Auskünfte zu Bestandsdaten, Verkehrsdaten und Telekommunikationsüberwachungen: Anforderungen und Umfang

Berlin, 10.01.2019. Das Internet ist ein Abbild unserer Gesellschaft, im Positiven wie im Negativen. Da es kein rechtsfreier Raum ist, werden Betrug, Verleumdung und schwere Kriminalität verfolgt – für die Polizei kein leichtes Pflaster. Neben rechtlich einwandfreien Anfragen erreichen uns als E-Mail-Anbieter aber auch immer wieder Auskunftsanfragen von Polizei und Behörden, die nicht den gesetzlichen Vorgaben entsprechen. Also, kurz gesagt: Die illegal sind.

Um Auskunftsanfragen korrekt zu stellen und zu beantworten, ist einiges an Wissen auf Seiten der Behörden und der Anbieter gefragt. Und auch manche Privatperson hat sich sicher schon mal gefragt, was eigentlich wann erlaubt ist und was eben nicht. Im Folgenden bringen wir Licht ins Dunkel – für alle Seiten.

> Hinweis: Hier finden Sie die aktuellen mailbox.org Transparenzberichte: https://mailbox.org/de/unternehmen#transparenzbericht

Text + Konzeption: Peer Heinlein (mailbox.org)
Juristische Überprüfung + Beratung: Rechtsanwalt Matthias Bergt (von BOETTICHER Rechtsanwälte)

Vorwort

Die Rolle des Providers: Zwischen den Fronten

Bevor wir uns im juristischen Dickicht der Anforderungen (und wie permanent dagegen verstoßen wird) verheddern, betrachten wir zuerst das Gesamtbild: In allgemeinen Gesetzesgrundlagen wie DSGVO („Datenschutzgrundverordnung“) und BDSG („Bundesdatenschutzgesetz), und auch durch eine spezielle Gesetzgebung wie dem TKG („Telekommunikationsgesetz“) sind für uns Telekommunikationsanbieter sehr strenge und klare Regeln festgelegt, wann wir Daten herausgeben müssen. Vor allem aber auch: wann wir das überhaupt nur dürfen.

Bei Verstößen gegen Datenschutzrecht – insbesondere auch gegen das Telekommunikationsrecht der Provider – drohen teils drastische Strafen mit bis zu fünf Jahren Gefängnis. -Für denjenigen, der die Tat (Handlung) begangen hat. Also insbesondere auch für die „normalen“ Mitarbeiter der Provider.

Unsere Systemadministratoren laufen also Gefahr, selbst als Straftäter dazustehen, wenn sie rechtswidrige Anfragen von Behörden folglich rechtswidrig beantworten würden. Eine Situation, die ein Arbeitgeber auf dem Schirm haben muss, um seine Mitarbeiter zu schützen.

Gleichzeitig jedoch auch eine Situation, die Polizei und Ermittlungsbehörden zu besonderer Vorsicht veranlassen muss, um nicht durch ihr Vorgehen etwaige Straftaten der Mitarbeiter eines Provider auszulösen!

Die Rolle der Ermittlungsbehörden: Anstifter zu Straftaten?

Denn, das muss man sich mal auf der Zunge zergehen lassen: Rechtswidrige Auskunftsanfragen der Polizei kann und muss man folgerichtig als (versuchte? vollendete?) Anstiftung zur Begehung einer Straftat verstehen – durch den jeweiligen Polizisten. Und eine Strafandrohung von bis zu fünf Jahren Gefängnis ist keine Lappalie.

Für die von uns immer wieder erlebten, umfangreich rechtswidrigen Anfragen, kann es keine Entschuldigung geben. Die Polizei hat sich bei ihren Ermittlungen ohne Wenn und Aber an Recht und Gesetz zu halten. Auch, wenn es unbequem ist, auch wenn dadurch Ermittlungen stocken oder Details vielleicht nicht ermittelt werden können. Und auch für die Polizei gilt wie für jeden Bürger: Unwissenheit schützt vor Strafe nicht. Wenn Provider rechtswidrig nach Daten angefragt werden, kann dies als versuchte Anstiftung zu werten sein.

Aus vielen Einzelfallgesprächen mit ermittelnden Polizisten (Begrüßung unsererseits: „Guten Tag. Sie wollten uns zu einer Straftat anstiften?“) wissen wir jedoch, dass landauf, landab, blanke Unwissenheit über die Gesetzeslage herrscht. Polizei ist Ländersache, und auch innerhalb der vielen großen und kleinen Polizeidienststellen ist nicht jeder sattelfest in Sachen Internet und den Daten, die bei einem Provider so anfallen. Und auch nicht jeder Polizist ist mit dem Internet im Blut aufgewachsen. Für manche ist es auch… Neuland. Allerdings: Selbst spezielle Abteilungen zu „Cybercrime“ haben bei uns schon rechtswidrig angefragt und mussten von uns aufgeklärt werden. Das ist dann schon sehr bitter.

Doch: Es bringt nichts, jedes Jahr empörte „Transparenzberichte“ der Provider zu veröffentlichen und ein allgemeines Wehklagen ob der Unkenntnis von Polizei und Ermittlungsbehörden anzustimmen. Das ist zwar grundsätzlich wichtig für den politischen Druck (und wird von Anbietern gerne für‘s eigene Marketing verwendet!), ist aber ansonsten nur bedingt wirkungsvoll, um die Ursachen aus der Welt zu schaffen und die Situation für Nutzer tatsächlich zu verbessern.

Drum: Getreu dem mailbox.org-Motto „Beklage nicht, was Du nicht ändern kannst, aber ändere, was du zu beklagen hast“, leisten wir hiermit Aufklärungsarbeit und bringen Licht ins Dunkel.

Die nachfolgende – zugegebenermaßen sehr umfangreiche – Zusammenfassung bietet eine Übersicht für interessierte Privatpersonen, Journalisten – aber gerade auch für Polizisten und andere Ermittlungsbeamte.

Übersicht zu gesetzlichen Grundlagen der behördlichen Auskunftsersuchen

- Einhaltung der Datenschutzgesetze durch die Polizei selbst (Kommunikationsweg, notwendige Daten)
- Arten von Auskunftsverfahren und deren Anforderung (Bestandsdaten, Verkehrsdaten, Telekommunikationsüberwachung)
- Wer darf Anfragen stellen?
- Tabellarische Kurzübersicht

Ein Herzlicher Dank geht vorab an unseren langjährigen Anwalt, den IT-Rechtsexperten Matthias Bergt von der Kanzlei von BOETTICHER Rechtsanwälte (https://www.boetticher.com) für die redaktionelle Mitarbeit und juristische Überprüfung dieses Beitrages!

Einhaltung der Datenschutzgesetze durch die Polizei selbst

Sicherer datenschützender Kommunikationsweg

Datenschutzrechtliche Vorschriften gelten (natürlich! Erst recht!) auch für Polizeibeamte oder Richter, keine Frage. Da schon die jeweilige Anfrage der Polizei mit der Nennung des betroffenen Accounts im Zusammenhang mit einem Ermittlungsverfahren „personenbezogene Daten“ beinhaltet, muss die Anfrage selbst auf einem „sicheren Kommunikationsweg“ erfolgen. Alles andere ist ein rechtswidriger und ggf. sogar strafbarer Verstoß gegen geltendes Recht.

Egal ob Anfragen nach Bestandsdaten, Verkehrsdaten oder die Abwicklung einer Telekommunikationsüberwachung: Diese Kommunikation per unverschlüsselter E-Mail ist stets rechtswidrig.

Polizisten und Staatsanwälte verstoßen hier regelmäßig ihrerseits gegen geltendes Datenschutz- wie Strafrecht und machen sich ggf. gemäß §§ 203, 353b StGB (und wenn man der abwegigen Ansicht des BGH zu Detektiven folgt, auch § 42 BDSG) strafbar und setzen sich außerdem persönlich dem Risiko von Geldbußen bis zu 20 Millionen Euro aus. Nebenbei gefährden sie auch ihre eigenen Ermittlungen, weil Täter gewarnt werden könnten.

Doch genau das ist beklagenswerterweise der Regelfall. In Sachen Datenschutzbewusstsein, aber auch der technische Kompetenz zur sicheren Kommunikation (Verschlüsselung!) haben fast alle Polizeidienststellen skandalösen und unentschuldbaren Nachholbedarf. Selbst auf Anfrage steht für uns in der Regel keine Möglichkeit zur verschlüsselten Übertragung zur Verfügung, sodass wir i.d.R. auf einen Faxversand ausweichen müssen.

Denn: Fax wird nach geltender Rechtslage als ausreichend sicher empfunden und ist damit für beide Seiten zulässig (sofern nicht weitere Vorschriften einen Gerichtsbeschluss im Original erfordern, siehe unten).

Also:

- Keine Übermittlung von Anfragen mit personenbezogenen Angaben (einschließlich Postfach-Name) per unverschlüsselter E-Mail.

