Praktische Nutzung der Vorratsdatenspeicherung

Artikel von Holger Münch, Präsident des Bundeskriminalamts, in der Zeitschrift für Rechtspolitik, Heft 5, 2015

Seit den 90er Jahren hat sich die Welt gravierend verändert: Globalisierung und die Entwicklung von World Wide Web und mobiler Erreichbarkeit führten zu völlig neuen Formen der Vernetzung. Weltweite Kommunikation und Zusammenarbeit ist heute so einfach und selbstverständlich wie nie zuvor. Dies gilt für Wirtschaft, Wissenschaft und Gesellschaft, aber leider auch für Kriminelle. Die Arbeit der Sicherheitsbehörden muss an diese Gegebenheiten und die damit einhergehenden neuen Möglichkeiten für Kriminelle und die neuen Kriminalitätsphänomene angepasst werden. Ein wichtiger Baustein ist hierbei, dass die Strafverfolgungsbehörden auf digitale Spuren an Cyber-Tatorten zurückgreifen können, die für die Tataufklärung ebenso maßgeblich sind wie zum Beispiel Fingerabdrücke oder DNA-Spuren an realen Tatorten.

I. AUSWIRKUNGEN DES WEGFALLS VON MINDESTSPEICHERFRISTEN

Nachdem das BVerfG am 2.3.2010 entschieden hat, dass die Regelungen zu Mindestspeicherfristen mit dem deutschen Grundgesetz nicht vereinbar sind, hat das BKA eine Erhebung zu den Auswirkungen des Wegfalls der Mindestspeicherfristen auf die Strafverfolgung durchgeführt.[1] Insgesamt wurden Auskunftsersuche bezogen auf 5082 Anschlüsse im Zeitraum vom 2.3.2010 bis 26.4.2011 erfasst und ausgewertet. Anlasstat für die Auskunftsanfrage war in 1898 Fällen (rd. 45) besonders schwerer sowie banden- und gewerbsmäßig begangener (Computer-) Betrug, 1639 Fälle (rd. 39) entfielen auf den Deliktsbereich der Verbreitung, des Erwerbs oder Besitzes kinder- und jugendpornografischer Schriften oder Straftaten gegen die sexuelle Selbstbestimmung.

Mit Abstand am häufigsten (zu rd. 90) war die Anfrage auf die hinter einer IP-Adresse stehenden Bestandsdaten gerichtet. Zu wurden retrograde Verkehrsdaten, vor allem in Fällen schwerster Kriminalität, angefragt. Diese Verteilung ergibt sich zum einen aus dem Aufgabenzuschnitt des BKA angesichts der gem. § BKAG § 4 BKAG geführten Ermittlungsverfahren und kann nicht 1:1 auf die Bandbreite der generellen Länderzuständigkeiten übertragen werden. Zudem ist zu be-

[1] Bundeskriminalamt, Abschlussbericht Stand der statischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu
ten“ http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html (zuletzt aufgerufen am 7.5.2015).

rücksichtigen, dass das Anfragevolumen bezüglich der Zuordnung dynamisch vergebener IP-Adressen deutlich höher ist als bei der Auskunft von Verkehrsdaten bei der klassischen Telefonie (Festnetz oder Mobilfunk). Anders als bei sich ständig ändernden IP-Adressen sind die Anschlüsse bei der Telefonie (Rufnummern) in der Regel statisch.

Untersucht wurde auch, welche Auswirkungen die Nichtbeauskunftung auf die Aufklärung der Straftaten bzw. die Gefahrenabwehr hatte. Im Bereich der Strafverfolgung konnte in 83 der Fälle (3521 Anschlüsse) die Straftat nicht aufgeklärt werden. Dieses Ergebnis verdeutlicht, dass Verkehrsdaten bei der Strafverfolgung häufig den ersten, sichersten und zugleich effizientesten Ermittlungsansatz darstellen.

