Humanistische Union

Das Ende des Datenschutzes?

Die geplante Umsetzung der Vorratsspeicherung von Telekommunikationsdaten

Mitteilungen Nr. 196, S. 6-7

Mit seinem Gesetzentwurf vom November 2006 bereitet das Bundesministerium für Justiz den Weg für die Umsetzung der umstrittenen EU-Richtlinie über die Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten. Neben den zahlreichen Änderungen verdeckter Ermittlungsmethoden der Strafverfolgung (siehe Bericht S. 4) sieht der Gesetzentwurf deshalb auch eine Änderung des Telekommunikationsgesetzes (TKG) vor. Der Deutsche Bundestag sowie zahlreiche deutsche Rechtspolitiker haben die Einführung einer Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten lange Zeit wegen schwerwiegender verfassungsrechtlicher Bedenken abgelehnt. Nachdem sich jedoch die EU-Justizminister im Dezember 2005 auf einen Richtlinienentwurf einigten und das Europäische Parlament zustimmte, sprach sich auch der Bundestag (gegen die Stimmen aller Oppositionsfraktionen) für den Erlass der Vorratsdatenspeicherungsrichtlinie und ihre Umsetzung in das deutsche Recht aus. Dabei forderte er die Bundesregierung auf, bei der Umsetzung der Richtlinie nicht über deren Vorgaben hinaus zu gehen. Unabhängig von allen grundsätzlichen Bedenken gegen das Vorhaben und das Zustandekommen der Richtlinie ist es deshalb Zeit zu prüfen, ob der deutsche Gesetzgeber sich bei der Umsetzung der Richtlinie an deren Mindestvorgaben orientiert, und in welchen Punkten er möglicherweise über die Vorgaben der Richtlinie hinausgeht.

Verfassungsrechtliche und rechtspolitische Bedenken

Die verdachtsunabhängige Speicherung aller Verbindungsdaten bei der Nutzung von (Mobil-) Telefonen, Internetzugängen, E-Mail- und Anonymisierungsdiensten greift tief in die Kommunikationsfreiheit ein. Sie stellt das Fernmeldegeheimnis, die informationelle Selbstbestimmung sowie die Unternehmensfreiheit der Dienstanbieter in Frage.
Die Begründung des Sinn und Zwecks der Vorratsdatenspeicherung fällt im Gesetzentwurf recht knapp aus: Es wird nur darauf verwiesen, dass die Daten für die Zwecke der (künftigen) Strafverfolgung gespeichert werden. Bisher sind jedoch längst nicht alle kriminell geworden, die einmal Telefone, Handys oder Computer benutzt haben, um sich mit anderen auszutauschen. Eine "vorsorgende Strafverfolgung" für Taten, die bisher noch gar nicht begangen wurden, ist nach geltendem Recht in Deutschland nur dann zulässig, wenn es konkrete Gefahrenhinweise gibt bzw. die negative Kriminalprognose der Betroffenen zu der Vermutung veranlasst, diese könnten bald straffällig werden. Ansonsten gilt immer noch die Unschuldsvermutung. Deshalb halten wir den Zweck der Vorratsdatenspeicherung für illegitim.
Verbindungsdaten sind für Strafverfolger zweifelsohne eine wahre Fundgrube. Aufgrund solcher Daten können sie auf das Kommunikations- und Bewegungsverhalten, auf das soziale Umfeld der Betroffenen und im begrenzten Maße sogar auf die Inhalte ihres Austauschs schließen. Die als Beruhigung der Kritiker beschworene Trennung zwischen Verbindungsdaten – die "nur" Teilnehmer, Zeitpunkt, Dauer, Standort und Art der Kommunikation erfasse – und den Inhalten der Gespräche ist beim genaueren Hinsehen nämlich brüchig: Mit wem ich nachts drei Stunden oder zu den Geschäftszeiten tagsüber fünf Minuten telefoniere, verrät viel über die Art unserer Beziehung. Gegenüber der Überwachung von Kommunikationsinhalten haben die Verbindungsdaten aber noch einen entscheidenden Vorteil für die Strafverfolger: Sie lassen sich automatisiert auswerten. Eine Überwachung des Telefonverkehrs (TKÜ), mit dem der Verdacht gegen einen Verdächtigen überprüft werden soll, kann im Zweifelsfall gut sechs Monate in Anspruch nehmen, in denen

