Speicherrechte nach dem Telemediengesetz und dem Telekommunikationsgesetz

Inhaltsverzeichnis

A. Einleitung

B. Anwendungsbereiche und Abgrenzung von TMG und TKG

C. Befugnisse zur Datenspeicherung nach TMG und TKG

I. Datenspeicherung im Telemediengesetz

Sonderproblem: Die Behandlung von IP-Adressen im TMG

Sonderproblem: Verwendung von Cookies

II. Datenspeicherung im Telekommunikationsgesetz

1. Speicherungsrechte von Bestandsdaten

2. Speicherungsrechte von Verkehrsdaten

3. Sonderproblem: Die Behandlung von IP-Adressen im TKG

A. Einleitung

Das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) regeln jeweils verschiedene Teledienste. Daher müssen die Gesetze voneinander abgegrenzt werden, um die Rechte und Pflichten der Diensteanbieter in Bezug auf die Erhebung und Verwendung von Nutzerdaten herauszufiltern, welche im Rahmen der Nutzung der Dienste anfallen. Erschwert wird diese Abgrenzung durch Überschneidungen der Gesetze, insbesondere im Falle der Zugangsvermittlung zum Internet (Access-Providing). Darüber hinaus differenzieren die Gesetze zwischen verschiedenen Arten von Daten, nämlich zwischen Bestands- und Nutzungs- bzw. Verkehrsdaten. Hierbei ist ebenfalls eine genaue Unterscheidung erforderlich, da an den Umgang mit den Daten unterschiedlich hohe Anforderungen geknüpft werden. Besonderes Augenmerk muss ferner auf die Rechte zur Erhebung und Verwendung von IP-Adressen gelegt werden. Hierüber kann keine allgemeingültige Aussage getroffen werden, da sich der Umfang der Verwendungsbefugnisse oftmals nur unter Betrachtung des konkreten Einzelfalls bestimmen lässt, was sowohl im TMG als auch im TKG Schwierigkeiten bereiten kann.

B. Anwendungsbereiche und Abgrenzung von TMG und TKG

Das Telemediengesetz gilt gemäß § 1 Abs. 1 TMG für Telemedien. Darunter versteht man alle elektronischen Informations- und Kommunikationsdienste, die keine Telekommunikationsdienste (§ 3 Nr. 24 TKG), telekommunikationsgestützte Dienste (§ 3 Nr. 25 TKG) oder Rundfunk (§ 2 RStV) darstellen. Eine genaue Einordnung eines Dienstes als Telemedium ist somit nur durch Abgrenzung möglich. Im Ergebnis erfasst der Begriff aber nahezu jeden Online-Auftritt[1]. Zum besseren Begriffsverständnis können einige Telemedien beispielhaft hervorgehoben werden. So zählen dazu Online-Angebote wie Börsen-, Umwelt-, Verkehrs- und Wetterdaten-, Newsgroups, Chatrooms und elektronische Presse sowie auch Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen (z.B. Internet-Suchmaschinen). Das TMG richtet sich an alle Diensteanbieter einschließlich der öffentlichen Stellen, unabhängig davon, ob für die Nutzung der Dienste ein Entgelt erhoben wird. Ein Diensteanbieter wird in § 2 Satz 1 Nr. 1 TMG definiert als eine „natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“. Umfasst sind hiervon im Wesentlichen Tätigkeiten von sog. Host- und Content-Providern, etwa die Bereitstellung von Webspeicherplatz für fremde Inhalte oder die Veröffentlichung eigener redaktioneller Beiträge und Inhalte.