Schließlich wurde auch die polizeifachlich erforderliche Speicherdauer untersucht. Ergebnis war hier, dass in 33 der Fälle (1427 Anschlüsse) ein Mindestspeicherzeitraum von zwei bis fünf Monaten und in 61 der Fälle (2628 Anschlüsse) ein Mindestspeicherzeitraum von sechs Monaten erforderlich gewesen wäre. Nur in 6 der Fälle (237 Anschlüsse) wäre ein Mindestspeicherzeitraum von einem Monat ausreichend gewesen. Die Ergebnisse der Untersuchung des BKA zeigen zudem, dass die polizeiliche Reaktionszeit nur geringen Einfluss auf den erforderlichen Mindestspeicherzeitraum hat, da die Polizei in der Regel innerhalb von maximal sieben Tagen reagiert. Das heißt konkret, dass zwischen Kenntniserlangung über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens in 86 der Fälle maximal sieben Tage lagen, die Polizei also schnell handelte, nachdem sie von der Tat erfuhr. Da Polizei bzw. Staatsanwaltschaft jedoch keinen Einfluss darauf haben, wie schnell sie durch Anzeige oder Ähnliches überhaupt von dem Fall und somit dem Vorliegen möglicherweise ermittlungsrelevanter Verkehrsdaten erfahren, ist es wichtig, dass Daten nicht nur für wenige Tage gespeichert werden, sondern auch dann noch zur Verfügung stehen, wenn die Polizei zu einem späteren Zeitpunkt von der Straftat erfährt.

II. PRAKTISCHE FÄLLE

Verkehrsdaten sind bei der Polizeiarbeit in verschiedenen Konstellationen und unterschiedlicher Form von Bedeutung: 1. Durch die Zuordnung von IP-Adressen zu einer Person kann etwa herausgefunden werden, wer Kinderpornografie auf einer Internetseite aufgerufen hat, 2. durch die Auswertung von Funkzellendaten kann geklärt werden, wer sich an einem Tatort, an dem beispielsweise ein Mord geschehen ist, aufgehalten hat und 3. durch die Auswertung von Telekommunikationsverkehrsdaten kann zum Beispiel nachvollzogen werden, mit wem ein mutmaßlicher Terrorist in Kontakt stand und steht. Nachfolgende Beispiele zeigen auf, wie unentbehrlich Mindestspeicherfristen für die Strafverfolgungsbehörden sind.

1. Feststellung der Inhaber von IP-Adressen

Die Feststellung des Inhabers einer IP-Adresse ist in vielen Deliktsbereichen ein wichtiger, manchmal sogar der einzige Ermittlungsansatz.

a) Kinderpornografie

Der Austausch von kinder- und jugendpornografischem Material, von entsprechenden Bildern und Videos, findet inzwischen weitgehend über das Internet statt. Die Bilder und Videos werden zum Teil in versteckten Foren, zum Teil aber auch öffentlich gehandelt und getauscht. Die Strafverfolgungsbehörden erfahren von dem inkriminierten Material auf verschiedenen Wegen: Manchmal melden Bürger die Webseiten, häufiger erfahren die deutschen Behörden von solchen Seiten aber von ausländischen Sicherheitsbehörden, wenn diese Server sicherstellen oder die Informationen anderweitig im Zuge eigener Ermittlungen erhalten. In den allermeisten Fällen ist der einzige Hinweis auf den Täter die IP-Adresse. Aufgabe der Strafverfolgungsbehörden ist es dann, die Personen hinter den IP-Adressen zu ermitteln und aufzuklären, wer sich kinderpornografisches Material bestellt oder dieses verbreitet hat. Allein im Jahr 2014 wurden über 6000 Fälle des Besitzes und der Verbreitung von kinderpornografischem Material in der Polizeilichen Kriminalstatistik registriert. Ohne die Möglichkeit die genutzten IP-Adressen Personen zuzuordnen, können die Sicherheitsbehörden diese Täter nur schwer und häufig nicht identifizieren.

Deutlich wird die Bedeutung der Mindestspeicherfristen für den Phänomenbereich Kinderpornografie an einem Beispiel aus der Zeit, als Verkehrsdaten in Deutschland noch retrograd gespeichert wurden. Die deutsche Polizei erhielt von einer ausländischen Sicherheitsbehörde Protokolldateien, die von einem Server mit kinderpornografischem Material sichergestellt wurden. Diese Protokolldateien dokumentierten die Zugriffe auf die Bilder. Es wurde festgestellt, dass mehr als 3500 Browser-Zugriffe mit deutschen IP-Adressen erfolgt waren. Mit Hilfe von Anfragen bei den Zugangsprovidern zu den IP-Adressen konnten fast alle Anschlussinhaber identifiziert werden. Ein Erfolg, der ohne Mindestspeicherfristen nicht möglich gewesen wäre.

b) Betrug

Betrugsstraftaten werden immer häufiger im Internet oder mit Hilfe von Telekommunikationseinrichtungen begangen. Indem sich Täter beispielsweise mit fremden oder gefälschten Zugangsdaten bei Internet-Providern einloggen, können sie unbefugt so genannte SIM-Locks bei Mobiltelefonen entsperren und erhalten so Zugang zu Telefonanschlüssen. Mit diesem Zugang können sie 900er-Nummern anwählen und so hohe Kosten für die Betroffenen verursachen. Notwendig, um den Täter zu ermitteln ist die IP-Adresse. Mit der IP-Adresse können die bei der Zugangserschleichung zu Telefonanschlüssen/-anlagen anfallenden Logdaten ausgewertet und Täter identifiziert werden.[2]

