

Sicherheitspolizei vs Grundrechte ::

**verfassungsrechtliche Grenzen der
Überwachung nach dem Sicherheitspolizeigesetz**

Wolfram Proksch

:: Territorialstaat

- das (völkerrechtliche) System des sog **Westfälischen Realismus** sieht den **Staat als Territorialmacht mit Souveränität**.
 - *Cuius regio, eius religio!* oder
 - *Look at the prince and no farther!*
- der **Staat** hat die **höchste Befehlsgewalt** innerhalb seines Staatsgebietes
 - Permanent Court of International Justice (PCIJ), *Lotus case*, 1925
 - UN Charter, Art 2
 - "All law is *prima facie* territorial."
(US Supreme Court, *American Banana Co. v. United Fruit Co.*)
- Jurisdiktionen unterscheiden sich freilich hinsichtlich ihrer Formen und Prinzipien
- territoriale Souveränität ist nach wie vor ein allgemein akzeptiertes und **erfolgreiches Prinzip des Friedens**

:: Verfassungsstaat

- **oberstes bzw höchstrangiges „Recht“ eines Staates** ist die sog **Verfassung**.
- liberal-demokratischen Verfassungen sehen in Rechtsstaaten vor, dass die konstituierte Staatsgewalt zur Begrenzung der Macht auf verschiedene Staatsorgane bzw „Gewalten“ aufgeteilt wird – nämlich im Rahmen der sog. „**Gewaltenteilung**“:
 - Legislative (Gesetzgebung)
 - Judikative (Rechtsprechung)
 - Exekutive (Verwaltung)
- die **Verfassung** regelt neben dem organisatorischen Staatsaufbau, der territorialen Gliederung des Staates oder der Kompetenzverteilung auch **das Verhältnis des Staates zu seinen BürgerInnen und deren bedeutendste Rechte und Pflichten**.
 - B-VG, BVG (Bundesverfassungsgesetz)
 - StGG (Staatsgrundgesetz)
 - EMRK (Europäische Menschenrechtskonvention)

:: Grund- und Menschenrechte

- **Grundrechte** sind grundlegende **Freiheiten der BürgerInnen gegen den Staat**. Sie sind primär als „**Abwehrrechte**“ konzipiert. Sie sollen den Normunterworfenen dauerhaft, beständig und effizient bzw einklagbar (verfassungsgesetzlich gewährleistet) vor Eingriffen des Staates schützen.

- Grund- und Menschenrechte sind verfassungsgesetzlich geregelt in/im
 - B-VG (Bundes-Verfassungsgesetz)
 - der **EMRK** (Konvention zum Schutz der Menschenrechte und Grundfreiheiten)
 - Art 8 (Achtung der Privat- und Familienlebens)
 - Art 10 (Freiheit der Meinungsäußerung)
 - StGG (Staatsgrundgesetz)
 - Art 10a (Fernmeldegeheimnis)

- Eingriffe des Staates sind nur im Rahmen der sog. „**Grundrechtsschranken**“ zulässig.

:: Problem „Kontrollverlust“

- Staaten verlieren die Kontrolle über „ihr“ Territorium bzw „ihre“ BürgerInnen. (Tele-)Kommunikation erfolgt zunehmend grenzüberschreitend und scheinbar „unkontrollierbar“; das Internet bzw der dadurch geschaffene Cyberspace ist **extra-territorial**, nur **virtuell räumlich**

“Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.” (Johnson/Post, 1996)

§ 53 Abs 3a SPG

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie
3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

§ 53 Abs 3b SPG

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen. Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung - ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

- Briefkopf der Dienststelle -

Betreff: **Auskunftsverlangen gemäß § 53 Abs. 3a u. 3b SPG bzw. § 98 TKG**
 GZ:

per FAX – Nr.: □□□□□

- Anfrage betreffend: (Daten gemäß § 53 Abs. 3a Z 1 SPG (Auskunft erfolgt kostenlos)
 (Daten gemäß § 53 Abs. 3a Z 2 SPG (Auskunft erfolgt kostenlos)
 (Daten gemäß § 53 Abs. 3a Z 3 SPG (Auskunft erfolgt kostenlos)
 (Daten gemäß § 53 Abs. 3a 2. Satz SPG (Auskunft erfolgt kostenlos)
 (Daten gemäß § 53 Abs. 3b SPG (Auskunft ist kostenpflichtig)
 (Daten gemäß § 98 TKG (Auskunft erfolgt kostenlos)

Die oben angeführte Behörde/Dienststelle ersucht um unverzügliche Übermittlung der unter Anfrage angeführten Daten.

