Was das Wort “Vorratsdatenspeicherung” eigentlich bedeutet

30.03.2025 Dieser Text soll einen Überblick über die technischen Hintergründe der Vorratsdatenspeicherung geben. Es geht also nicht um die juristischen Aspekte und die verfassungsrechtliche Bewertung, sondern um die technischen Grundlagen, den Umfang, die Bewertung und die Herausforderungen einer anlasslosen Speicherung von Verbindungsdaten über einen Zeitraum von mehreren Monaten. Wer an der rechtlichen Dimension interessiert ist, findet hierzu im Netz bereits eine Vielzahl fundierter juristischer Analysen und Stellungnahmen.

Vorratsdatenspeicherung - Ziel und Abgrenzung
Die Vorratsdatenspeicherung ist darauf ausgerichtet, Kommunikationszusammenhänge aufzudecken. Hierbei werden beispielsweise Verbindungs- und Standortdaten vorgehalten, um im Nachhinein mögliche Beziehungsgeflechte zwischen Personen oder Gruppen analysieren zu können.

Das entscheidende Unterscheidungsmerkmal zur Telekommunikationsüberwachung (TKÜ) besteht darin, dass bei der TKÜ Inhalte von Gesprächen, Nachrichten oder E-Mails mitgelesen beziehungsweise abgehört werden. Die Vorratsdatenspeicherung hingegen speichert zwar umfassend die Rahmendaten (z. B. wer wann mit wem in Verbindung stand), nicht aber die Gesprächs- bzw. Inhaltsdaten.

Aus technischer Sicht ist die Vorratsdatenspeicherung dafür gedacht, große Datenmengen automatisiert zu erfassen und zu speichern. Sie ist weder ausgelegt noch geeignet, um einzelne Täter in Echtzeit zu stoppen oder unmittelbar festzustellen, was genau gesprochen oder geschrieben wurde. Der Begriff Vorratsdatenspeicherung meint immer die anlasslose und verdachtsunabhängige Speicherung der Daten aller Bürgerinnen und Bürger. Für gezielte Speicherung konkreter Daten gibt es beispielsweise den Vorschlag eines sogenannten ‘Quick-Freeze’-Modells, der insbesondere je nach Ausgestaltung aber auch nicht unumstritten ist.

Was wird überhaupt alles gespeichert?
In den vergangenen Jahren hat sich der Umfang der möglichen Vorratsdatenspeicherung stetig erweitert. Schon das gekippte deutsche Gesetz von 2010 sah die anlasslose Speicherung sämtlicher Verkehrsdaten für Telefondienste (Festnetz, Mobilfunk mitsamt Standortdaten, Fax, SMS, MMS) und Internetdienste (Zuordnung von IP-Adressen zu Nutzenden, Nutzungszeiten usw.) vor. Damals lag der Fokus stark auf dem Mobilfunk. Heute ist die Kommunikationslandschaft weitaus komplexer: Messenger wie WhatsApp und Signal, Videokonferenz-Anbieter, E-Mail-Provider, Social-Media-Plattformen und viele weitere Dienste wären potenziell von einer Vorratsdatenspeicherung betroffen.

Was wird ohnehin gespeichert?
Unabhängig von einer gesetzlichen Vorratsdatenspeicherung gibt es bereits heute Speicherungen zu Geschäftszwecken. Große Telekommunikationsanbieter wie die Deutsche Telekom bewahren beispielsweise IP-Adressen nach Ende einer Verbindung noch für einige Tage (in vielen Fällen 7 Tage) auf, aus unternehmerischen Gründen, beispielsweise für Abrechnungen. Die hier gespeicherten Daten sind für Behörden bei Ermittlungen in diesem Zeitraum zugänglich.

Bei internationalen Unternehmen – etwa US-amerikanischen oder chinesischen Messenger- und App-Betreibern – wird in der Praxis oft länger gespeichert, etwa zu Werbezwecken oder für Profilbildungen. Die geltende Datenschutz-Grundverordnung (DSGVO) schränkt diese Speicherung in der EU zwar ein, doch außerhalb Europas gelten andere bzw. vielfach deutlich niedrigere Datenschutzstandards.

Wie lange wird gespeichert
Die vorgeschlagene Dauer der Vorratsdatenspeicherung hat sich in den letzten Jahren immer wieder geändert. Beispielsweise sah das 2010 vom Bundesverfassungsgericht für verfassungswidrig erklärte Gesetz eine Speicherfrist von 6 Monaten vor, plus einen weiteren Monat zur geordneten Löschung.

Je nach Entwurf oder Gesetzgebungsvorschlag könnten die Speicherfristen kürzer oder länger ausfallen. Sofern juristisch überhaupt denkbar, würde eine Verlängerung die Datenmenge entsprechend erhöhen.

Wer speichert?
Juristisch vermutlich nicht haltbar, aber technisch wäre es natürlich eine Option, dass der Staat die Daten selbst speichert: Also eine Behörde schafft, die ein Rechenzentrum selbst betreibt. Bzw. eine Behörde, die eine Ausschreibung macht, dass jemand ein Rechenzentrum für sie betreibt. Das klingt aus Kontrollperspektive erstmal verlockend, weil ja 'nichts ungesehen' bleibt, allerdings muss eine staatliche Institution auch keine Strafen fürchten, wenn sie ihren Datenschutz bzw. zugehörige IT-Sicherheit vernachlässigt.

