

Videoüberwachung, Vorratsdaten- speicherung und Onlinedurchsuchungen

STAATLICHE ÜBERWACHUNGSMASSNAHMEN

UND IHRE VERFASSUNGSRECHTLICHEN GRENZEN

Das Bundesverfassungsgericht hat das Recht auf informationelle Selbstbestimmung und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 Grundgesetz (GG) entwickelt. Diese Grundrechte des Einzelnen werden berührt durch die staatlichen Maßnahmen der Videoüberwachung, der Vorratsdatenspeicherung und der Onlinedurchsuchung. Eine Wissenschaftlerin der Juristischen Fakultät geht der Frage nach, ob die Abwägung zwischen Persönlichkeitsschutz und Sicherheitsbedürfnis des Staates gelingt.

Das Grundgesetz, unsere Verfassung, statuiert in seinem Artikel 1 die Pflicht des Staates, die Würde des Menschen zu schützen. Artikel 2 Absatz 1 GG garantiert jedem Menschen das Recht auf freie Entfaltung seiner Persönlichkeit. In der Kombination dieser Schutzstandards hat der Einzelne ein Abwehrrecht gegenüber dem Staat gegen Eingriffe in seine persönliche Sphäre.

Das Bundesverfassungsgericht hat zwei spezifische Persönlichkeitsrechte des Bürgers entwickelt, das Recht auf informationelle Selbstbestimmung und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme.

1. Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung erfordert, dass Daten des Bürgers nur auf gesetzlicher Grundlage und aufgrund detaillierter Regelungen erhoben werden dürfen. Dementsprechend enthalten die Polizeigesetze der Länder und die Datenschutzgesetze genaue Voraussetzungen für die Datenerhebung.

Welche Voraussetzungen für eine **Videoüberwachung** bestehen, ist stark umstritten.

Das Bundesverfassungsgericht hat sich hierzu nur in einem



Beschluss vom 23. Februar 2007 geäußert, der die städtische Videoüberwachung eines Kunstwerks (Grundriss der ehemaligen Synagoge auf dem Neupfarrplatz) in Regensburg betraf. Nach der Rechtsprechung des Gerichts verwirklicht die Videoüberwachung Unbeteiligter einen schweren Eingriff in das Grundrecht der informationellen Selbstbestimmung, da das grund-

sätzlich anlasslos gefertigte Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden kann. Daher ist für entsprechende Maßnahmen eine hinreichend bestimmte und normklare Rechtsgrundlage erforderlich.

Grundlegend war allerdings das Volkszählungsurteil des Gerichts vom 15. Dezember

1983. Das Urteil ist als richtungweisend für die Stellung des Datenschutzes anzusehen. Das Bundesverfassungsgericht erkennt:

»Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.«

In diese Rechtsprechung muss die Frage der Videoüberwachung eingefügt werden.

Neben der ausreichenden Rechtsgrundlage ist das sogenannte Übermaßverbot zu beachten. Für die Überwachung muss ein hinreichender Anlass bestehen, und sie darf nicht räumlich und zeitlich übermäßig sein.

Daher haben die Gerichte zum Beispiel eine dauerhafte Videoüberwachung von amtlichen Autokennzeichen, etwa auf Autobahnen, mit dem Ziel der Ermittlung verdächtiger Personen für unrechtmäßig erachtet. Dagegen hat das Bundesverfassungsgericht in einem Beschluss vom 12. August 2010 die Anfertigung von Videoaufnahmen dann für verhältnismäßig erachtet, wenn der Verdacht eines bußgeldbewehrten Verkehrsverstößes (hier: Unterschreitung des erforderlichen Sicherheitsabstandes) besteht.

Ebenso wurde der Klage einer Mieterin auf Entfernung einer vom Vermieter im Treppenhaus seines Mietshauses angebrachten Videokamera stattgegeben, mit der von

innen der Hauseingang überwacht wurde. Denn die Videoüberwachung eines Hauseingangs greife erheblich in das Persönlichkeitsrecht der Mieter ein und sei nur dann gerechtfertigt, wenn sie zur Abwehr schwerwiegender Beeinträchtigungen erforderlich ist und eine drohende Rechtsverletzung anderweitig nicht verhindert werden kann.

Die offene Videobeobachtung von Bibliotheksräumen einer Universität zur Verhinderung von Diebstahl und Sachbeschädigung der vorhandenen Bücher verstößt dagegen nicht gegen die Persönlichkeitsrechte der Benutzer, wenn diese keiner ständigen Beobachtung ausgesetzt sind. Eine generelle Speicherung der Bilder aus der Videoüberwachung ist jedoch unzulässig.

munikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der europäischen Richtlinie 2006/24/EG vom 21. Dezember 2007. Mit diesem Gesetz wurde die **Vorratsdatenspeicherung** von Telekommunikationsverkehrsdaten zu Zwecken der öffentlichen Sicherheit eingeführt.

