/// Recht auf Sicherheit

VORRATSDATENSPEICHERUNG IST NOTWENDIG

JOACHIM HERRMANN /// Die neuere Rechtsprechung bietet Anlass, sich nochmals grundsätzlich mit der Zulässigkeit einer Vorratsdatenspeicherung auseinanderzusetzen. Dies ist nicht nur rechtlich zulässig, sondern sogar geboten, damit der Staat seiner Schutzpflicht gegenüber dem Bürger umfassend nachkommen kann. Dabei sind Freiheit und Sicherheit keine Gegensätze, sondern bedingen sich gegenseitig.

Einleitung

Bei der Vorratsdatenspeicherung geht es um eine wichtige Grundsatzfrage, die weit über die Diskussion darum hinausgeht. Im Vordergrund stehen die Befürchtungen, dass der Staat seine Bürger ohne Anlass ausspionieren kann, wenn er über entsprechende Befugnisse verfügt. Die aktuelle Berichterstattung zur NSA-Affäre hat dabei die Sensibilität der Bevölkerung in Bezug auf den Datenschutz noch weiter erhöht. Ich nehme diese Befürchtungen sehr ernst, denn wir messen dem Datenschutz einen sehr hohen Stellenwert bei. Eine Entwicklung in Richtung „Big Brother" oder „Gläserner Bürger" darf es nicht geben. Das Grundrecht der informationellen Selbstbestimmung hat für mich höchste Priorität.

Auf der anderen Seite steht allerdings die Schutzpflicht des Staates. Das beinhaltet schon Art. 1 Abs. 1 GG: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt." Der Staat muss also sicherstellen, dass strafbares Verhalten verfolgt und angemessen geahndet werden kann. Noch mehr muss er in der Lage sein, konkrete Gefahren für Leib und Leben abzuwenden. Dies setzt aber voraus, dass den Sicherheitsbehörden die erforderlichen Befugnisse an die Hand gegeben werden. Ansonsten würde diese Schutzpflicht ins Leere laufen.

Die Sicherheitsbehörden benötigen die Vorratsdatenspeicherung für ihre AUFGABE der staatlichen Schutzpflicht.

Und hierzu brauchen wir die Vorratsdatenspeicherung. Präziser gesagt geht es dabei um eine Mindestspeicher-

Quelle: nmann77/fotolia.com

Die Ermittlungsarbeit braucht dringend eine genau definierte gesetzliche Grundlage.

frist von Telekommunikationsverkehrsdaten. Eine Neuregelung würde hier im Ergebnis den Zustand herstellen, den wir in Zeiten vor „Flatrates" und „Prepaid-Karten" schon einmal hatten. Damals mussten die Provider die Verbindungsdaten grundsätzlich zu eigenen Zwecken speichern, weil sie etwa zur Rechnungslegung erforderlich waren.

Rechtliche Anforderungen

Die bisherige gesetzliche Grundlage für die Speicherung von Verkehrsdaten waren die §§ 113a, 113b des Telekommunikationsgesetzes (TKG). Das Bundesverfassungsgericht hat 2010 diese Normen allerdings wegen Verstoßes gegen das Fernmeldegeheimnis (Art. 10 Abs. 1 Grundgesetz) für nichtig erklärt. Es hat jedoch die anlasslose Speicherung von Verkehrsdaten auf Vorrat nicht schlechthin für unvereinbar mit dem Grundgesetz erklärt. Eine verfassungsmäßige Ausgestaltung der Vorratsdatenspeicherung ist auch mit einer sechsmonatigen Frist grundsätzlich möglich.

Nach dem Bundesverfassungsgericht sind aber enge Schranken beim Datenabruf vorzusehen: Er ist grundsätzlich unter Richtervorbehalt zu stellen. Zudem darf er nur bei schweren Straftaten und erheblichen Gefahren für die öffentliche Sicherheit erfolgen. Wichtig ist weiterhin insbesondere die Gewährleistung eines hohen Niveaus der Datensicherheit. Ähnliche Anforderungen stellte auch der Europäische Gerichtshof in seinem Urteil vom 8. April 2014.

Notwendigkeit einer bundesgesetzlichen Regelung

Zum Schutz unserer Bürger muss nun auf Bundesebene zügig ein entsprechender Gesetzentwurf vorgelegt werden, der den Anforderungen der Gerichte Rechnung trägt. Wir können es uns nicht leisten, auf eine derzeit noch gar nicht absehbare Neufassung der Richtlinie auf europäischer Ebene zu warten.

