

# Strafprozessuale Zulässigkeit des Zugriffs auf Anonymisierungsserver und darauf gespeicherte Logdaten zum Zwecke der Rückverfolgung dynamischer IP-Adressen

**Gericht**

LG Konstanz

**Datum**

27.10.2006

**Aktenzeichen**

4 Qs 92/06

**Branche/ Lebenslage**

Zugriff auf Anonymisierungsserver, strafprozessuale Ermittlungsmaßnahme, dynamische IP-Daten, Zugriff auf Logdaten

**Akteure**

Betroffener, Ermittlungsbehörde

**Wer haftet?**

Zulässige Beschlagnahmeanordnung eines Servers mitsamt IP- und Login-Daten

**Haftungsart**

-

**Haftungsumfang**

-

**Haftungsbegründendes Verhalten**

Anlass der Beschlagnahmeanordnung waren Ermittlung wegen des Verdachtes der Begehung kinderpornografischer Straftaten

**Technische Umstände**

Der Zugriff auf Login- und IP-Daten ist erforderlich, wenn aufgrund der dynamischen Zuordnung von IP-Adressen die Identifizierung des Tatverdächtigen anders nicht möglich ist

**Persönliche Umstände**

-

**Möglichkeiten der Haftungsvermeidung**

Die Beschlagnahme von Datenträgern ist nur dann zulässig, wenn keine weniger einschneidenden Mittel zur Verfolgung der Straftat zur Verfügung stehen

## Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Ein Dritte hatte bei einem Unternehmen einen [Server](#) angemietet. Der Geschäftsführer des Unternehmens wandte sich gegen eine gerichtlich angeordnete Beschlagnahme des gemieteten Servers mitsamt IP- und Login-Daten. Diese Daten sollten helfen, einen Tatverdächtigen zu identifizieren.

Das Gericht wies den Antrag zurück. Es sei keine Rechtsverletzung in der Beschlagnahmeanordnung zu sehen. Die Beschlagnahme des Servers sei notwendig und als Beweismittel i.S.d. § 94 StPO von Bedeutung, weil der Server zur Anonymisierung auch des Tatverdächtigen genutzt wurde:

*Aus den auf dem Bouncer [als Bouncer werden Server bezeichnet, die genutzt werden, um eine Verbindung zum eigentlichen Zielsever aufzubauen] gespeicherten Daten kann die „echte“ vom Internetservice Provider zugeteilte dynamische IP-Adresse eines Users festgestellt werden vorausgesetzt, die Daten der User wurden in so genannten Logdateien gespeichert. Diese Dateien sind somit als Beweismittel von Bedeutung.*

*Die §§ 94 ff. StPO erlauben auch die Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten als Beweisgegenstände im Strafverfahren. Zu berücksichtigen ist hier allerdings, dass sich auf den sichergestellten Datenträgern eine Vielzahl von Daten befindet, die in keiner Beziehung zu dem Tatvorwurf stehen. Dem Grundsatz der Verhältnismäßigkeit kommt insofern besondere Bedeutung zu. Dies bedeutet, dass die Sicherstellung und Beschlagnahme der Datenträger und der darauf gespeicherten Daten zur Verfolgung des gesetzlichen Strafverfolgungszweckes nicht nur Erfolg versprechend sein muss, sondern zur Ermittlung und Verfolgung der Straftat erforderlich sein muss.*

## ANMERKUNGEN

Entscheidungsgrundlage waren die §§ 94 ff StPO. Das Gericht betonte, dass im Rahmen der Ermittlungsmaßnahmen stets der Verhältnismäßigkeitsgrundsatz zu berücksichtigen sei.

Als eine weniger einschneidende Maßnahme kommt gem. §§ 100g, 100h StPO die Anordnung zur Auskunftserteilung über die Verbindungsdaten in Betracht. In diesem Fall sah das Gericht aber keine vergleichbaren Erfolgsaussichten der Maßnahme, zumal der Adressat der Anordnung ein drittes Unternehmen hätte sein müssen, bei dem die mögliche Rückmeldung, die geforderten Daten existierten nicht, nicht überprüfbar gewesen wäre. Das Gericht folgte damit nicht der Ansicht, dass bei anonymisierten Daten zunächst die Betreiber nach den Logdateien der Nutzer zu befragen wären, um evtl. anschließend eine Auskunftsanordnung zu erlassen (vgl. Spoenle, jurisPR-ITR 12/ 2007 Anm. 2).

Gesetzesänderung: Die §§ 100g, 100h StPO sind seit der Entscheidung mehrfach neu gefasst und teils erheblich geändert worden (aktuelle Fassung § 100g StPO in Kraft seit 22.07.2017; aktuelle Fassung § 100h StPO in Kraft seit 25.07.2015).