



1998/28 Inland

<https://jungle.world/artikel/1998/28/wwwueberwachungde>

www.ueberwachung.de

Von **André Reß**

Die Bundesregierung hat Schwierigkeiten, die beschlossene umfassende Beobachtung des Internet umzusetzen

Seit zwei Jahren gibt es ein Gesetz, das dem Staat die Überwachung im Internet erlaubt. In der Praxis allerdings kommen die Behörden nicht voran. Sie scheitern weniger an datenschutzrechtlichen Bedenken als an technischen Schwierigkeiten und den hohen Kosten einer Überwachung.

Das Ende Juli 1996 in Kraft getretene Telekommunikationsgesetz (TKG) verpflichtet geschäftsmäßige Anbieter von Internetdiensten (Provider), die Überwachungstechnik "auf eigene Kosten zu gestalten und vorzuhalten". Näheres sollte in einer "Telekommunikations-Überwachungsverordnung" (TKÜV) geregelt werden, die das Bundeskabinett in diesen Tagen verabschieden wollte. Daraus wurde nichts.

Nachdem die Computerzeitschrift c't vorgerechnet hatte, daß die Umsetzung des Verordnungsentwurfs die Provider nach vorsichtigen Schätzungen zwischen 15 000 und 50 000 Mark allein für technische Ausstattung kosten würde, auch die Wirtschaftswoche ihre finanzkräftige Klientel alarmierte und selbst der CDU-Wirtschaftsrat von "überzogenen staatlichen Überwachungsmaßnahmen" sprach, bekam das Wirtschaftsministerium kalte Füße. Offenbar, um die so sehr umworbenen "Zukunftsindustrien" nicht zu vergraulen, soll jetzt auf einer neu angesetzten Anhörung am 15. Juli die Meinung von Providern, Banken, Versicherungen und Datenschützern zu der Verordnung eingeholt werden.

Viel Aufsehen um längst beschlossene Dinge? Nicht ganz. Zwar sind im TKG weitgehende Überwachungsbefugnisse festgeschrieben, doch die "technische und organisatorische Umsetzung" bleibt einer Verordnung der Bundesregierung überlassen. Die bisherige Fernmeldeüberwachungsverordnung (FÜV) ist auf konventionellen Telefonverkehr zugeschnitten, so daß Anbieter von Online-Diensten bisher die auch für sie geltenden Auflagen ignorieren konnten. Wenn die Pläne aus dem Wirtschaftsministerium umgesetzt werden, gäbe es keine Ausflüchte mehr. Den Providern wird in dem Entwurf der TKÜV mit Strafen von bis zu einer Million Mark gedroht, wenn sie sich ihrer Pflicht zum Installieren einer Abhörleitung für "berechtigte Stellen", also Geheimdienste, Staatsanwaltschaften oder das Zollkriminalamt, entziehen.

Der zu überwachende Anschluß ist dabei als "diejenige technische Einrichtung" definiert, "die Ursprung oder Ziel der Telekommunikation ist und durch eine Rufnummer oder andere Kennung eindeutig gekennzeichnet ist". Eine Formulierung, die die Überwachung auf jeglichen Internetgebrauch ausweitete, wie der Internetexperte der SPD, Jörg Tauss, kritisiert. Nimmt man die Formulierung ernst, so müßten die Provider beispielsweise die Daten von allen eventuell Hunderten Beteiligten in einem Chatroom weiterleiten, in den sich der überwachte Internet-Surfer eingewählt hat.

Die Grünen kritisieren nicht nur die technische Seite der weitreichenden Überwachungspläne, sondern beziehen die in der Strafprozeßordnung festgeschriebenen Gründe für eine Überwachungserlaubnis mit ein. "Der Katalog von Legitimationen, um eine Überwachung durchzuführen, ist seit dessen Einführung 1968 circa alle zwei Jahre erweitert worden", so Ingo Ruhmann, Fachautor und wissenschaftlicher Mitarbeiter des Forschungspolitischen Sprechers der Grünen, Manuel Kiper. Er habe nichts dagegen, daß bei einer schweren Straftat Individualkommunikation abgehört werde, doch gehöre "der Grundrechtsbruch mittlerweile zum polizeilichen Normalmittel". Es sei nicht hinnehmbar, daß zu den "Straftaten von erheblicher Bedeutung", die nach der Strafprozeßordnung eine Überwachung rechtfertigen, auch die "qualifizierte Sachbeschädigung" - z. B. das Sprühen eines schwarzen Sterns auf eine Hauswand - als Überwachungsgrund ausreiche.