Das Telekommunikationsgesetz hingegen regelt sogenannte Telekommunikationsdienste. Dies sind nach der Legaldefinition von § 3 Nr. 24 TKG „in der Regel gegen Entgelt erbrachte Dienste, die ganz

[1] *Müller-Broich*, Telemediengesetz, 2012, § 13 Rn. 6.

oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen“. Das TKG betrifft nach dieser Definition im Wesentlichen die Telekommunikationsinfrastruktur sowie die hierüber erbrachten Telekommunikationsdienstleistungen des Aussendens, Übermittelns und Empfangens von Signalen. Gemeint sind damit üblicherweise Dienstleistungen des sog. Access-Providers, etwa die Internetzugangsvermittlung, die Bereitstellung eines E-Mail-Accounts oder das Betreiben eines Telefonnetzes. Das TKG regelt damit die Transportebene, ohne dass es auf die konkreten übertragenen Inhalte ankäme.

Besonders die Zuordnung der Tätigkeit von Access-Providern in die Anwendungsbereiche von TMG und TKG bereitet Schwierigkeiten. Grundsätzlich sind von der Definition der Telekommunikationsdienste gerade Angebote von Access-Providern umfasst, solange es um die reine Zugangsvermittlung im Bereich des Internets geht. Der technische Vorgang des Aussendens, Übermittelns und Empfangens ist damit als reine Transportleistung dem TKG unterworfen. Durch einen Umkehrschluss aus § 11 Abs. 3 TMG lässt sich jedoch erkennen, dass ein Access-Provider auch von den Regelungen des TMG betroffen ist, da für ihn einige Regelungen des TMG außer Acht zu bleiben haben.

Die demzufolge erforderliche Abgrenzung zwischen TKG und TMG erfolgt anhand der jeweiligen Funktion der Dienste: Sind die Infrastruktur, das Leitungsnetz oder andere technische Belange betroffen, gilt das TKG. Stehen hingegen die übertragenen Inhalte im Vordergrund und nicht der reine Übertragungsvorgang, ist das TMG anwendbar. Das bedeutet, dass bei jeder einzelnen Dienstleistung eines Access-Providers genau geschaut werden muss, ob die Transportleistung im Vordergrund steht oder der transportierte Inhalt. TMG und TKG können unter Umständen auch parallel zur Anwendung kommen, zumal das TKG gemäß § 1 Abs. 3 TMG von der Anwendung des Telemediengesetzes unberührt bleibt. Dies ist etwa dann der Fall, wenn zusätzlich zum Netzzugang auch inhaltliche Dienstleistungen wie die Möglichkeit einer E-Mail-Übertragung angeboten werden.

C. Befugnisse zur Datenspeicherung nach TMG und TKG

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung (EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.

Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.
Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

I. Datenspeicherung im Telemediengesetz

§ 12 Abs. 1 TMG legt fest, dass ein Diensteanbieter personenbezogene Daten – also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)) – zur Bereitstellung von Telemedien nur erheben und verwenden darf, soweit es gesetzliche Vorschriften, die sich ausdrücklich auf Telemedien beziehen, erlauben oder der Nutzer eingewilligt hat.

Sobald der Diensteanbieter dieses Recht ausübt, hat er den Nutzer nach § 13 Abs. 1 TMG zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung der personenbezogenen Daten in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei Verwendung eines automatisierten Verfahrens, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Bei einer Einwilligung in elektronischer Form sind weiterhin die Vorschriften des § 13 Abs. 2 TMG zu beachten. Diensteanbieter müssen sicherstellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, sowie dass der Nutzer den Inhalt der Einwilligung jederzeit abrufen und mit Wirkung für die Zukunft widerrufen kann. Hierfür ist ausreichend, dass die Einwilligungserklärung durch eine bestätigende Wiederholung des Übermittlungsbefehls durch Anklicken eines Kontrollkästchens bei gleichzeitiger zumindest auszugsweiser Darstellung der Einwilligungserklärung auf dem Bildschirm erteilt wird.[2]

Das TMG differenziert zwischen zwei Arten von personenbezogenen Daten – Bestandsdaten und Nutzungsdaten – und stellt an die Erhebung und Verwendung der jeweiligen Daten unterschiedliche Anforderungen:

[2] *Müller-Broich*, Telemediengesetz, 2012, § 13 Rn. 5.