Keine rechtswidrige Bekanntgabe von nicht notwendigen Daten

Egal ob einfache polizeiliche Anfrage oder formvollendeter Gerichtsbeschluss: Fast alle Anfragen enthalten Angaben zur beschuldigten Person (Name/Wohnort), zum Tatzeitpunkt, zum Tatvorwurf oder weiteren Details des Ermittlungsverfahrens, die den Provider beim allerbesten Willen in diesem Zusammenhang nichts angehen und die ihm aus Datenschutzgründen auch keinesfalls zur Kenntnis gebracht werden dürfen.

Polizisten, Staatsanwälte und sonstige seitens der Justiz Beteiligte verstoßen hier regelmäßig ihrerseits gegen geltendes Datenschutzrecht und machen sich ggf. gemäß §§ 203, 353b StGB (und wenn man der abwegigen Ansicht des BGH zu Detektiven folgt, auch § 42 BDSG) strafbar und setzen sich außerdem persönlich dem Risiko von Geldbußen bis zu 20 Millionen Euro aus.

Zu beachten ist allerdings umgekehrt, dass seit dem 24. August 2017 für bestimmte Beschlüsse – Verkehrsdatenabfragen und Telekommunikationsüberwachungen – detaillierte Angaben im Tenor der Entscheidung vorgeschrieben sind (§ 100e Abs. 3 S. 2 StPO). Der Gesetzgeber hat hier die Selbstkontrolle der Justiz und die Kontrollmöglichkeit auch für den Provider als wichtiger angesehen. Dennoch scheint sich dieses noch relativ neue Recht bei Staatsanwaltschaften und Gerichten noch nicht sehr weit herumgesprochen zu haben. Solchen formal fehlerhaften und rechtswidrigen Beschlüssen dürfen wir nicht nachkommen – hier verlieren die Strafverfolgungsbehörden durch die Extra-Runde möglicherweise wichtige Zeit.

Also:

- Keine Angaben zu Fall und Beschuldigten, die nicht zur Bearbeitung der Anfrage durch den Provider zwingend notwendig oder gesetzlich (§ 100e Abs. 3 S. 2 StPO, § 101a Abs. 1 StPO) vorgeschrieben sind.

Arten von Auskunftsverfahren und deren Anforderung

Zunächst ist zwischen drei verschiedenen Arten von Daten, die herausgegeben werden können, zu unterscheiden:

1. Bestandsdaten
2. Verkehrsdaten
3. Telekommunikations-Inhaltsdaten

Je nachdem, welche Art von Daten herausgegeben werden sollen, sind unterschiedliche Voraussetzungen zu erfüllen.

Bestandsdaten

Bestandsdaten sind gemäß § 3 Nr. 3 Telekommunikationsgesetz (TKG) „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“. Umgangssprachlich erklärt sind das Daten, die der Anbieter zum **Inhaber eines Accounts** speichert, um den zugrundeliegenden Vertrag ordentlich abwickeln zu können.

Beispiele für Bestandsdaten

Bestandsdaten sind also beispielsweise…

- Telefonnummer bzw. Postfach-Kennung,
- Name und Anschrift des Inhabers,
- Geburtsdatum,
- Datum von Vertragsbeginn und -ende,
- Angaben zum Vertrag und Tarifmerkmalen.

Dabei sind die oben aufgezählten Daten nicht zwingend zu speichern. Das TKG verpflichtet Anbieter jedoch in § 111 TKG, einige Daten für Bestandsdatenabfragen vorzuhalten, darunter Name, Anschrift, Geburtsdatum und das Datum des Vertragsbeginns. Allerdings sieht § 111 Abs. 2 TKG eine **Ausnahme für E-Mail-Anbieter** vor: Gespeichert werden müssen überhaupt nur Postfach-Kennung und Inhaber – und das auch nur dann, wenn der Anbieter diese Daten überhaupt erhebt. Benötigt der Anbieter andere Daten nicht, darf er sie nicht speichern und kann sie dann natürlich auch nicht herausgeben.

Da bei mailbox.org Accounts auch vollständig anonym eingerichtet werden können und wir kein Bit mehr speichern als unbedingt notwendig, sind Bestandsdatenauskünfte bei uns naturgemäß relativ ergebnislose Anfragen.

Hat ein Nutzer jedoch bei Vertragsabschluss entsprechende Daten angegeben, beispielsweise auch aus steuerlichen Gründen für den Abschluss eines geschäftlich genutzten Accounts, so würden wir diese bei Vorliegen der Voraussetzungen herausgeben müssen.

