder für Privacy-Projekte akquirieren lassen.

Dies bestätigt auch Kai Rannenberg, Inhaber der T-Mobile-Stiftungsprofessur für M-Commerce und mehrseitige Sicherheit an der Johann Wolfgang Goethe Universität in Frankfurt am Main. Als für sich prägend bezeichnet der 43-Jährige die Debatte um die nicht unterdrückbare Rufnummernanzeige bei ISDN: "Wenn Datenschutz und Datensicherheit erst kommen, nachdem die Standards bereits geschrieben sind und die Infrastruktur bereits gelegt ist, dann ist die Einflussnahme sehr schwierig."

Rannenberg rühmt sich, Schöpfer des Fachbegriffes "Mehrseitige Sicherheit" zu sein, der für eine bewusste Balance zwischen den Interessen der einzelnen Parteien in einem technischen System steht. Aktuell versucht er, sein Konzept bei den sogenannten ortsbasierten Diensten (location based services, LBS) zu verwirklichen. Handy-Nutzer geben dafür ihre Ortsinformationen frei und spezifizieren Interessen, um sich im Gegenzug Informationen über maßgeschneiderte Angebote oder anwesende Freunde in ihrer momentanen Umgebung aufs Mobiltelefon schicken zu lassen.

Aus der Sichtweise der Behörden aber verknüpfen Location Based Services die Ortsinformationen des Verdächtigen mit weiteren sensiblen Informationen, nämlich seinen Interessen: "Sie wissen, wer Ihre Freunde sind, wo Sie gerade sind – und das in Echtzeit. Das ermöglicht nicht nur eine Überwachung vom Schreibtisch aus, sondern auch eine viel aussagekräftigere Analyse Ihres sozialen Netzwerkes", erläutert Rannenberg. Die LBS schaffen somit das Überwachungsparadies auf Erden. Entwickeln sie sich zum umsatzstarken Geschäftsfeld, werden die Mobilfunkbetreiber in noch bessere Lokalisierungsverfahren investieren, die Anwender sogar aus eigener Tasche Handys mit genauen GPS-Sendern bezahlen.

"Zugriff auf alles"

Als Gegenmittel propagiert Rannenberg Datenaufteilung in Kombination mit Identitätsmanagement: Die Aufenthaltsdaten bleiben beim Mobilfunkbetreiber, das Herausfinden der besten Services für die aktuelle Position übernimmt der jeweilige Dienstanbieter. Zwischen den beiden vermittelt ein sogenannter Intermediär die notwendigen Anfragen, ohne zu verraten, vom wem sie kommen. Besser als nichts – doch sowohl Rannenberg als auch Federrath wollen auf Nummer sicher gehen und favorisieren daher den schärferen Schutz durch Mixe.

Für Rannenberg hat die frühzeitige Beschäftigung mit Fragen des Datenschutzes einen handfesten Hintergrund: "Wenn die Industrie anfängt, eine Infrastruktur aufzuziehen, um damit einen schöneren Service anzubieten, klopft doch ganz schnell der Staat an die Tür und will die Daten." Gegen solche Bestrebungen engagiert er sich als Vorsitzender des Sicherheits-Komitees im IFIP, dem weltweiten Verband der Informatik-Gesellschaften. Er gehört auch zu den Wissenschaftlern, die sich mit der sogenannten "Budapester Erklärung" öffentlich gegen unsichere RFID-Technologie in deutschen Reisepässen wandten (siehe TR 02/2007). Doch trotz aller Bemühungen bleibt seine Prognose düster: "Heute ist es der Bundestrojaner für den PC, morgen ist es der Bundestrojaner für das Handy. Das habe ich bei Technologietrends oft erlebt."

"Bundestrojaner" ist der inoffizielle Begriff für technische Tricks, mit denen Ermittler über das Internet auf

die Computer von Verdächtigen zugreifen und sie durchsuchen. Darüber, wie das vor sich gehen soll, existieren bislang kaum Informationen, bei Nachfragen verweist das BKA nur auf die "aktuelle politische Diskussion" und weiter ans Justizministerium. Dabei findet sich der Begriff "Online-Durchsuchungen" bereits im "Programm zur Stärkung der Inneren Sicherheit", das Innenminister Wolfgang Schäuble im Oktober 2006 vorgestellt hat.

Nur drei Monate später entschied allerdings der Bundesgerichtshof unter dem Aktenzeichen STB 18/06, dass die heimliche Durchsuchung nicht durch die Strafprozessordnung gedeckt ist. Trotzdem schlichen sich Bundesnachrichtendienst und Verfassungsschutz schon seit 2005 in an das Internet angeschlossene Heimrechner ein, wie die Antwort auf eine Anfrage der Abgeordneten Gisela Piltz im Bundestag ergab.

