

# Strafprozessualer Zugriff auf E-Mail-Kommunikation: Rechtsgrundlagen und Unzulässigkeit des Zugriffs auf Nachrichten in einer Mailbox in Gestalt des heimlichen Einwählens mit erlangten Log-In-Daten bei einem Server außerhalb Deutschlands

**Gericht**

LG Hamburg

**Datum**

08.01.2008

**Aktenzeichen**

619 Qs 1/08

**Branche/ Lebenslage**

Strafprozessualer Zugriff auf E-Mail-Kommunikation, Mailbox, strafprozessuale Ermittlungsmaßnahme

**Akteure**

Betroffener, Beschuldigter, Ermittlungsbehörde, Staatsanwaltschaft

**Wer haftet?**

Staatsanwaltschaftlicher Antrag auf Zugriff auf mehrere E-Mail-Accounts

**Haftungsart**

-

**Haftungsumfang**

-

**Haftungsbegründendes Verhalten**

Ermittlungen wegen der vermeintlichen Vornahme von Flugbuchungen für Drogenkuriere

**Technische Umstände**

-

**Persönliche Umstände**

-

**Möglichkeiten der Haftungsvermeidung**

-

## Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Die Ermittlungsbehörde (Staatsanwaltschaft) beantragte den Zugriff auf mehrere E-Mail-Accounts des Betroffenen, die von einem Provider mit Sitz in den USA bereitgehalten wurden. Hierüber wollte die Ermittlungsbehörde Auskünfte über etwaige Flugreisen des Betroffenen erhalten, die dieser für eingesetzte Drogenkuriere gebucht haben soll. Dem Antrag beigefügt war auch die „Befugnis zum Öffnen der auf den E-Mail-Accounts noch gespeicherten und verfügbaren Dateien“. Die Vorinstanz hatte den Antrag noch mit Verweis auf eine fehlende Rechtsgrundlage abgelehnt.

Diese Einordnung lehnte das LG Hamburg ab und entschied entsprechend des Antrags der Staatsanwaltschaft. Es stützte sich dabei auf §§ 100a, 100b StPO.

Das Gericht sah beim Zugriff auf die E-Mails von Betroffenen über [Server](#) des E-Mail-Providers den Schutzbereich der Kommunikationsfreiheit, Art. 10 GG eröffnet. §§ 100a 100b StPO stellten jedoch eine hinreichende Ermächtigungsgrundlage dar. Bei serverbasierter E-Mail-Speicherung sei gerade ein bedeutender Unterschied zur Abspeicherung von E-Mails nur auf dem eigenen Rechner gegeben.

*Bedürfnis, freie Kommunikation zu gewährleisten, besteht auch dann, wenn sich ein Kommunikationsteilnehmer der E-Mail-Kommunikation unter Einsatz von serverbasierten E-Mail-Postfächern bedient. In diesem Fall gibt er sich seiner alleinigen Herrschaftsbefugnis über die elektronischen Daten; insbesondere der E-Mail-Provider und damit auch die Ermittlungsbehörden sind in der Lage, auf diese Daten beliebig und jederzeit zuzugreifen. Dieser Mangel an Beherrschbarkeit unterscheidet den Nutzer eines servergestützten E-Mail-Postfachs auch von demjenigen, der die Nachrichten vom Server abrufen und auf seinen eigenen Computer gelangen lässt. Jedenfalls dann unterstehen die Daten nur noch seinem alleinigen Gewissens, so dass jedenfalls der Schutzbereich von Art. 10 Abs. 1 GG nicht mehr eröffnet ist.*

Der Anwendbarkeit von §§ 100a, 100b StPO stünde nicht der Wortlaut entgegen, demnach nur „die Telekommunikation überwacht und aufgezeichnet“ werden darf. Das umfasse im Ergebnis auch den Zugriff auf E-Mail-Postfächer. Das Gericht nahm hierbei an, dass bei der Kenntnisnahme von E-Mail-Inhalten (bei Speicherung auf einem Server), immer eine Überwachung der Telekommunikation gegeben sei, unabhängig davon, ob sich die E-Mails vorübergehend „in ruhendem Zustand“ befänden.

Auch lasse es § 100a StPO zu, dem [Stand der Technik](#) entsprechend dahingehend ausgelegt zu werden, dass die Überwachung von E-Mails mitumfasst sei.

## ANMERKUNGEN

Gesetzesänderung: Die §§ 100a, 100b StPO sind im Laufe der Jahre einige Male geändert worden. Die letzte Änderung der §§ 100a, 100b StPO erfolgte am 30.10.2017 durch das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“, BGBl I 3618. Insbesondere sind mittlerweile die Online-Durchsuchung sowie die „Quellen-TKÜ“ ausdrücklich geregelt worden („Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“, 17.08.2017, BGBl I 3202).

Die „Quellen-TKÜ“ ist eine Ermittlungsmaßnahme, bei der Kommunikationsdaten durch Zugriff auf die Systeme des Betroffenen noch vor ihrer [Verschlüsselung](#) und Versendung (verdeckt) abgegriffen werden können.

Praxishinweis: Zum Zeitpunkt der Entscheidung war die Befugnis zu strafprozessualen Zugriffen auf die E-Mail-Kommunikation der Betroffenen deutlich umstritten (vgl. MMR 2008, 186, 188). Schon hinsichtlich der Speicherungsphase von E-Mails wird unterschieden: Der BGH stützte sich in einer Entscheidung (BGH, 31.03.2009, 1 StR 76/09) für die Befugnis zum Zugriff auf beim Provider zwischengespeicherte E-Mails auf die Postbeschlagnahme, § 99f StPO. Entgegen der hier besprochenen Entscheidung sah der BGH bei (bereits) ruhenden E-Mails auf den Servern der Provider keinen Telekommunikationsvorgang. Es sei eher der Vergleich mit einer Postkarte geboten, die beim Postanbieter auf Weiterversand warte. Anders sah es das BVerfG in einer hierauf folgenden Entscheidung (16.06.2009, BvR 902/06): Bei der Zwischen- und Endspeicherung beim Provider liege weiterhin ein Telekommunikationsvorgang vor, die Eingriffsgrundlage bemesse sich jedoch unter anderem nach der Eingriffsintensität der Maßnahme. So sei der offene Zugriff, wie hier, auf die Beschlagnahme

§§ 94 ff StPO in Verbindung mit der Speicherdurchsicht, § 110 StPO zu stützen. Die Vorschriften zur Beschlagnahme unterliegen hierbei weniger strengen Voraussetzungen als die zur Telekommunikationsüberwachung.