Datenschutz und Datensicherheit DuD 28/8 (2004) 486-490

Speicherung von Nutzungsdaten durch Anonymisierungdienste im Internet

Welche strafprozessualen Vorschriften zur Überwachung der Telekommunikation sind auf Anonymisierungsdienste anwendbar?

Hannes Federrath und Claudia Golembiewski

Vor einem Jahr verpflichtete das AG Frankfurt den Anonymisierungsdienst AN.ON auf der Grundlage der § 100 g, h StPO zur Speicherung von Zugriffen auf ein Internetforum. Später hob das LG Frankfurt den Beschluss auf. Motiviert durch diesen Einzelfall stellt sich die Frage, welche Möglichkeiten der Strafverfolgung gerade im Hinblick auf Anonymisierungsdienste bestehen und inwiefern die bestehenden strafprozessualen Vorschriften auf AN.ON und andere Anonymisierungsdienste anwendbar sind.

1 Ermittlungsmaßnahmen gegen AN.ON

Im Juli 2003 entstand im Rahmen eines Ermittlungsverfahrens des BKA bzw. der StA Frankfurt am Main wegen des Verbreitens kinderpornographischer Schriften über das Internet der Verdacht, dass ein Benutzer eines u.a. zum Zwecke der Verbreitung von Kinderpornographie betriebenen Internetforums unter einer dem Anonymisierungsdienst AN.ON[1] zugeteilten IP-Adresse im Internet auftrat. Auf Antrag der StA Frankfurt am Main verpflichtete das AG Frankfurt die Betreiber des Anonymisierungsdienstes AN.ON auf der Grundlage der §§ 100 g, h StPO, § 3 Nr. 16 TKG, „Auskunft über die Telekommunikation für die unter der Bezeichnung ‚JAP' registrierten Remote-IP 141.76.1.122[2] für einen Zeitraum von drei Monaten zu erteilen.[3]" Auf die Beschwerde der Betreiber des Dienstes hob das LG Frankfurt den Beschluss mit der Begründung auf, der Beschwerdeführer wende sich zu Recht dagegen, dass es für die begehrte Aufzeichnung von Daten keine Rechtsgrundlage gebe. Die Vorschriften der §§ 100 g, h StPO regelten nur die Fälle, in denen Daten grundsätzlich aufgezeichnet und gespeichert würden, was vorliegend jedoch nicht der Fall sei.[4]

---

[1] Zum zwischen der TU Dresden, der Universität Regensburg und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein durchgeführten und vom Bundesministerium für Wirtschaft und Arbeit geförderten interdisziplinären Forschungsprojekt „AN.ON – Anonymität Online" vgl. Golembiewski, DuD 2003, 129ff.; dieselbe DuD 2003, 596; Berthold/Golembiewski/Steinbrecher, Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Tagungsband zum 8. Dt. Sicherheitskongress, 2003, S. 203ff.; Köpsell/Federrath/Hansen, DuD 2003, 139ff. jeweils m.w.N.

[2] Bei der IP-Adresse 141.76.1.122 handelt es sich um eine derjenigen IP-Adressen, unter der die Nutzer des Anonymisierungsdienstes anonym im Internet surfen.

[3] DuD 2003, 711.

[4] DuD 2003, 712; zusammenfassende Darstellung der Vorgänge bei Golembiewski, DuD 2003, 596 sowie unter http://www.datenschutzzentrum.de/projekte/anon/bericht.pdf.

Ausgehend von diesem Einzelfall bedarf es einer Klärung der Frage, welche Möglichkeiten der Strafverfolgung im Hinblick auf Anonymisierungsdienste bestehen und inwiefern die bestehenden strafprozessualen Vorschriften anwendbar sind. Zunächst werden jedoch kurz die relevanten technischen Sachverhalte erläutert.

2 Technische Grundlagen

Anonymisierungsdienste verbergen den Ursprung oder das Ziel einer Kommunikationsverbindung vor einem Angreifer. Ein Angreifer beobachtet ein Kommunikationsereignis (z.B. Absenden oder Empfangen einer Nachricht), kann es aber dem Absender oder Adressaten nicht zuordnen.

