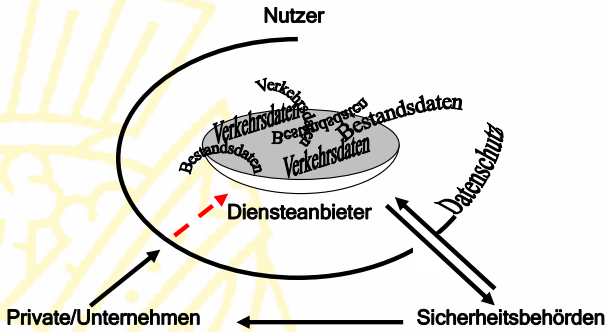
Informations- und Datenschutzrecht II

Cybersurveillance -

Vorratsdatenorganisation? (FÖR-Terminologie)

Cybersurveillance | Datenspeicherung | Vorratsdatenorganisation | Prepaid-Kundendaten | Auskunftsrechte Dritter



Zum einen fordert das **Datenschutzinteresse (P-pas**) des Nutzers, dass

- grundsätzlich keine Daten gespeichert werden. Wenn die Speicherung dennoch erforderlich ist, dass so wenige wie möglich gespeichert werden (§ 3a BDSG: Grundsatz der Datenvermeidung und Datensparsamkeit).
- soweit Daten gespeichert werden, die Daten grundsätzlich nicht übermittelt werden.

Zum anderen könnte das **Sicherheitsinteresse** (**P-akt**) des Staates erfordern, dass

- grundsätzlich alle Daten der Bürger organisiert und Zugriffe des Staates ermöglicht werden.

Darüber hinaus haben Dritte als natürliche oder juristische Personen ein Interesse (**P-akt**), dass

- sie im Einzelfall zur **Verfolgung der Verletzung ihrer Rechtsgüter** auf die gespeicherten Daten wie der Staat zugreifen können.

Schließlich sind Dienstanbieter daran interessiert, dass

- sie die Kosten und den Aufwand der Speicherung nicht tragen zu müssen (**P-pas Inf**).

N ist – nach seiner Überzeugung – genauso rechtstreu wie prozessscheu. Er tauscht mit der Flatrate Musikdateien und lädt sie „herunter“. Die Einzelheiten der urheberrechtlichen Würdigung solcher Tauschbörsen sind ihm nicht einfach durchschaubar – und deshalb möchte er jedes Prozessrisiko vermeiden. Als er deshalb in einer verbreiteten Computerzeitschrift liest, dass ein Provider mit beträchtlicher Marktmacht die Praxis übt, beim Surfen anfallenden Daten (etwa die (dynamische) IP-Nummer, Datum, Uhrzeit und Länge der Internetsitzung) zu speichern, erschrickt er. Er wendet sich an de Aufsichtsbehörde, das Regierungspräsidiums Darmstadt, um diese Organisation der Daten datenschutzrechtlich überprüfen zu lassen.

Schema

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

1 a)	P-aktiv	
1 b)	P-aktiv Informationskosten	
2	Personal-passiv Datenschutz	
3.	Objekt	
4	KausalZ	
5.	Qualinf	
6.	Verfahren	
7.	Rechtfertigung/Verhältnismäßigkeit	

Kompetenz des Regierungspräsidiums Darmstadt (1)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

➢ Access-Provider als Diensteanbieter des TDG

Das Regierungspräsidium Darmstadt trat als Datenschutzaufsichtsbehörde im nicht öffentlichen Bereich nach § 1 Abs. 2 TDDSG i.V.m. § 38 BDSG auf.

§ 1 Abs. 2 TDDSG [Geltungsbereich]
Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.
§ 38 Abs. 6 BDSG [Aufsichtsbehörde]
Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.
§ 1 Nr. 1 Verordnung zur Regelung der Zuständigkeiten nach dem BDSG und anderen Gesetzen zum Datenschutz vom 10.2.2005, Land Hessen,
Das Regierungspräsidium Darmstadt ist zuständige Behörde
1. nach § 38 Abs. 6 des Bundesdatenschutzgesetzes für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes, (…)

Kompetenz des Regierungspräsidiums Darmstadt (2)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

➢ Access-Provider als Diensteanbieter des TKG

Die zuständige Aufsichtsbehörde über datenschutzrechtliche Fragen des Access-Provider als Diensteanbieter des TKG wäre der Bundesbeauftragte für den Datenschutz, der neben der Regulierungsbehörde die Einhaltung der datenschutzrechtlichen Vorschriften sicherstellt.

§ 115 Abs. 1 und 4 TKG [Kontrolle und Durchsetzung von Verpflichtungen]
(1) Die Regulierungsbehörde kann Anordnungen und andere geeignete Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen (...) sicherzustellen.(…)
(4) Soweit für die geschäftsmäßige Erbringung von Telekommunikations-diensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, **tritt bei den Unternehmen an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend den §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes**. (…)

Qualität der Informationstechnik

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

§ 3 Abs. 3 und 4 BDSG
(3) **Erheben** ist das Beschaffen von Daten über den Betroffenen.
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. **Speichern** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung, (...)