Mit dieser Sammlung von Straftatbeständen, so Ruhmann, wurde zunächst das Fernmeldegeheimnis eingeschränkt, was wiederum Auswirkungen nach den neuen Gesetzen auch auf Telekommunikation allgemein und jetzt auch das Internet hatte. Zu befürchten sei, daß die Fallgebundenheit einer Überwachung immer mehr in den Hintergrund trete. Während beispielsweise in den USA Telefonate eines Überwachten, die mit dem Arzt oder anderen Unbeteiligten geführt werden, nicht protokolliert würden, sei die geplante Verordnung ein gutes Beispiel für die deutsche Devise: "Wir überwachen erst mal alles, dann entgeht uns nichts."

Aus dieser Mentalität ergibt sich nach der geplanten Verordnung das Kuriosum der doppelten Überwachung: Bis auf wenige Ausnahmen verwenden Nutzer des Internet eine Telefonleitung, um sich einzuwählen. Dieser einfache Fernmeldeverkehr kann schon seit eh und je mit richterlicher Genehmigung abgehört werden, unabhängig davon, ob die Leitung nun Sprache oder Datenpakete transportiert. Eine gesonderte Abhörschnittstelle beim Provider führt also dazu, daß der belauschte Datenverkehr ein weiteres Mal auf die Festplatten der staatlichen Mitleser gelangt.

Nach Meinung der Grünen entwickelt sich die Überwachung "mit der Dynamik eines Rüstungswettlaufes": Was zunächst als einfaches Abhören durch den Kleinen Lauschangriff begonnen wurde, setzte sich mit der Einschränkung der Unverletzlichkeit der Wohnung im Großen Lauschangriff fort und macht nun auch vor der Telekommunikation nicht Halt. Der logisch nächste Schritt in dieser Kette wäre das Verbot von Verschlüsselungsmethoden, die für staatliche Stellen nicht zu knacken sind. Schließlich handelt es sich dabei um eine effiziente Möglichkeit, die Lauschattacken ins Leere laufen zu lassen. Tatsächlich hatte das Innenministerium bereits letztes Jahr ein entsprechendes Kryptographiegesetz vorgeschlagen, war aber damals vor allem am Widerstand der Wirtschaftslobby gescheitert.

Entsprechend sieht Michael Müller, der zuständige Beamte für TK-Überwachung im niedersächsischen Landeskriminalamt, nur einen kleinen Fortschritt in der jetzt geplanten

Verordnung: "Früher standen wir komplett im Dunkeln, heute sehen wir immerhin schon mal die Rücklichter." Viele Rücklichter können es nicht sein, denn, so Müller: "Die Erfahrung zeigt, daß Kriminelle die Möglichkeiten von Computertechnik in der Regel nicht nutzen." Und selbst wenn, dann wird zunächst der Aufwand einer Entschlüsselung gegen andere Mittel abgewogen. Eine Hausdurchsuchung oder die Beschattung eines Verdächtigen bringe oft mehr Ergebnisse. Die neue Verordnung sei deshalb weniger wegen der geschaffenen Abhörbefugnisse interessant, als vielmehr wegen der Möglichkeit, einem Provider die Lizenz zu entziehen, wenn dieser sich weigert, mit den Behörden zusammenzuarbeiten.

Auch das Wirtschaftsministerium versucht, die Bedeutung der TKÜV herunterzuspielen. Die relevanten Gesetzesänderungen seien lange vollzogen; so der Referatsleiter Engelhard Wagner. Lediglich die Verordnung, die das Gesetz in der Praxis handhabbar mache, habe bisher gefehlt. Außerdem habe es "nie die Absicht, den Entwurf der Verordnung ohne Debatte ins Kabinett zu bringen" gegeben. Und falls diese neue Verordnung nicht schnell genug kommt, will man sich aber offenbar mit einem Trick behelfen: Die Regulierungsbehörde hat, aufbauend auf die alte Fernmeldeüberwachungsverordnung (FÜV), eine neue "Technische Richtlinie FÜV" angekündigt - ergänzt um den Teil Internet.