Eine gesetzliche Regelung für das staatliche Hacking wird wohl noch eine Weile auf sich warten lassen. Es sei jedoch auf jeden Fall sichergestellt, dass private Dateien nicht zur Kenntnis genommen würden und der Kernbereich der privaten Lebensgestaltung geschützt bleibe, versicherte der BKA-Präsident Jörg Ziercke bereits in einem Interview.

Für solche Beschwichtigungsversuche allerdings hat Alexis "Lexi" Pimenidis nur ein Kopfschütteln übrig: "Für 90 Prozent aller Rechner gilt: Wenn Sie drauf sind, haben Sie auf alles Zugriff." Der 31 Jahre alte Doktorand an der RWTH Aachen gehört zur Szene um Pfitzmann, unterscheidet sich aber nicht nur im Aussehen deutlich von ihm: Kurze schwarze Haare, Bart, das rechte Ohrläppchen zieren ein Ohrclip und ein Pentagramm; Schnürstiefel, Cargohose und Fleecejacke sind sämtlich in Schwarz gehalten. Pimenidis beschreibt seine Forschung als eher "offensiv ausgelegt" – er bietet Hacker-Seminare an, nimmt mit Studenten an Hacker-Wettbewerben teil und nennt Malware-Engineering und sonstige Wege des Rechner-Knackens seine Forschungsgebiete.

Ein klassischer Hacker also? Pimenidis wiegt mit dem Kopf: "Je nachdem welche Definition Sie nehmen: Ja, das war ich." Aufgrund seiner Vergangenheit und auch Gegenwart weiß er in Bezug auf den gefürchteten Bundestrojaner nur zu genau: "Je nachdem welchen Rechner Sie wählen, sind die Löcher so groß wie Scheunentore." Zum Schutz empfiehlt Pimenidis deshalb nicht Software, sondern Sachverstand – "das Einzige, was Sie machen können, ist im Endeffekt eine Schulung besuchen, die Ihnen genau sagt, was Sie machen können und nicht machen dürfen." Als kleine Hilfe entwickelt der Forscher mit seinen Studenten Werkzeuge, die Anwendern zeigen, was sicherheitstechnisch im Inneren ihres Computers vorgeht.

Außerdem arbeitet er zusammen mit Pfitzmann, Federrath und Rannenberg im EU-Projekt PRIME (Privacy and Identity Management for Europe), das bis Februar 2008 mit 16 Millionen Euro gefördert wird und "Das Schloß" von Franz Kafka in seiner Literaturliste aufführt. PRIME soll dem Bürger das Vertrauen in seine digitale Privatsphäre zurückgeben und setzt dabei auf die Minimierung personenbezogener Daten und "privacy by design" – Datenschutz soll also von vornherein mit eingebaut werden. So sollen die Bürger technisch in die Lage versetzt werden, eigenständig mit Dienstanbietern auszuhandeln, bis zu welchem Grad sie Daten offenlegen – im Rahmen der europäischen Gesetze und dennoch unter dem Schutz von Pseudonymität und Anonymität.

Das klingt erst einmal gut – ganz ähnlich wie die schönen Worte, mit denen einst die Förderung für das AN.ON-Projekt begründet wurde, dessen Funktion jetzt ausgehöhlt zu werden droht. Doch wie der vom Projekt-Paper explizit erwähnte gesetzliche Rahmen in Zukunft aussehen wird, das steht noch in den zwölf Sternen der Europa-Flagge. Der Europäischen Union haben wir immerhin die Richtlinie zur Vorratsdatenspeicherung zu verdanken, die jetzt in den Mitgliedsländern umgesetzt werden muss. Während also EU-Forschungskommissar Janez Potocnik durchaus noch Millionen für Datenschutz-Projekte lockermacht, besteht Anlass zur Befürchtung, dass die Legislative bei Fragen der Sicherheit einen zu einseitigen Blick bekommen hat.

"Bezahlen mit der Freiheit anderer"

Burkhard Hirsch, Vizepräsident des Deutschen Bundestages a.D., plant eine Verfassungsbeschwerde gegen ein Gesetz, das die auf EU-Ebene beschlossene Pflicht zur Vorratsspeicherung von Verbindungsdaten in deutsches Recht umsetzt. Mit solchen Klagen hat Hirsch schon Erfahrung: Anfang 2005 setzte er sich vor dem Bundesverfassungsgericht gegen das Luftsicherheitsgesetz durch, das den Abschuss von Passagiermaschinen erlaubt hatte, die zum Zweck von Terror-anschlägen entführt worden sind.

Ebenso gab das Bundesverfassungsgericht im März 2004 der Beschwerde von Hirsch und seinen Parteifreunden Sabine Leutheusser-Schnarrenberger und Gerhart Baum gegen den sogenannten "großen Lauschangriff" recht und erklärte weite Teile des Gesetzes über das Abhören von Gesprächen in der Wohnung für verfassungswidrig. Im amtlichen Auftrag untersuchte Hirsch im Jahr 1998 die Vorgänge um die Aktenvernichtung im Kanzleramt unter Helmut Kohl. Ein Interview.