Die anfragende Behörde/Dienststelle bestätigt ausdrücklich, dass sie im Sinne des § 7 Abs. 2 Z. 2 DSG 2000 zur Durchführung der zugrunde liegenden Amtshandlung gesetzlich zuständig ist, wobei die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des obigen Auskunftsbegehrens trifft.

Die Verwendung der Daten durch die anfragende Behörde/Dienststelle ist wesentliche Voraussetzung für die Wahrnehmung der sicherheitspolizeilichen Aufgabe nach der jeweiligen unter Anfrage angeführten Bestimmung.

Es wird ersucht, die Auskunft wie folgt zu erteilen:

- (per Fax unter □□□□□
- (per E-Mail unter □□□□□
- (fermündlich □□□□□
- unter □□□□□

Beilage: Liste

Bei der Sicherheitsexekutive bekannte Anfragekriterien	
Name	
Anschrift	
Teilnehmernummer	
Zeitraum und passive Teilnehmernummer eines geführten Telefongespräches	
Bekannte Informationen zu einer bestimmten Nachricht im Internet	
IP-Adresse und bestimmter Zeitpunkt (inklusive Zeitzone) ihrer Übermittlung	
Dokumentation bei Auskunftsverlangen gem. § 53 Abs. 3b SPG und § 98 TKG: Anführung der SPG-Aufgabe (z. B. erste allgem. Hilfeleistungspflicht)	

Umfang des Auskunftsbegehrens und Auskunft des Betreibers/Diensteanbieters		
Sicherheitsexekutive kreuzt in der mittleren Spalte die begehrte Auskunft an		
Betreiber/Diensteanbieter beauskunftet die begehrten Daten in der rechten Spalte		
Name		
Anschrift		
Teilnehmernummer		
IP-Adresse zur bei der Sicherheitsexekutive vorliegenden Nachricht und Zeitpunkt (inklusive Zeitzone) der Übermittlung		
Standortdaten		
Internationale Mobilteilnehmerkennung (IMSI)		

:: Eingriff in das Fernmeldegeheimnis (I)

- Das Fernmeldegeheimnis ist verfassungsgesetzlich in Art 10a StGG geregelt :
 - Das Fernmeldegeheimnis darf nicht verletzt werden.
 - Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur **auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze** zulässig.
- einfachgesetzlich wurde das Fernmeldegeheimnis in § 93 TKG 2003 (idF BGBl I Nr 133/2005) neu geregelt:
 - Demnach unterliegen die **Inhaltsdaten**, die **Verkehrsdaten** und die **Standortdaten** dem so genannten „Kommunikationsgeheimnis“, welches sich auch auf die Daten erfolgloser Verbindungsversuche erstreckt.
- nach herrschender Judikatur und Literatur unterliegen auch **Verkehrsdaten** jedenfalls dem Fernmeldegeheimnis iSd Art 10a StGG

:: Eingriff in das Fernmeldegeheimnis (II)

- Die Bestimmungen §§ 53 Abs 3a u 3b SPG berechtigen die Sicherheitsbehörden, von Betreibern öffentlicher Telekommunikationsdienste und von sonstigen Diensteanbietern iSd ECG sowohl Auskunft über „Stammdaten“ als auch über „Verkehrsdaten“ und „Inhaltsdaten“ zu verlangen, **ohne dass für die beiden letztgenannten Datenkategorien ein richterlicher Befehl notwendig wäre**
- Die in § 53 Abs 3a SPG geregelte Verpflichtung, Sicherheitsbehörden über Anfrage Internetprotokolladressen (IP-Adressen) zu einer bestimmten Nachricht und den Zeitpunkt der Übermittlung mitzuteilen (Z 2) und auch Auskunft über Name und Anschrift eines bestimmten Benutzers zu erteilen, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war (Z 3), **geht weit über eine reine Stammdatenabfrage und sogar über eine Verkehrsdatenabfrage hinaus**

