TE OGH 2005/2/23 9Bs35/05v

JUSLINE Entscheidung

Veröffentlicht am 23.02.2005

Kopf

Das Oberlandesgericht Linz hat durch die Richter Dr. Schütz als Vorsitzenden, Dr. Gföllner und Dr. Koch in der Strafsache gegen u.T. wegen § 91 Abs 1 UrhG über die Beschwerde der Privatanklägerin L***** gegen den Beschluss der Untersuchungsrichterin des Landesgerichtes Salzburg vom 31.12.2004, 28 Ur 339/04z-3, in nichtöffentlicher Sitzung entschieden:Das Oberlandesgericht Linz hat durch die Richter Dr. Schütz als Vorsitzenden, Dr. Gföllner und Dr. Koch in der Strafsache gegen u.T. wegen Paragraph 91, Absatz eins, UrhG über die Beschwerde der Privatanklägerin L***** gegen den Beschluss der Untersuchungsrichterin des Landesgerichtes Salzburg vom 31.12.2004, 28 Ur 339/04z-3, in nichtöffentlicher Sitzung entschieden:

Spruch

Der Beschwerde wird nicht Folge gegeben.

Text

Begründung:

Mit am 21.12.2004 bei Gericht eingelangtem Schriftsatz vom 17.12.2004 (ON 2) beantragte die L***** als Privatanklägerin die Einleitung gerichtlicher Vorerhebungen gegen u.T. wegen § 91 Abs 1 iVm § 86 Abs 1 Z 3 und 4 UrhG - im Zusammenhang mit der ungenehmigten Verwertung von geschützten Tonaufnahmen im Internet - durch Erlassung eines gerichtlichen Beschlusses, mit welchem der Internet-Service-Provider (Access Provider) S*****, angewiesen werde, Name und Anschrift jener (insgesamt sieben) Kunden bekanntzugeben, die verdächtig seien, zu jeweils bestimmten Zeitpunkten unter Verwendung einer bestimmten IP-Adresse über das Filesharingsystem KaZaA jeweils mehr als 1000 leistungsschutzrechtlich geschützte Musikfiles aus dem Repertoire der Privatanklägerin unbefugt der Öffentlichkeit via Internet zum Download zur Verfügung gestellt zu haben.Mit am 21.12.2004 bei Gericht eingelangtem Schriftsatz vom 17.12.2004 (ON 2) beantragte die L***** als Privatanklägerin die Einleitung gerichtlicher Vorerhebungen gegen u.T. wegen Paragraph 91, Absatz eins, in Verbindung mit Paragraph 86, Absatz eins, Ziffer 3 und 4 UrhG - im Zusammenhang mit der ungenehmigten Verwertung von geschützten Tonaufnahmen im Internet - durch Erlassung eines gerichtlichen Beschlusses, mit welchem der Internet-Service-Provider (Access Provider) S*****, angewiesen werde, Name und Anschrift jener (insgesamt sieben) Kunden bekanntzugeben, die verdächtig seien, zu jeweils bestimmten Zeitpunkten unter Verwendung einer bestimmten IP-Adresse über das Filesharingsystem KaZaA jeweils mehr als 1000 leistungsschutzrechtlich geschützte Musikfiles aus dem Repertoire der Privatanklägerin unbefugt der Öffentlichkeit via Internet zum Download zur Verfügung gestellt zu haben.

Dazu führte die Privatanklägerin (eine Verwertungsgesellschaft) aus, dass angesichts der den durch die Privatanklägerin repräsentierten Tonträgerherstellern durch ungenehmigte Musikangebote im Internet jährlich entstehenden Schäden in Höhe von Hunderten Millionen Euro die auf das Internet spezialisierte Firma MediaSentry im Auftrag der Privatanklägerin bzw der Zentrale der ifpi in London Filesharingsysteme auf rechtsverletzende Angebote

überprüft habe. Die genannte Firma habe während der Monate September und Oktober 2004 an den öffentlich zugänglichen Internet-Filesharingsystemen die verschiedensten Musikstücke im Rahmen dieses Peer-to-Peer-Netzwerks nachgefragt und sei durch die jeweilige Software solcher Filesharingsysteme (zB KaZaA) auf den Computer eines jener Teilnehmer geleitet worden, der das angefragte Musikstück zum Download gegenüber jedermann zur Verfügung gestellt habe. Während der Zeit des Herunterladens erlaube es der anbietende User, sich darüber Information zu verschaffen, wie viele und welche weiteren Dateien sonst noch von seinem Rechner aus zum Download zur Verfügung stehen. Die Firma MediaSentry habe dokumentiert und festgestellt, bei welchen angebotenen Dateien es sich um Musikfiles bzw um andere Inhalte handle. Weiters sei die IP-Adresse des Users, der die dokumentierten Musikfiles zur Verfügung gestellt habe, samt Zeitraum der Verbindung festgehalten worden. Diese Dateien zu mehr als 500 solcher Anbieter seien der Privatanklägerin Mitte November 2004 von der Firma MediaSentry übersandt worden. Aufgrund der Sichtung dieser Dateien seien sieben Kunden des Internet-Service-Providers S***** dringend verdächtig, (zumindest) zu den exakt dokumentierten Zeitpunkten durch Anbieten von jeweils mehr als 1000 kompletten Musikfiles zum Download Urheberrechtsdelikte begangen zu haben. Mit Hilfe der IP-Adresse einerseits und dem Zeitraum, in dem diese benutzt wurde, andererseits, könne der jeweilige Internet-Service-Provider (Access Provider), der dem User den Zugang zum Internet bewerkstelligt habe, die persönlichen Daten (Name und Adresse) des Users eindeutig feststellen.

Mit dem angefochtenen Beschluss wies die Untersuchungsrichterin den (Ausforschungs-)Antrag der Privatanklägerin im Wesentlichen mit der Begründung ab, dass es sich bei der Bekanntgabe von Stammdaten einer

dynamischen Internetadresse um eine Rufdatenrückerfassung handle,

die nur unter den Voraussetzungen der §§ 149a ff StPO zulässigdie nur unter den Voraussetzungen der Paragraphen 149 a, ff StPO zulässig

sei. § 91 Abs 1 UrhG stelle angesichts einer Strafdrohung von bis zu sechs Monaten Freiheitsstrafe oder Geldstrafe bis zu 360 Tagessätzen hiefür keine ausreichende Basis dar. Eine gewerbsmäßige Begehungsweise, welche nach § 91 Abs 2a UrhG mit Freiheitsstrafe bis zu zwei Jahren bedroht sei, sei nicht indiziert.sei. Paragraph 91, Absatz eins, UrhG stelle angesichts einer Strafdrohung von bis zu sechs Monaten Freiheitsstrafe oder Geldstrafe bis zu 360 Tagessätzen hiefür keine ausreichende Basis dar. Eine gewerbsmäßige Begehungsweise, welche nach Paragraph 91, Absatz 2 a, UrhG mit Freiheitsstrafe bis zu zwei Jahren bedroht sei, sei nicht indiziert.

Die dagegen von der Privatanklägerin erhobene Beschwerde (ON 4) ist nicht berechtigt.

Rechtliche Beurteilung

IP-Adressen (das Kürzel IP steht für „Internet Protocol") dienen innerhalb von Netzwerken, die das TCP/IP-Protokoll („Transmission Control Protocol/Internet Protocol") verwenden, so auch das Internet, zur Identifizierung jedes angeschlossenen Rechners über eine numerische (aus vier durch einen Punkt getrennte Zahlen, die jeweils einen Wert zwischen 0 und 255 annehmen können) Adresse. Auch der Rechner eines Anwenders, der sich über einen Provider in das Internet einwählt, erhält eine IP-Adresse. Diese ist entweder immer gleich (statische IP-Adresse) oder wird bei jedem Verbindungsaufbau neu vergeben (dynamische IP-Adresse). Das Übertragungsprotokoll definiert die Regeln, welche den Datenaustausch in einem Verbund von Rechner koordiniert.

IP-Adressen, die beim Zugang eines Teilnehmers zu einem öffentlichen

Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der

zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten

Netzwerkadressierungen zum Teilnehmer notwendig sind, sind als

Verkehrs- bzw. Zugangsdaten iSd § 92 Abs 3 Z 4 bzw. Z 4a TKG

anzusehen (Zanger/Schöll TKG 20032 § 92 Rz 51) und fallen damit

unter das Kommunikationsgeheimnis. Gemäß § 93 Abs 1 TKG unterliegen dem Kommunikationsgeheimnis nicht nur die Inhaltsdaten, sondern auch die Verkehrsdaten und die Standortdaten, also auch die näheren Umstände der Kommunikation. Darunter ist insbesondere die Tatsache zu verstehen, ob jemand am Telekommunikationsvorgang beteiligt ist oder war, sowie der erfolglose Verbindungsversuch (Zanger/Schöll, aaO, § 93 Rz 9). Alle im Zuge eines Verbindungsaufbaus entstehenden Informationen stehen damit unter dem verfassungsrechtlichen Schutz (auch) des

Telekommunikationsgeheimnisses.unter das Kommunikationsgeheimnis. Gemäß Paragraph 93, Absatz eins, TKG unterliegen dem Kommunikationsgeheimnis nicht nur die Inhaltsdaten, sondern auch die Verkehrsdaten und die Standortdaten, also auch die näheren Umstände der Kommunikation. Darunter ist insbesondere die Tatsache zu verstehen, ob jemand am Telekommunikationsvorgang beteiligt ist oder war, sowie der erfolglose Verbindungsversuch (Zanger/Schöll, aaO, Paragraph 93, Rz 9). Alle im Zuge eines Verbindungsaufbaus entstehenden Informationen stehen damit unter dem verfassungsrechtlichen Schutz (auch) des Telekommunikationsgeheimnisses.

Die Offenlegung seitens des Access Providers, welcher Teilnehmer mittels einer bestimmten IP-Adresse zu einem bestimmten Zeitpunkt an der öffentlichen Telekommunikation teilgenommen hat, ist - jedenfalls wenn es sich um eine dynamische, also nicht dauerhafte IP-Adresse handelt - als Telefonüberwachung iSd § 149a Abs 1 Z 1 lit b StPO zu beurteilen. Es handelt sich dabei um eine Rufdatenrückerfassung, durch welche festgestellt werden soll, welcher Teilnehmeranschluss Ursprung bzw Ziel einer Telekommunikation war.Die Offenlegung seitens des Access Providers, welcher Teilnehmer mittels einer bestimmten IP-Adresse zu einem bestimmten Zeitpunkt an der öffentlichen Telekommunikation teilgenommen hat, ist - jedenfalls wenn es sich um eine dynamische, also nicht dauerhafte IP-Adresse handelt - als Telefonüberwachung iSd Paragraph 149 a, Absatz eins, Ziffer eins, Litera b, StPO zu beurteilen. Es handelt sich dabei um eine Rufdatenrückerfassung, durch welche festgestellt werden soll, welcher Teilnehmeranschluss Ursprung bzw Ziel einer Telekommunikation war.

Daran vermag - dem Beschwerdevorbringen zuwider - auch der Umstand nichts zu ändern, dass der gegenständliche Kommunikationsvorgang (Online-Zurverfügungstellung) samt Inhalt von den u.T. an die Öffentlichkeit gerichtet wurde, weil dies nur im Fall einer Inhaltsüberwachung von Relevanz sein könnte.

Die Argumentation des Beschwerdeführers, es liege hier kein Fall des § 149a Abs 1 Z 1 lit b StPO vor, weil bereits aktenkundig sei, „welcher Teilnehmeranschluss Ursprung der gegenständlichen Telekommunikation war", ist nicht schlüssig. Aktenkundig sind bislang lediglich die (netzinternen) IP-Adressen. Die anbietenden User sind im Unterschied zu einer bloßen Stammdatenabfrage (wie etwa bei Bekanntgabe der Identität des Teilnehmers anhand einer bestimmten Telefonnummer) nur im Wege eines rückwirkenden Auswertungsvorganges aufgrund der im Zuge des Kommunikationsvorganges angefallenen Daten feststellbar. Die beantragte Zuordnung dieser (dynamischen) IP-Adressen auf Grund von Datum und Uhrzeit zu Namen und Wohnanschriften der User stellt damit keine völlig unbedenkliche Zuordnungstätigkeit - im Sinn einer bloßen Stammdatenabfrage - mehr dar. Die zur Ausforschung der User erforderliche Auswertung der anlässlich des konkreten Verbindungsaufbaues entstandenen Informationen unterliegt vielmehr dem Telekommunikationsgeheimnis. Auch die Bestimmung des § 18 Abs 2 ECG ist für sich alleine keine ausreichende Grundlage zur beantragten Ausforschung. Die im ECG normierte Informationspflicht auf Grund einer gerichtlichen Anordnung nach § 18 Abs 2 ECG muss sich aus einer weiteren gesetzlichen Bestimmung ergeben, durch welche das Verfahren der Auskunftserteilung bzw. Mitwirkung konkretisiert wird. Einschlägige Normen sind grundsätzlich die §§ 139 ff und 143 Abs 2 StPO (in Zusammenhang mit körperlichen Sachen) bzw §§ 149a ff StPO (in Zusammenhang mit Inhalts- oder Vermittlungsdaten einer Telekommunikation). Bei einem Eingriff in das Fernmeldegeheimnis müssen demnach die Bestimmungen der StPO eingehalten werden (vgl. Fallenböck/Tillian in MR 2003, 404ff).Die Argumentation des Beschwerdeführers, es liege hier kein Fall des Paragraph 149 a, Absatz eins, Ziffer eins, Litera b, StPO vor, weil bereits aktenkundig sei, „welcher Teilnehmeranschluss Ursprung der gegenständlichen Telekommunikation war", ist nicht schlüssig. Aktenkundig sind bislang lediglich die (netzinternen) IP-Adressen. Die anbietenden User sind im Unterschied zu einer bloßen Stammdatenabfrage (wie etwa bei Bekanntgabe der Identität des Teilnehmers anhand einer bestimmten Telefonnummer) nur im Wege eines rückwirkenden Auswertungsvorganges aufgrund der im Zuge des Kommunikationsvorganges angefallenen Daten feststellbar. Die beantragte Zuordnung dieser (dynamischen) IP-Adressen auf Grund von Datum und Uhrzeit zu Namen und Wohnanschriften der User stellt damit keine völlig unbedenkliche Zuordnungstätigkeit - im Sinn einer bloßen Stammdatenabfrage - mehr dar. Die zur Ausforschung der User erforderliche Auswertung der anlässlich des konkreten Verbindungsaufbaues entstandenen Informationen unterliegt vielmehr dem Telekommunikationsgeheimnis. Auch die Bestimmung des Paragraph 18, Absatz 2, ECG ist für sich alleine keine ausreichende Grundlage zur beantragten Ausforschung. Die im ECG normierte Informationspflicht auf Grund einer gerichtlichen Anordnung nach Paragraph 18, Absatz 2, ECG muss sich aus einer weiteren gesetzlichen Bestimmung ergeben, durch welche das Verfahren der Auskunftserteilung bzw. Mitwirkung konkretisiert wird. Einschlägige Normen sind grundsätzlich die Paragraphen 139, ff und 143 Absatz 2, StPO (in

Zusammenhang mit körperlichen Sachen) bzw Paragraphen 149 a, ff StPO (in Zusammenhang mit Inhalts- oder Vermittlungsdaten einer Telekommunikation). Bei einem Eingriff in das Fernmeldegeheimnis müssen demnach die Bestimmungen der StPO eingehalten werden vergleiche Fallenböck/Tillian in MR 2003, 404ff).

Die Beschwerde musste daher, weil die Voraussetzungen für eine Überwachung der Telekommunikation nach§ 149a Abs 2 StPO beim hier relevanten Vergehen nach§ 91 Abs 1 UrhG nicht vorliegen, erfolglos bleiben.Die Beschwerde musste daher, weil die Voraussetzungen für eine Überwachung der Telekommunikation nach Paragraph 149 a, Absatz 2, StPO beim hier relevanten Vergehen nach Paragraph 91, Absatz eins, UrhG nicht vorliegen, erfolglos bleiben.

Oberlandesgericht Linz, Abt. 9,

Anmerkung

EL00084 9Bs35.05

European Case Law Identifier (ECLI)

ECLI:AT:OLG0459:2005:0090BS00035.05.0223.000

Dokumentnummer

JJT_20050223_OLG0459_0090BS00035_0500000_000