→ Erhebung und Speicherung von dynamischen IP-Adressen durch einen Telekommunikationsdiensteanbieter

Kausal/Zweck: Qualität der Abrechnung (1)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

§ 45 TKG [Kundenschutzverordnung]
(1) Die Bundesregierung wird ermächtigt, zum besonderen Schutz der Endnutzer (Kunden), insbesondere der Verbraucher, durch Rechtsverordnung (…) Rahmenvorschriften für die Inanspruchnahme von Telekommunikations-diensten und für die Sicherstellung der Genauigkeit und Richtigkeit der Entgeltabrechnungen zu erlassen. (…)

Kausal/Zweck: Qualität der Abrechnung (2)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

§ 15 Telekommunikationskundenschutzverordnung TKV [Rechnungsstellung]
(1) **Soweit der Kunde mit anderen Anbietern von Telekommunikationsdienst-leistungen für die Öffentlichkeit nicht etwas anderes vereinbart, ist ihm von seinem Anbieter des Zugangs zum öffentlichen Telekommunikationsnetz (Rechnungsersteller) eine Rechnung zu erstellen, die auch die Entgelte für Verbindungen ausweist, die durch Auswahl anderer Anbieter von Netzdienst-leistungen über den Netzzugang des Kunden entstehen**. Die Rechnung muß die Namen, ladungsfähigen Anschriften und kostenfreie Servicenummer der einzelnen Anbieter von Netzdienstleistungen und zumindest die Gesamthöhe der auf sie entfallenden Entgelte erkennen lassen. § 14 bleibt unberührt. Die Zahlung an den Rechnungsersteller hat befreiende Wirkung auch gegenüber den anderen auf der Rechnung aufgeführten Anbietern. Zum Zwecke der Durchsetzung der Forderungen gegenüber ihren Kunden hat der Rechnungsersteller den anderen Anbietern die erforderlichen Bestands- und Verbindungsdaten zu übermitteln. (….)

Kausal/Zweck: Qualität der Abrechnung (3)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

§ 16 TKV [Nachweis der Entgeltforderung]
(1) Erhebt der Kunde bei Telekommunikationsdienstleistungen für die Öffentlichkeit, die auf den für die Sprachkommunikation für die Öffentlichkeit vorgesehenen Telekommunikationsnetzen erbracht werden, **Einwendungen gegen die Höhe der ihm in Rechnung gestellten Verbindungsentgelte**, so ist das Verbindungsaufkommen unter Wahrung des Schutzes der Mitbenutzer auch ohne Auftrag zur Erteilung eines Einzelentgeltnachweises **nach den einzelnen Verbindungsdaten aufzuschlüsseln** und eine technische Prüfung durchzuführen, deren Dokumentation dem Kunden auf Verlangen vorzulegen ist.
(2) **Soweit aus technischen Gründen oder auf Wunsch des Kunden keine Ver-bindungsdaten gespeichert oder gespeicherte Verbindungsdaten auf Wunsch des Kunden oder auf Grund rechtlicher Verpflichtung gelöscht wurden,** trifft den Anbieter keine Nachweispflicht für die Einzelverbindungen, wenn der Kunde in der Rechnung auf die nach den gesetzlichen Bestimmungen gelten-den Fristen für die Löschung gespeicherter Verbindungsdaten in drucktechnisch deutlich gestalteter Form hingewiesen wurde. (…)

Kausal/Zweck: Qualität der Abrechnung (4)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

§ 16 TKV [Nachweis der Entgeltforderung]
(3) Dem Anbieter obliegt der Nachweis, **die Leistung bis zu der Schnittstelle, an der der allgemeine Netzzugang dem Kunden bereitgestellt wird, technisch einwandfrei erbracht und richtig berechnet zu haben**. Ergibt die technische Prüfung Mängel, die die beanstandete Entgeltermittlung beeinflußt haben könnten, wird widerleglich vermutet, daß die Verbindungsentgelte des Anbieters unrichtig ermittelt sind. Ist der Nachweis erbracht, daß der Netzzugang in vom Kunden nicht zu vertretendem Umfang genutzt wurde, oder rechtfertigen Tatsachen die Annahme, daß die Höhe der Verbindungsentgelte auf Manipulationen Dritter an öffentlichen Telekommunikationsnetzen zurückzuführen ist, ist der Anbieter nicht berechtigt, die betreffenden Verbindungsentgelte vom Kunden zu fordern.

Kausal/Zweck: Qualität der Abrechnung (5)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

Legaldefinition „Verkehrsdaten“ (synomym mit „Verbindungsdaten“):

§ 3 Nr. 30 TKG [Begriffsbestimmmungen]
30. **„Verkehrsdaten“** Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden;

- Der (Kunden-)Schutz des Äquivalenzinteresses geht nur soweit, wie der (Kunden-) Schutz des Integritätsinteresses reicht (und umgekehrt).
- Der Schutz des Äquivalenzinteresses an der Speicherung von „Verkehrsdaten“ realisiert sich in der Nachweispflicht des Verbindungsaufkommens.
- Die Nachweispflicht kann zugunsten des Schutzes des Integritätsinteresses des Kunden („auf Wunsch des Kunden“) wegfallen

Kausal/Zweck: Qualität der Abrechnung (6)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

Ist die Speicherung der IP-Adresse auch bei Flatrate-Kunden zur Abrechnung erforderlich?

