Wilderei, Stalking, falsche Angaben bei Behörden und Verkehrsunfälle mit tödlichem Ausgang reichen für Zugriff auf Telefon- und Internetdaten - Überwachungsvorhaben der österreichischen Bundesregierung geht weit über EG-Richtlinie hinaus - Österreich wird zum Musterschüler der Grundrechtsverletzungen - Milliarden Datensätze müssen permanent vorrätig gehalten werden - BotNets werden in Zukunft Kommunikation krimineller Vereinigungen bestimmten - Journalisten werden in Zukunft auf Beamteninformationen verzichten müssen - Musikindustrie fordert noch leichteren Zugriff auf Daten - ARGE DATEN gibt negative Stellungnahme ab

Vorratsdatenspeicherung bietet Basis für jede Menge von Zugriffsmöglichkeiten

Der nunmehrige Entwurf erlaubt einen derartig einfachen Zugriff auf die aufgezeichneten Daten, dass kaum ein Vorwurf oder Verdacht, der gegen eine Person erhoben wird, nicht auch den Zugriff auf die Telekom- und später Internet-Daten rechtfertigen würde.

So genügt es, den glaubwürdigen Verdacht zu äußern, jemand hätte vor einer Behörde falsche Angaben gemacht, er würde Betriebsgeheimnisse ausspähen, er hätte vertrauliche Unterlagen an einen Journalisten weitergegeben oder er würde jemanden "beharrlich verfolgen".

Schon müßten die Telefon- und Internetkontakte offen gelegt werden. Der Schaden bliebe bestehen, auch dann wenn sich kurz darauf herausstellt, man habe sich geirrt, der Verdacht sei doch nicht zu erhärten oder er betreffe eine ganz andere Person.

Mit der weitreichenden Verwendungsermächtigung wäre eine völlig neue Dimension in Sachen gegenseitige Vernaderung und Beschuldigung eröffnet.

Besonders stark betroffen sind auch Journalisten, Rechtsanwälte und andere Vertrauensberufe. Ihre Kommunikationsnetzwerke können durch die neue Regelung systematisch offengelegt werden, bisherige Schutzmechanismen greifen nicht mehr.

Vorhaben findet keine Deckung in EG-Richtlinie

Zentrale Voraussetzung für die verabschiedete EG-Richtlinie war Bekämpfung von Terrorismus und organisiserter Kriminalität. Diese Voraussetzung findet sich mehrfach in den Erwägungsgründen der Richtlinie, die zentraler Bestandteil der Richtlinie sind (Art. 8 EG). Mit der Hereinnahme von Allerweltsdelikten wird Österreich wieder einmal zum Musterschüler für Grundrechtsverletzungen.

Hans G. Zeger, Obmann der ARGE DATEN und Mitglied im Datenschutzrat: "Es gibt keinerlei rechtssystematische Begründung mit Bezug auf §17 SPG die gespeicherten Daten für eine Vielzahl von Delikten zugänglich zu machen, die überhaupt keinen Bezug zu Terrorismus haben. Selbst der bezug auf §17 StGB, der zwischen Vergehen und Verbrechen unterscheidet wäre sinnvoller, obwohl auch diese Bestimmung noch weit über die Intentionen der EG-Richtlinie hinausgeht."

Sinnvoll wäre für dieses Spezialgesetz wohl nur eine vollständige Aufzählung jener Delikte, die tatsächlich einen nachvollziehbaren Konnex zu Terrorismus haben. Dies wäre die Gruppe der Tatbestände, wie sie unter §278ff StGB (Terrorismus, organisierte Kriminalität) beschrieben sind (ftp://ftp.freenet.at/int/stgb-organisationsdelikte.pdf).

Hans G. Zeger: "Offenbar ist den österreichischen Politikern bewusst, dass die Vorratsdatenspeicherung im Zusammenhang mit organisierter Kriminalität kaum Ergebnisse bringen wird. Allzuleicht ist es für diejenigen, 'die etwas zu verbergen haben', die Bestimmungen zu umgehen. Vorsorglich wird daher der Zugriff auf die Daten auch für zehntausende Allerweltsdelikte sichergestellt, damit man nach einigen Jahren zumindest einige dutzend 'Erfolgsmeldungen' verbreiten kann. Eine Verbesserung der Gesamtsicherheitslage oder einen Beitrag zur Terrorismusbekämpfung wird es nicht geben. Eine Rechtfertigung für die Bürgerüberwachung wird man aber sehr wohl herauslesen können."

Gerade im Zusammenhang mit einem Modedelikt, wie Stalking, ließen sich dann trefflich "Erfolgsmeldungen" produzieren. Fehlt doch vielen Stalkern mit ihrer oft krankhaften Neigung anderen Personen nachzustellen, jedes Unrechtsbewusstsein. Sie werden daher auch keine Verschleierungsmaßnahmen für ihre Taten treffen und könnten dann durch die Vorratsdatenspeicherung noch leichter ausgeforscht werden als es bisher schon der Fall ist.

Umgekehrt ist das Stalking-Delikt geradezu ein Musterbeispiel für den Missbrauch der neuen Datenaufzeichnungen. Charakteristisches Merkmal von Stalking ist die "Beharrlichkeit" in der Nachstellung. Ein Stalkingopfer hat daher schon jetzt durch zeitgerechte Anzeige und gezielte Überwachung seines Telefonanschlusses jede denkbare Möglichkeit der Verfolgung und Aufklärung des Delikts. Das nachträgliche Herumschnüffeln in Daten unbescholtener Bürger ist dazu überhaupt nicht erforderlich.

Milliarden Datensätze müssen permanent vorrätig gehalten werden

Die Daten von - konservativ geschätzten - mindestens 14 Mrd. Telefonanrufen und - sobald auch Internet erfasst ist - rund 28 Mrd. eMailkontakten müssten für Schnüffeldienste aller Art permanent bereit gehalten werden (die Zahlen sind eine Schätzung, basierend auf einer angenommenen Mindestnutzung und den in Österreich bekannten Anschlusszahlen).

Bisher unbeachtet blieb, dass nicht einmal die Löschungsverpflichtung nach Ablauf der Sechsmonatsfrist für die Datenaufbewahrung bedingungslos eingehalten wird. Dies würde eine tägliche Löschung der über diesen Zeitraum liegenden Daten erfordern. Schon jetzt sind die Vorbehalte der Telekomanbieter absehbar.

Beamte werden keine Informationen mehr weitergeben

Auf Informationen aus Beamtenkreisen werden Journalisten noch stärker verzichten müssen als bisher. Steht doch bei jeder Informationsweitergabe der Verdacht des Amtsmissbrauchs im Raum. Bei einem Strafrahmen von bis zu drei Jahren hoch genug um auf Vorratsdaten zugreifen zu dürfen. Selbst wenn sich anschließend der Verdacht nicht bestätigt, Ruf und wohl auch Karriere des Beamten sind durch die durchgeführte Untersuchung nachhaltig beschädigt. Kein vernünftiger Beamter wird in Zukunft noch einen eMail- oder Telefonkontakt mit

einem Journalisten pflegen, auch wenn er nichts zu verbergen hat, das Risiko in eine Untersuchung hineingezogen zu werden ist zu groß.

Musikindustrie fordert noch leichtern Zugriff auf Daten

In nahezu wortidenten Stellungnahmen haben die Vertreter der Musikindustrie in einer konzertierten Aktion, namentlich ifpi, VTMÖ, VGR, austro mechana, LSG und VBT eine Senkung der Zugriffsschwelle auf Vergehen mit nur 6 Monaten Strafdrohung gefordert. Dies ist der Strafrahmen, mit dem Jugendliche theoretisch rechnen müssen, wenn sie über eine Tauschbörse auch nur einen einzigen Song verbreiten.

Damit dreht Musikindustrie, die schon in der Vergangenheit mit äußerst dubiosen Methoden Bürger als Urheberrechtsverletzer jagte und durch überzogene Abmahnschreiben einschüchterte, weiter an der Kriminalisierungsschraube.

Schon der jetztige Entwurf erlaubt fast ungehemmten Zugriff auf die Vorratsdaten. Reicht es doch den gewerbsmäßigen illegalen Download bloß zu behaupten (§91 Abs. 2a, UrhG), schon würde sie Zugang zu den Internetdaten haben.