Bestandsdaten sind Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (§ 14 Abs. 1 TMG), beispielsweise Name, Benutzerkennung oder Anschrift des Nutzers. In dieser Definition sind gleichzeitig die Voraussetzungen für die Datenspeicherung enthalten, nämlich der Zweck der Erhebung und die Erforderlichkeitsschwelle. Zu beachten ist, dass grundsätzlich ein strenger Maßstab an die Erforderlichkeit und die Zweckbindung anzulegen ist. Die Voraussetzungen, unter denen der Diensteanbieter zur Weitergabe der erhobenen Bestandsdaten befugt ist, sind in § 14 Abs. 2 TMG geregelt. Demnach darf der Diensteanbieter auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Mangels Erwähnung in dieser Aufzählung dürfen deshalb beispielsweise Bestandsdaten nicht an private Anspruchsteller herausgegeben werden, die diese zur Ahndung von Persönlichkeitsrechtsverletzungen benötigen.

Nutzungsdaten sind hingegen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (§ 15 Abs. 1 TMG). Als Beispiele werden Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien aufgeführt. Der höherrangige Art. 7 Buchstabe f der EG-Datenschutzrichtlinie lässt für eine Datenverarbeitung jedoch allgemein ein berechtigtes Interesse des für die Verarbeitung Verantwortlichen ausreichen, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Der EuGH hat in dieser Hinsicht entschieden, dass § 15 Abs. 1 TMG zu restriktiv gefasst ist, den Anforderungen der Datenschutzrichtlinie nicht gerecht wird und daher europarechtskonform ausgelegt werden muss. Eine über den Webseitenbesuch hinausgehende Speicherung von Nutzungsdaten kann daher nicht nur für die Ermöglichung und Abrechnung der Inanspruchnahme von Telemedien, sondern darüber hinaus auch bei anderen gewichtigen Gründen zulässig sein.

Explizit geregelt ist außerdem die Verwendung von Nutzungsdaten zu Abrechnungszwecken (§ 15 Abs. 4-7 TMG) geregelt. Da Hochschulen Telemedien jedoch in aller Regel nicht einzeln abrechnen, werden die Einzelheiten hier nicht dargestellt.

Des Weiteren darf der Diensteanbieter mit den Nutzungsdaten zu Werbe- und Forschungszwecken oder zur bedarfsgerechten Gestaltung der Telemedien zwar auch Nutzungsprofile erstellen, er muss aber Pseudonyme verwenden und der Nutzer darf der Erstellung eines Profils nicht widersprochen haben. Eine Zusammenführung der pseudonymisierten Daten mit weiteren Daten über den

Betroffenen darf aber nicht erfolgen. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen ausschließlich anonymisierte Nutzungsdaten übermittelt werden, § 15 Abs. 5 S. 3 TMG.

Zur Störungsabwehr oder zur Missbrauchsbekämpfung dürfen die Nutzungsdaten nur gespeichert werden, wenn tatsächliche Anhaltspunkte vorliegen, dass der betroffene Nutzer nicht das geschuldete Entgelt entrichten wird. Nach der Entscheidung des EuGH wird nun aber auch eine Verwendung zu anderen Zwecken, etwa zur Abwehr von „Denial of Service"-Angiffen, zulässig sein, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Sonderproblem: Die Behandlung von IP-Adressen im TMG

Um in den Regelungsbereich des TMG zu fallen, muss es sich bei IP-Adressen zunächst um personenbezogene Daten handeln. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 BDSG. Als bestimmbar gilt eine Person dann, wenn eine Identifikation durch die Verknüpfung verschiedener Informationen ohne unverhältnismäßigen Aufwand möglich ist. Für die Identifizierung kann auch ein Dritter eingesetzt werden. Personendaten sind somit dann bestimmbar, wenn sie persönlich oder von einem beauftragten Dritten ohne unverhältnismäßigen Aufwand in Erfahrung gebracht werden können. Die Verhältnismäßigkeit des Aufwands muss anhand des konkreten technischen und organisatorischen Kontextes im Einzelfall beurteilt werden. Eine IP-Adresse hat von sich aus noch keinen Personenbezug, möglicherweise ist durch sie jedoch eine natürliche Person bestimmbar.