- Argumentation mit der Qualität der Abrechnung

§ 6 TDDSG [Nutzungsdaten]
(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit dies **erforderlich** ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). (…)
(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer **erforderlich** sind (Abrechnungsdaten). (…)

Regierungspräsidium Darmstadt: Die zusätzliche Möglichkeit der Inanspruchnahme kostenpflichtiger Dienste rechtfertigt die Speicherung

Kausal/Zweck: Datensicherheit (1)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

- Argumentation mit der Datensicherheit (1)

§ 9 BDSG [Technische und organisatorische Maßnahmen]
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage zu § 9 Satz 1 BDSG
(…)
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verar-beitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**), (…)

Kausal/Zweck: Datensicherheit (2)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorganisation Prepaid-Kundendaten Auskunftsrechte Dritter

- Argumentation mit der Datensicherheit (2)

Durch die Speicherung der IP-Adresse sollen mögliche Angreifer ermittelt werden können. Für die Zulässigkeit der Speicherung könnte vorgebracht werden, dass die Datensicherungsmaßnahme nicht von der Erforderlichkeit der Datenspeicherung für Abrechnungszwecke abhängen kann. Ob die Zulässigkeit § 9 BDSG entnommen werden kann, kann hinterfragt werden, da dies über den Zweck des § 9 BDSG hinausgeht, der dem Schutz der eigenen Datenorganisation dient.

Im Ergebnis ist ein Konflikt von Kundenschutz und Datenschutz und Datensicherheit festzustellen. Dies führt zu der Frage des Verhält-nisses von Kundenschutz (Äquivalenzinteresse), Datenschutz (individuelles Integritätsinteresse) und Datensicherheit (kollektives Integritätsinteresse). Die vorliegende Entscheidung hat sich für den Vorrang von Kundenschutz und Dat-ensicherheit vor Datenschutz entschieden.

Kausal/Zweck: Ergebnis

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorgansisation Prepaid-Kundendaten Auskunftsrechte Dritter

Zivilrechtliches Verfahren:

- „Fortsetzung“ nach der Entscheidung des RP Darmstadt
- Durchsetzung (?) eines Unterlassungsanspruches

→ Entscheidung des AG Darmstadt für 30.06.2005 angekündigt.

Integration (geänderter) Vorschriften der TKV in das TKG:

§ 45h TKG-Gesetzentwurf vom 7.4.2005
[Rechnungsinhalt, Teilzahlungen]
(1) Soweit ein Anbieter von Telekommunikationsdiensten für die Öffentlichkeit dem Endnutzer eine Rechnung erstellt, die auch Entgelte für Telekommunikationsdienste, Leistungen nach § 78 Abs. 2 Nr. 3 TKG und telekommunikationsgestützte Dienste anderer Anbieter ausweist, die über den Netzzugang des Endnutzers in Anspruch genommen werden, muss die Rechnung dieses Anbieters die Namen, ladungsfähigen Anschriften und kostenfreien Kundendiensttelefonnummern der einzelnen Anbieter von Netzdienstleistungen und zumindest die Gesamthöhe der auf sie entfallenden Entgelte erkennen lassen. § 45e bleibt unberührt. Zahlt der Endnutzer den Gesamtbetrag der Rechnung an den rechnungsstellenden Anbieter, so befreit ihn diese Zahlung von der Zahlungsverpflichtung auch gegenüber den anderen auf der Rechnung aufgeführten Anbietern.
(2) Hat der Endnutzer vor oder bei der Zahlung nichts Anderes bestimmt, so sind Teilzahlungen des Endnutzers an den rechnungsstellenden Anbieter auf die in der Rechnung ausgewiesenen Forderungen nach ihrem Anteil an der Gesamtforderung der Rechnung zu verrechnen.
(3) Das rechnungsstellende Unternehmen muss den Rechnungsempfänger in der Rechnung darauf hinweisen, dass dieser berechtigt ist, begründete Einwendungen gegen einzelne in der Rechnung gestellte Forderungen zu erheben.

Erneute Novellierung des TKG (2)

§ FÖR ONLINE

Cybersurveillance **Datenspeicherung** Vorratsdatenorgansisation Prepaid-Kundendaten Auskunftsrechte Dritter

Integration (geänderter) Vorschriften der TKV in das TKG:

§ 45i TKG-Gesetzentwurf vom 7.4.2005 [Beanstandungen]
(1) Beanstandet ein Endnutzer innerhalb der mit dem Anbieter von Telekommunikationsdiensten für die Öffentlichkeit vereinbarten Frist und in der mit ihm vereinbarten Form die ihm erteilte Abrechnung, so ist in der Regel innerhalb eines Monats das in Rechnung gestellte Verbindungsaufkommen durch den Anbieter unter Wahrung der datenschutzrechtlichen Belange etwaiger Mitbenutzer des Anschlusses in der Form eines Einzelverbindungsnachweises aufzuschlüsseln und eine technische Prüfung durch-zuführen. Der Endnutzer kann verlangen, dass ihm der Einzelverbindungsnachweis und die Ergebnisse der technischen Prüfung vorgelegt werden. Die Regulierungsbehörde veröffentlicht, welche Verfahren zur Durchführung der technischen Prüfung geeignet sind.
(…)
(4) Soweit der Endnutzer nachweist, dass ihm die Inanspruchnahme von Leistungen des Anbieters nicht zugerechnet werden kann, hat der Anbieter keinen Anspruch auf Entgelt gegen den Endnutzer. Der Anspruch entfällt auch, soweit Tatsachen die Annahme recht-fertigen, dass Dritte durch unbefugte Veränderungen an öffentlichen Telekommunikationsnetzen das in Rechnung gestellte Verbindungsentgelt beeinflusst haben.