Das zugrunde liegende technische Verfahren eines Anonymisierungsdienstes bestimmt, gegen welche Angreifer ein solcher Dienst schützt. Mögliche Angreifer können sein:

A1. außenstehende Beobachter auf den Kommunikationsleitungen,

A2. einer oder mehrere Betreiber von an der Anonymisierung beteiligten Anonymisierstationen, die beobachtend angreifen,

A3. einzelne oder mehrere *aktive* Angreifer.

Um die Anonymisierung zu erreichen, werden bei allen heute verfügbaren Anonymisierungsdiensten die Nachrichten vom Sender zum Empfänger nicht direkt, sondern über **eine oder mehrere Zwischenstationen** gesendet. Dies gilt sowohl für die inzwischen weit verbreiteten Web-Anonymisierer, mit denen die Inhalte des World Wide Web anonym genutzt werden können, als auch für sog. Remailer, die dem anonymen Versand und Empfang von E-Mails dienen.

2.1 Einzelne Zwischenstation

Anonymisierungsdienste, die als eine einzelne Zwischenstation realisiert sind, können nur vor Außenstehenden (A1) schützen. Beispielsweise kann ein Proxy, der zwischen den Browser und den Webserver geschaltet wird, wie ein Anonymisierungsdienst wirken. Nach diesem Prinzip arbeiten beispielsweise die Anonymisierungsdienste Anonymizer[5] und Rewebber[6]. Da der Anonymisierungsdienst durch genau eine Zwischenstation realisiert wird, kennt dessen Betreiber die IP-Adressen und ggf. weitere identifizierende Informationen des Senders und des Empfängers, d.h. die Kommunikationsverbindung zwischen Sender und Empfänger ist ihm vollständig bekannt. Ein Proxy anonymisiert somit nur gegen außenstehende Beobachter (A1), aber nicht gegen den Betreiber (A2). Zum Schutz vor Außenstehenden muss allerdings die Kommunikation zwischen dem Proxy und den Nutzern verbindungsverschlüsselt erfolgen. Andernfalls könnten Außenstehende leicht die ein- und ausgehenden Nachrichten des Proxys anhand ihrer Bitmuster und ggf. Länge miteinander verketten.

2.2 Mehr als eine Zwischenstation

Anonymisierungsdienste, die durch mehr als eine Zwischenstation realisiert sind, schützen sowohl vor Außenstehenden (A1), als auch auch vor den Betreibern des Anonymisierungsdienstes (A2). Nach diesem Prinzip arbeitet beispielsweise der Anonymisierungsdienst AN.ON, der auf dem von David Chaum erfundenen **Mix-Netz**[7] basiert. Ein Mix verarbeitet mehrfach verschlüsselte Nachrichten, indem er sie umkodiert und zusammen mit weiteren

[5] http://www.anonymizer.com

[6] http://www.rewebber.de

[7] Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

empfangenen Nachrichten anderer Nutzer in veränderter Reihenfolge wieder ausgibt. Praktisch werden mehrere Mixe (wenigstens zwei, bei höherem Sicherheitsbedürfnis auch mehr) von unterschiedlichen Betreibern hintereinander geschaltet, um zu verhindern, dass die gesamte Anonymisierkette von einem einzigen Angreifer beherrscht wird. Der erste Mix kennt den Absender der Nachricht, der letzte Mix kennt den Empfänger der Nachricht. Mittlere Mixe, soweit vorhanden, kennen ihren Vorgänger- und Nachfolger-Mix. Somit kennt der einzelne Mix-Betreiber stets nur einen Teil der gesamten Kommunikationsverbindung. Die praktische Nutzung zum anonymen Zugriff auf das World Wide Web geschieht im AN.ON-Dienst durch das Programm JAP[8], das sich die Benutzer auf ihrem PC installieren. JAP informiert über die verfügbaren Mixe, verschlüsselt die Web-Requests für die ausgewählte Mix-Kaskade und liefert die Webseiten ohne Verlust der Anonymität auf dem Rückweg an den Nutzer.

