# Thema Vorratsdaten-speicherung im neuen TKG

Manuel Kiper // BTQ Niedersachsen, Oldenburg

**HIER LESEN SIE:**

- warum die neuen Bestimmungen im Telekommunikationsgesetz massive Auswirkungen auch für die Arbeitnehmer in Betrieben und Dienststellen haben können
- welche Daten über das „Telekommunikationsverhalten" von Arbeitnehmern erfasst und gespeichert werden müssen
- warum das Verbot einer privaten Nutzung dienstlicher Telekommunikationseinrichtungen der falsche Weg wäre, um sich vor der Vorratsdatenspeicherung und den damit verbundenen Kosten zu schützen

**„Ich sei, gewährt mir die Bitte, in Eurem Computer der Dritte!" (aus Stasi 2.0) … Die lange umstrittene sogenannte Vorratsdatenspeicherung wurde mit dem am 1.1.2008 in Kraft getretenen „Gesetz zur Neuregelung der Telekommunikation …" rechtlich verankert. Die dadurch entstandenen neuen Bestimmungen im Telekommunikationsgesetz (TKG) sind nicht ohne Auswirkungen auf Betriebe und Dienststellen, soweit diese die private Nutzung von Telekommunikation (z.B. E-Mail, Internet) am Arbeitsplatz erlauben oder dulden. Auch sie müssen zukünftig für Zwecke einer eventuellen Strafverfolgung Daten über die Nutzung des elektronischen Postverkehrs vorhalten.**

„Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007"[1], so heißt das umfangreiche Paket, mit dem zukünftig kriminelle oder auch terroristische Aktivitäten erfolgreicher ermittelt und möglichst verhindert werden sollen.

Ein Eckstein dieses Pakets ist die Verankerung der sogenannten Vorratsdatenspeicherung im § 113a TKG. Die Vorratsdatenspeicherung, so befürchten Kritiker, trifft nicht nur die gewerblichen Telekommunikationsanbieter, sondern auch Betriebe und Dienststellen, soweit diese privates Internetsurfen und private E-Mails, Telefaxe oder Telefongespräche – sei es über Festnetz oder Handy – erlauben oder jedenfalls wissentlich dulden.

Die Beschäftigten würden in diesen Fällen nämlich gleichsam als „Kunden" gelten, die die von ihrem Arbeitgeber „angebotenen" Telekommunikationsleistungen nutzen – unabhängig davon, ob der Arbeitgeber dafür ein Entgelt verlangt oder nicht (auch in diesen Fällen handelt es sich um das sogenannte „geschäftsmäßige" Erbringen von Telekommunikationsdiensten).

## Speicherung der Stammdaten

Das neue TKG schreibt zunächst im geänderten § 111 ausdrücklich für geschäftsmäßiges Erbringen von Telekommunikationsdiensten vor, dass nunmehr alle Stammdaten dieser Beschäftigten für Strafverfolgungsbehörden und Geheimdienste aktuell abrufbar sein müssen. Ob Handy, Festnetztelefon oder Internetzugang: Die folgenden Stammdaten müssen vor einer Freischaltung oder „unverzüglich" erhoben und gespeichert werden, selbst wenn diese Daten für dienstliche Zwecke gar nicht erforderlich sein sollten:

- die Rufnummern und andere Anschlusskennungen/E-Mail-Adressen,
- der Name und die Anschrift des Anschluss-/Postfachinhabers,
- bei natürlichen Personen deren Geburtsdatum,
- bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
- in Fällen, in denen neben einem Mobilfunkanschluss auch ein entsprechendes „Endgerät" (z.B. ein Handy) überlassen wird, die Gerätenummer dieses Geräts sowie
- das Datum des Vertragsbeginns,
- das Datum des Vertragsendes bei Bekanntwerden.

Diese Daten sind erst mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahrs zu löschen, müssen also auch bei kurzfristigen Arbeitsverhältnissen stets länger als 12 Monate aufgehoben werden. Eine Entschädigung für den mit der Datenerhebung und -speicherung verbundenen Aufwand gibt es nicht.

## Speicherung der Verkehrsdaten

Die sogenannten Verkehrsdaten sind Daten, die sich auf die Umstände eines Telekommunikationsvorgangs beziehen – nicht auf den Inhalt. Im neuen § 113 a TKG sind umfassende Speicherungspflichten für Daten verankert worden.

Bei Telefonaten beispielsweise wird gespeichert, wer (identifiziert über Telefonnummer, Name und Adresse) wann mit wem wie lange telefoniert hat. Bei Gesprächen über Mobiltelefone wird zusätzlich gespeichert, in welcher Funkzelle sich die beiden Telefonpartner dabei befunden haben. Beim Versand von SMS-Nachrichten und der Nutzung anderer Mitteilungs- und Multimediadienste ist es ebenso.

Internetzugangs-Dienste, Dienste der elektronischen Post oder Internet-Telefondienste müssen wegen technischer Probleme erst ab dem 1.1.2009 ihren Speicherpflichten nachkommen.