Jedenfalls im Fall von statischen IP-Adressen, die den jeweiligen Anschlüssen auf Dauer zugewiesen werden, wird von einem Personenbezug ausgegangen, da über die IP-Adresse mittels einer Whois-Abfrage verhältnismäßig leicht festgestellt werden kann, wer hinter der Adresse steht.

Die Beurteilung von dynamischen IP-Adressen gestaltet sich hingegen schwieriger. Während ein Access-Provider, der noch über die Logdateien verfügt, wann er welchem Nutzer welche IP-Adresse zugewiesen hat, die dynamische IP-Adresse mit geringem Aufwand mit dem Zeitstempel verknüpfen und somit den jeweiligen Nutzer identifizieren kann, besteht diese Möglichkeit für Host- und Content-Provider nicht ohne weiteres.

Ob dynamische IP-Adressen nicht nur gegenüber Access-Providern, sondern auch allen anderen Kommunikationspartnern personenbezogen sind, war lange Zeit umstritten. Einige gingen von einem absoluten Verständnis der Bestimmbarkeit aus, sodass es ausreichend sein sollte, wenn irgendein Dritter die Möglichkeit besaß, den Personenbezug herzustellen. Zu dem insofern heranzuziehenden Weltwissen gehörte natürlich auch das Wissen des Access-Providers, sodass bei IP-Adressen in der

Regel von einem Personenbezug auszugehen sein sollte. Die meisten befürworteten jedoch ein relatives Begriffsverständnis, demzufolge es auf die konkreten Kenntnisse und Fähigkeiten der datenverarbeitenden Stelle ankäme. Das Wissen Dritter war insoweit nur relevant, wenn es ohne unverhältnismäßigen Aufwand vernünftigerweise für die verarbeitende Stelle erreichbar war.

Diese Frage ist mittlerweile durch eine Entscheidung des EuGH vom 19. Oktober 2016 zugunsten einer Variante der relativen Ansicht entschieden worden. Danach soll nicht jedes Wissen eines hypothetischen Dritten ausreichen, um Personenbezug herzustellen. Eine Bestimmbarkeit ist aber dann zu bejahen, wenn Host- und Content-Betreibern rechtliche Mittel zur Verfügung stehen, die es ihnen erlauben, die hinter einer IP-Adresse stehende Person bestimmen zu lassen (z.B. im Falle von Cyberattacken oder bei offensichtlichen Urheberrechtsverstößen[3]).

Weiterhin offen bleibt die Frage des Personenbezugs bei IPv6-Adressen. Da eine dynamische Verteilung von IP-Adressen unter diesem Protokoll nicht mehr notwendig ist, besteht theoretisch die Möglichkeit der zielgenauen Identifizierung eines jeden internetfähigen Endgeräts. Es ist jedoch nicht auszuschließen, dass Access-Provider auch IPv6-Adressen dynamisch verteilen werden, um etwa statische Adressen als Premiumdienste vermarkten zu können. Gegen einen grundsätzlichen Personenbezug bei IPv6-Adressen spricht auch, dass sog. Privacy Extensions dem Nutzer ermöglichen, eine Identifizierbarkeit wieder aufzuheben. Solche Extensions sind bei gängigen Betriebssystemen wie Windows, MacOS und iOS mittlerweile ab Werk eingeschaltet und lassen sich bei Linux und Android eigenständig einschalten. Es spricht daher vieles dafür, die Maßstäbe des EuGH für dynamische IPv4-Adressen auch bei IPv6-Adressen anzuwenden.

Vor allem für Access-Provider ist die Differenzierung zwischen statischen und dynamischen Adressen dann auch in weiterer Hinsicht relevant. Statische IP-Adressen werden nach herrschender Ansicht als Bestandsdaten angesehen, so dass die Regelungen des § 14 TMG anwendbar sind. Dynamische IP-Adressen stellen hingegen Nutzungsdaten dar und unterfallen daher den Bestimmungen von § 15 TMG.

Sonderproblem: Verwendung von Cookies

Auch die Verwendung von Cookies ist nach dem TMG problematisch, also die Erstellung einer Datei durch einen Diensteanbieter, in der verschiedene Informationen des Aufrufs der Webseite durch den Nutzer gespeichert werden. Diese Datei wird lokal auf dem Rechner des Nutzers gespeichert. Bei einem erneuten Aufruf des Dienstes werden die bisher gesetzten Cookies wiederum an den Diensteanbieter übermittelt, so dass diesem einzelne Daten aus der letzten Sitzung zur Verfügung

[3] dazu schon Handlungsempfehlung des DFN “Auskunftsansprüche Privater gegen Internet-Access-Provider”

stehen. Hiermit wird etwa eine „automatisierte“ Eingabe des Passworts ermöglicht, sofern der Nutzer stets denselben Rechner verwendet.

Für die Anwendbarkeit des TMG ist entscheidend, ob es sich bei einem Cookie um ein personenbezogenes Datum handelt. Dies lässt sich nur unter Berücksichtigung des konkreten Verwendungszusammenhangs beantworten: Ermöglicht der Cookie die Identifizierung des Nutzers, ist der Anwendungsbereich des TMG eröffnet und dessen Datenschutznormen müssen beachtet werden. Bereits in dem Anlegen der Datei liegt ein datenschutzrechtlich relevantes Speichern von personenbezogenen Daten. Es bedarf also nach § 12 TMG einer Einwilligung des Nutzers, sofern die Datenverarbeitung nicht von einer gesetzlichen Erlaubnisnorm gedeckt ist. Auch hier gelten die zuvor genannten Pflichten für Diensteanbieter gem. § 13 TMG.

Ob Cookies als Bestandsdaten i.S.d. § 14 TMG oder als Nutzungsdaten nach § 15 TMG einzuordnen sind, hängt von dem geplanten Einsatz ab. Bei einer längerfristigen Speicherung von Cookies (mehrere Monate oder Jahre) besteht die Vermutung eines Bestandsdatums, da der Zusammenhang mit einer einzelnen Nutzung des Mediums verloren geht. Letztlich kann die Frage aber unbeantwortet bleiben, da weder § 14 TMG noch § 15 TMG die Speicherung von Cookies zur erleichterten Nutzung eines Dienstes zulassen. Nach § 14 TMG dürfen Bestandsdaten nur verwendet werden, soweit sie für die Begründung oder inhaltliche Ausgestaltung des Vertragsverhältnisses erforderlich sind. Vorherrschend ist hier eine enge Auslegung der Erforderlichkeit, so dass die Speicherung für die Vertragsabwicklung unerlässlich sein muss. Dies ist bei einer Speicherung in einem Cookie nicht der Fall. Nach § 15 Abs. 4 TMG sind Nutzungsdaten ohnehin zu löschen, sofern sie zu Abrechnungszwecken nicht erforderlich sind.

Bei bestimmten Cookies kann es sich aber auch um ein zulässiges Pseudonym i.S.d. § 15 Abs. 3 TMG handeln, soweit eine Zuordnungsmöglichkeit ausgeschlossen ist. Sobald eine Webseite jedoch die Möglichkeit zur Anmeldung oder Registrierung anbietet, wird von einer solchen Zuordnungsmöglichkeit ausgegangen werden müssen. Pseudonymisierte Cookies dürfen auch ohne Einwilligung des Nutzers gesetzt werden, dieser muss jedoch hierauf hingewiesen werden und die Möglichkeit haben, der Setzung solcher Cookies zu widersprechen (Opt-Out), §§ 13 Abs. 1 S. 2, 15 Abs. 3 S. 2 TMG.

Insgesamt ist die Rechtslage beim Einsatz von Cookies zurzeit nicht eindeutig geklärt, da fraglich ist, ob die europäische E-Privacy-Richtlinie im nationalen Recht hinreichend umgesetzt wurde. Diese soll so zu verstehen sein, dass Cookies nur nach ausdrücklicher Einwilligung des Nutzers (Opt-In) und entsprechender Information gesetzt werden dürfen. Ein solch strenges Erfordernis ergibt sich aus

dem Wortlaut des TMG nicht, dennoch gehen sowohl die Bundesregierung und die EU-Kommission davon aus, dass das deutsche Recht den Anforderungen der E-Privacy-Richtlinie gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder teilen diese Auffassung jedoch nicht und auch im Übrigen gibt es zahlreiche Stimmen, die eine Anpassung des deutschen Rechts fordern oder die Richtlinie mangels ausreichender Umsetzung sogar unmittelbar anwenden wollen.

Angesichts dieser Streitfragen ist es für Hochschulen empfehlenswert, Cookies nur bei der vorherigen Erteilung einer Einwilligung des Nutzers im Opt-In-Verfahren einzusetzen, um sich keinen Risiken auszusetzen. Eine Einwilligung ist allerdings auch nach der E-Privacy-Richtlinie nicht erforderlich, wenn der Einsatz des Cookies unbedingt erforderlich ist, um den vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen, was insbesondere Authentifizierungs-Cookies, Sicherheits-Cookies oder Cookies, mit denen Nutzereingaben verwaltet werden, betrifft. Zudem ist der Nutzer gemäß § 13 Abs. 1 Satz 2 TMG über die Einzelheiten des automatisierten Verfahrens zu unterrichten, wenn dadurch eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet wird. Bei der Installation und dem Auswerten der Cookies handelt es sich um einen automatisierten Vorgang. Da die Cookies auch der Identifizierung des Nutzers dienen, fallen sie unter die Unterrichtungspflicht.

II. Datenspeicherung im Telekommunikationsgesetz

Auch das TKG differenziert zwischen zwei Arten von Daten – Bestands- und Verkehrsdaten –, an deren Speicherung wie im TMG unterschiedliche rechtliche Anforderungen gestellt werden.

Bestandsdaten sind in § 3 Nr. 3 TKG als Daten eines Teilnehmers definiert, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Diese dürfen erhoben und verwendet werden, soweit es zur Erreichung dieser Zwecke erforderlich ist. Da die Definition keine konkreten Beispiele enthält und nicht abschließend ist, orientiert sich die Beurteilung des Datums immer am konkreten Vertragsverhältnis. Üblicherweise gehören Name, Vorname und Anschrift des Teilnehmers hierzu.

Verkehrsdaten sind dagegen Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, § 3 Nr. 30 TKG. Sie dürfen nur dann erhoben und verwendet werden, wenn dies für die im TKG ausdrücklich zugelassenen Zwecke erforderlich ist. Hierunter fallen u. a. Nummer oder Kennung der beteiligten Anschlüsse oder Endeinrichtungen, personenbezogene Berechtigungskennungen, Beginn und Ende der jeweiligen Verbindungen nach Datum und Uhrzeit und die übermittelten Datenmengen.

Zu beachten ist, dass ein Datum sowohl Bestands- als auch Verkehrsdatum sein kann, zumal es bei der Beurteilung auf den konkreten Kontext der Datenverarbeitung im Einzelfall ankommt.

1. Speicherungsrechte von Bestandsdaten

Gemäß § 95 Abs. 1 TKG dürfen Bestandsdaten erhoben und verwendet werden, soweit dies zur Erreichung eines der in § 3 Nr. 3 TKG genannten Zwecke erforderlich ist, also für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses. Die Übermittlung dieser Daten an Dritte ist nur zulässig, wenn eine gesetzliche Regelung dies erlaubt oder der Teilnehmer in die Übermittlung eingewilligt hat. Solch eine Einwilligung ist ebenfalls notwendig, wenn die Bestandsdaten zur Beratung, zur Werbung für eigene Angebote und zur Marktforschung verwendet werden sollen. Doch selbst dann dürfen die Verkehrsdaten nur so weit verwendet werden, wie dies für die genannten Zwecke erforderlich ist. Nach dem Ende des Vertragsverhältnisses müssen die Bestandsdaten mit Ablauf des auf die Beendigung folgenden Kalenderjahres gelöscht oder – in Ausnahmefällen – gesperrt werden, § 95 Abs. 3 TKG.

2. Speicherungsrechte von Verkehrsdaten

Für Verkehrsdaten enthält § 96 TKG Regeln über deren Erhebung und Verwendung. Zu beachten ist, dass ausschließlich die im Katalog des Absatz 1 aufgezählten Arten von Daten erhoben und verwendet werden dürfen, andere Verkehrsdaten müssen außer Acht gelassen werden. § 96 Abs. 1 Nr. 5 TKG enthält allerdings einen Auffangtatbestand, nach dem auch „sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten“ erhoben und verwendet werden dürfen.

Grundsätzlich sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen. Ausnahmen von der Löschungspflicht müssen gesetzlich geregelt sein, wie es beispielsweise in § 97 TKG (Entgeltermittlung und Entgeltabrechnung), § 99 TKG (Einzelverbindungsnachweis), § 100 TKG (Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten) und § 101 TKG (Mitteilen ankommender Verbindungen) geschehen ist. Soll die Speicherung und Verwendung auf eine Norm außerhalb des TKG gestützt werden, ist dies nur möglich, wenn diese sich ausdrücklich auf Telekommunikationsvorgänge bezieht (§ 88 Abs. 3 S. 3 TKG). Generell sind diese Ausnahmen jedoch sehr eng und erfordern durchgehend die Einhaltung der Erforderlichkeitsgrenze. Diese gilt insbesondere für die Art der benötigten Daten und den Speicherungszeitraum.

3. Sonderproblem: Die Behandlung von IP-Adressen im TKG

Schwierig ist wieder die Beurteilung, in welchem Umfang das TKG die Speicherung von IP-Adressen erlaubt. Auch im TKG sind statische IP-Adressen als Bestandsdaten und dynamische IP-Adressen als Verkehrsdaten anzusehen. Im Hinblick auf einen konkreten Kommunikationsvorgang sind aber auch statische IP-Adressen, jedenfalls in Verbindung mit sonstigen Daten zur konkreten Verbindung, als Verkehrsdaten einzustufen und unterliegen insofern der strengeren Regelung des § 96 TKG. Problematisch ist deshalb vor allem die Speicherung von IP-Adressen im Rahmen von Kommunikationsvorgängen, wobei sich insbesondere aus § 97 TKG (Entgeltermittlung und Entgeltabrechnung) und aus § 100 TKG (Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten) Rechte zur Speicherung ergeben können.

Da Internetzugänge außerhalb des Mobilfunkbereichs heutzutage üblicherweise mit einer Flatrate angeboten werden, ist eine Protokollierung der einzelnen Verbindungen für Abrechnungszwecke nicht mehr erforderlich, sodass § 97 TKG in dem Bereich keine praktische Relevanz mehr zukommt. Dies gilt für Hochschulen in besonderem Maße, in denen der Zugang zum Hochschulnetz für Mitglieder der Hochschule keinem besonderen Entgelt unterliegt. Die dynamische IP-Adresse ist folglich unverzüglich nach Beendigung der Verbindung zu löschen, sofern nicht ein anderer Erlaubnistatbestand einschlägig ist.

Ein weiteres, praktisch sehr bedeutsames Speicherrecht ergibt sich insbesondere aus § 100 Abs. 1 TKG. Zum Erkennen, Eingrenzen und Beseitigen von Störungen oder Fehlern an den Telekommunikationsanlagen dürfen IP-Adressen erhoben und verwendet werden, soweit es zu diesen Zwecken erforderlich ist. Wenn dynamische IP-Adressen vergeben worden sind, wird dem Provider nach der Rechtsprechung (BGH, Urt. v. 3.7.2014 – III ZR 391/13; BGH, Urt. v. 13.1.2011 – III ZR 146/10) eine Frist von sieben Tagen nach Ende der jeweiligen Internetverbindung zugestanden, in der die IP-Adresse in Verbindung mit den Anfangs- und Enddaten der Verbindung auch vorsorglich ohne konkrete Anhaltspunkte für eine Störung gespeichert werden darf. Dies gilt jedenfalls, solange es nach dem Stand der Technik keine anderen Möglichkeiten gibt, um Störungen der Telekommunikationsanlagen effektiv zu erkennen, einzugrenzen und notfalls zu beseitigen. Nach Ablauf der Frist müssen die Daten gelöscht werden, wenn bis zu diesem Zeitpunkt keine Störung gefunden wurde und die IP-Adresse nicht zu anderen Zwecken benötigt wird, für die eine gesonderte Speicherungsbefugnis existiert, beispielsweise zur Entgeltabrechnung. Im Falle einer Störung müssen die Daten gelöscht werden, sobald diese beseitigt wurde. Solange die Datenspeicherung also erforderlich ist, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken, ist eine siebentägige Speicherung zulässig.

Die Rechte des Access-Providers beim Missbrauch seiner Telekommunikationsnetze durch eine rechtswidrige Inanspruchnahme – beispielsweise zur Leistungserschleichung, zum Hacking in andere Netzwerke oder zur Umgehung der Gebührenerfassung – regelt § 100 Abs. 3 TKG. Hiernach darf der Diensteanbieter IP-Adressen erheben und verwenden, soweit es für das Aufdecken und das Unterbinden der rechtswidrigen Inanspruchnahme notwendig ist. Dem Provider müssen für eine solche Speicherung allerdings tatsächliche Anhaltspunkte vorliegen. Eine verdachtsunabhängige (präventive) Speicherung von IP-Adressen zur Missbrauchsbekämpfung ist nicht zulässig. Entscheidet sich ein Access-Provider, ein Verfahren zum Aufdecken und Unterbinden rechtswidriger Inanspruchnahme einzuführen oder ein hierfür bestehendes Verfahren zu ändern, hat er gemäß § 100 Abs. 3 Satz 5 TKG die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz zu informieren. Diese Informationspflicht gilt nur für das technische Verfahren als solches, nicht jedoch für Einzelfallmaßnahmen gegen einzelne Nutzer oder reine Tests. Die konkrete Missbrauchsverfolgung fällt also nicht unter diese Verpflichtung. Informiert werden muss ferner lediglich über die Aufnahme und Abänderung des Verfahrens, nicht jedoch über die einzelnen Mittel des Verfahrens oder den Abbruch der Überwachung. Enthalten sollte die Meldung die Punkte, die im Katalog des § 4e BDSG aufgezählt sind, also insbesondere Angaben zur Identifikation des verantwortlichen Diensteanbieters, den Zweck des Verfahrens und das Verfahren in groben Zügen.

Weitere Speicherpflichten und damit einhergehend auch Speicherrechte mit Bezug zum Internetzugang sind zudem in §§ 113a ff. TKG (Vorratsdatenspeicherung von Verkehrsdaten) geregelt. Diese gelten aber ausschließlich für Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer.

Münster, Dezember 2016

Forschungsstelle Recht im DFN

Die Forschungsstelle Recht im DFN ist ein Projekt an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung unter Leitung von Prof. Dr. Thomas Hoeren, Leonardo-Campus 9, D-48149 Münster, E-Mail: recht@dfn.de.