2.3 Irrwege

Prinzipiell könnten die Nutzer auch auf die Idee kommen, **mehrere Proxies hintereinander** zu schalten, um eine Beobachtbarkeit durch einzelne Betreiber zu verhindern (A2), anstatt das recht aufwendige Mix-Verfahren zu nutzen. Dies führt jedoch zu keiner signifikant erhöhten Sicherheit gegenüber einem einzelnen Proxy. Im ersten und letzten Proxy liegen jeweils die Klartexte der Requests und Responses (unverschlüsselt) vor. Somit ist eine Verbindung enttarnt. Die Hintereinanderschaltung mehrerer Proxies erschwert Außenstehenden (A1) lediglich die zeitliche Korrelation von Nachrichten.

2.4 Kaum Schutz gegen aktive Angreifer

Gegen aktive Angreifer (A3) schützen alle verfügbaren Anonymisierungsdienste leider nur eingeschränkt. Beispielsweise könnte der Betreiber eines Webservers selbst aktiv an alle potentiellen Nutzer seines Webangebots (z.B. als attraktives Werbeangebot getarnte) individualisierte Links schicken. Selbst wenn der anschließende Zugriff über einen Anonymisierer erfolgt, lässt sich der Request seinem Urheber zuordnen. Es gibt nur einen Nutzer, der diesen Link kannte.

Dieses Prinzip wird im Übrigen von Spammern verwendet, um die Gültigkeit einer E-Mail-Adresse zu erkennen. Hierzu kodiert der Spammer in den Link eine für jede E-Mail-Adresse verschiedene Zufallszahl und speichert sie zusammen mit der E-Mail-Adresse in einer Datenbank. Wenn das Opfer den Link abruft, erfährt der Spammer die Zufallszahl und markiert die E-Mail-Adresse des Opfers als gültig. Wird ein solcher Link als abzurufendes Bild in eine HTML-Mail eingebettet, geschieht dies sogar für das Opfer unbemerkt.

Wegen des eingeschränkten Schutzes *aller* praktisch verfügbaren Anonymisierungsdienste vor aktiven Angriffen (A3) sollen diese in den weiteren Betrachtungen unberücksichtigt bleiben.

3 Protokollierung von Nutzungsdaten

Anonymisierungsdienste sollten sinnvollerweise keine Protokolle über die von ihnen anonymisierten Verbindungen führen. Nur unter der Annahme, dass der Benutzer dem Betreiber eines Proxy oder den Betreibern einer Mix-Kaskade vertraut, dass die Protokolle nicht missbraucht werden, ist die Dienstnutzung trotz des Führens von Log-Files für ihn sinnvoll.

Anonymisierungsdienste dürfen nach § 6 Abs. 1 TDDSG Protokolle über die Dienstnutzung nur führen, soweit dies zur Aufrechterhaltung des Dienstes oder für Abrechnungszwecke erforderlich ist. Ungeachtet dessen ist das Speichern von Nutzungsdaten für das Vertrauen der

[8] JAP ist unter http://www.anon-online.de kostenlos verfügbar.

Nutzer in den Anonymisierungsdienst völlig kontraproduktiv, da es eine nachträgliche Rückverfolgung ermöglicht und somit dem Ziel der Anonymisierung prinzipiell entgegensteht.

Die Protokollierung der Nutzungsdaten durch einen Anonymisierer genügt allein nicht, um Kommunikationsverbindungen bis zu einer Person zurückzuverfolgen. In den Log-Files des Anonymisierers werden lediglich die IP-Adressen der Benutzer gespeichert. Nur der Access-Provider kann, soweit er seinerseits Protokolle führt, über die Zuordnung einer IP-Adresse zur Identität des dahinter stehenden Nutzers Auskunft erteilen.

4 Auskunftspflicht für die Vergangenheit

Anonymisierungsdienste sind nicht verpflichtet, Protokolle über die Dienstnutzung zu führen. Somit besteht bei deren **Nichtvorhandensein** für Strafverfolgungsbehörden, andere Bedarfsträger sowie Auskunftssuchende (z.B. Rechteinhaber bei Verstößen gegen das Urheberrecht) auch keine Möglichkeit, Auskunft über vergangene Kommunikationsereignisse vom Anonymisierungsdienst zu bekommen, da keinerlei Daten vorhanden sind, die herausgegeben werden könnten.

Sofern **Nutzungsdaten vorhanden** sind, ist der Betreiber zur Auskunft verpflichtet. §§ 100 g, h StPO ermöglichen als Nachfolgeregelung zu § 12 FAG den Erlass einer Auskunftsanordnung über Telekommunikationsverbindungsdaten. Diese Daten werden in § 100 g Abs. 3 StPO näher definiert. Der in Abs. 3 Nr. 1 StPO genannte Begriff der *Kennung* erfasst hierbei auch die IP-Adresse eines Computers.[9] Die Auskunftsverpflichtung nach §§ 100 g, h StPO unterliegt einem richterlichen Vorbehalt.

Handelt es sich beim Anonymisierungsdienst um eine einzelne Zwischenstation (Proxy), genügt allein deren Protokoll zur Enttarnung der Kommunikationsbeziehungen. Werden mehrere Zwischenstationen verwendet, genügt normalerweise das Protokoll einer einzelnen Zwischenstation nicht mehr: Bei Mix-Kaskaden müssen alle beteiligten Mixe Protokolle führen, um über die Vergangenheit Auskunft geben zu können.

Praxis

Im AN.ON-Dienst[10] und bei Anonymizer[11] werden von vornherein keine Nutzungsdaten gespeichert. Eine Auskunftserteilung für die Vergangenheit ist daher nicht möglich. Bei Rewebber werden die Domain, Top-Level-Domain und die ersten drei Stellen der vierstelligen IP-Adresse mitprotokolliert.[12] Bei mehreren Nutzern aus der gleichen Domain bleibt der Einzelne trotz Protokollierung somit in dieser Gruppe anonym.

Der AN.ON-Dienst und Anonymizer sind insoweit praktische Beispiele dafür, dass das Argument, die Protokollierung von Nutzungsdaten sei zur Aufrechterhaltung eines Dienstes erforderlich, widerlegt werden kann. Einschränkend ist jedoch festzuhalten, dass in Situationen, die vom Anonymisierer als Angriff gewertet werden, tatsächlich im Einzelfall eine Protokollierung erfolgen kann. Beispielsweise können viele beim ersten Mix schnell hintereinander eintreffende Verbindungsversuche, die von einer einzigen IP-Adresse ausgehen, als Überflutungsangriff gewertet und diese IP-Adresse vorübergehend (z.B. einige Minuten) von der Dienstnutzung ausgeschlossen werden. Hierzu genügt es, die Angriffsereignisse im Hauptspeicher zu halten. Nicht immer ist es nötig, derartige Situationen in eine Datei zu protokollieren und damit zu fixieren.

[9] BT-Drucksache 14/7008, S. 7; Meyer-Goßner, StPO, 46. Aufl., § 100g Rn. 4.
[10] http://anon.inf.tu-dresden.de/fragen/konzept.html, Stand 5. Juli 2004.
[11] http://www.anonymizer.com/docs/privacy_statement.shtml, Stand 5. Juli 2004.
[12] http://www.rewebber.de/policy/index.php3.de, Stand 5. Juli 2004.

5 Auskunftspflicht für die Zukunft

Nach dem Wortlaut des § 100 g Abs. 1 Satz 3 StPO darf sich die Auskunft auch auf einen **zukünftigen Zeitraum** erstrecken. Sobald innerhalb des Verpflichtungszeitraums ein Ereignis protokolliert wird, das von der Auskunftsverpflichtung erfasst wird, ist Auskunft zu geben. Der Auskunftsanspruch ist allerdings auf solche Daten beschränkt, die seitens des Anonymisierungsdienstes nach bestehenden Regelungen zulässigerweise erhoben und gespeichert werden und insoweit bereits vorliegen.

Bei einer einzelnen Zwischenstation (Proxy) genügt dessen Protokoll zur Enttarnung, bei hintereinander geschalteten Mixen müssten alle Mixe Protokolle führen.

Wie oben dargelegt, werden beim AN.ON-Dienst entsprechend den Vorgaben des TDDSG keine Daten erhoben und gespeichert, die Rückschlüsse auf Nutzer zulassen könnten. Ein Beschluss auf der Grundlage der §§ 100 g, h StPO wird daher nicht zu verwertbaren Ergebnissen führen. Aus §§ 100 g, h StPO lässt sich auch keine Verpflichtung entnehmen, Daten nur für Zwecke der Strafverfolgung zu speichern, wie sie § 100 a StPO ermöglicht[13]. Allerdings ist der Wortlaut der Vorschrift missverständlich. So führt *Gercke* aus, es könne sogar die Auffassung vertreten werden, die Herausgabeanordnung beinhalte eine Pflicht, sämtliche in § 100 g Abs. 3 StPO genannten Daten zu erheben und zu speichern.[14] Entgegen im Gesetzgebungsverfahren mehrfach geäußerter Wünsche ist allerdings gerade davon abgesehen worden, die Möglichkeit einer Verpflichtung zur Anordnung der Aufzeichnung zu schaffen, weil die Diensteanbieter hinsichtlich solcher Daten, die sie nach dem Telekommunikationsrecht nicht erheben und speichern dürfen, lediglich zur Ermöglichung der Überwachung und Aufzeichnung unter den Voraussetzungen der §§ 100 a, b StPO verpflichtet bleiben sollen.[15]

Speicherbegriff

Den aus seiner Sicht bestehenden Widerspruch zwischen Wortlaut und Gesetzesbegründung versucht *Gercke* auf andere Weise zu lösen. So vertritt er die Auffassung, sämtliche in § 100 g Abs. 3 StPO genannten Verbindungsdaten müssten zur Ermöglichung eines Datenübertragungsvorgangs von den Diensteanbietern zumindest kurzfristig zwischengespeichert werden. Es liege daher eine technisch notwendige kurzfristige Speicherung vor, so dass sämtliche Daten an die Strafverfolgungsbehörden herausgegeben werden müssten.[16] Dieser Auffassung kann nicht gefolgt werden.

Zur Anonymisierung von Verbindungen im AN.ON-Dienst ist es notwendig, die Zuordnung zwischen der eingehenden und ausgehenden Verbindung eines Mixes für die Dauer der Verbindung in einer entsprechenden Datenstruktur *im Hauptspeicher* zu halten. Beim ersten Mix wird in dieser Datenstruktur die IP-Adresse des Absenders und eine Kanalnummer, auf der die Daten an den nächsten Mix weitergereicht werden, gespeichert. Bei mittleren Mixen ist es jeweils die eingehende und ausgehende Kanalnummer. Beim letzten Mix wird die eingehende Kanalnummer und die IP-Adresse des aufgerufenen Servers gespeichert.

Solange auf einer anonymisierten Verbindung Daten empfangen oder gesendet werden, bleibt der dadurch hergestellte anonyme Kanal erhalten. Nachdem alle Daten gesendet wurden, werden die Datenstrukturen wieder aus dem Hauptspeicher der Mixe entfernt. Die Dauer einer Verbindung bestimmt somit die Speicherdauer dieser Datenstrukturen. Typischerweise liegt sie zwischen einigen Millisekunden (beim Abruf gewöhnlicher Webseiten) und einigen Minuten (beispielsweise beim Abruf sehr großer Dateien, während die Internetverbindung sehr

[13] Siehe BT-Drucksache 14/7008, S. 7.
[14] Gercke, DuD 2004, 210 (213).
[15] Meyer-Goßner, StPO, 46. Aufl., § 100g Rn. 10 unter Hinweis auf BT-Drucks. 14/7258, S. 4.
[16] Gercke, DuD 2004, 210 (213).

langsam ist). Zu keinem Zeitpunkt werden die Daten in einem nicht-flüchtigen Speicher abgelegt, da dies für die Diensterbringung weder notwendig noch für den effizienten Betrieb eines Mixes sinnvoll wäre, da der Speichervorgang bei Verwendung eines nicht-flüchtigen Speichers (z.B. einer Festplatte) vergleichsweise erhebliche Zeit beansprucht.