Das Bundesverfassungsgericht hat inzwischen nach einem in der Öffentlichkeit viel beachteten Verfahren am 2. März 2010 ein Urteil in der Sache gefällt. Das Gericht hatte im Wesentlichen über die Verfassungsmäßigkeit dreier Gesetzesbestimmungen zu entscheiden. Es ging um einen um Paragraph 113 a Telekommunikationsgesetz (TKG), der regelte, dass



2. Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

a) Von ganz entscheidender Relevanz für den Schutz der Persönlichkeit des Einzelnen sind die Regelungen zur Telekommunikationsüberwachung. Besondere juristische Bedeutung hat dieses Thema erlangt durch das Gesetz zur Neuregelung der Telekom-

öffentlich zugängliche Telekommunikationsdiensteanbieter verpflichtet sind, praktisch sämtliche Verkehrsdaten von Telefondiensten, E-Mail-Diensten und Internetdiensten vorsorglich anlasslos zu speichern. Paragraph 113 b TKG erweiterte den Zweck der Vorratsdatenspeicherung über die Strafverfolgung hinaus auf die Abwehr von erheblichen Gefahren für die öffentliche Si-

Abbildung 1 (gegenüber) *Videoüberwachung: Abwägen zwischen Persönlichkeitsschutz des Einzelnen und Sicherheitsbedürfnis des Staates*
Quelle: Phototom – Fotolia.com

Abbildung 2 *Für Videoüberwachungen ist eine hinreichend bestimmte und normklare Rechtsgrundlage erforderlich. So muss etwa ein hinreichender Anlass bestehen und die Überwachung darf nicht räumlich und zeitlich übermäßig sein.*
Quelle: LaCatrina – Fotolia.com



Apl. Prof. Dr. iur. Jutta Stender-Vorwachs LL.M (Virginia)

Jahrgang 1954, ist seit 1998 Mitarbeiterin an der Juristischen Fakultät der Leibniz Universität Hannover. Kontakt: jutta.stender-vorwachs@jura.uni-hannover.de

cherheit und die Erfüllung der Aufgaben von Verfassungsschutzbehörden, von Bundesnachrichtendienst (BND) und Militärischem Abschirmdienst (MAD). Zudem war über Paragraph 100 g Strafprozessordnung (StPO) zu entscheiden, der die unmittelbare Verwendung der gespeicherten Daten für die Verfolgung von Straftaten von erheblicher Bedeutung regelt. Die genannten Vorschriften verstoßen nach Ansicht des Bundesverfassungsgerichts gegen das Fernmeldegeheimnis des Artikel 10 Absatz 1 GG. Sie gewährleisten weder eine hinreichende Datensicherheit noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Die Regelungen sind daher nichtig. Zugleich ordnete das Gericht an, dass die von den Diensteanbietern im Rahmen von Auskunftersuchen erhobenen, aber einstweilen nicht an die ersuchenden Behörden übermittelten, sondern gespeicherten Telekommunikationsverkehrsdaten unverzüglich zu löschen sind.

Das Gericht hält allerdings eine sechsmonatige, vorsorglich-anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter nicht schlechthin mit Artikel 10 GG für unvereinbar. Der Grundsatz der Verhältnismäßigkeit verlangt aber hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes. Im Bereich der Strafverfolgung wird ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat vorausgesetzt. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürfen Abruf und unmittelbare Nutzung der Daten nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben

oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.

Das Urteil wird auf die Neuregelung des Datenschutzes im Bereich der Telekommunikation entscheidende Auswirkungen haben.

Zudem sind Ende August 2010 zwei Verfassungsbeschwerden gegen das »Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes« beim Bundesverfassungsgericht eingereicht worden. Die Beschwerdeführer halten es für verfassungswidrig, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Gesetz zur Vorratsdatenspeicherung der Internetnutzung dazu ermächtigt wird, anlasslos Informationen über die elektronische Kommunikation jedes Bürgers mit Bundesbehörden und Bundestagsabgeordneten aufzuzeichnen. Es bleibt abzuwarten, inwiefern auch diese Regelung für verfassungswidrig erklärt werden wird.

b) Persönlichkeitsrelevant sind im Übrigen die Bestrebungen zur **Onlinedurchsuchung.**

Das Bundesverfassungsgericht hat mit Urteil vom 27. Februar 2008 die Vorschriften zur Onlinedurchsuchung sowie zur Aufklärung im Internet des Verfassungsschutzgesetzes Nordrhein-Westfalen für nichtig erklärt.

Das Persönlichkeitsrecht erfordert die Normierung von konkreten Eingriffsschwellen im Falle der Bedrohung eines überragend wichtigen Gemeinschaftsguts (Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Men-

schen berührt) und den Schutz des Kernbereichs privater Lebensgestaltung. Zudem ist eine richterliche Anordnung für heimliche Infiltrationen eines informationstechnischen Systems erforderlich.

Der Gesetzgeber hat diese Anforderungen in Paragraph 20 k Bundeskriminalamts-Gesetz (BKA-Gesetz) vom 12. November 2008 umgesetzt. Die Vorschrift erfordert zunächst eine existentielle Bedrohungslage, die mittels Onlinedurchsuchung aufzuklären ist. Das Infiltrieren ist nur via Datenleitung zulässig. Es darf nur das System der tatverdächtigen Zielperson betreffen; wobei die Ausforschung eines unbeteiligten Dritten grundsätzlich nicht ausgeschlossen werden kann. Daten dürfen nicht erhoben werden, wenn allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Diese Fälle werden allerdings praktisch kaum vorkommen. Die Onlinedurchsuchungsmaßnahmen sind also auch dann zulässig, wenn zu erwarten ist, dass auch beziehungsweise unter anderem Kernbereichsdaten erfasst werden.

Die Kernbereichsrelevanz erhobener Daten wird durch den Datenschutzbeauftragten des BKA sowie zwei weitere BKA-Bedienstete unter Sachleitung des anordnenden Gerichts beurteilt. Ist der Kernbereich betroffen, sieht das Gesetz ein Verwertungsverbot sowie ein Lösungsgebot vor.

Mehrere Verfassungsbeschwerden von Journalisten, Rechtsanwälten und Ärzten sind beim Bundesverfassungsgericht anhängig. Nach ihrer Ansicht schränkt das BKA-Gesetz die Bürgerrechte und die Pressefreiheit unverhältnismäßig ein und ist damit verfassungswidrig. Die Entscheidung des Gerichts wird mit Spannung erwartet.