Voraussetzungen für die Herausgabe von Bestandsdaten

Wichtigste Voraussetzung für die Rechtmäßigkeit einer Bestandsdatenabfrage ist, dass die Daten zur **Ermittlung des Sachverhalts** notwendig sind.

Eine Bestandsdatenabfrage kann direkt durch einen **ermittelnden Polizeibeamten** oder verschiedene andere Behörden (§ 113 Abs. 3 TKG) erfolgen. Sie **unterliegt nicht dem Richtervorbehalt**. Die anfragende Behörde muss aber eine gesetzliche Erlaubnis für die Erhebung der Daten haben.

Bezieht sich die Anfrage auf die Herausgabe von **Passwörtern**, muss die Anfrage von der **Staatsanwaltschaft beim Gericht** beantragt und von diesem genehmigt werden (§ 100j Abs. 3 S. 1 StPO). Bei Gefahr im Verzug kann auch ohne richterliche Erlaubnis abgefragt werden, diese ist aber immerhin anschließend einzuholen.

Bei mailbox.org werden die Passwörter allerdings in einer Form („Hash“) gespeichert, die es nur ermöglicht, festzustellen, ob ein bekanntes Passwort richtig ist – nicht aber umgekehrt, das Klartext-Passwort herauszufinden. Wir können daher aus rein tatsächlichen Gründen **keine Auskunft über Nutzer-Passwörter** erteilen.

Bestandsdatenauskünfte können also
- per Brief,
- per Fax (das wird als „sicher“ gewertet) oder
- per verschlüsselter E-Mail

erfolgen. Der PGP-Key von mailbox.org befindet sich öffentlich downloadbar im Impressum.

Zwingende Voraussetzung ist
- die Angabe einer gesetzlichen Bestimmung, die der anfragenden Behörde eine Erhebung der verlangten Daten erlaubt und
- dass die Auskunft im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Militärischen Abschirmdienstes oder des Bundesnachrichtendienstes erforderlich ist.

Illegal sind Bestandsdatenauskünfte, die
- auf nicht-datenschützendem Kommunikationsweg,
- unter Bekanntgabe zu vieler Daten an den Provider,
- ohne gesetzliche Erlaubnisnorm für die anfragende Behörde oder ohne deren Nennung oder

- unter Missachtung des Richtervorbehalts in bestimmten Fällen

erfolgen – oder die unter dem Deckmantel einer Bestandsdatenauskunft in Wirklichkeit andere Daten anfragen.

Verkehrsdaten

Verkehrsdaten sind nach § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“. Es handelt sich also um die Daten, die durch die Nutzung des Accounts durch den Accountinhaber entstehen und vom Provider zum Zwecke der Fehleranalyse, der Abrechnung oder aufgrund von gesetzlichen Vorschriften (Vorratsdatenspeicherung) gespeichert werden. Es sind also „laufende“ Daten, die sich üblicherweise in den Logfiles des Providers wiederfinden und sich auf einen konkreten Zeitpunkt beziehen.

Beispiele für Verkehrsdaten

Verkehrsdaten sind also beispielsweise…

- IP-Adressen, von denen Logins auf den Mailserver stattfinden,
- IP-Adressen, von denen aus E-Mails abgesandt wurden,
- Sender und/der Empfänger einer gesendeten oder empfangenen E-Mail des Accounts,
- weitere Aktivitäten des Nutzers in seinem Account, sofern vom Anbieter protokolliert (Abruf von konkreten E-Mails, Speicherung von E-Mails im Entwurfs-Ordner, Löschen von E-Mails).

Umstritten ist, inwieweit beispielsweise der Zahlungsverkehr eines Nutzers als Verkehrsdatum zu verstehen ist, also Zeitpunkt und Ursprungskonto einer Überweisung zur Accountbezahlung oder die Speicherung eines Paypal-Kontos, das die Bezahlung vorgenommen hat.

Manche Auffassungen sehen diese Informationen als Bestandsdaten an – wir teilen diese Ansicht nicht, da sich diese Daten mit jedem Zahlungsvorgang ändern können und wir diese auch nicht zur Vertragserfüllung und Identifizierung des Accountinhabers speichern, auch wenn diese natürlich in der steuerlichen Dokumentation (Buchhaltung, Kontoauszüge) grundsätzlich auffindbar sind.

Voraussetzungen der Herausgabe von Verkehrsdaten

Anordnungen auf Herausgabe von Verkehrsdaten unterliegen strengen Voraussetzungen. Sie sind nach § 100g StPO nur zulässig, wenn jemand im Verdacht steht, eine **Straftat „von auch im Einzelfall erheblicher Bedeutung“** (etwa Mord, Totschlag, Verbreitung, Erwerb oder Besitz von jugend- oder kinderpornographischen Schriften, Raub, Betrug

oder Computerbetrug, aber auch Verleitung zur missbräuchlichen Asylantragstellung) oder mittels Telekommunikation begangen zu haben.

Die Erhebung der besonders sensiblen Verkehrsdaten muss zudem für die Erforschung des Sachverhalts erforderlich sein und die Erhebung der Daten **in einem angemessenen Verhältnis zur Bedeutung der Sache** stehen. Mit anderen Worten: Mit Kanonen auf Spatzen schießen ist unzulässig. Ist die Straftat mittels Telekommunikation begangen worden, muss die Aufklärung auf anderen Wegen sogar komplett aussichtslos sein.

Anders als Anfragen zu Bestandsdaten unterliegen Anfragen zu Verkehrsdaten **stets einem Richtervorbehalt** (§ 101a Abs. 1 i.V.m. § 100e Abs. 1 StPO); auch in Eilfällen muss eine Anordnung der Staatsanwaltschaft innerhalb von drei Werktagen durch das Gericht bestätigt werden. Die ermittelnde Stelle muss beim zuständigen Gericht einen entsprechenden Beschluss auf Herausgabe der Daten erwirken – salopp ausgedrückt eine Art „Durchsuchungsbeschluss“, bekannt aus Film und Fernsehen. Dieser Durchsuchungsbeschluss muss **im Original** an den Telekommunikationsanbieter übersandt werden. Ein Fax oder ein PDF-Scan reicht nicht (und letzteres schon gar nicht mit unverschlüsselter E-Mail!).

Wichtig ist, dass seit dem 24. August 2017 eine Reihe von **Angaben bereits in der Entscheidungsformel** enthalten sein (§ 101a Abs. 1 i.V.m. § 100e Abs. 3 StPO) und damit naturgemäß dem Provider offengelegt werden müssen:

- genaue Bezeichnung der Daten
- Tatvorwurf
- Dauer der Verkehrsdatenerhebung
- bei rückwirkender Erhebung genauer Zeitraum
- Art der zu erhebenden Informationen
- und ihre Bedeutung für das Verfahren

-Eine wesentliche Änderung gegenüber der früheren Rechtslage.

Dabei müssen vom zuständigen Gericht nicht nur der genaue Account und die angeordneten Maßnahmen bestimmt werden, sondern auch der **Zeitraum**, für den die Verkehrsdaten abgefragt werden, ist konkret festzulegen. Das gilt nicht nur für Verkehrsdatenabfragen in die Zukunft, sondern nach § 101a Abs. 1 S. 1 Nr. 1 StPO auch für Abfragen in die Vergangenheit und soll verhindern, dass verfassungswidrig pauschal alle vorhandenen Daten abgerufen werden.

Gesetzlich ist auch eine **umfassende Begründung** zwingend vorgeschrieben (§ 101a Abs. 2 StPO), die sich auf den konkreten Einzelfall beziehen muss. Die früher üblichen Floskeln, dass die Anordnung erforderlich und verhältnismäßig sei, sind nach der Rechtsprechung des Bundesverfassungsgerichts, die der Bundestag ausdrücklich in das Gesetz übernommen hat, unzulässig. Allerdings gehen diese Details den Provider nichts an. **Der Provider sollte nur eine abgekürzte Ausfertigung des Beschlusses erhalten, in dem die Begründung z.B. durch „...“ ersetzt ist.**

Ist **Gefahr im Verzug**, darf die Staatsanwaltschaft die Maßnahme auch selbst anordnen. Sie muss sie sich allerdings **nachträglich innerhalb von drei Werktagen durch einen Richter bestätigen** lassen. Nach Abschluss der Maßnahme müssen im Regelfall alle Betroffenen informiert werden, also auch die Kommunikationspartner (§ 101a Abs. 6 StPO). Nur im Ausnahmefall darf das unterbleiben.

Richtet sich eine Abfrage von Verkehrsdaten auf Daten aus der Vergangenheit, kann natürlich **nur herausgegeben werden, was ohnehin gespeichert** ist. Um die Anbieter zu einer Speicherung zu verpflichten, wurde vom Gesetzgeber immer wieder versucht, eine anlasslose Speicherung von Verkehrsdaten gesetzlich vorzuschreiben, die berüchtigte **Vorratsdatenspeicherung**. Diese ist allerdings bei Europäischem Gerichtshof und Bundesverfassungsgericht auf wenig Gegenliebe gestoßen. Zwar gilt momentan theoretisch eine reformierte Pflicht zur Datenspeicherung – weil aber auch diese Pflicht offensichtlich grundrechtswidrig ist, weil sie anlasslos jeden Bürger als Straftäter behandelt, ist sie **nach entsprechenden Gerichtsurteilen faktisch ausgesetzt.**

- mailbox.org hat im Herbst 2016 zusammen mit Digitalcourage, dem Deutschen Journalistenverband und anderen prominenten Verbänden, Künstlern und Anwälten Verfassungsbeschwerde beim Bundesverfassungsgericht in Karlsruhe eingelegt. Wir hoffen auf eine Verhandlung in 2019.

Ist die Erwirkung eines entsprechenden Gerichtsbeschlusses angekündigt, kann der Anbieter die Daten bereits intern sichern („Freeze“), damit diese nicht durch Zeitablauf automatisch gelöscht werden. Dazu verpflichtet ist er allerdings nicht – der mehrfach angedachte „Quick Freeze“ wurde durch den Gesetzgeber ausdrücklich nicht eingeführt.

Ist klar, dass ein solcher Beschluss erfolgt ist und vorliegt, wird es nach allgemeiner Auffassung als zulässig erachtet, wenn ein Anbieter Verkehrsdaten aufgrund eines **vorab per Fax** übermittelten Beschlusses herausgibt und das **Original dann auf dem Postweg** umgehend nachgereicht wird.

Verkehrsdaten müssen also
- per ausreichend konkretem Gerichtsbeschluss, der bereits in der Entscheidungsformel (und nicht erst in der Begründung) alle in § 100e Abs. 3 und § 101a Abs. 1 S. 1 StPO genannten Angaben enthält
- im Original auf dem Postweg

angefragt werden.

Illegal sind Verkehrsdatenauskünfte, wenn sie
- ohne Gerichtsbeschluss,
- nur in Kopie/Faksimile,
- auf nicht-datenschützendem Kommunikationsweg oder
- unter Bekanntgabe zu vieler Daten an den Provider

erfolgen.

Telekommunikationsüberwachung (TKÜ)

Eine TKÜ gemäß § 100a StPO ist eine sehr weitreichende weil **grundrechtseingreifende Maßnahme**. Dabei wird über einen bestimmten Zeitraum die Telekommunikation eines Verdächtigen oder einer Person, die diesem vermutlich in bestimmter Weise nahesteht, vollständig überwacht und mitgeschnitten.

Der Unterschied zu der Überwachung von Verkehrsdaten ist, dass hierbei nicht nur Daten zu den Verbindungen, sondern auch der Inhalt der Kommunikation selbst aufgezeichnet wird.

Salopp ausgedrückt: **Es wird abgehört.** Telefonanschlüsse, Chat-Anschlüsse oder auch der E-Mail-Verkehr eines Betroffenen müssen dabei auf Anordnung der Ermittlungsbehörden vom Provider mitgeschnitten und auf verschiedenen Wegen der Polizei zur Verfügung gestellt werden.

Beispiele für eine Telekommunikationsüberwachung

Eine TKÜ umfasst für die Dauer der Überwachung beispielsweise…

- alle empfangenen und gesendeten E-Mails,
- alle innerhalb des Accounts hochgeladenen E-Mails (Draft-Folder!)

Dabei sind E-Mails so auszuleiten, wie sie vom Provider empfangen wurden. Verschlüsselte E-Mails logischerweise verschlüsselt. Denn, selbst wenn er es könnte: Der Provider ist nicht verpflichtet, die Daten für die Ermittlungsbehörde zu entschlüsseln oder an einer Ermittlung des Schlüssels mitzuwirken. Er stellt nur Kopien des Mailverkehrs zur Verfügung.

Voraussetzungen für die Durchführung einer TKÜ

Wesentliche Voraussetzung für die Rechtmäßigkeit einer TKÜ ist der Verdacht auf das **Vorliegen einer in § 100a Abs. 2 StPO bezeichneten Straftat**. Dazu zählen etwa Mord, Totschlag, Raub, Vergewaltigung oder Verbreitung, Erwerb oder Besitz von jugend- oder kinderpornographischen Schriften, aber auch Verleitung zur missbräuchlichen Asylantragstellung. Der Verdacht muss auf konkreten Tatsachen beruhen, ein bloßes „Gefühl“ ist nicht ausreichend.

Weiterhin muss die TKÜ **verhältnismäßig** sein, die Schwere des Eingriffs in das Grundrecht des Post- und Fernmeldegeheimnisses (Art. 10 GG) muss also in einem vernünftigen Verhältnis zu der mutmaßlichen Tat stehen. Darüber hinaus muss die Aufklärung der Tat **wesentlich erschwert werden, wenn nicht auf das Mittel einer TKÜ zugegriffen würde**.

Als erheblicher Eingriff in die Grundrechte des Betroffenen unterliegt die TKÜ natürlich einem **Richtervorbehalt**. Dabei müssen vom zuständigen Gericht nicht nur der **genaue Account** und die **angeordneten Maßnahmen** bestimmt werden, sondern auch die **Dauer der TKÜ** ist verbindlich festzulegen.

Wichtig ist, dass seit dem 24. August 2017 eine Reihe von **Angaben bereits in der Entscheidungsformel** enthalten sein (§ 100e Abs. 3 StPO) und damit naturgemäß dem Provider offengelegt werden müssen:

- genaue Bezeichnung der Daten
- Tatvorwurf
- Dauer der Überwachung
- Art der zu erhebenden Informationen
- und ihre Bedeutung für das Verfahren

-Eine wesentliche Änderung gegenüber der früheren Rechtslage.

Gesetzlich zwingend vorgeschrieben (§ 100e Abs. 4 StPO) ist auch eine **umfassende Begründung**, die sich auf den konkreten Einzelfall beziehen muss. Die früher üblichen Floskeln, dass die Anordnung erforderlich und verhältnismäßig sei, sind nach der Rechtsprechung des Bundesverfassungsgerichts, die der Bundestag ausdrücklich in das Gesetz übernommen hat, unzulässig. Allerdings gehen diese Details den Provider nichts an. Der Provider sollte nur eine **abgekürzte Ausfertigung** des Beschlusses erhalten, in dem die Begründung z.B. durch „...“ ersetzt ist.

Ist Gefahr im Verzug, darf die Staatsanwaltschaft die Maßnahme auch selbst anordnen. Sie muss sie sich allerdings innerhalb von drei Tagen durch einen Richter bestätigen lassen. Nach Abschluss der Maßnahme müssen im Regelfall alle Beteiligten der Kommunikation informiert werden (§ 100e Abs. 4 ff. StPO). Nur im Ausnahmefall darf das unterbleiben.

Eine TKÜ muss zwar bereits auf eine **Anordnung per Fax** gestartet werden, wird aber wieder abgeschaltet, wenn das **Original oder eine beglaubigte Abschrift nicht binnen einer Woche** vorliegt.

Eine TKÜ muss also
- per ausreichend konkretem Gerichtsbeschluss, der bereits in der Entscheidungsformel (und nicht erst in der Begründung) alle in § 100e Abs. 3 StPO genannten Angaben enthält
- im Original auf dem Postweg

angefragt werden.

Illegal sind Anfragen nach einer TKÜ, wenn sie
- ohne rechtmäßigen und in der Entscheidungsformel vollständigen Gerichtsbeschluss,
- nur in Kopie/Faksimile,

- auf nicht-datenschützendem Kommunikationsweg oder
- unter Bekanntgabe zu vieler Daten an den Provider

erfolgen.

Wer darf Anfragen stellen?

Anfragen aus dem Inland

Bei Anfragen aus Deutschland schreiben die deutschen Gesetze vor, welche Behörden berechtigt sind. Wir haben hier vor allem die praxisrelevanten Anfragen von **Strafverfolgungsbehörden** berücksichtigt.

Unter bestimmten Bedingungen sind aber **auch andere Behörden** zu Anfragen berechtigt, etwa

- Zoll,
- Bundesnachrichtendienst (BND),
- Bundesamt und Landesämter für Verfassungsschutz (BfV/LfV),
- Militärischer Abschirmdienst (MAD),
- bei Bestandsdaten jede Behörde, die für die Verfolgung von Ordnungswidrigkeiten oder für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständig ist, wenn eine entsprechende Ermächtigungsnorm für die Behörde besteht (§ 113 Abs. 3 TKG).

Zusätzlich gibt es einen **urheberrechtlichen Auskunftsanspruch** eines Verletzten gegen Diensteanbieter nach § 101 Abs. 2, 9 UrhG. Auch hier ist eine gerichtliche Anordnung erforderlich, soweit Verkehrsdaten verwendet werden müssen.

Um Unterlassungsansprüche geltend zu machen, können außerdem nach § 13 UKlaG **bestimmte Verbände wie Verbraucher- und Wettbewerbszentrale** und nach § 13a UKlaG z.B. Spam-Empfänger unter bestimmten Bedingungen die Herausgabe von Bestandsdaten verlangen.