Entgegen den Ausführungen von *Gercke* handelt es sich bei der gerade beschriebenen technisch notwendigen Zwischenspeicherung von Daten beim AN.ON-Dienst nicht um eine Speicherung im datenschutzrechtlichen Sinne. Die Speicherung von Daten wird beispielsweise in § 3 Abs. 4 Satz 2 Nr. 1 BDSG definiert. Nach dieser Legaldefinition ist unter dem Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung zu verstehen. Der Begriff des Speicherns enthält vier Komponenten. So besteht die Tätigkeit im Erfassen, Aufnehmen oder Aufbewahren; ihr Objekt sind personenbezogene Daten; das Medium ist ein Datenträger; und der Zweck besteht in der weiteren Verarbeitung oder Nutzung.[17] Entscheidend ist an dieser Stelle das Vorliegen des letztgenannten Merkmals. Eine Speicherung liegt nämlich nur dann vor, wenn die Daten zum „Zwecke ihrer weiteren Verarbeitung oder Nutzung“ fixiert werden, denn nicht die Existenz von Daten, sondern erst ihre drohende Verwendung tangiert die Belange Betroffener.[18] So kommt die Zweck-Klausel nicht bei sog. Zwischenspeicherungen im Ablauf eines automatisierten Verarbeitungsprozesses zum Tragen. Nur wenn die zwischengespeicherten Daten nicht alsbald gelöscht werden, kann ihre Wirkung nach außen dringen und die Daten sind in diesem Falle „gespeichert.“[19]

Beim AN.ON-Dienst handelt es sich um eine Zwischenspeicherung im genannten Sinne. Die Daten werden lediglich kurzzeitig zwischengespeichert, um dem Nutzer den anonymen Abruf der angefragten Inhalte zu ermöglichen. Nach dem Ende der Verbindung erfolgt eine sofortige Löschung. Die Daten werden zu keinem Zeitpunkt fixiert, da eine weitere Verarbeitung oder Nutzung nicht bezweckt ist. Personenbezogene Daten über die Nutzer des Anonymisierungsdienstes werden insoweit nicht gespeichert und können daher auch nicht der Auskunftsverpflichtung gemäß §§ 100 g, h StPO unterliegen. Im Ergebnis kann eine Anordnung zur Aufzeichnung von Zugriffen über den AN.ON-Dienst somit nicht auf der Grundlage der §§ 100 g, h StPO erfolgen. Diese Rechtsauffassung hat das LG Frankfurt am Main in seinem Beschluss vom 15. September 2003 bestätigt.

Träfe die Auffassung von *Gercke* zu, dass die Verbindungsdaten durch die Betreiber von Anonymisierungsdiensten i.S.d. Legaldefinition von „Speichern“ gespeichert werden, wäre ein Auskunftsersuchen nach § 100 a StPO überflüssig, da ein Auskunftsersuchen nach § 100 g StPO stets Erfolg hätte, soweit sich die Auskunft auf Verbindungsdaten i.S.d. § 100 g Abs. 3 StPO bezieht. Dies beträfe im Übrigen nicht nur Anonymisierungsdienste, sondern *alle* von der Vorschrift adressierten Dienste, da eine (kurzzeitige) Zwischenspeicherung zur Diensterbringung stets erforderlich ist. Somit müsste in allen Fällen, in denen die übrigen Voraussetzungen nach § 100 g StPO vorliegen, stets aufgezeichnet werden. Gerade dies entspräche jedoch nicht dem Sinn und Zweck der Norm und war auch vom Gesetzgeber nicht gewollt.

6 Speicherpflicht für die Zukunft

Im Folgenden ist die Frage zu beantworten, ob und wie ein Anonymisierungsdienst dazu verpflichtet werden kann, Nutzungsdaten zu erheben und in Protokollen zu speichern.

---

[17] Dammann, in: Simitis (Hrsg.), BDSG, 7. Aufl., § 3 Rn. 120.

[18] Ebenda, Rn. 126.

[19] Ebenda, Rn. 130, in diesem Sinne auch Nungesser, HDSG, 2. Aufl., § 2 Rn. 46 und Gola/Schomerus, BDSG, 7. Aufl., § 3 Rn. 28.

Während §§ 100 g, h StPO grundsätzlich nur die Auskunft über vorhandene Telekommunikationsverbindungsdaten ermöglichen, kann auf der Rechtsgrundlage von §§ 100 a, b StPO die *künftige Überwachung* der Telekommunikation angeordnet werden. Eine Verpflichtung zur Protokollierung personenbezogener Daten der Nutzer eines Telekommunikationsdienstes kann insoweit lediglich auf Grund letztgenannter Rechtsvorschriften angeordnet werden. Unter den dort genannten Voraussetzungen darf die Überwachung und Aufzeichnung der Telekommunikation angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine der im Katalog dieser Vorschriften genannten Taten begangen hat oder zu begehen versucht. Voraussetzung ist außerdem, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt. Die materiellen und formellen Hürden für eine Überwachung nach § 100 a StPO (Straftat nach einem präzisen Straftatenkatalog) liegen erheblich höher als bei einer Auskunft gemäß §§ 100 g, h StPO („Straftat von erheblicher Bedeutung“).