Gerade unsere Polizei braucht hier Befugnisse. Denn diese Informationen sind für die Sicherheitsbehörden ein wichtiger und manchmal auch der einzige Ermittlungsansatz bei Strafverfolgung und Gefahrenabwehr. Dabei geht es um den Abruf von Kommunikationsverbindungsdaten, also um die Frage: Zu welchen Telefonnummern bzw. IP-Adressen bestand wann eine Verbindung? Es geht also nicht um die Kommunikationsinhalte, sondern nur darum, ob es eine Verbindung gab. Das wird leider immer wieder missverstanden.

Seit dem Wegfall der §§ 113a und 113b TKG werden Telekommunikationsverbindungsdaten bei den einzelnen Providern unterschiedlich lang gespeichert. Die Dauer ist meist nur noch abhängig von der individuellen Vertragsgestaltung. Bei Flatrate- oder Prepaidverträgen sind sie extrem kurz, bei Einzelverbindungsnachweisen entsprechend länger. Daher sind die Daten oftmals gelöscht, wenn die zuständigen Behörden zur Strafverfolgung (nach § 100 g Strafprozessordnung) oder Gefahrenabwehr (nach Art. 34 b PAG) um entsprechende Auskünfte ersuchen. Das liegt zum Beispiel daran, dass Geschädigte einer Straftat meist erst mehrere Tage nach der Tat einen Vermögensschaden feststellen. Zum Zeitpunkt der Anzeigenerstattung sind die providerinternen Speicherfristen dann aber oft bereits überschritten und die Daten schon gelöscht. Bei Internetstraftaten steht die Polizei regelmäßig vor diesem Problem und kann sie deshalb oft nicht klären.

Für die polizeiliche Arbeit bedarf es umgehend genau definierter **RECHTLICHER** Befugnisse.

Dieses Manko ist auch an unserer Polizeilichen Kriminalstatistik deutlich abzulesen. In Bayern registrierten wir letztes Jahr „quer durch das Strafgesetzbuch“ insgesamt rund 24.300 Straftaten mit Internetbezug – eine Steigerung um 10,6 % gegenüber 2012. Anstiege verzeichnen wir bei Waren- und Warenkreditbetrug (+ 983 Fälle), Computerbetrug (+ 177 Fälle), Erpressungen (+ 99 Fälle) und Kinderpornographie (+ 60 Fälle). Wir gehen allerdings von einem hohen Dunkelfeld aus. Die Aufklärungsquote beträgt gerade einmal 42,7 %. Besonders tragisch ist dieser Umstand bei Delikten im Zusammenhang mit Kinderpornographie. Hinter jedem kinderpornographischen Bild steckt ein sexueller Missbrauch.

Internetstraftaten werden uns in den kommenden Jahren immer mehr beschäftigen, denn Kriminelle gehen hier ein ungleich geringeres Entdeckungsrisiko ein. Sie können von ihrem Wohnzimmer aus weltweit ihr Unwesen treiben und dabei anonym bleiben. Verdächtige Wahrnehmungen durch Zeugen wie beim klassischen Diebstahl oder bei Raubdelikten gibt es bei der virtuellen Kriminalität so gut wie keine. Die Täter hinterlassen zwar digitale

Spuren, diese können aber aufgrund fehlender Regelungen über Mindestspeicherfristen oft nicht weiter verfolgt werden.

Der Zugriff auf Verkehrsdaten ist insbesondere in Ermittlungsverfahren zur Aufklärung schwerster Straftaten aber dringend erforderlich. Mit ihm können beispielsweise Strukturen und Verbindungen innerhalb von Pädophilenringen, Gruppierungen der Organisierten Kriminalität oder terroristischen Ver-

Bei Internetstraftaten reichen die KLASSISCHEN Ermittlungsmethoden nicht mehr aus.

eingungen festgestellt werden. Diese Informationen ermöglichen manchmal erst Ermittlungserfolge. Sie sind für eine gerichtsfeste Beweisführung notwendig, so wie in einem Mordfall an einem türkischen Staatsangehörigen. Der Täter war von der Ehefrau des Opfers zu dem Mord angestiftet worden. Die Ermittlungen und der Tatverdacht basierten wesentlich auf den vorhandenen Verkehrsdaten. Der Tatzeitpunkt fiel noch unter die vor 2010 gültige Verkehrsdatenspeicherfrist von sechs Monaten. Teile der Daten, die für die Beweisführung von Bedeutung waren, waren dabei schon über zwei Monate vor der Tat angefallen.