Gemeinsame Abrechnung?

- Aktuelle TKV: Anschlussanbieter ist verpflichtet, auch Dienste alternativer Anbieter mit abzurechnen
- TKG-Entwurf: Berücksichtigung alternativer Anbieter „soweit“ (§ 45h Abs. 1 TKG-Entwurf) (überhaupt?) gemeinsame Rechnung erstellt wird

→ Gemeinsame Abrechnung im Ermessen des Anschlussanbieters?

→ Konsequenzen für Wettbewerb?

Eine Vorratsdatenorganisation (herkömmlich: Vorratsdaten-speicherung)speicherung ist dadurch gekennzeichnet, dass

- die Speicherung (temporal) über den eigentlichen Zweck hinaus und/oder
- für weitere Zwecke als für den ursprünglichen Zweck (Zweck durch Vertrag inter partes konturiert – siehe das Beispiel der Organisation von Prepaid-Kundendaten) der Erhebung erfolgt.

- Recht: Recht auf informationelle Selbstbestimmung:

  Entscheidung, wie lange und wofür Daten gespeichert werden sollen.
- Eingriff: Überwachung durch Datenspuren ermöglicht
- Rechtfertigung: (1) …

  (2)…

  (3) Abwägung von Schwere des Eingriffs in das Eingriffsrechtsgut mit der Qualität des Schutzes für das Rechtfertigungsrechtsgut erforderlich

- Gesetzesvorbehalt oder Notwendigkeit der Einwilligung:

§ 4 Abs. 1 BDSG [Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung]
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

- Datenvermeidung und Datensparsamkeit

§ 3a BDSG [Datenvermeidung und Datensparsamkeit]
Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Durchbrechung datenschutzrechtlicher Prinzipien? (2)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

➢Datensicherheit

§ 9 BDSG [Technische und organisatorische Maßnahmen]
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

➢Auskunftspflicht

§ 6c BDSG [Mobile personenbezogene Speicher- und Verarbeitungsmedien]
(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung (…) Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, **muss den Betroffenen**
1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

Spezifikation der Daten

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

§ 3 TKG [Begriffsbestimmungen]
(…)
3. "Bestandsdaten" Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden;
19. "Standortdaten" Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikations-dienstes für die Öffentlichkeit angeben; (…)
30. "Verkehrsdaten" Daten, die bei der Erbringung eines Telekommunikations-dienstes erhoben, verarbeitet oder genutzt werden;

Völkerrecht (1)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

Regelungen zur Datenspeicherung in der CCC:

Article 20 - Real-time collection of traffic data
1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
a. collect or record through application of technical means on the territory of that Party, and
b. compel a service provider, within its existing technical capability, to:
i. collect or record through application of technical means on the territory of that Party, or
ii. co-operate and assist the competent authorities in the collection or recording of,
traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Völkerrecht (2)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

Regelungen zur Datenspeicherung in der CCC:

Article 14 - Scope of procedural provisions
1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings. (…)

Article 15 - Conditions and safeguards
1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

→ Keine Bestimmungen von Mindest- und/oder Höchstspeicherfristen, Zweckbindung

Europarecht (1)

Sektorspezifische Datenschutzrichtlinie (2002/58/EG):

Art. 15 Abs. 1 Datenschutzrichtlinie
(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die **nationale Sicherheit**, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. **Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden.** Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

→ Regelung einer Vorratsdatenorganisation den Mitgliedstaaten freigestellt.

EU-Rahmenbeschluss (1)

Art. 1 EU
Durch diesen Vertrag gründen die HOHEN VERTRAGSPARTEIEN untereinander eine EUROPÄISCHE UNION, im Folgenden als "Union" bezeichnet.

Art. 34 Abs. 2 lit b) EU
Der Rat ergreift Maßnahmen und fördert in der geeigneten Form und nach den geeigneten Verfahren, die in diesem Titel festgelegt sind, eine Zusammenarbeit, die den Zielen der Union dient. Hierzu kann er auf Initiative eines Mitgliedstaats oder der Kommission einstimmig (...)
b) **Rahmenbeschlüsse zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten annehmen.** Rahmenbeschlüsse sind für die Mitgliedstaaten hinsichtlich des **zu erreichenden Ziels verbindlich**, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Sie sind nicht unmittelbar wirksam;

EU-Rahmenbeschluss (2)

Entwurf eines Rahmenbeschlusses der EU vom 24.05.2005:

Art. 1 Abs. 1 des Rahmenbeschluss-Entwurfs vom 24.05.2005 [Geltungsbereich und Ziel]
(1) Mit diesem Rahmenbeschluss soll die justizielle Zusammenarbeit in Strafsachen erleichtert werden, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsspeicherung von Kommunikationsdaten, die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, für die Zwecke der Untersuchung, Feststellung und Verfolgung von Straftaten angeglichen werden.
(...)