Ab diesem Zeitpunkt können dann auch Bußgelder von bis zu 500 000 Euro gegen ▶ Provider und Erbringer von Telekommunikationsdiensten verhängt werden, wenn diese ihren Speicherpflichten nicht nachkommen. Bei der Internetnutzung muss protokolliert werden, wer wann mit seinem jeweiligen Internetprovider verbunden war, allerdings nicht, welche Seiten er sich angeschaut hat. Beim Versand von E-Mails wird ebenfalls gespeichert werden, wer wann mit wem in Kontakt stand, ähnlich auch bei der Internettelefonie (▶ VoIP).

Manche Kommentatoren und Kritiker der Vorratsdatenspeicherung lesen aus dem Wortlaut des neuen §113 a Absatz 3 und 4 TKG heraus, dass auch Betriebe und Dienststellen bei der privaten Nutzung von E-Mail und Internet am Arbeitsplatz die Verkehrsdaten sechs Monate speichern müssen.

Der § 113 a Abs. 1 und 2 bezieht sich allerdings ausdrücklich nur auf die Speicherpflichten für diejenigen, die „öffentlich zugängliche Telekommunikationsdienste für Endnutzer" erbringen. Die Absätze 3 und 4 des § 113 a TKG beziehen sich hingegen pauschal auf „Anbieter von Diensten der elektronischen Post" und „Anbieter von Internetzugangsdiensten". Hier wird erst die Gesetzeskommentierung und Rechtsprechung Klarheit bringen, wer davon betroffen ist.

Das deutsche Gesetz sieht – anders übrigens als die EU-Richtlinie – vor, dass die gespeicherten Daten zur Aufklärung aller Verbrechen genutzt werden, die durch Telekommunikation begangen wurden, und zwar unabhängig von deren Schwere. Sie können also auch zur Verfolgung von Bagatelldelikten herangezogen werden, etwa bei unerlaubtem Herunterladen von Musik.

Und während die EU-Richtlinie den Zugriff auf Strafverfolgungsbehörden beschränkt, ist im deutschen Gesetz zusätzlich eine Zugriffsmöglichkeit für die Geheimdienste vorgesehen. Für einen Zugriff durch die Geheimdienste ist auch kein Richtervorbehalt nötig und selbst Vertrauensberufe wie Ärzte, Anwälte oder Seelsorger sind nicht ausgenommen.

## Unnötiger Aufwand?!

Wie fragwürdig diese Vorratsdatenspeicherung ist, erweist sich bereits daran, dass ein manuelles Auskunftsverfahren schon seit 2004 etabliert ist. Nach § 113 TKG hatten Telekommunikationsanbieter wie z.B. Telefongesellschaften und Provider auch bisher im begründeten Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte zu erteilen.

Dies galt immer dann, wenn es für die Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich war, oder auch zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung sowie für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes. In vielen Betriebs- und Dienstvereinbarungen hatte dies seinen Niederschlag in der Form gefunden, dass für den Fall solcher staatlichen IKT-Kontrollen die Zustimmungspflicht der Belegschaftsvertretung für Eingriffe ins Fernmeldegeheimnis am Arbeitsplatz entfalle.

Werfen wir einen Blick auf die „Geschichte" der neuen Regelung: Noch im Jahre 2004 hatten sich Bundesrat und Bundestag im Rahmen der Novellierung des Telekommunikationsgesetzes (TKG) ausdrücklich gegen die Einführung einer Vorratsdatenspeiche-

rung entschieden. Dieser Entscheidung lag die Erkenntnis zugrunde, dass die entstehenden Belastungen der Wirtschaft und die Eingriffe in die Rechte der Betroffenen dem Grundsatz der Datensparsamkeit, dem Recht auf ► informationelle Selbstbestimmung und der Vertraulichkeit von Daten widersprächen.

Und tatsächlich kalkuliert die Internetwirtschaft aktuell die Kosten für die Vorratsdatenspeicherung auf über 300 Millionen Euro. Auch ist eine von vielen Verbänden und Einzelpersonen ausgehende Verfassungsbeschwerde anhängig.[2]

Zudem ist ein konkreter Nutzen der neuen Regelungen für die Strafverfolgung schwer zu sehen. Das Max-Planck-Institut für ausländisches und internationales Strafrecht hat in einer Untersuchung aus dem Jahr 2007 für die ohne sechs Monate Vorratsspeicherung verfügbaren Kommunikationsdaten festgestellt, dass „die Aktenanalyse selbst unter den heutigen rechtlichen Bedingungen nur für etwa 2 % der Abfragen nachweist, dass sie wegen Löschungen ins Leere gehen."[3] Sprich: Die Strafverfolgungsbehörden konnten in 98 % der Fälle auch ohne Vorratsdatenspeicherung die interessierenden Daten sicherstellen. Der Nutzen der neuen Regelungen dürfte damit gegen Null tendieren.

## Auswirkungen auf Arbeitnehmer

Die zusätzlichen Pflichten (und damit verbundenen Kosten) zur Datenspeicherung bei geschäftsmäßigen Telekommunikationsanbietern werden mit Sicherheit dazu führen, die vielfach zugelassene/geduldete private Nutzung der dienstlichen Informations- und Kommunikationseinrichtungen einer erneuten Prüfung zu unterziehen – zumal es einen rechtlichen Anspruch auf eine solche Nutzung ja nicht gibt.

