

Germering, den 08.12.2015

**Vortrag EuGH**  
**am 09.12.2015**

**1. Einleitung**

Im vorliegenden Fall geht es um die Frage, ob der Unternehmer als Inhaber eines offenen WLAN-Anschlusses für urheberrechtliche Rechtsverletzungen, die ein Dritter über den Anschluss durchführt, überhaupt in Anspruch genommen werden kann und innerhalb welcher Grenzen.

Entsprechend der Bitte des Gerichts werden die nunmehrigen Ausführungen auf die Fragen 4, 5 und 9 konzentriert.

**2. Fragen 4 und 5**

Die Fragen 4 und 5 zielen auf die Verantwortlichkeit des Access-Providers ab.

**a) Grundsatz des Art. 12 Abs. 1 HS. 1 der Richtlinie 2000/31/EG**

Ein Access-Provider ist gem. Art. 12 Abs. 1 Hauptsatz 1 der RL 2000/31/EG grundsätzlich „nicht für übermittelte Informationen verantwortlich“, wenn er die vorgegebenen Kriterien erfüllt. Dementsprechend kann er auch nicht dazu verurteilt werden, sich vor Rechtsverletzungen durch Dritte schützen zu müssen.

## b) Europarechtliche Auslegung

Nach der wörtlichen, der historischen und der teleologischen Auslegung ist eine Verantwortlichkeit auszuschießen – und zwar auch im Hinblick auf etwaige Unterlassungsansprüche; hierzu verweise ich auf unseren Schriftsatz. Die gesetzgebenden Organe haben sich dabei insbesondere von der Erwägung leiten lassen, dass die anonyme Nutzung offener Netze wie des Internets gerade nicht unterbunden werden kann. (Erwäg. grund 14)

Nach dem Wortlaut sind keine Unterlassungsansprüche zugunsten Privater zugelassen, sondern nur gerichtliche oder behördliche Anordnungen. Insbesondere besteht auch kein Anspruch auf Ersatz der Abmahnkosten im Hinblick auf etwaige Unterlassungsansprüche, da Art. 12 Schadensersatzansprüche gerade ausschließt.

## c) Eingehen auf Schriftsätze der anderen Beteiligten

Soweit die Kommission der Auffassung ist, dass Art. 12 Abs.3 es den Mitgliedstaaten freistellt, vom Diensteanbieter die Verhinderung oder Beseitigung zu verlangen, widerspricht dies dem ursprünglich gewollten Inhalt der Richtlinie. Soweit die Richtlinie in Abs.3 den nationalen Regelungen offenlässt, weitergehende Regelungen betreffend die Ausgestaltung des Verfahrens – ausdrücklich aber nicht der Sanktion – vorzusehen, geht es dabei nur um Maßnahmen des Abstellens oder des Verhinderns, aber nicht der generellen Unterlassung, was dem Wortlaut nach nur zu einer Beseitigungspflicht, aber nicht zu einer generellen Unterlassungspflicht führt. Diesbezüglich ist die Auffassung der Kommission etwas zu oberflächlich und lässt hierbei sämtliche europarechtlichen Auslegungsgrundsätze außer Betracht. Zudem führt dies – entsprechend den schriftlichen Erklärungen Polens – vielmehr dazu, das reibungslose Funktionieren des Binnenmarkts zu erschweren, indem die Wettbewerbsfähigkeit der europäischen Staaten bspw. gegenüber Vereinigten Staaten oder Kanada eingeschränkt wird; diese Staaten haben eine Haftung des Access Providers nicht vorgesehen.

Soweit die Beteiligten von Sony anführen, dass es mit dem Unionsrecht vereinbar sei, dem Betreiber im Falle einer durch Dritten begangenen Rechtsverletzung zu verbieten, eine Unterlassungspflicht aufzuerlegen, ist dies nicht korrekt. In der Sache LSG hat der Gerichtshof lediglich entschieden, dass der Access-Provider Vermittler ist, und gegen diesen aufgrund Art. 8 Abs. 3 der Richtlinie 2001/29 (UrhRL) gerichtliche Anordnungen erlassen werden können. Die Angelegenheit bezog sich allerdings auf Auskunftsansprüche und zudem auch auf einen Telekommunikationsanbieter und nicht – wie hier – auf Unterlassung, Schadensersatz und auf einen Anbieter eines offenen WLAN. In der Sache Scarlet Extended hat der Gerichtshof nicht entschieden, dass Art. 8 Abs.3 der Urheberrechtsrichtlinie gerichtliche Anordnungen immer erlaubt. Vielmehr wurde entschieden, dass die Anordnungen gem. Art. 8 Abs.3 nicht die Bestimmungen der Art. 12–15 berühren dürfen. Entgegen den Anführungen von Sony kann die Rechtsprechung von L'Oréal gerade nicht 1:1 herangezogen werden, da es hierbei im Gegensatz zum vorliegenden Ausgangsverfahren um eine Hostprovider-Haftung ging und Ebay als Hostprovider ganz andere technische Mittel zur Verfügung stehen als einem Access-Provider. Von einem Mindestniveau in Art. 12 Abs.3 der Richtlinie kann überhaupt keine Rede sein, da anerkannt ist, dass es den Mitgliedstaaten freisteht, überhaupt eine Haftung vorzusehen. Sofern Sony damit argumentiert, dass irgendeine Möglichkeit des Ausschlusses von Urheberrechtsverletzung gegeben sein muss, so sollte vielleicht so langsam daran gedacht werden, dieses Problem präventiv anzugehen. Dem Interesse der Rechteinhaber dagegen könnte man bspw. durch die Einführung einer Pauschalvergütung (ähnlich der Geräteabgabe) gerecht werden.

