

## „Die konkrete Ausgestaltung der Vorratsdatenspeicherung ist nicht verfassungsgemäß“

Pressemitteilung des Bundesverfassungsgerichts vom 2. März 2010 (Auszüge)

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht festgestellt, dass die praktizierte Vorratsdatenspeicherung mit dem Grundgesetz nicht in Übereinstimmung steht (vgl. dazu auch den Artikel von Ralf Bendrath in dieser Ausgabe). Wir dokumentieren die wesentlichen Entscheidungsgründe, den Wortlaut der Entscheidung dokumentieren wir auf [www.blaetter.de](http://www.blaetter.de). – D. Red.

[...] Der Erste Senat des Bundesverfassungsgerichts hat entschieden, dass die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG nicht vereinbar sind. Zwar ist eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehlt aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügen sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz- und Rechtsschutzanforderungen. Die Regelung ist damit insgesamt verfassungswidrig und nichtig.

**Der Entscheidung liegen im Wesentlichen folgende Erwägungen zu Grunde: [...]**

### 3. Möglichkeit einer anlasslosen Speicherung von Telekommunikationsverkehrsdaten

Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste, wie sie die §§ 113a, 113b TKG anordnen, ist mit Art. 10 GG nicht schlechthin unvereinbar. Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Eingebunden in eine dem Eingriff adäquate gesetzliche Ausgestaltung kann sie den Verhältnismäßigkeitsanforderungen genügen.

Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Auch steigt das Risiko von Bürgern, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst hierzu Anlass gegeben zu haben. Darüber hinaus verschärfen die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, deren belastende Wirkung. Zumal die Speicherung und Datenverwendung nicht bemerkt werden, ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.

Dennoch kann eine solche Speicherung unter bestimmten Maßgaben mit Art. 10 Abs. 1 GG vereinbar sein. Maßgeblich dafür ist zunächst, dass die vorgesehene Speicherung der Telekommunikationsverkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht wird. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen und stehen dem Staat unmittelbar als Gesamtheit nicht zur Verfügung. Eine Speicherung der Telekommunikationsverkehrsdaten für sechs Monate stellt sich auch nicht als eine Maßnahme dar, die auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt wäre. Sie knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt voraus, dass diese eine Ausnahme bleibt. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.

#### **4. Verhältnismäßigkeit der gesetzlichen Ausgestaltung der Regelung (Maßstäbe)**

Angesichts des besonderen Gewichts einer vorsorglichen Telekommunikationsverkehrsdatenspeicherung ist diese nur dann mit Art. 10 Abs. 1 GG vereinbar, wenn ihre Ausgestaltung besonderen verfassungsrechtlichen Anforderungen entspricht. Es bedarf insoweit hinreichend anspruchsvoller und normenklarer Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz.

**Anforderungen an die Datensicherheit:** [...] Erforderlich sind gesetzliche Regelungen, die ein besonders hohes Maß an Sicherheit jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt.

**Anforderungen an die unmittelbare Datenverwendung:** Angesichts des Gewichts der Datenspeicherung kommt eine Verwendung der Daten nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht. Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer auch im Einzelfall schwerwiegenden Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Für die Gefahrenabwehr ergibt sich aus dem Verhältnismäßigkeitsgrundsatz, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur bei Vorliegen einer durch bestimmte Tatsachen hinreichend belegten, konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf. Diese Anforderungen gelten, da es auch insoweit um eine Form der Gefahrenprävention geht, gleichermaßen für die Verwendung der Daten durch die Nachrichtendienste. Eine Verwendung der Daten von Seiten der Nachrichtendienste dürfte damit freilich in vielen Fällen ausscheiden. [...] Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes überdies, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen.

Zu denken ist hier etwa an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen.

**Anforderungen an die Transparenz der Datenübermittlung:** Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die als solche nicht spürbare Datenspeicherung und -verwendung für die Bürger erhalten können, durch wirksame Transparenzregeln auffangen. Hierzu zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht. Eine heimliche Verwendung der Daten darf hier nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist. Soweit die Verwendung der Daten heimlich erfolgt, hat der Gesetzgeber die Pflicht einer zumindest nachträglichen Benachrichtigung vorzusehen. Diese muss gewährleisten, dass diejenigen, auf die sich eine Datenabfrage unmittelbar bezogen hat, wenigstens im Nachhinein grundsätzlich in Kenntnis zu setzen sind. Ausnahmen hiervon bedürfen der richterlichen Kontrolle.

**Anforderungen an den Rechtsschutz und an Sanktionen:** Eine Übermittlung und Nutzung der gespeicherten Daten ist grundsätzlich unter Richtervorbehalt zu stellen. Sofern ein Betroffener vor Durchführung der Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen. Eine verhältnismäßige Ausgestaltung setzt weiterhin wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen. [...]

**Anforderungen an die mittelbare Nutzung der Daten zur Identifizierung von IP-Adressen:** Weniger strenge verfassungsrechtliche Maßgaben gelten für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter, bereits bekannter IP-Adressen. Von Bedeutung ist hierfür zum einen, dass dabei die Behörden selbst keine Kenntnis der vorsorglich zu speichernden Daten erhalten. Die Behörden rufen im Rahmen solcher Auskunftsansprüche nicht die vorsorglich anlasslos gespeicherten Daten selbst ab, sondern erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen. Maßgeblich ist zum anderen, dass für solche Auskünfte nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet wird, deren Speicherung für sich genommen geringeres Eingriffsgewicht hat und damit unter deutlich geringeren Voraussetzungen angeordnet werden könnte. [...]

Hinsichtlich der Eingriffsschwellen ist allerdings sicherzustellen, dass eine Auskunft nicht ins Blaue hinein eingeholt wird, sondern nur aufgrund eines hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen darf. [...]