Dabei könnten Arbeitgeber eine – allerdings nur scheinbar einfache – Lösung des beschriebenen Problems in einem generellen Verbot der privaten Nutzung von Internet und anderen Kommunikationstechniken am Arbeitsplatz sehen. Und in der Tat würde in diesem Fall das TKG nicht gelten und damit die Pflicht zur Datenspeicherung entfallen.

Ein solches vollständiges Verbot privater Nutzung dürfte allerdings nicht nur zu einer erheblichen Verunsicherung bei den Beschäftigten führen und den produktiven Umgang mit der Informations-/Kommunikationstechnik (IKT) allgemein stark beeinträchtigen.

**„Die Kosten der Vorratsdatenspeicherung könnten für Arbeitgeber ein Motiv sein, die private Nutzung von Internet und E-Mail am Arbeitsplatz ganz zu verbieten."**

Für etliche Berufe ist die uneingeschränkte Nutzung von E-Mail und Internet inzwischen eine wichtige Voraussetzung, um Arbeit und Leben organisieren zu können (siehe den Artikel ab Seite 26). Große Finanzdienstleister verpflichten und schulen ihre Mitarbeiter sogar darauf, private Kontakte zu pflegen und dienstlich „abzuschöpfen".

Und alle mobil Arbeitenden (siehe auch den Artikel ab Seite 15) sind zwingend auf die Nutzung von Handys und Internet als Voraussetzung für Kommunikation innerhalb der Belegschaft angewiesen, ob nun dienstlich oder – was für ein gutes Betriebsklima unabdingbar ist – auch privat.

Angesichts dieser Argumente sollte der zusätzliche (Kosten-)Aufwand für eine Datenvorhaltung sicher nicht ausschlaggebend dafür sein dafür, ein generelles privates Nutzungsverbot für die dienstliche Informations- und Kommunikationstechnik auszusprechen (siehe auch M. Kiper: „Betriebs- und Dienstvereinbarungen zu E-Mail und Internet" in CF 9/04).

Viele Landesdatenschutzbeauftragte empfehlen übrigens als „ Ausweichmodell" zur Umgehung der rechtlichen Probleme (wie auch zur Verhinderung drohenderEinschleppung von ► Viren), Arbeitnehmern für Abruf und Versenden privater Mails die Nutzung sogenannter ► Free-Mail-Anbieter im Internet zu gestatten. Unternehmen und Dienststellen, die das täten, würden nämlich nicht als „geschäftsmäßige" Telekommunikationsanbieter gelten und wären damit auch nicht zur Vorratsdatenspeicherung verpflichtet.

Auch eine solche Lösung sollte auf jeden Fall ins Auge gefasst werden, ehe daran gedacht wird, ein Verbot privater elektronischer Kommunikation am Arbeitsplatz zu verhängen.

*Autor*

**Dr. Manuel Kiper** ist Technologie- und Arbeitsschutzberater bei der BTQ Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441 82068, kiper@btq.de, www.btq.de

*Quellen im Internet*

www.vorratsdatenspeicherung.de/

www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.htm

*Lexikon*

**Free-Mail** ► (englisch: *free* = frei, kostenlos, *mail* = Post) Angebot einer E-Mail-Adresse zur kostenlosen Nutzung (meist werbefinanziert)

**informationelle Selbstbestimmung** ► siehe Lexikon Seite 10

**Provider** ► (englisch: *to provide* = versorgen) Dienstleister der z.B. Internetzugänge bereitstellt/vermittelt

**Virus/Viren** ► sich selbst vermehrende kleine Programme, die sich meist via E-Mail oder Internet in ein IKT-System einschleusen und dort nicht kontrollierbare Veränderungen vor allem am Betriebssystem oder an anderer Software vornehmen; oft auch als Sammelbegriff für alle Arten von Schadsoftware benutzt

**VoIP** = Voice over IP (englisch: *voice* = Stimme) Nutzen von Internetverbindungen (IP = *Internet Protocol* = Internet-Übertragungsstandard), um mithilfe von speziellen Telefonanlagen oder von PC, Software und Kopfhörer-/Mikrofoneinheit (Headset) über eine Internetverbindung zu telefonieren

*Fußnoten*

1 www.bgblportal.de/BGBL/bgbl1f/bgbl107s3198.pdf – Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (TKÜ-Gesetz) in der vom Bundestag beschlossenen Fassung (Bundesrat Drucksache 798/07): www.bundesrat.de/cln_051/SharedDocs/Drucksachen/2007/0701-800/798-07,templateId=raw,property=publicationFile.pdf/798-07.pdf

2 Beschwerdeschrift vom 31.12.2007: www.starostik.de/downloads/anwalt-berlin-verfassungsbeschwerde-vorratsdatenspeicherung.pdf

3 Rechtswirklichkeit der Auskunfterteilung über Telekommunikationsverbindungsdaten nach § 100 g und § 100 h Strafprozessordnung, www.Vorratsdatenspeicherung.de/images/mpi-gutachten.pdf, Seite 407