TR: Wenn nächste Woche ein Anschlag passiert und die Täter entkommen, weil sie weder von Videokameras aufgezeichnet noch ihre konspirativen E-Mails gespeichert wurden, tragen Sie dann eine Mitschuld daran?

Burkhard Hirsch: Ich sehe natürlich voraus, dass man in einem solchen Fall Schuldige suchen und versuchen wird, daraus Vorwürfe herzuleiten. Aber genauso könnten Sie dann denjenigen verantwortlich machen, der gegen die Todesstrafe ist oder denjenigen, der an der Unschuldsvermutung festhalten will. Sie können im Grunde genommen dann jeden verantwortlich machen, der sagt, in einem Rechtsstaat darf der Staat nicht alles machen, was er theoretisch machen könnte.

TR: Aber was ist an der Vorbeugung für den Fall des Anschlages so verkehrt?

Hirsch: Sie müssen sich bei staatlichen Maßnahmen immer fragen, wo das Vorbeugen ein Ende haben soll. Sie können sagen, ich mache von allen Bürgern eine Fingerabdruck-Sammlung, Sie können sagen, ich pflanze jedem Kind von Geburt an einen Chip ein, damit ich seine Bewegungen verfolgen kann, Sie können sagen, ich nehme von jedem Bürger eine DNA-Analyse – alles vorbeugend. Man muss sehen, dass die Maßnahmen, über die gerade in unserer Republik gestritten wird, in der Tat dabei sind, unseren Staat zu verändern: Nämlich ihn zu einem Überwachungsstaat zu machen.

TR: Was macht Bürgerrechte und Privatsphäre so wertvoll, dass Sie die Zugriffsrechte des Staates begrenzen wollen?

Hirsch: Der Staat muss akzeptieren, dass in einer freien Gesellschaft jeder einen Kern der privaten Lebensführung besitzt, in dem der Staat nichts zu suchen hat. Wenn ich diesen Grundsatz aufgebe, dann bleibt nichts mehr vor staatlichen Eingriffen geschützt und gesichert. Die Bürger werden unfrei. Sie werden nicht mehr sagen, was sie denken, sie werden nicht offen reden wollen. Sie werden sich anpassen, sie werden sich eben verhalten wie Untertanen, sie werden anfangen, dem Staat zu misstrauen. Wir haben in der DDR ein Maximum an Überwachung gehabt, aber auch mit der Folge, dass die Menschen nicht mehr frei geredet haben. Ich habe dasselbe im Dritten Reich erlebt.

TR: Ein altes Argument in diesem Zusammenhang lautet: Wer nichts zu verbergen hat, hat auch nichts zu befürchten...

Hirsch: Die Leute, die das sagen, wollen ein Mehr an Sicherheit bezahlen mit der Freiheit anderer. Sie sind der felsenfesten Überzeugung, da sie alles ehrli-che Leute sind, dass alle Maßnahmen, über die wir reden, sie nicht betref- fen werden. Aber die Tatsache, dass ich alles offenbaren kann, kann doch nicht dazu verpflichten, tatsächlich alles zu offenbaren. Jeden, der sagt, er habe mit Datenschutz nichts zu tun, frage ich daher: Haben Sie zu Hause eine Gardine? Eine Gardine ist klassischer Datenschutz.

TR: Sie haben in einem Zeitungsbeitrag zum Widerstand gegen zunehmende Überwachung aufgefordert. Wie soll dieser Widerstand aussehen?

Hirsch: Mehr Menschen werden sich für die technischen Möglichkeiten interessieren, sich dieser Überwachung zu entziehen – Verschlüsselung, Festplatten wechseln, Firewalls. Mir wäre aber wichtiger, dass die Bürger, die dafür einen Sinn haben, ihrem Abgeordneten sagen: Wir wollen das nicht mehr. Ich will, dass das politische Klima sich verändert. Ich wünschte, dass sie ihren Abgeordneten schreiben, dass sie Leserbriefe schreiben. Ich will auch, dass Hardliner begreifen, dass die Welle der Zustimmung nicht da ist.

TR: Wie schützt sich der Bürger Burkhard Hirsch?

Hirsch: Ich habe ein Prepaid-Handy, dessen Nummer keiner kennt, und ich stelle das Ding nur an, wenn ich wirklich telefoniere. Mein PC ist nicht an das Internet angeschlossen. Das habe ich von Herrn Kohl gelernt: In seinem Büro hatte er eine zusätzliche Datenverarbeitung, auf der er seine eigenen Akten führte. Ich habe also bei Herrn Kohl gelernt, warum es sinnvoll ist, ein Stand-alone-System zu benutzen.

(**bsc[1]**/Technology Review)

URL dieses Artikels:
http://www.heise.de/tr/artikel/90508

Links in diesem Artikel:
[1] mailto:bsc@tr.heise.de