Erhält ein anonymisierender Proxy eine derartige Anordnung, ist er verpflichtet, alle zu anonymisierenden Verbindungen auf die im Beschluss genannte Kennung zu überprüfen und die Telekommunikation aufzuzeichnen. Die Aufzeichnungspflicht umfasst neben den Inhalten auch die Verbindungsdaten. Für die Rückverfolgung (Enttarnung bzw. Deanonymisierung) einer anonymisierten Verbindung sind jedoch primär die Verbindungsdaten interessant.

Besteht der Anonymisierungsdienst aus mehreren Mixen mit unabhängigen Betreibern, müssen alle Mix-Betreiber eine richterliche Anordnung erhalten, da eine anonyme Kommunikationsverbindung nur unter Mithilfe aller beteiligten Mix-Betreiber rückverfolgt werden kann.

Je nachdem, ob der Absender oder der Empfänger einer Nachricht enttarnt werden soll, ist dem jeweils gegenüber liegenden Endpunkt der anonymisierten Verbindung die zu überwachende Kennung mitzuteilen:

– Soll der Absender eines Web-Requests enttarnt werden, so ist dem letzten Mix die Kennung (IP-Adresse oder URL) des Ziels mitzuteilen.

– Soll ermittelt werden, mit welchen IP-Adressen ein Nutzer anonym kommuniziert bzw. welche URLs er anonym aufruft, ist dem ersten Mix die Kennung (IP-Adresse) des zu überwachenden Nutzers mitzuteilen.

Alle anderen Mixe müssen verpflichtet werden, die Überwachung zu unterstützen. Da die Kanalnummern für die zu enttarnenden Verbindungen zum Zeitpunkt der Anordnung noch nicht bekannt sind (sie werden erst während des Aufbaus der anonymen Verbindung erzeugt), kann die Anordnung keine Kennung enthalten.

Sobald der End-Mix, dem die Kennung bekannt ist, eine zu überwachende Verbindung entdeckt, speichert er die Kennung und Zugriffszeit und teilt seinem benachbarten Mix die zu enttarnende Verbindung mit u.s.w. bis der Mix des anderen Endpunkts informiert ist.

Nur der andere End-Mix kennt die gesuchte IP-Adresse und speichert sie zusammen mit der Zugriffszeit in einem Log-File ab.

Schließlich werden die im ersten und letzen Mix aufgezeichneten Daten miteinander verknüpft. Die Kommunikationsbeziehung ist damit enttarnt.

Fazit

Eine Anordnung zur Auskunft über vergangene und zukünftige Telekommunikationsverbindungen nach §§ 100 g, h StPO verpflichtet die Betreiber von Anonymisierungsdiensten *nicht* zur Erhebung und Speicherung von Nutzungsdaten. Die Erhebung und Speicherung von Nutzungsdaten ist detailliert in § 6 Abs. 1 TDDSG geregelt. Die Speicherung personenbezogener Daten über Nutzer, zu denen auch die IP-Adresse gehört, ist lediglich in eng begrenzten Fällen zulässig, nämlich dann, wenn es technisch erforderlich ist, um den Dienst zu erbringen oder wenn dies für Abrechnungszwecke erforderlich ist. Dies ist bei AN.ON jedoch nicht der Fall.

Eine Anordnung zur Auskunft über die Telekommunikation nach §§ 100 a, b StPO verpflichtet die Betreiber eines Anonymisierungsdienstes zur Aufzeichnung der Nutzungsdaten. Während bei einfachen Proxies für die Überbrückung des Anonymisierungsdienstes eine einzige Anordnung genügt, müssen bei Mix-Kaskaden alle beteiligten Betreiber einer Anonymisierkette (Mix-Kaskade) verpflichtet werden.