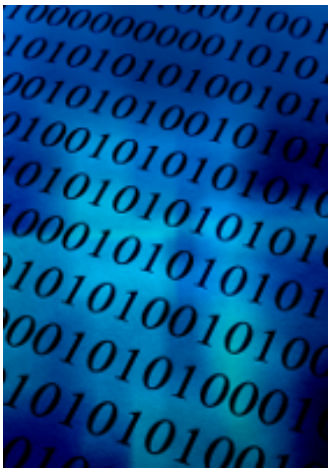
Vorratsdatenspeicherung: Löschen statt Lauschen

Im Zeichen des „Großen Lauschangriffs“ durch Strafverfolgungsbehörden und Nachrichtendienste hat der Gesetzgeber zu Lasten der Bürgerrechte die Grenzen des Grundgesetzes weit überschritten. Mit dem Gesetz zur Vorratsdatenspeicherung versuchte er, sich zum Herrscher über Bits und Bytes seiner Bürger emporzuschwingen. Doch Karlsruhe hat dem nun einen Riegel vorgeschoben und angeordnet, dass die flächendeckend in den letzten zwei Jahren gespeicherten Telekommunikationsverkehrsdaten von allen Telefonaten, E-Mails und Internetseitenaufrufen sofort und unverzüglich zu löschen sind. Damit ziehen die Verfassungsrichter die Notbremse. Aber es wurde auch Kritik an der Entscheidung aus Karlsruhe laut, etwa dass sich das Gericht gegen eine Vorlage der EU-Richtlinie beim Europäischen Gerichtshof (EuGH) entschieden hat.



Der binäre Code gilt auch für den Datenschutz: In Karlsruhe lautete das Ergebnis 1 zu 0 für das Grundgesetz.

EU-Richtlinie ist verfassungskonform

Darum zu Beginn ein Plädoyer für das Urteil des höchsten deutschen Gerichts: Die Vereinbarkeit der dem Gesetz zur Vorratsdatenspeicherung zugrunde liegenden EU-Richtlinie mit dem Grundgesetz ergibt sich zwangsläufig aus dem Inhalt der Richtlinie, ihrem Regelungsinhalt. Die Richtlinie 2006/24/EG wurde erlassen, damit innerhalb der EU eine einheitliche Speicherung der Telekommunikationsverkehrsdaten ermöglicht wird. Bislang haben die Mitgliedstaaten bei der Vorratsdatenspeicherung zur Terrorismusbekämpfung, zur Verfolgung der organisierten Kriminalität und schwerer Straftaten stark voneinander abweichende Regelungen getroffen. Die EU-Richtlinie zielt in erster Linie auf die Harmonisierung der verschiedenen Gesetze für die Vorratsdatenspeicherung ab. Die Regelung der Vorratsdatenspeicherung selbst und bei welchen Straftaten die Behörden auf die Daten Zugriff haben, bleibt laut der Richtlinie dem Gesetzgeber des Mitgliedstaates überlassen.

Damit ist klar, dass die EU-Richtlinie den deutschen Gesetzgeber nur dazu verpflichtet, dass er ein Gesetz zur Vorratsdatenspeicherung erlässt und nur im Bereich der Strafverfolgung. Die Umsetzung und die vom deutschen Gesetzgeber initiierte Ausdehnung des behördlichen Datenzugriffs auf die Bereiche der Gefahrenabwehr und der Nachrichtendienste, ist allein eine autarke Entscheidung des Gesetzgebers gewesen. Wer sich nun beklagt, dass mit dem Urteil des Bundesverfassungsgerichts den Strafverfolgungsbehörden ein wichtiges Instrument genommen wird, der muss sich an die eigene Nase fassen, wenn er als Gesetzgeber beteiligt war. Niemand anderes als er - also Regierung, Bundestag und Bundesrat - hatten es 2007 allein in der Hand, dass die Vorratsdatenspeicherung in einem Gesetz umgesetzt wird, das die Grundrechte der Bürger wahrt. Umgekehrt gilt dies natürlich auch für diejenigen, die damals dem Gesetz zugestimmt haben und heute über die Entscheidung aus Karlsruhe frohlocken.

Keine Vorlage an den EuGH

Die Verfassungsrichter haben sich korrekt gegen eine Vorlage beim EuGH entschieden. Zum einen ist es nicht die Aufgabe des Bundesverfassungsgerichts, EU-Richtlinien auf die Vereinbarkeit mit den Gemeinschaftsgrundrechten auf EU-Ebene zu prüfen. Sein Prüfungsmaßstab erschöpft sich auf die Vereinbarkeit der Richtlinie mit dem

Grundgesetz. Zum anderen überlässt die EU-Richtlinie dem nationalen Gesetzgeber einen derart großen Ermessensspielraum bei der Umsetzung in nationales Gesetz, dass kein Verfassungsverstoß erkennbar ist. Mit anderen Worten: Was die EU-Richtlinie nicht regelt, kann auch nicht gegen die Verfassung verstoßen. Und ein generelles Verbot der Vorratsdatenspeicherung konnten die Karlsruher Richter dem Grundgesetz nicht entnehmen. Entscheidend für die Vereinbarkeit mit dem Grundgesetz ist, welche Vorsichtsmaßnahmen der deutsche Gesetzgeber zum Schutz der Grundrechte in dem Gesetz trifft. Und hier attestierten die Verfassungsrichter wieder einmal einem Gesetz im Bereich des Datenschutzes die Verfassungswidrigkeit.

Das Urteil des Bundesverfassungsgerichts sagt nichts über die Zulässigkeit der Vorratsdatenspeicherung in Hinblick auf die Gemeinschaftsgrundrechte aus. Diese Entscheidung wird der EuGH noch zu treffen haben. Zwar hat er bereits eine Nichtigkeitsklage von Irland gegen die Vorratsdatenspeicherung abgewiesen *(Urteil v. 10.02.2010 - Rs. C-301/06)*, die für die Richtlinie Einstimmigkeit gefordert hatte, weil die Vorratsdaten für Strafverfolgungszwecke genutzt werden sollen. Über die Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Gemeinschaftsgrundrechten sagt dieses EuGH-Urteil jedoch nichts aus. Das hat der Europäische Gerichtshof ausdrücklich in der Urteilsbegründung betont.

Die Chancen der Gegner der Vorratsdatenspeicherung, wie bereits angekündigt auf EU-Ebene erfolgreich gegen die Richtlinie vorzugehen, stehen folglich nicht schlecht. Denn inzwischen regt sich nicht nur Zweifel mit der Vereinbarkeit der Richtlinie mit den Gemeinschaftsgrundrechten, z.B. im EU-Parlament, sondern auch in Hinblick darauf, ob damals der Erlass der Richtlinie überhaupt im Kompetenzbereich der Europäischen Gemeinschaft lag. Was die Vorratsdatenspeicherung anbelangt, bleibt es also weiter spannend.

Gesetz zur Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat klar und deutlich geurteilt und reagiert: Das Gesetz zur Vorratsdatenspeicherung verstößt gegen Artikel 10 Absatz 1 Grundgesetz (GG) und ist damit nichtig. Alle Daten, die inzwischen gespeichert wurden, sind unverzüglich zu löschen. Warum musste Karlsruhe so hart durchgreifen?

Die §§ 113a, 113b Telekommunikationsgesetz (TKG) regeln die vorsorgliche anlasslose Speicherung und den Abruf von Verkehrsdaten durch Behörden zu Strafverfolgungszwecken, zur Gefahrenabwehr und zur Erfüllung nachrichtendienstlicher Aufgaben. Die Behörden werden zum Abruf der Daten durch die jeweiligen Fachgesetze ermächtigt. Bei den Strafverfolgungsbehörden ist dies § 100g Strafprozessordnung (StPO), beim Bundeskriminalamt ist es § 20m Gesetz über das Bundeskriminalamt (BKA-Gesetz). Weitere Bestimmungen finden sich in den Polizeigesetzen der Bundesländer, z.B. in Artikel 34b Bayerisches Polizeiaufgabengesetz (BayPAG).

> *Weitere Informationen zu dem Regelungsbereich des Gesetzes zur Vorratsdatenspeicherung finden Sie im anwalt.de-Rechtstipp „Bundestag beschließt Vorratsdatenspeicherung - droht die gläserne Kommunikation?“.*

Verfassungsrechtliche Defizite attestierten die Karlsruher Richter, weil der Gesetzgeber keine ausreichenden Regelungen für die Datensicherheit, die Begrenzung der Datenverwendung, die erforderliche Transparenz und hinsichtlich des Rechtsschutzes getroffen hat.

Eine wichtige Grenze hat das Verfassungsgericht für die Nutzung der Vorratsdatenspeicherung betont: Sollte der Gesetzgeber auf die Vorratsdatenspeicherung zurückgreifen, bleibt ihm nach Ansicht der Verfassungsrichter nur noch ein sehr geringer Spielraum in Hinblick auf die Regelung weiterer Datensammlungen. Das betrifft insbesondere auch die Umsetzung von Richtlinien über den Weg der EU. Das Urteil zur Vorratsdatenspeicherung

kann sich also auch auf die inzwischen installierten Datensammlungen wie etwa ELENA auswirken.

In welchen Lebensbereichen bisher Daten der Bürger gesammelt werden und welche Risiken die Speicherung der Daten birgt, erfahren Sie im anwalt.de-Rechtstipp „Datenschutz: Der gläserne Bürger“.

Datensicherheit muss gewährleistet sein

Weil es sich bei den Vorratsdaten um sensible Verkehrsdaten handelt, ist eine genaue und verbindliche Regelung der Datensicherheit erforderlich. Erfasst werden Daten, die per Telefon, Internet, E-Mail, Mobilfunk und auch per SMS oder MMS übertragen werden; etwa Zeit und Ort des Empfangs oder Absendens der Nachricht, Absender und Empfänger der Nachricht u.Ä. Laut dem Gesetz sollen die Inhalte selbst nicht auf Vorrat gespeichert werden. Das mag bei Internetseiten zwar funktionieren, bei Text- und Bilddateien ist eine Speicherung ohne Inhalt schon allein aus technischen Gründen gar nicht möglich. Und selbst wenn keine Inhalte der Informationen gespeichert werden, lassen sich anhand der Verkehrsdaten trotzdem leicht Rückschlüsse auf Schwächen und Vorlieben des Betroffenen ziehen und Bewegungs- und sogar Persönlichkeitsprofile erstellen.

Aus diesem Grund fordert das Bundesverfassungsgericht, dass bei einer Vorratsdatenspeicherung bei den Telekommunikationsunternehmen höchste Sicherheitsstandards gewährleistet werden. Da die Telekommunikationsfirmen unter Kostendruck und in Konkurrenz stehen, ist es zwingend notwendig, dass der Gesetzgeber ihnen hohe technische Sicherheitsanforderungen verbindlich vorgibt. Die Speicherung der Daten bei den Telekommunikationsunternehmen selbst beanstandeten die Verfassungsrichter dagegen nicht, auch nicht dass die Unternehmen selbst die Kosten der Datenspeicherung zu tragen haben. Den Verfassungsrichtern ist wichtig, dass die Speicherung stets dezentral und auf gar keinen Fall bei einer zentralen Super-Daten-Behörde gespeichert wird. Ein Direktzugriff auf die Vorratsdaten ist den Behörden vom Grundgesetz ebenfalls verwehrt. Der Erste Senat hat ausdrücklich betont, dass die Sicherheitsstandards, die ansonsten bei der Speicherung anderer Daten von den Telekommunikationsunternehmen zu beachten sind, für die äußerst sensiblen Daten der Vorratsdatenspeicherung nicht einfach übertragen werden dürfen. Hier ist der höchste und technisch mögliche Standard zu erfüllen.

Begrenzung der Datenverwendung

Die Speicherung und Nutzung der Verkehrsdaten gemäß § 113a TKG stellt einen derart gravierender Eingriff in das Persönlichkeitsrecht des Bürgers dar, der nur für die Erfüllung von Aufgaben zulässig sein kann, mit denen überragend wichtige Rechtsgüter geschützt werden sollen. Damit hängt die Begrenzung der Datenverwendung von den Aufgaben der Behörden ab. Sollen die Daten zur Strafverfolgung verwendet werden, muss im Einzelfall ein durch Tatsachen begründeter Verdacht auf eine schwerwiegende Straftat vorliegen. Zur Gefahrenabwehr dürfen die Verkehrsdaten von den Behörden nur abgerufen werden, wenn eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Bundeslandes oder zur Abwehr einer gemeinen Gefahr besteht. Der Erste Senat betonte, dass diese hohen Hürden insbesondere ebenfalls für die Nachrichtendienste gelten müssen. Dass die Geheimdienste oftmals zur Vorfeldaufklärung eingesetzt werden und bei ihnen daher in vielen Fällen ein Datenzugriff ausscheidet, hat das Verfassungsgericht ausdrücklich zugunsten des Telekommunikationsgeheimnisses bestätigt.

Diese hohen Hürden hat der Gesetzgeber ebenso wenig geregelt wie ein Übermittlungsverbot für besonders persönliche und intime Daten. Nicht nur Bürger und Datenschützer gehören zu den knapp 35.000 Beschwerdeführern, es haben auch Angehörige besonderer Berufsgruppen geklagt, beispielsweise Seelsorger,

Sozialdienste, Ärzte, Anwälte, Lehrer und weitere Personen, die Menschen in schwierigen persönlichen Notlagen Unterstützung per Telefon, E-Mail und anderer Kommunikationswege zukommen lassen. Die Notlage dieser Menschen darf nicht von den Behörden ausgenutzt werden. Daher fordern die Richter ein striktes, generelles Übermittlungsverbot für solche Daten z.B. bei seelsorgerischen Notdiensten.

Transparenz der Speicherung und Verwendung

Weiter mangelt es dem Gesetz zur Vorratsdatenspeicherung ebenfalls an Transparenz. Mit der anlasslosen Datenspeicherung erhöht sich das Risiko für den Bürger, weiteren Ermittlungen durch die staatlichen Behörden ausgesetzt zu sein, ohne dafür selbst einen Anlass gegeben zu haben. Hinzu kommt, dass mangels einer Benachrichtigungspflicht und nachträglichem Rechtsschutz beim Bürger das diffuse Gefühl entstehen kann, unter staatlicher Beobachtung zu stehen. Und dieses Gefühl des Einzelnen kann die Kommunikation und Intimität aller beeinflussen und so die Gesellschaft insgesamt prägen.

Durch Transparenz, meint das Bundesverfassungsgericht, muss dem Bürger das diffuse Gefühl der Bedrohung durch Dauerüberwachung etwas genommen werden. Deshalb müssen personenbezogene Daten offen erhoben und genutzt werden. Eine Nutzung ohne Wissen des Betroffenen ist daher strikt auf die Fälle zu begrenzen, in denen andernfalls der Zweck der Untersuchung vereitelt wird. Nur wenn die heimliche Datennutzung erforderlich und von einem Richter angeordnet wird, ist sie zulässig.

Ist dem so, muss allerdings der von der Maßnahme Betroffene darüber informiert werden. Eine Benachrichtigungspflicht muss der Gesetzgeber regeln, damit der Betroffene zumindest nachträglich von der Nutzung seiner persönlichen Daten weiß. Ausnahmen von der Benachrichtigungspflicht müssen richterlicher Kontrolle unterstehen.

Rechtsschutz und Sanktionen bei Missbrauch

Schließlich muss der Gesetzgeber ein geeignetes Rechtsschutzsystem und auch Sanktionsmittel für den Fall einer unbefugten Nutzung der Vorratsdaten von Behörden schaffen. Jeder muss die Möglichkeit haben, den Behördenzugriff auf seine persönlichen Daten gerichtlich überprüfen zu lassen. Das folgt aus der Pflicht des Staates, die freie Persönlichkeitsentfaltung seiner Bürger zu schützen.

Dabei kann der Gesetzgeber auf die bereits bestehenden Sanktionsmöglichkeiten zurückgreifen, also beispielsweise ein Beweisverwertungsverbot vorsehen und auch eine entsprechende staatliche Haftung, besonders auch für immaterielle Schäden. In diesem Zusammenhang ist eine Bemerkung des Bundesverfassungsgerichts äußerst interessant: Verstößt ein Telekommunikationsdienst gegen seine Verpflichtung zur Vorratsdatenspeicherung, droht ihm ein höheres Bußgeld als es für die unbefugte Datennutzung durch die Behörden vorgesehen ist. Diese Ungleichgewichtung auf der Sanktionsebene muss er im Interesse des Datenschutzes seiner Bürger beseitigen.

Der Gesetzgeber wird eine Neuregelung für die Vorratsdatenspeicherung treffen müssen, da er hierzu durch die EU-Richtlinie verpflichtet ist. Nur bitte diesmal im Einklang mit unserem Grundgesetz. Gewiss kann dies allein nicht bei jedem letzte Zweifel und ein ungutes Gefühl ausräumen. Insbesondere wenn man daran denkt, dass jede Speicherung von Daten auch einen Missbrauch derselben nach sich ziehen kann. Hinzu kommt, dass inzwischen immer mehr Daten zentral gesammelt und gespeichert werden.

Eines steht jedoch fest: Die Kosten für die gesetzgeberische Fehlleistung muss der Bund tragen, also die Steuerzahler. Doch das ist das geringere Übel. Zweifellos hätte die Aufrechterhaltung des Gesetzes zur

Vorratsdatenspeicherung den Bürger mehr gekostet, nämlich seine Privatsphäre. Und die ist ein unbezahlbares Gut. Das hat das Bundesverfassungsgerichtsurteil deutlich gemacht.

(WEL)

Rechtsfragen? Die Experten von anwalt.de stehen Ihnen in allen Rechtsgebieten mit fachkundiger Rechtsberatung zur Verfügung - wahlweise via E-Mail, direkt telefonisch oder vor Ort.