Diese Ansprüche sind allerdings wenig praxisrelevant und daher hier nicht weiter behandelt.

Anfragen aus dem Ausland

Das Internet macht an Landesgrenzen nicht halt und so erreichen uns als Provider auch Anfragen aus dem europäischen Ausland – aber auch aus aller Welt.

Die Antwort auf die Frage, wie diese Anliegen zu behandeln sind, ist am Ende recht einfach: Sofern man davon ausgeht, dass die angefragten Daten deutschem Recht unterliegen, weil sie

a) zu einer deutschen Firma gehören oder
b) auf deutschem Grund und Boden erhoben und gespeichert werden,

gilt **ausschließlich deutsches Recht** – und damit die oben genannten Anforderungen. Nach allgemeinen völkerrechtlichen Grundsätzen endet die Staatsgewalt eines jeden Staates grundsätzlich an seinen Grenzen. **Keine ausländische Behörde kann daher ein deutsches Unternehmen zur Herausgabe von Daten zwingen** – eine Ausnahme innerhalb der EU wird aktuell diskutiert und zeigt, wie sinnvoll dieser Grundsatz doch ist.

Art. 48 der Datenschutz-Grundverordnung (DSGVO) **verbietet ausdrücklich, ausländische Urteile und Verwaltungsentscheidungen anzuerkennen**, wenn diese nicht auf Rechtshilfeabkommen o.ä. gestützt sind oder jedenfalls eine andere gesetzliche Erlaubnisnorm für die Beantwortung besteht.

Ermittlungsbehörden aus dem Ausland wenden sich daher bitte mittels Rechtshilfeersuchen an die zuständigen deutschen Behörden.

Uns ist bewusst, dass Rechtshilfeverfahren aufwendig und langwierig sein können und die gesuchten Daten am Ende bereits gelöscht sein können. In besonders bedeutenden Ausnahmefällen werden wir prüfen, ob wir bereits auf eine Information einer ausländischen Behörde hin **Daten vorläufig sichern** können, um diese für ein Auskunftsverlangen im Rechtshilfeweg verfügbar zu haben.

Wir bitten aber um Verständnis, dass dies auch für uns ein rechtliches Risiko bedeutet und daher nur dann in Betracht kommen kann, wenn es im wahrsten Sinne **um Leben und Tod** geht.

Niemals sind wir zu einer solchen Zusammenarbeit bereit, wenn es zum Beispiel um die Unterdrückung missliebiger Meinungen, Zensur und andere Bereiche geht, die den Grundsätzen unserer **freiheitlich demokratischen Grundordnung** und der deutschen Verfassung widersprechen

Tabellarische Kurzübersicht

Was?	Durch wen?	Tatvorwurf	Wie?	Muss beinhalten	Unzulässig
Bestandsdaten („Daten zur Vertrags-abwicklung“) u.a. §3 Nr. 3 TKG, §100j StPO	Polizei u.a.	Allg. Straftat oder Ordnungs-widrigkeit oder Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung	Brief, Fax, verschlüsselte E-Mail	Angabe der Erlaubnisnorm	Ungeschützter Kommunika-tionsweg, Bekanntgabe zu vieler Daten an den Provider
Verkehrsdaten („Daten zur Accountnutzung“) §3 Nr. 30 TKG, §96 TKG Abs. 1, §100g StPO	Staatsanwalt mit Richter-vorbehalt	Straftaten von „erheblicher Bedeutung“, §100g Abs. 2 StPO	Gerichtsbe-schluss im Original, gekürzte Ausfertigung ohne Begründung	Vollständige Entscheidungs-formel §100e Abs. 3 StPO, Zeitraum, genaue Maßnahme, Angabe des Vorwurfs, Begründung	Ungeschützter Kommunika-tionsweg, Bekanntgabe zu vieler Daten + Begründung an den Provider
TKÜ („Inhalt der Kommunikation“) §100a StPO	Staatsanwalt mit Richter-vorbehalt	Ausgewählte Straftaten nach Katalog in §100a Abs. 2 StPO	Gerichtsbe-schluss im Original (ggf. Fax vorab), gekürzte Ausfertigung ohne Begründung aber mit Angabe des Vorwurfs	Vollständige Entscheidungs-formel nach §101a Abs. 1 und §100e Abs. 3 StPO, Verhältnismäßig-keit, Dauer, genaue Maßnahme, Angabe des Vorwurfs, Begründung	Ungeschützter Kommunika-tionsweg, Bekanntgabe zu vieler Daten + Begründung an den Provider

Quelle: https://mailbox.org