EU-Rahmenbeschluss (3)

Entwurf eines Rahmenbeschlusses der EU vom 24.05.2005:

Art. 2 des Rahmenbeschluss-Entwurfs vom 24.05.2005 [Begriffsbestimmungen]
Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck "Kommunikationsdaten"
a) Verkehrsdaten und Standortdaten nach Artikel 2 der Richtlinie 2002/58/EG;
b) Nutzerdaten, d.h. Daten zu einem Nutzer 1, der einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne dass er diesen Dienst notwendigerweise abonniert haben muss;
c) Teilnehmerdaten, d.h. Daten zu einer juristischen oder natürlichen Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke abonniert hat, ohne diesen Dienst notwendigerweise in Anspruch genommen zu haben.
(...)

EU-Rahmenbeschluss (4)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

Entwurf eines Rahmenbeschlusses der EU vom 24.05.2005:

Art. 4 des Rahmenbeschluss-Entwurf vom 24.05.2005 [Fristen für die Vorratsspeicherung von Kommunikationsdaten]
Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die in Artikel 3 genannten Kommunikationsdaten nach ihrer Erzeugung 12 Monate lang auf Vorrat gespeichert werden. Für Teilnehmerdaten läuft diese Frist ab dem Ende des Abonnements.
(2) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratsspeicherung der in Artikel 3 genannten Kommunikationsdaten gemäß den nationalen Kriterien längere Fristen von bis zu 48 Monaten vorsehen, wenn dies eine notwendige, angemessene und verhältnismäßige Maßnahme innerhalb einer demokratischen Gesellschaft darstellt.
(3) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratspeicherung der in Artikel 3 genannten Kommunikationsdaten in Bezug auf die Kommunikationsform nach Artikel 1 Absatz 2 3 kürzere Fristen von mindestens 6 Monaten vorsehen, wenn er die Fristen für die Vorratsspeicherung nach Absatz 1 gemäß nationalen Verfahrens- oder Konsultationsprozessen nicht für annehmbar hält.
(4) Ein Mitgliedstaat, der beschließt, Absatz 2 oder 3 anzuwenden, setzt den Rat und die Kommission von den für die Vorratsspeicherung vorgesehenen Fristen unter Angabe der betreffenden Kommunikationsdaten in Kenntnis. Diese Ausnahmen werden mindestens alle fünf Jahre überprüft.

Deutsches Recht (1)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

§ 95 TKG [Vertragsverhältnisse]
(1) Der Dienstanbieter darf Bestandsdaten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. (…)
(3) Endet das Vertragsverhältnis, sind die Bestandsdaten vom Dienstanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. (…)

§ 96 TKG [Verkehrsdaten]
(1) Der Dienstanbieter darf folgende Verkehrsdaten erheben und verwenden, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:
1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechung notwendigen Verkehrsdaten.
(2) Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie für den Aufbau weiterer Verbindungen oder für die (…) genannten Zweck erforderlich sind. Im Übrigen sind die Verkehrsdaten vom Dienstanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

Deutsches Recht (2)

§ FÖR ONLINE

Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

§ 97 Abs. 3 TKG [Entgeltermittlung und Entgeltabrechung]
(3) Der Dienstanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich dir für die Berechung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Die Verkehrsdaten dürfen - vorbehaltlich des Absatzes 4 Satz 1 Nr. 2 - höchstens sechs Monate nach Versendung der Rechung gespeichert werden.

§ 98 Abs. 1 TKG [Standortdaten]
(1) Standortdaten (…) dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Der Teil-nehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

Deutsches Recht (3)

§ FÖR ONLINE

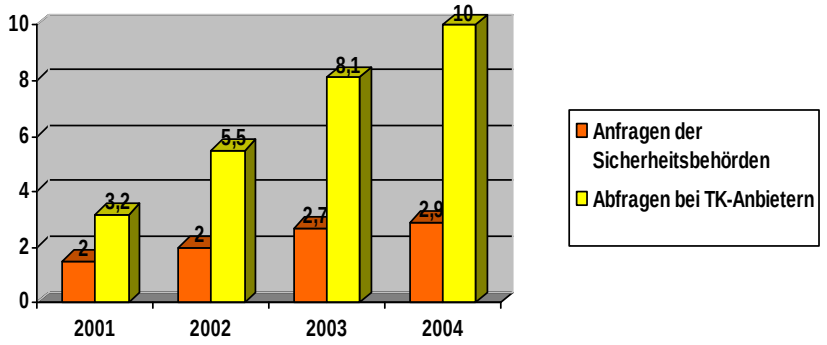
Cybersurveillance Datenspeicherung **Vorratsdatenorganisation** Prepaid-Kundendaten Auskunftsrechte Dritter

§ 5 TDDSG [Bestandsdaten]
Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten). (…)

§ 6 TDDSG [Nutzungsdaten]
(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). (…)
(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus ver-arbeiten und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). (…)
(7) Der Dienstanbieter darf Abrechungsdaten (…) höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechung speichern. (…)

→ Zweck wird durch Art der Verbindung und durch den Vertrag konturiert
→ Höchstdauer grundsätzlich sechs Monate
→ Keine Speicherung zu Zwecken der öffentlichen Sicherheit

§ 88 TKG [Fernmeldegeheimnis]
(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.



[Quelle: Jahresbericht 2004 der RegTP]

Szenario „Prepaid-Kundendaten“ in Anlehnung an Bundesverwaltungsgericht (BVerwG), Urteil vom 22.10.2003 – 6 C 23.02
T erbringt geschäftsmäßig Mobilfunkdienstleistungen. Sie bietet auch Leistungen auf der Grundlage von Prepaid-Karten an. Dabei erwirbt der Kunde eine Prepaid-Karte, mit der er in Höhe des jeweiligen Kartenbetrages telefonieren kann. Im Gegensatz zu Standardverträgen ist bei solchen Prepaid-Verträgen die Erhebung und Speicherung personenbezogener Daten zur Begründung und Abwicklung eines Vertragsverhältnisses nicht erforderlich. 1997 teilte die RegTP T mit, dass sie bei der Vermarktung von Prepaid-Produkten bestimmte „Leitlinien“ zu befolgen habe. Die Identität der Kunden müsse durch amtlichen Nachweis, etwa Lichtbildausweis festgestellt werden, die Ausweisnummer sei von der Klägerin festzuhalten. Weiter müssten Name und Adresse der Kunden sowie die Kennzeichnung der verkauften Karte in die Verzeichnisse nach § 90 Abs. 1 Telekommunikationsgesetz eingestellt werden. Vorher dürfe keine Freischaltung zur Nutzung der Karte erfolgen.
Ist T verpflichtet, Prepaid-Kundendaten in einer Datei zum Abruf bereitzuhalten?

§ 90 Abs. 1 TKG a.F. [Auskunftsersuchen der Sicherheitsbehörden]
(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind. (...)

nach BVerwG zu beachten:

- Bestimmtheitsgrundsatz
- Wertigkeit des Rechts auf informationelle Selbstbestimmung der Kunden des Telekommunikationsanbieters

→ nach BVerwG mittelbarer Grundrechtseingriff
(Anbieter haben keine Handlungsalternative, deshalb ist Verhalten gegenüber Anbietern dem Staat als Eingriff Grundrechte der Bürger zuzurechnen).

→ kein wirksamer Grundrechtsverzicht bei Vertragsschluss mangels Freiwilligkeit (ohne Vertragsschluss könne die Sprachtelefonie als unverzichtbares Medium der Kommunikation nicht genutzt werden)

Grammatische Auslegung:

„Kundendateien zu führen, in die (...) Name und Anschrift (...) aufzunehmen sind (...)“ (§ 90 Abs. 1 TKG a.F.)

≠

„erheben, speichern, verarbeiten,...“ als „eingeführte“ Begrifflichkeit für Daten“organisation“ im Sinne des BDSG

§ 3 Abs. 2 S. 1 BDSG
(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (...)

Systematische Auslegung:

§ 89 Abs. 1 S. 1 TKG a. F. [Datenschutz]
(2) (...) die Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist
1. zur betrieblichen Abwicklung ihrer jeweiligen geschäftsmäßigen Telekommunikationsdienste, nämlich für
a) das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses,
b) das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,(...)

§89 TKG a. F. erlaubt Unternehmen auch Bestandsdaten zu erheben (, verarbeiten, ...)
→ Bestandsdaten bei Prepaidverfahren systematisch auch von § 90 a. F. TKG erfasst?

Contra:
- § 89 TKG a. F. regelt Beziehung Unternehmen - Kunden
- § 90 TKG a. F. regelt Beziehung Staat - Unternehmen

Systematische Auslegung:

§ 89 Abs. 1 S. 1 TKG a. F. [Datenschutz]
(2) (...) die Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist
1. zur betrieblichen Abwicklung ihrer jeweiligen geschäftsmäßigen Telekommunikationsdienste, nämlich für
a) das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses,
b) das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,(...)

§89 TKG a. F. erlaubt Unternehmen auch Bestandsdaten zu erheben (, verarbeiten, ...)
→ Bestandsdaten bei Prepaidverfahren systematisch auch von § 90 a. F. TKG erfasst?

Contra:
- § 89 TKG a. F. regelt Beziehung Unternehmen - Kunden
- § 90 TKG a. F. regelt Beziehung Staat - Unternehmen

Teleologische Auslegung:

Sinn und Zweck des § 90 TKG a. F. ist die Sicherstellung des öffentlichen Strafverfolgungs- und Sicherheitsinteresses. Zwar kann ein Interesse an möglichst umfangreicher Daten"organisation" bestehen. Dieses kommt aber in der Norm angesichts der Wertigkeit des Rechts auf informationelle Selbstbestimmung nicht klar genug zum Ausdruck. Dass eine Pflicht zur Datenerhebung auch bei Prepaid-Karten dem Gesetzeszweck entspricht, kann man daher nicht mit der gebotenen Eindeutigkeit (Bestimmtheitsgrundsatz) bejahen.

Historische Auslegung:

Die Erforschung der Motivation des „historischen" Gesetzgebers (des TKG vor der TKG-Novelle 2004) führt ebenfalls nicht zu einer pflichtigen Einbeziehung von Prepaid-Kundendaten. Denn dem Gesetzgeber war das Prepaid-Verfahren bei der Gesetzgebung bekannt. Er hätte die entsprechende Daten"organisation" also regeln können.

Dynamische (technikorientierte) Auslegung:

Eine Auslegung, die den technischen Wandel berücksichtigt, kommt hier zu keinem anderen Ergebnis, da der technische Wandel (Prepaid-Verfahren) dem „historischen" Gesetzgeber bereits bekannt war.

Rechtsvergleichende / Europarechtliche Auslegung:

Das TKG a. F. beruht (auch) auf europarechtlichen Richtlinien. In diesen findet sich jedoch keine Verpflichtung zur Organisation von Prepaid-Kundendaten.

Ergebnis BVerwG:
→ keine Verpflichtung der T zur „Organisation" von Prepaid- Kundendaten.

TKG-Novelle 2004 → (ein Ziel:) Prepaid-Kundendaten erfasst (?)

§ 111 Abs. 1 TKG [Daten für Auskunftsersuchen der Sicherheitsbehörden]

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen auch die Anschrift des Anschlusses vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse eingetragen werden. (…) Nach Ende des Vertragsverhältnisses sind die Daten mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt. (...)

1	**Personal-Aktiv**	RegTP, als „Auskunftsvermittler“ gem. § 112 Abs. 4 TKG für Behörden nach §112 Abs. 2 TKG: Strafverfolgungsbehörden, Polizei, Zollfahndungsämter, Verfassungsschutz
2 a)	**Personal-passiv** Datenschutz	Diensteanbieter
2 b)	**Personal-passiv** Informationskosten	Informationskosten durch: ➢Pflicht zur Führung von Kundendateien nach § 112 Abs. 1 TKG ➢keine Entschädigung für Datenerhebung- und Speicherung § 111 Abs. 1 S. 4 TKG ➢Gewährleistung der Abrufbarkeit nach § 112 Abs. 1 S. 4 TKG ➢Sicherstellung der „geheimen“ Abrufbarkeit nasch § 112 Abs. 1 S. 6 TKG durch technische und organisatorische Maßnahmen
3	**Objekt**	Kundendateien (auch bei Prepaid-Verfahren): ➢Rufnummern ➢Name und Anschrift der Inhaber der Rufnummern ➢Geburtsdatum der Inhaber der Rufnummern

4	**Kausal/Zweck**	➢Kriminalitätsbekämpfung
5	**Qualität der Informationstechnik**	➢Abruf durch RegTP im automatisiertes Verfahren ➢Übermittlung an in § 112 Abs. 2 TKG genannte Behörden nach § 112 Abs. 4 S. 1 TKG
6	**Verfahren**	➢Automatisiertes Verfahren, in dem Personal-Passiv-Datenschutz nicht einmal Kenntnis von dem konkreten Auskunftsersuchen hat, § 112 Abs. 1 S. 6 TKG ➢Zulässigkeit der Übermittlung wird ohne Anlass nicht geprüft, § 112 Abs. 4 S. 2 TKG
7	**Rechtfertigung/ Verhältnismäßigkeit**	

Ausgangsfall:
N ist – nach seiner Überzeugung – genauso rechtstreu wie prozessscheu. Er tauscht mit der Flatrate Musikdateien und lädt sie „herunter“. Die Einzelheiten der urheberrechtlichen Würdigung solcher Tauschbörsen sind ihm nicht einfach durchschaubar – und deshalb möchte er jedes Prozessrisiko vermeiden. Als er deshalb in einer verbreiteten Computerzeitschrift liest, dass ein Access-Provider mit beträchtlicher Marktmacht die Praxis übt, beim Surfen anfallenden Daten (etwa die (dynamische) IP-Nummer, Datum, Uhrzeit und Länge der Internetsitzung) zu speichern, erschrickt er.

Ergänzung:
Nachdem T – der Provider des N- von M, einer Herstellerin von Tonträgern, aufgefordert wird, die gespeicherten Daten des N an sie herauszugeben, fragt sich auch T nun, ob er hierzu verpflichtet sei.

§ 101 a UrhG Anspruch auf Auskunft hinsichtlich Dritter
(1) Wer im geschäftlichen Verkehr durch die Herstellung oder Verbreitung von Vervielfältigungsstücken das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht verletzt, kann vom Verletzten auf unverzügliche Auskunft über die Herkunft und den Vertriebsweg dieser Vervielfältigungsstücke in Anspruch genommen werden, es sei denn, daß dies im Einzelfall unverhältnismäßig ist.
(2) Der nach Absatz 1 zur Auskunft Verpflichtete hat Angaben zu machen über Namen und Anschrift des Herstellers, des Lieferanten und anderer Vorbesitzer der Vervielfältigungsstücke, des gewerblichen Abnehmers oder Auftraggebers sowie über die Menge der hergestellten, ausgelieferten, erhaltenen oder bestellten Vervielfältigungsstücke.
(3) In Fällen offensichtlicher Rechtsverletzung kann die Verpflichtung zur Erteilung der Auskunft im Wege der einstweiligen Verfügung nach den Vorschriften der Zivilprozeßordnung angeordnet werden.