Realistischer wäre eine Speicherung durch Privatunternehmen: Also die Unternehmen, bei denen Daten anfallen müssen diese vorhalten. Das stellt hohe Anforderungen an Datenschutz bzw. die zugehörige IT-Sicherheit. Das wird für die Unternehmen teuer und realistischerweise werden die Kosten an die Kunden weitergegeben (vgl. Versteigerung Mobilfunkfrequenzen). Oder es wird nicht teuer, weil die IT-Sicherheit ungenügend ist und da anders als bei den ersten Anläufen der Vorratsdatenspeicherung heute viel mehr Unternehmen mit der Speicherung beauftragt wären, ist es dann wohl nur eine Frage der Zeit, bis solche Daten in nicht autorisierte Hände geraten.

Unmengen an Daten - Kosten und Sicherheit
Das Datenvolumen, das eine heutige Vorratsdatenspeicherung erfassen würde, ist enorm: Bereits 2009 speicherte die Deutsche Telekom etwa 19,5 Terabyte an Vorratsdaten. Damals besaßen in Deutschland rund 6 Millionen Menschen ein Smartphone (mit sehr begrenzten Funktionen). Heute werden rund 68,5 Millionen Smartphone-Nutzende geschätzt. Hinzu kommen Messenger-Dienste, Video-Telefonie, soziale Medien und andere datenintensive Anwendungen.

Das wirkt sich auch direkt auf die Speicher- und Betriebskosten aus. Schon 2008 fielen nur bei der Telekom laut Berichten rund 5,2 Millionen Euro für die technische Einrichtung an, zuzüglich mehrerer Millionen Euro laufender Kosten pro Jahr. Angesichts des drastisch gestiegenen Datenaufkommens und aktueller Kosten für IT würden die damaligen Kosten heute wohl lächerlich gering wirken. Diese Mehrkosten könnten wiederum auf die Kundschaft umgelegt werden – oder dazu führen, dass an der IT-Sicherheit gespart wird.

Ausblick
Technisch gesehen müsste man also eine immer größere Vielfalt an Protokollen und Plattformen erfassen. Gleichzeitig steigen die Datenmengen rasant. Spätestens wenn dann automatisierte Auswertungen ins Spiel kommen, geht es nicht mehr nur um das anlasslose verdachtsunabhängige Speichern der Daten aller Bürgerinnen und Bürger, sondern dann auch um die automatisierte Verarbeitung und die Grenze zur staatlichen Profilbildung rückt noch näher.

Die Herausforderungen der IT-Sicherheit werden größer und nicht kleiner. Schon heute zweifeln eine Vielzahl an Menschen aus der IT an dem Sicherheitsniveau, auf dem große Datenmengen gespeichert werden. Die Daten, die bei der Vorratsdatenspeicherung in einem großen Zentralarchiv - entweder staatlich oder privat - gespeichert werden, sind für Angriffe sehr interessant. Aus Datensicherheitsperspektive ist daher die Nicht-Speicherung klar die bessere Wahl.

Häufig wird das Quick-Freeze Verfahren als Alternative zur Vorratsdatenspeicherung genannt. Bei Verdacht auf schwere Straftaten kann mithilfe eines richterlichen Beschlusses ein "Einfrieren" der Daten erwirkt werden. Wenn sich der Verdacht erhärtet, werden dann - ebenfalls mit richterlichem Beschluss - die Daten den Ermittlungsbehörden zur Verfügung gestellt. Anders als bei der Vorratsdatenspeicherung werden hier nicht anlasslos von jeder Bürgerin und jedem Bürger die Daten bevorratet. Aus technischer Sicht bleiben die kritischen Punkte auch hier bestehen, wobei sie durch die geringeren Datenmengen zumindest abgeschwächt werden, da beispielsweise der Datenschatz für gezielte Angriffe geringer ist.

Quellen und weiterführende Links:

Betrachtung von 2025 über die allgemeine rechtliche Lage:
https://netzpolitik.org/2025/bundesrechtsanwaltskammer-vorratsdatenspeicherung-von-ip-adressen-unzulaessig/

Stellungnahme des BKA zu Speicherfristen 2023:
https://www.bundestag.de/resource/blob/970516/8bbf8a86fd621d3ec354ea92a849f9c0/Stellungnahme-Link_BKA.pdf

Quick-Freeze-Vorschlag des Bundesministeriums der Justiz 2024:
https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Dokumente/Infopapier_Quick_Freeze_Verfahren.pdf?__blob=publicationFile

Artikel der FAZ von 2015: Unklarheit über die neue Vorratsdatenspeicherung
https://www.faz.net/aktuell/politik/unklarheit-ueber-die-neue-vorratsdatenspeicherung-13692465.html

Bundesverfassungsgericht 2010 und EUGH 2014
https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011
https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf