Zulässigkeit der Überwachung der Internet-Telefonie (konkret: via Skype) sowie Vornahme der insoweit erforderlichen Maßnahmen im Rahmen einer Fernsteuerung

Gericht

LG Hamburg

Datum

13.09.2010

Aktenzeichen

608 Qs 17/10

Branche/ Lebenslage

Überwachung von Skype-Kommunikation, TKÜ, Skype-Kommunikation, Vornahme der erforderlichen technischen Maßnahmen

Akteure

Überwachter, Ermittlungsbehörde

Wer haftet?

Die Überwachung und Aufzeichnung des Beschuldigten im Rahmen von Telekommunikationsvorgängen gem. § 100a StPO umfasst in seiner Gesamtheit auch das heimliche Einspielen eines Computerprogramms in das informationstechnische System des Überwachten

Haftungsart

–

Haftungsumfang

–

Haftungsbegründendes Verhalten

–

Technische Umstände

Eine „Quellen-TKÜ“ (Abgreifen von Kommunikationsdaten vor einer möglichen Verschlüsselung) kann nur durchgeführt werden, wenn sie auch die technische Vorbereitungsmaßnahme hierzu umfasst

Persönliche Umstände

–

Möglichkeiten der Haftungsvermeidung

Die Überwachung darf sich nur auf den Telekommunikationsvorgang selbst konzentrieren, andere Daten dürfen im Rahmen einer TKÜ nicht abgefragt und gespeichert werden

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Gegenstand der Entscheidung war die Durchführung einer gerichtlich angeordneten technischen Überwachung der Kommunikation eines Beschuldigten. Als vorbereitende Maßnahme wurde eine staatlich entwickelte Software verdeckt auf dem Computer des Überwachten installiert.

> *Das Gericht entschied, dass insbesondere auch die Installation dieser Software als notwendige Vorbereitungsmaßnahme von § 100a StPO gedeckt sei:*
>
> *Der Beschuldigte [war] einer täterschaftlich begangenen vollendeten gewerbsmäßigen und bandenmäßigen Hinterziehung von Einfuhrabgaben verdächtig.*
>
> *Die Voraussetzungen der Anordnung der beantragten Überwachungsmaßnahme liegen vor, insbesondere ist entgegen der Auffassung des Ermittlungsrichters auch die Überwachung und Aufzeichnung sämtlicher zur Kommunikation vorgesehener Daten einschließlich solcher, die Bild- oder Videoaufzeichnungen betreffen, zulässig.*
>
> *Dabei ist im Hinblick auf die für den Eingriff erforderliche Rechtsgrundlage grundsätzlich zwischen dem Primäreingriff – der in der Weiterleitung der Kommunikationsdaten an die Ermittlungsbehörden liegt […] – und dem zur Durchführung dieser Maßnahme erforderlichen sekundären Eingriff – der im Aufspielen und in der Aktivität des die Kommunikationsdaten an die Ermittlungsbehörden versendenden Computerprogramms besteht […] – zu differenzieren. Beide Eingriffe sind im Rahmen der geltenden Vorschriften der Strafprozessordnung zulässig.*

Das technische Überwachen der Kommunikation sei auch bei Abgreifen der Informationen direkt von den Systemen des Überwachten, noch bevor diese verschlüsselt werden können, zulässig. Andernfalls sei eine TKÜ nicht zuverlässig durchführbar:

> *Da die im Internet versandten verschlüsselten Daten – entsprechend dem Zweck der Verschlüsselung – selbst mit hohem technischem Aufwand nicht oder jedenfalls nicht zeitnah entschlüsselt werden können, erfordert die Überwachung dieser Art des Nachrichtenverkehrs einen Zugriff auf die Kommunikationsdaten innerhalb eines der beteiligten technischen Systeme (Computer), bevor diese vom jeweiligen Kommunikationsprogramm verschlüsselt oder nachdem sie beim Empfänger entschlüsselt worden sind, durch ein hierzu geeignetes, dem Überwachungszweck entsprechend heimlich in das informationstechnische System eines Nutzers eingebrachtes Programm.*
>
> *ANMERKUNGEN*

Das Gericht entschied, dass eine Überwachung und Speicherung von Telekommunikation im Sinne des § 100a StPO sämtliche Kommunikationsdaten, einschließlich Bilder- oder Videoaufzeichnungen, umfasst.

Ebenso sei auch die sog. „Quellen-TKÜ“ zulässig, bei der Daten, die im Rahmen eines Telekommunikationsvorgangs entstehen, noch vor der eigentlichen Übertragung von einem installierten Überwachungsprogramm an die Ermittlungsbehörden weitergeleitet werden. Das Gericht setzte sich mit der Begründung der Rechtmäßigkeit dieser Maßnahme umfassend auseinander.

Dass durch die Überwachungsmaßnahme auch Inhalte des Kernbereichs privater Lebensgestaltung berührt

werden, mache die Maßnahme nicht automatisch rechtswidrig. Vielmehr seien hier lediglich die strengen Durchführungsvorgaben des § 100a Abs. 4 StPO (z.B. Löschung von, den Kernbereich privater Lebensgestaltung betreffenden, Inhalten) einzuhalten.

Auch wenn das Aufspielen eines Computerprogramms auf den Computer des Beschuldigten nicht ausdrücklich von einer gesetzlichen Grundlage gedeckt ist, so sei das als Vorbereitungsmaßnahme, soweit zur Durchführung der TKÜ erforderlich, zumindest von § 100a StPO als „Annexkompetenz“ umfasst.

Das Gericht sprach auch die verfassungsrechtlichen Grundlagen der Maßnahme an. Einen denkbaren Eingriff in das Fernmeldegeheimnis sah es allerdings als gerechtfertigt an. Der Eingriff im Rahmen der Vorbereitungsmaßnahme dürfe in seiner Intensität allerdings nicht die Eingriffsintensität der eigentlichen Überwachungsmaßnahme überschreiten.

Weitere verfassungsrechtliche Voraussetzungen wurden, mit Hinweis auf die Rechtsprechung des BVerfG (27.02.2008, 1 BvR 370/07), ebenfalls als erfüllt angesehen.

Praxishinweis: Die Grenzen der Quellen-Telekommunikationsüberwachungen sind in Literatur und Rechtsprechung umstritten, vgl. MMR 2001, 690, daher schafft das vorliegende Urteil nur bedingt Klarheit. Eine Parallel-Entscheidung des LG-Landshut (20.01.2011, 4 Qs 346/10) vertrat allerdings eine ähnliche Auffassung wie das LG Hamburg, was zumindest eine grobe Richtung erkennen lässt. Das LG Hamburg selbst scheint mit dieser Entscheidung seine bisherige Rechtsprechung aufgegeben zu haben (vgl. MMR 2001, 690; LG Hamburg, 1.10.2007, 629 Qs 29/07).