§ 8 TDG Allgemeine Grundsätze
(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.
(2) Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 unberührt. Das Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes ist zu wahren.

§ 9 TDG Durchleitung von Informationen
(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.
Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.
(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

§ 10 TDG Zwischenspeicherung zur beschleunigten Übermittlung von Informationen
Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie
1. die Informationen nicht verändern,
2. die Bedingungen für den Zugang zu den Informationen beachten,
3. die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.
§ 9 Abs. 1 Satz 2 gilt entsprechend.

Plattformentscheidungen pro Auskunftsanspruch

➢ LG Hamburg - Urteil vom 07.07.2004, 308 O 264/04

Das Gericht bejaht einen Anspruch auf Auskunft gegenüber Access-Providern über die Identität von Kunden, die den vermittelten Internetzugang zu Uhreberrechtsverletzungen nutzen (§ 101a UrhG)

➢ LG München I - Urteil vom 28.07.2004, 21 O 10372/04

Das LG München bejaht den Auskunftsanspruch aus dem UrhG, da das Gesetz „auch auf unkörperliche Vervielfältigungsstücke anwendbar (sei). Der Wortlaut der Vorschrift steht einem solchen Verständnis nicht entgegen (...) Der im Gesetzestext verwendete Begriff des Vervielfältigungsstücks deutet zwar auf eine Körperlichkeit hin, ist jedoch keinesfalls so eindeutig.“ Das Gericht stellt vielmehr auf die übertragene Bedeutung des Wortes im Sinne der Verwendung im Kontext ab. So sei „das (im Duden) angeführte „Stück deutscher Geschichte“ (...) ebenso wenig körperlich vorhanden wie etwa ein improvisiertes Musikstück“. (§ 101a UrhG)

Plattformentscheidungen contra Auskunftsanspruch

➢ OLG Franfurt am Main – Urteil vom 25.01.2005, 11 U 51/04

Das OLG geht davon aus, dass bereits die Normlage nicht gegeben sei; weder sei T selbst „Verletzer" im Sinne der Norm, noch käme er als Teilnehmer in Betracht. (**§ 101a UrhG)** Auch ließe sich aus der genannten Bestimmung keine Störerhaftung konstruieren, da dem T bereits die „Bösgläubigkeit" fehle. Eine Kenntnis nämlich über die rechtswidrige Praxis von den Access-Dienst nutzenden Kunden, könne T erst dann erlangt haben, wenn ihm Informationen diesbezüglich zugingen. Zur Durchforstung des Internet nach etwaigen seinen Dienst nutzenden „Piraten" sei T vorher nicht verpflichtet (**§ 8 Abs. 2 TDG**). Ein Beseitigungsanspruch käme hier auch nicht in Betracht. (**§§ 862, 1004 BGB oder § 19 Markengesetz bzw. § 242 BGB**)

➢ OLG München – Urteil vom 24.03.2005, 6 U 4696/04

Ob ein Anspruch bestünde bzw. eine Normanwendung gegeben sei, wird nicht weiter erörtert. (**§ 101a UrhG).** Das Gericht ist der Auffassung, dass bereits eine offensichtliche Urheberrechtsverletzung nicht gegeben sei (**§ 101a III UrhG**). Im Übrigen verweist das Gericht auf die in der Literatur befindliche Diskussion.

Plattformentscheidungen contra Auskunftsanspruch

➢ Hanseatisches Oberlandesgericht, Urteil vom 28.04.2005, 5 U 156/04

Das OLG hält § 101a UrhG nicht für direkt anwendbar. Einer analoge Anwendbarkeit begegneten erheblichen Zweifeln. Selbst wenn man diese unterstelle, liege aber keine offensichtliche Rechtsverletzung (§ 101 Abs. 3 UrhG) vor. Denn es sei zweifelhaft, ob zum einen die Antragsstellerin tatsächlich Rechteinhaberin sei und zum anderen eine Verantwortlichkeit der Antragsgegnerin vorliege (§101a Abs. 1 UrhG). Selbst wenn eine Störerverantwortlichkeit der Antragsstellerin bestehe, müsse sich diese nicht auf die Auskunftserteilung erstrecken. Denn der Auskunftsanspruch aus § 101a UrhG sei kein „minus", sondern ein „anderer" Anspruch als die „Verpflichtung zur Entfernung oder Sperrung" (i.S.d. § 8 Abs. 2 TDG).

➢ Volker Kitz, Die Zukunft der Auskunft oder: Die abenteuerliche Karriere des § 101a UrhG, MMR 2005, S 133f.

➢ Volker Kitz, „Die Auskunftspflicht des Zugangsvermittlers bei Urheberrechtsverletzungen durch seine Nutzer", GRUR 2003, S. 1014f.

➢ Christian Czychowski, Auskunftsansprüche gegenüber Internetzungangsprovidern „vor" dem 2. Korb und „nach" der Enforcement - Richtlinie der EU, MMR 2004, S. 514f.

➢ Sieber/Höfinger, Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen, MMR 2004, S. 575f.

➢ Allgemein zum Auskunftsanspruch im Urheberrecht: Manfred Rehbinder, Urheberrecht, 2001 München, S. 350f.