:: Eingriff in das Fernmeldegeheimnis (III)

- Setzt man die Kenntnis eines bestimmten Kommunikationsverhaltens voraus und werden dazu IP-Adresse und Übermittlungszeit oder auch Name und Anschrift des Benutzers, dem eine IP-Adresse bestimmten Zeitpunkt zugewiesen war, bekannt gegeben, **lässt sich in aller Regel auch auf den Inhalt der „Nachricht“ schließen**, wenn man etwa wiederum den Inhalt der aufgerufenen Website oder der Newsforen-Einträge kennt.
- Da die Inhalte einer Website, von Gästebucheinträgen, Newsforen, Blogs etc zu einem bestimmten Zeitpunkt wesentlich leichter nachzuvollziehen sind (vgl etwa Web-Archive wie <http://www.archive.org/>) als die Inhalte eines mündlich geführten Telefongesprächs, sind auch derartige Daten keineswegs mit jenen „Verkehrsdaten“ vergleichbar, die bei der Führung eines Ferngesprächs anfallen. Die Daten sind **informationell angereichert**.
- Die Grenze zwischen „Verkehrsdaten“ und „Inhaltsdaten“ verschwimmt– es geht in Wahrheit nicht (nur) um die Frage, ob bzw wann jemand kommuniziert hat, sondern **was mit wem kommuniziert wurde** (zB welche Inhalte von wem wann heruntergeladen oder zum download bereitgestellt wurden, wer wann welche Website besucht hat, wer welchen Eintrag in einem Forum veröffentlicht hat etc.

:: Eingriff in das Privat- & Familienleben (I)

- **Art 8 Abs 1 EMRK** regelt das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs. Auch der **Fernmeldeverkehr** wird dem Privatleben bzw dem Briefverkehr zugeordnet. Dem **Schutzbereich des Art 8 Abs 1 EMRK** sind abgesehen von Inhaltsdaten auch sog **äußere Gesprächsdaten zuzurechnen**. Zu diesen äußeren Gesprächsdaten zählen nach Ansicht des EGMR auch die Nummern beteiligter Anschlüsse sowie Zeitpunkt und Dauer des Gesprächs
 - *Malone/Vereinigtes Königreich* [EGMR 2.8.1984; EuGZR 1985, 23f]
 - *Klass/Bundesrepublik Deutschland* [EGMR 6.9.1978; EuGZR 1979, 278ff]
- Ein Eingriff in die in Art 8 Abs 1 EMRK statuierten Rechte durch eine öffentliche Behörde darf gem Art 8 Abs 2 EMRK nur stattfinden, insoweit dieser **Eingriff gesetzlich vorgesehen** ist und eine Maßnahme darstellt, die **in einer demokratischen Gesellschaft** für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer **notwendig** ist

:: Eingriff in das Privat- & Familienleben (II)

Die **Verhältnismäßigkeit** ist nach der Rsp des EGMR nur dann gewahrt, wenn

- tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen
- die Maßnahme nur die verdächtigten Personen erfasst
- dasselbe Ziel nicht mit anderen (gelinderen) Maßnahmen erreicht werden kann
- ein besonderes Verfahren für die Überwachung besteht
- die Überwachung zeitlich beschränkt ist
- eine möglichst richterliche Kontrolle der Überwachung erfolgt
- die überwachte Person nachträglich jedenfalls von der Maßnahme informiert wird, wenn der ursprüngliche Zweck der Überwachung dadurch nicht vereitelt wird

FAZIT: §§ 53 Abs 3a u 3b SPG sind

- **viel zu vage,**
- **fordern Missbrauch geradezu heraus und**
- **greifen völlig unverhältnismäßig in das Grundrecht ein**

.ende

PROKSCH & FRITZSCHE | RECHTSANWÄLTE

RA Dr. Wolfram Proksch
Nibelungeng. 11/4, A-1010 Wien
+43 (1) 877 04 54
FAX +43 (1) 877 04 56

✉ office@pfr.at
www.pfr.at