viel technisches Gerät und Personal gebunden ist. Um sich einen Überblick über alle Kommunikationsverbindungen während der letzten sechs Monate eines Menschen zu verschaffen, reichen bei erfolgter Vorratsdatenspeicherung ein paar Anfragen an Telekommunikationsbetreiber und ein Knopfdruck am Computer, um sich das ganze Beziehungsgeflecht des Überwachten auswerten zu lassen. Es wäre deshalb eine Illusion, glauben zu wollen, seine Verbindungsdaten sagten weniger über einen Menschen aus als sein gesprochenes Wort. Nicht umsonst ordnet das Bundesverfassungsgericht die Umstände der Kommunikation dem Fernmeldegeheimnis zu.
Ob mit der Vorratsdatenspeicherung jedoch das gewünschte Ziel, die Bekämpfung schwerer Straftaten (die Richtlinie nennt vor allem Terrorismus und organisierte Kriminalität) erreicht werden kann, ist fraglich. Findige Geister nutzen beispielsweise eigene Webserver, um ihre vertrauliche Kommunikation direkt miteinander, abseits der öffentlichen Anbieter, abzuwickeln. Die Benutzung außereuropäischer Dienstleister oder öffentlicher Telefon- und Internetzugänge sind weitere Schlupflöcher im Überwachungsteppich. Angesichts einer praktischen Unmöglichkeit der totalen Überwachung stellt sich umso stärker die Frage, warum nicht auf schonendere Mittel wie das so genannte "Quick-freeze-Verfahren" ausgewichen wird, das bisher auch für die amerikanischen Sicherheitsbedürfnisse ausreicht. (Bei dieser Methode werden die Daten eines Verdächtigen nach Aufforderung durch die Strafverfolgungsbehörden ab sofort gespeichert, der spätere Zugriff darauf ist nach Erlass einer richterlichen Anordnung möglich.) Bisher sind in der Praxis nur wenige Ermittlungsverfahren daran gescheitert, weil die benötigten Verbindungsdaten fehlten. Im Falle eines konkreten Verdachts nutzen die Strafverfolgungsbehörden regelmäßig die Möglichkeit, durch die Beschlagnahme der Rechner oder Mobiltelefone der Beschuldigten an die dort gespeicherten Verbindungsdaten zu gelangen.
Neben der Datensparsamkeit würde auch ein weiteres zentrales Element der informationellen Selbstbestimmung, die Zweckbindung von gespeicherten Daten, entfallen, wenn die Vorratsdatenspeicherung in der angekündigten Form umgesetzt wird. Der Gesetzentwurf sieht gegenüber der Richtlinie bereits eine Erweiterung für den Zugriff auf die gespeicherten Daten vor: Demnach können die Behörden nicht nur beim Verdacht auf schwere Straftaten, sondern auch bei mittelschweren Straftaten und solchen, die mittels Telekommunikationseinrichtungen begangen wurden (etwa: die Beleidigung am Telefon) die vorrätigen Verbindungsdaten abfragen. Das nach der Einführung der Regelung weitere Vergehen auftauchen werden, für deren Aufklärung unbedingt ein Zugriff auf diese Daten notwendig sein wird, ist bereits jetzt absehbar. Die Film- und Musikindustrie hat ihre diesbezüglichen Wünsche bereits geäußert.

Die praktische Umsetzung - Mehr geht immer!

Bereits bei den Regeln,wie auf die Verkehrsdaten zugegriffen werden darf, schießt der Gesetzgeber über das Ziel der EU-Richtlinie hinaus. Den Strafverfolgungsbehörden wird künftig nicht nur ein Auskunftsanspruch gegenüber den Anbietern der Kommunikationsdienste eingeräumt, sie werden durch die Änderung des § 100g der Strafprozessordnung zugleich ermächtigt, diese Verkehrsdaten auch selbst (bei Bedarf in Echtzeit) zu erheben und auszuwerten. Offenbar fühlten sich die Strafverfolger von Anbietern wie T-Mobile in ihrer Arbeit behindert, die sich zeitweise erlaubt hatten, die formelle Rechtmäßigkeit von Zugriffsanordnungen zu prüfen. Außerdem wird so endlich der Einsatz der "stillen SMS" legalisiert, bei dem die Strafverfolger über verborgene Nachrichten an das Mobiltelefon eines Verdächtigten dessen Standort ermitteln können - bei Bedarf wie gesagt in Echtzeit.
Auch bei der Frage, wer auf die gespeicherten Verbindungsdaten zugreifen darf, lässt der Gesetzentwurf eine Lücke offen. Im Entwurf des Telekommunikationsgesetzes (TKG) wird festgeschrieben, dass auf die vorrätig gespeicherten Verbindungsdaten (der letzten sechs Monate) nur für Zwecke der Strafverfolgung zugegriffen werden dürfe (§ 110b Absatz 1 Satz 3), die dann nach den Vorschriften der Strafprozessordnung (§ 100g StPO) zu erfolgen hätten. Demnach wäre eine Nutzung der gespeicherten Daten für die Gefahrenabwehr und durch die Geheimdienste ausgeschlossen. Letztere verfügen jedoch über eigenständige Befugnisse für den Zugriff auf die Bestands- und Verkehrsdaten der Telekommunikation. Es ist kaum vorstellbar, dass der Gesetzgeber sie von der Nutzung der Vorratsdaten ausschließen will. Dies würde auch

voraussetzen, dass bei jedem Datensatz vermerkt wird, ob die jeweiligen Kommunikationsdaten aus technischen Gründen (etwa zu Abrechnungszwecken) gespeichert wurden - dann dürften auch die Geheimdienste darauf zugreifen - oder ob die Daten aufgrund der für die künftige Strafverfolgung eingerichteten Vorratsdatenspeicherung anfallen - dann wären sie für geheimdienstliche Zwecke tabu. Eine derart genaue Erfassung des Speicherungsgrundes ist aber weder vorgesehen noch technisch sinnvoll umsetzbar. Vielmehr ist davon auszugehen, dass den Geheimdiensten "natürlich" auch diese Daten zugänglich sein sollen. Dann wäre aber die Beschreibung des Verwendungszwecks im Gesetz unvollständig.
Gefahren drohen aber nicht nur von staatlicher Seite. Wenn die Vorratsdatenspeicherung für alle Anbieter von Telefonverbindungen, Mailkonten und Webservern Pflicht wird, bedeutet dies, dass an vielen verschiedenen Stellen viele personenbezogene Daten gespeichert werden. Diese lassen sich nicht nur zur Strafverfolgung nutzen, sondern sind auch unter wirtschaftlichen Gesichtspunkten zu verwerten. Zahlreiche Fälle des Diebstahls oder der unbeabsichtigten Veröffentlichung von Kundendaten bei Internetdienstleistern machen das deutlich. Vor diesem Hintergrund ist die Gefahr einer missbräuchlichen Verwendung solcher Daten durch Dritte relativ hoch einzuschätzen. Im Gesetzentwurf fehlt - außer dem Verweis, dass die zur Speicherung verpflichteten Anbieter den unberechtigten Zugriff zu verhindern hätten - aber jeder Hinweis darauf, welche Sicherungen der Gesetzgeber für die auf seine Anordnung hin zu speichernden Daten vorsieht. Scheinbar reicht die gesetzgeberische Verantwortung nur für die Sicherstellung der Strafverfolgung, der Schutz der zwangsweise gesammelten Personendaten wird als private Angelegenheit der Anbieter gesehen.
Schließlich ist nach dem vorliegenden Gesetzentwurf offen, wer letztlich alles zur Speicherung der Verbindungsdaten verpflichtet sein wird. Folgt man der Begründung, zählen beispielsweise universitäre Rechenzentren nicht zu den öffentlichen TK-Anbietern, weil bei ihnen nur Mitarbeiter und Studenten einen entsprechenden Zugang erhalten. Andererseits sollen aber die Betreiber von Anonymisierungsdiensten, die nach bisherigem Verständnis keinen Telekommunikationsdienst, sondern einen Mediendienst bereitstellen und deshalb von der Speicherungspflicht nicht betroffen wären, doch zur Speicherung ihrer Nutzerdaten verpflichtet werden.

Wie weiter?

Für April hat die Regierung die Verabschiedung des (überarbeiteten) Gesetzentwurfs im Bundeskabinett angekündigt. Die Humanistische Union wird den Gesetzgebungsprozess weiterhin kritisch begleiten und ist auf die parlamentarischen Diskussionen vorbereitet. Darüber hinaus werden wir versuchen, die mit der Vorratsdatenspeicherung verbundenen Probleme in der Öffentlichkeit präsent darzustellen. Für den 1. Juni planen wir eine Fachkonferenz, die unter Beteiligung von prominenten Rechtspolitikern und Rechtsexperten in Berlin stattfindet. Sollte das Umsetzungsgesetz vom Deutschen Bundestag verabschiedet werden, wird die Humanistische Union alle rechtlichen Mittel prüfen und ggf. eine Verfassungsbeschwerde gegen das Gesetz erheben.

Die ausführliche Stellungnahme der Humanistischen Union zum Referentenentwurf und weitere Informationen zum Thema Vorratsdatenspeicherung sowie zur geplanten Fachtagung sind zu finden unter https://www.humanistische-union.de/vorratsdaten/.