Wenn wir den Terrorismus und andere Formen der Schwerkriminalität effektiv bekämpfen wollen, führt kein Weg an der gesetzlichen Verankerung von Mindestspeicherfristen der Telekommunikationsverbindungsdaten vorbei. Fachleute bestätigen, dass wir die Daten auch zur Verhinderung eines Amoklaufes, der zuvor im Internet angekündigt wurde, bei der Suche nach Suizidgefährdeten oder nach Vermissten in Bergnot brauchen. Ohne Verbindungsdaten stoßen wir schnell an die Grenzen polizeilicher Möglichkeiten. Das bestätigt auch eine Studie des Bundeskriminalamtes (BKA). Es hat Auskunftsersuchen für 1.157 Anschlüsse untersucht. Im Ergebnis wurden 76 % der Anfragen durch den Telekommunikationsanbieter nicht beantwortet. Dadurch konnten letztlich 56 % der Strafverfahren nicht geklärt werden.

Daher fordere ich, dass die Mindestspeicherdauer für relevante Verbindungsdaten gesetzlich einheitlich für alle Diensteanbieter geregelt werden muss. Zur Strafverfolgung wie auch zur Gefahrenabwehr ist eine Speicherdauer von zumindest drei Monaten notwendig. Eine solche Frist schöpft den vom Bundesverfassungsgericht anerkannten Rahmen also bei weitem nicht aus und ist auch mit der Entscheidung des EuGH vereinbar.

Der Abruf der Verkehrsdaten darf wie schon erwähnt grundsätzlich nur durch einen Richter angeordnet werden. Im Bereich der Strafverfolgung muss dabei der Gesetzgeber mittels eines Straftatenkatalogs vorgeben, in welchen Fällen ein solcher Abruf in Betracht kommen kann. Ausnahmeregelungen sind insoweit allerdings für Berufsgeheimnisträger wie Rechtsanwälte, Ärzte oder Geistliche vorzusehen. Von größter Bedeutung ist zudem die Gewährleistung der Datensicherheit. Ich begrüße hier auch die Vorgabe des EuGH, dass die notwendigen Datenserver der Provider innerhalb der EU stehen müssen. Die Übermittlung der Daten muss für den Betroffenen zudem transparent sein.
Das viel diskutierte Quick Freeze-Verfahren ist keine Alternative zu den Min-

Zur **EFFEKTIVEN** Bekämpfung von Terrorismus und Schwerstkriminalität braucht es eine gesetzliche Verankerung der Mindestspeicherfristen von Telekommunikationsverbindungsdaten.

destspeicherfristen. Bei diesem Verfahren werden vorhandene Verkehrsdaten mittels einer Sicherungsanordnung beim Serviceprovider „eingefroren". Selbst wenn die „Quick-Freeze"-Anordnung schnell ergeht, sind die meisten Daten nicht mehr oder nur bruchstückhaft vorhanden, da die Diensteanbieter nach geltender Rechtslage zur Löschung gesetzlich verpflichtet sind, soweit diese zur Vertragserfüllung nicht mehr gebraucht werden.

Fazit

„Ohne Sicherheit ist keine Freiheit". Diesen Satz hat Wilhelm von Humboldt – ein überzeugter Demokrat – vor etwa 200 Jahren geprägt. Er ist heute vor dem Hintergrund terroristischer Anschläge und aktueller Meldungen über erschreckende Gewaltexzesse aktueller denn je. Wer Angst hat, Opfer einer Straftat zu werden, zieht sich zurück und traut sich nicht mehr auf die Straße. Sicherheit ist daher unerlässlich für ein Leben in Freiheit. Vielmehr gehen die Gefahren für die individuelle Freiheit von den Bedrohungen für die Innere Sicherheit aus: Von Straftätern, die sich rücksichtslos über die Rechte ihrer Mitbürger hinwegsetzen, um ihre eigenen kriminellen Ziele zu erreichen, von Straftätern, die mit ihrem illegalen Handeln unsere Bevölkerung in Angst und Schrecken versetzen.

Deshalb muss sich ein wehrhafter Rechtsstaat zum Ziel setzen, die Bevölkerung wirkungsvoll vor Straftaten zu schützen. Dies kann im Einzelfall auch bedeuten, einen rechtsstaatlich legitimierten und mit Augenmaß durchgeführten Eingriff in die Grundrechte vorzunehmen. Sicherheit und Freiheit stehen daher nicht im Widerspruch zueinander. Sie bedingen sich vielmehr gegenseitig. Es sind zwei Seiten ein und derselben Medaille.

Sicherheit ist unerlässlich für ein Leben in **FREIHEIT.**

Deshalb müssen die Verantwortungsträger die bestehenden Sicherheitsdefizite offen beim Namen nennen und die Menschen über die Folgen und Risiken aufklären, wenn wir notwendige Instrumentarien nicht schaffen, obwohl wir es rechtlich könnten und dürften.///

/// JOACHIM HERRMANN MDL

ist Bayerischer Staatsminister des Innern, für Bau und Verkehr, München.