Freilich, noch ist es nicht soweit, die Internetbestimmungen zur Vorratsdatenspeicherung sollen erst in einigen Monaten beschlossen werden. Doch werden schon allein aus Gründen der Gleichbehandlung die niedrigen Strafrahmen für Datenzugriffe ident gehalten werden.

Bestimmungen leicht zu umgehen

Für denjenigen, der "etwas zu verbergen hat" und tatsächlich im Bereich der organisisierten Kriminalität tätig ist, ist es weiterhin leicht unidentifiziert zu kommunizieren.

Ausweichmöglichkeiten gibt es genug: Diensteanbieter außerhalb der EU für Internettelefonie und e-mail; innerhalb der EU werden diese Fremdhandys dann über Roaming-Verträge unidentifizierbar genutzt; Anonymisierungsdienste; Wertkartenhandys; Telefonzellen; Internetcafes; etc... Das sind die Möglichkeiten, die schon dem Normalbürger spontan einfallen. Daher: Wenn ein Krimineller auch nur einigermaßen professionell agiert, wird er sich eben auf die neuen Rahmenbedingungen problemlos umstellen können.

Wie die Herkunft von eMails "professionell" zu verschleiern ist, zeigen uns die täglichen Phishingattacken. Mails werden nicht über offzielle und somit durch die Vorratsdatenspeicherung erfasste Mailserver verschickt, sondern heimlich über geknackte Privat-PCs, auf denen mittels Würmer entsprechende Serverprogramme installiert wurden. BotNets, also illegale Internet-Netzwerke können nicht nur für Hackerangriffe genutzt werden, sondern auch für Internettelefonie oder als eMail- und Web-Netzwerke. Mehrere zehntausend derartiger Netze existieren bereits, mit jeweils mehreren tausend bis eine Million Computern, allesamt geknackte PrivatPCs.

Negative Stellungnahme abgegeben

Hans G. Zeger: "Die ARGE DATEN hat nach gründlicher Analyse des Entwurfes eine umfassende und sehr detaillierte Stellungnahme abgegeben."

Dass diese Stellungnahme negativ ist, überrascht nicht wirklich, was die ARGE DATEN jedoch überrascht hat, war die unverfrorenheit in der Beamte des BMJ und des BMVIT, offensichtlich mit Rückendeckung aus der Regierung, aus einer Regelung zur Terrorismusbekämpfung ein Allerweltsinstrument zur Aushebelung von Grundrechten gemacht haben.

Hans G. Zeger: "Persönlich musste ich auch im Datenschutzrat eine gesonderte Stellungnahme abgeben. Auch in diesem Gremium standen nur kosmetische Fragen zur Diskussion und die längst vorbereitete Mehrheits-Stellungnahme musste als ungenügend angesehen werden."

Die Stellungnahme im Volltext -->

ftp://ftp.freenet.at/privacy/gesetze/stellungnahme-vorratsdatenspeicherung.pdf

mehr -->

http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=28764tot

http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=79697twr

ftp://ftp.freenet.at/int/stgb-organisationsdelikte.pdf

ftp://ftp.freenet.at/int/rl_de.pdf

ftp://ftp.freenet.at/int/urhg-91.pdf

ftp://ftp.freenet.at/int/dsr-vorratsdatenspeicherung.pdf

andere -->

http://www.parlament.gv.at/portal/page?_pageid=908,4662640&_dad=portal&_schema=PORTAL

artikel - redaktionell/public (2007/05/23-9999/99/99) powered by e-CMS

Informationsdienst: https://secure.argedaten.at/AD_info_anfordern.html

Antrag Mitgliedschaft: https://secure.argedaten.at/AD_mitgliedsantrag.html

Info abbestellen: https://secure.argedaten.at/AD_loeschung_mail.html

Mailadresse ändern: https://secure.argedaten.at/AD_wartung_mail.html

Freies Dokumentenservice: ftp://ftp.freenet.at

ARGE DATEN - Österreichische Gesellschaft für Datenschutz

A-1160 Wien, Redtenbacherg. 20

fon (+43)(0)676 9107032 fax (+43)(0)1 4803209

info@argedaten.at http://www.argedaten.at