[2] Vgl. Presseinformation des BKA v. 8.11.2010 \u201eDie Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung\u201c;

c) Botnetz

Die Gefahr, Opfer eines Cyberangriffs zu werden, nimmt ständig zu. Jeden Tag werden Firmen, Regierungen und Privatleute angegriffen und geschädigt. Rechner und Haushaltsgeräte werden von Cyberkriminellen für ihre Zwecke missbraucht. Um solche Straftaten aufklären zu können, und die Botnetze zu vernichten, ist es unentbehrlich zu wissen, welche Geräte Teil des Netzes sind. Wenn bekannt ist, wer hinter der IP-Adresse eines Bot steht, wer Inhaber eines missbrauchten Geräts ist, können die Opfer kontaktiert werden, die dann ihre missbrauchten Geräte bereinigen und aus dem Botnetz trennen können. Anfang 2014 wurden zum Beispiel durch ein aus mehr als 100.000 Geräten bestehendes Botnetz 750.000 Spammails versandt. Das Botnetz bestand aus Heimroutern, Multimedia-Anlagen, Smart-TVs, auch ein Kühlschrank konnte als Bot identifiziert werden. Wegen fehlender Mindestspeicherfristen war es allerdings nicht möglich, die IP-Adressen zuzuordnen und so das Botnetz auszuschalten.

2. Digitale Spuren: Funkzellenauswertung

Mit Funkzellendaten kann im Einzelfall festgestellt werden, welches Mobiltelefon wann in welcher Funkzelle eingeloggt war bzw. wann ein Kommunikationsvorgang stattfand. Dies lässt, je nachdem wie groß die Funkzelle ist, Rückschlüsse zu, wo sich das Mobilfunkendgerät (bzw. die SIM-Karte) wann befand.

a) Enkeltrick

Zunehmend geraten auch ältere Menschen ins Visier von Kriminellen. Ein Beispiel ist der so genannte Enkeltrick, bei dem die Täter vorher ausfindig gemachte ältere Menschen anrufen und ihnen vorgaukeln, in einem verwandtschaftlichen Verhältnis zu ihnen zu stehen und dringend Geld zu benötigen. Diese Form des gewerbsmäßigen Betrugs hat häufig schwerwiegende finanzielle, seelische und gesundheitliche Folgen für die Opfer. Um die Täter ermitteln zu können, ist es notwendig zu wissen, wer das Opfer von wo aus angerufen hat, wer vom Täter zur Geldabholung beauftragt wurde und wer das Geld wo abgeholt hat. Hierzu sind Verkehrsdaten und insbesondere Standortdaten notwendig.

b) Autobahnschütze

Von 2009 bis 2013 kam es zu einer Serie von Schüssen auf deutschen Fernstraßen im fließenden Verkehr. Menschen wurden gefährdet, nur mit Glück kam es nicht zu Todesfällen. Durch die erfolgreiche Arbeit der Polizei konnte der Täter letztendlich gefasst werden. Nach der Identifizierung des Täters wurden zu den auf ihn registrierten Mobilfunknummern Verkehrsdaten erhoben. Auf Grund des glücklichen Umstands, dass der Tatverdächtige eine Rufnummer eines Anbieters hatte, der die abrechnungsrelevanten Daten 90 Tage speicherte, konnte dessen Anwesenheit mit Hilfe der Standortdaten an einigen eindeutig festgestellten Tatorten zur Tatzeit auch noch retrograd dokumentiert werden, was die Verdachtslage zu diesem Zeitpunkt deutlich verstärkte und

---

http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen.html (zuletzt aufgerufen am 8.5.2015).

wesentlich zur Anordnung der Untersuchungshaft beitrug. Wären die Daten gelöscht gewesen, hätte ein entscheidendes Puzzleteil zur Überführung des Täters gefehlt.

3. Strukturermittlungen: Retrograde Telekommunikationsverkehrsdaten

Mit Hilfe von Telekommunikationsverkehrsdaten kann herausgefunden werden, welche Telefonanschlüsse wann miteinander verbunden waren.

Wie wichtig die Speicherung von Verkehrsdaten ist, zeigt sich besonders eindrucksvoll am Beispiel der Bekämpfung des internationalen Terrorismus. Immer mehr Menschen reisen aus Deutschland und ganz Europa in den Krieg nach Syrien und in den Irak, um sich dort am \u201eJihad\u201c zu beteiligen. Der Ausreise geht in der Regel ein Radikalisierungsprozess voraus. In diesem haben die Frauen und Männer häufig Kontakt mit der salafistischen Szene und/oder mit Personen, die den Sicherheitsbehörden als radikale Islamisten bereits bekannt sind. Durch die Reisen in Kampfgebiete und Ausbildungslager ergeben sich neue Kontakte. So entsteht ein immer dichteres Netzwerk. Die Islamisten kommunizieren miteinander über verschiedenste Medien. Über die stattgefundene Kommunikation können die Sicherheitsbehörden Rückschlüsse ziehen, wer mit wem in Kontakt steht und gegebenenfalls auch welche Gefahr von diesen Personen ausgeht. Die Verbindungen zu kennen ist unerlässlich, um effektive Gefahrenabwehr zu betreiben, um Ausreisen zu verhindern und um die von aus Kampfgebieten Zurückgekehrten ausgehende Gefahr einschätzen zu können.

Praktisch zeigte sich die Bedeutung von Mindestspeicherfristen in diesem Bereich bei den Terroranschlägen von Paris im Januar 2015. Da Verkehrsdaten in Frankreich gespeichert werden, konnten die französischen Sicherheitsbehörden Kontakte der Terroristen untereinander und zu anderen Islamisten schnell nachvollziehen. Die gespeicherten Verbindungsdaten verhinderten die Anschläge zwar nicht, sie halfen aber bei einer schnellen Aufklärung und Bewertung der Bedrohung.

III. AUSGESTALTUNG DER SPEICHERUNG

Die hohe Bedeutung von Mindestspeicherfristen für Verkehrsdaten und deren Nutzung durch die Sicherheitsbehörden, haben das BVerfG[3] und der EuGH[4] in ihren Entscheidungen zu den Regelungen über die Mindestspeicherfristen hervorgehoben.

So hat das BVerfG in seinem Urteil festgestellt, dass eine Rekonstruktion der Telekommunikationsverbindungen für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Be-

3 NJW 2010, Seite 833.
4 NJW 2014, Seite 2169.

deutung ist und gesetzlich festgelegte Mindestspeicherfristen unter bestimmten Voraussetzungen mit Art. GG Artikel 10 GG vereinbar und daher nicht grundsätzlich verfassungswidrig sind.[5]

Der EuGH hat klar gemacht, dass die Speicherung von Verkehrsdaten ein geeignetes und nützliches Mittel zur Verhütung und Verfolgung schwerer Straftaten darstellt und damit in der Zielsetzung dem Gemeinwohl dient.[6] Er führte weiter aus, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die gespeicherten Daten Möglichkeiten zur Aufklärung schwerster Straftaten böten und die wirksame Bekämpfung von Organisierter Kriminalität und Terrorismus in hohem Maße von der Nutzung moderner Ermittlungstechniken abhinge.[7]

Insofern kann kein Zweifel an der Erforderlichkeit und grundsätzlichen rechtlichen Zulässigkeit von gesetzlich geregelten Speicherfristen für Verkehrsdaten bestehen. Entscheidend ist, dass die konkreten Regelungen zu den Speicherfristen verfassungskonform ausgestaltet sind. Nur so vertrauen die Bürgerinnen und Bürger dieser Maßnahme und nur so haben Telekommunikationsanbieter und Strafverfolgungsbehörden Handlungs- und Rechtssicherheit.

Nachdem über die Ausgestaltung von Mindestspeicherfristen lange verhandelt wurde, präsentierten Bundesjustizministerium und Bundesinnenministerium am 15.4.2015 gemeinsame Leitlinien zur verfassungs- und europarechtskonformen Ausgestaltung einer Regelung zu Mindestspeicherfristen.[8] Ein entsprechender Gesetzentwurf wurde erarbeitet.[9]

Nach diesen Plänen sollen Verkehrsdaten, wie etwa die beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, Standortdaten und IP-Adressen gespeichert werden. Dienste der elektronischen Post sind, im Gegensatz zu den alten Regelungen in der RL 2006/24/EG und dem alten TKG, ausgenommen und werden nicht gespeichert. Diese Regelung trägt der Forderung des EuGH Rechnung, dass nicht alle Daten gespeichert werden sollen.

Eine weitere Neuerung ist, dass die Speicherdauer zwischen Standortdaten und den weiteren Verkehrsdaten differenziert wird. Die Standortdaten werden für nur vier Wochen, die übrigen Verkehrsdaten im Bereich der Telefonie sowie IP-Adressen zehn Wochen gespeichert werden.

Die Nutzung der Standortdaten soll zudem eingeschränkt werden, indem Standortdaten, die zwar zu Abrechnungszwecken für bis zu sechs Monate gespeichert werden können (§ TKG § 97 TKG § 97 Absatz III TKG), retrograd nur noch unter den strengen Voraussetzungen des neuen § STPO § 100g STPO § 100G Absatz II StPO (Katalogtaten) und nur für den Zeitraum der nach § TKG § 113b TKG bestehenden Speicherpflicht von vier Wochen abgerufen werden dürfen. Die Erhebung von aus geschäftlichen Gründen gespeicherten Standortdaten wird damit grundsätzlich ausgeschlossen. Aus polizeilicher Sicht wäre wünschenswert, dass auf die zu Abrechnungs-

5 NJW 2010, Seite 833 Randnummer 215 ff.
6 NJW 2014, Seite 2169 Randnummer 41 - 43.
7 NJW 2014, 2169 Randnummer 49, 51.
8 Vgl. http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/20150415-Leitlinien-HSF.pdf?__blob=publicationFile (zuletzt aufgerufen am 7.3.2015).
9 BT-Drs. 18/5088 v. 9.6.2015.

zwecken gespeicherten Daten zumindest solange retrograd zurückgegriffen werden kann, wie diese rechtmäßig (also idR zu Abrechnungszwecken) gespeichert sind. Mit einer solchen Regelung würde auch keine Schutzlücke entstehen, da § STPO § 100g StPO einen Richtervorbehalt für die Abfrage von Verkehrsdaten vorsieht und eine Differenzierung zwischen Vorratsdaten und anlassbezogenen Verkehrsdaten erkennbar wird.

Vorgesehen ist weiterhin, dass der Datenabruf nur bei schwersten Straftaten nach einem Katalog, angelehnt an § STPO § 100c StPO, erfolgen darf. Mit dieser Vorgabe geht der Vorschlag über die Vorgaben des BVerfG hinaus, welches die Anknüpfung an den Straftatenkatalog des § STPO § 100a STPO § 100A Absatz II StPO als ausreichend erachtet hat.[10] Diese Beschränkung bedeutet Einschnitte für die Strafverfolgungsbehörden, etwa bei Betrugsstraftaten wie dem so genannten Enkeltrick, der vom Katalog des § STPO § 100c StPO nicht erfasst ist.

Im Ergebnis ist festzuhalten, dass der Entwurf an der einen oder anderen Stelle hinter dem Bedarf der Strafverfolgungsbehörden zurück bleibt. Ob insbesondere die Speicherfrist von zehn Wochen bzw. vier Wochen bei Standortdaten in allen Fällen den polizeipraktischen Anforderungen genügen wird, bleibt abzuwarten. Letztendlich wird die Neuregelung die Ermittlungsmöglichkeiten jedoch maßgeblich verbessern und Rechtssicherheit für die Bürgerinnen und Bürger, die Telekommunikationsanbieter und die Strafverfolgungsbehörden schaffen.

IV. FAZIT

In der heutigen globalen, digitalen und vernetzten Welt ist es unentbehrlich, dass die Polizei auf Verkehrsdaten zurückgreifen kann. Es ist zu hoffen, dass mit einem neuen Gesetz das Vertrauen in das Instrument der Mindestspeicherfristen wiederhergestellt wird. Die Befürchtungen, die in Begriffen wie Datensammelwut und Vorratsdatenspeicherung mitschwingen, sind unbegründet und stehen den Entwicklungen der tatsächlichen Möglichkeiten der Strafverfolgungsbehörden diametral entgegen. Das Postulat des jederzeit verfassungs- und rechtskonformen Handelns gilt für die Polizei analog wie digital. Um mit den Entwicklungen Schritt zu halten, bedarf es jedoch einer ständigen Überprüfung und Weiterentwicklung des Rechts und der polizeilichen Instrumente. Nur so kann den digitalen und international vernetzen Herausforderungen mit wirksamer Gefahrenabwehr und Strafverfolgung begegnet werden. Die Neuregelung zu den Mindestspeicherfristen ist hierbei ein wichtiger Schritt.

[10] Urteil des BVerfG vom 2. März 2010- 1 BvR 256/08, Rz 164; in den Eilanordnungen des BVerfG hatte der Senat die Auskunftsschwelle explizit auf Katalogtaten des § 100a StPO beschränkt.