**d) Fazit**

Sofern also ein Anspruch auf künftige Unterlassung bestünde, würde die Privilegierung des Access-Providers ad absurdum geführt. Denn letztlich würde der Access-Provider, der nach der Richtlinie selbst bei Kenntnis nicht verantwortlich sein soll, genauso haften wie der Hostprovider, was aber vom Gesetzgeber gar nicht gewollt war, wenn man die unterschiedliche Ausgestaltung der Haftung betrachtet. Der Gesetzgeber hat dabei – wie auch die Kommission ausführt – insbesondere nach dem Nähegrad des Diensteanbieters differenziert.

**3. Frage 9**

Die Frage 9 zielt letztlich darauf ab, welche Maßnahmen der Access-Provider ergreifen müsste, um dem Unterlassungsgebot bzw. dem Schutz nachzukommen.

**a) Eingehen auf die Schriftsätze der Beteiligten**

Die Kommission weist zu Recht und im Einklang mit der bisher ergangenen Rechtsprechung darauf hin, dass bei der Auslegung der Richtlinie der Grundsatz der Verhältnismäßigkeit, der Effektivität und der Schaffung eines Gleichgewichts zwischen den betroffenen Interessen und Grundrechten geschaffen werden muss. Die Kommission hat aber ebenso zugegeben, dass sich die Effektivität der vom Vorlagegericht vorgeschlagenen Maßnahmen deren Kenntnis entzieht. Die Kommission kommt aber dennoch zu dem Schluss, dass eine Sicherungsmaßnahme im vorliegenden Fall zu einer generellen – und damit unzulässigen – Überwachung führen würde. Auch die völlige Stilllegung des Internetanschlusses ebenso wie die Einführung eines Passwortschutzes sind nach der Beurteilung der Kommission nicht geeignet. Zu betonen ist jedoch auch mit Blick auf die Entscheidung zu *UPC*, dass es nicht geeignet oder angemessen ist, dem Access-Provider die Wahl der technischen Maßnahme zu überlassen, da dies die unternehmerische Freiheit einschränkt. Es wird einmal dem Access-Provider überlassen, welche technischen Mittel er anwendet und zudem muss er gleichzeitig darauf achten, die Grundrechte der Internetnutzer auf Informationsfreiheit zu beachten. Auf der anderen Seite sollen dem Access-Provider (wobei wir im vorliegenden Fall insbesondere nicht von einem großen Telekommunikationsanbieter sprechen) gem. Art.3 der RL 2004/48/EG keine Pflichten auferlegt werden, die unverhältnismäßig, teuer, dauerhaft oder kompliziert sind. Es wurde in Verfahren, wie bspw. *Scarlet Extended* oder *SABAM./ Netlog*, von rechtskundigen Personen überlegt, ob bestimmte technische Maßnahmen ausreichend sind. Es bedarf eines Sachverständigen, um diese Fragen zu klären. Ferner stellt sich die Frage, ob eine solche Anordnung überhaupt vollstreckbar ist? Eine solche Maßnahme widerspricht nicht nur dem Grundsatz der Rechtssicherheit, sondern lastet Adressaten auch jegliches Risiko auf, das er eigentlich nach den Art. 12 ff. nicht tragen sollte. Im Zweifelsfall würde der WLAN-Diensteanbieter zudem übertriebene Maßnahmen ergreifen, um eine Haftung auszuschließen, was sich wiederum auf die Grundrechte des Nutzers im Hinblick auf den Datenschutz und die Informationsfreiheit auswirkt. Ferner stünde dies dem deutschen Grundsatz der Klarheit der Klageanträge und der möglichen Vollstreckbarkeit entgegen.

Im Einklang mit der Stellungnahme der Republik Polen wird insbesondere auch nochmals auf die Sache *Scarlet Extended* Bezug genommen.

Sony führt an, dass der WLAN-Betreiber gehalten ist, die jeweils dem Stand der Technik entsprechenden Sicherungen bereitzuhalten. Sony macht es sich hierbei zu leicht und fordert einen für die Zukunft immer anpassbaren Tenor, um keine weiteren Prozesse führen zu müssen. Dies widerspricht im Übrigen auch der im deutschen Recht entwickelten Kerntheorie für Unterlassungsansprüche. Es kann auch nicht sein, dass

der Access-Provider letztlich weitergehend haftet als der eigentliche Täter. Dies wäre diesbezüglich der Fall, denn der Täter haftet nur selbst auf Unterlassung eines bestimmten Werks von seinem Anschluss aus, wohingegen der WLAN-Anbieter auf Unterlassung diverser urheberrechtlicher Verletzungen von einem Anschluss, aber durch verschiedene Nutzer haften würde.

#### **b) Verhältnismäßigkeit im Hinblick auf die vom Vorlagegericht vorgeschlagenen Maßnahmen**

Zum einen ist der Schutz des geistigen Eigentums nicht schrankenlos, zum anderen stellt sich die Frage der Verhältnismäßigkeit angesichts der dann erforderlichenfalls zu ergreifenden Maßnahmen und der Folgen.

Es sei anzumerken, dass es bei den Fällen der offenen WLAN-Nutzung oftmals nur um die kurzzeitige Vermittlung zum Internet geht und nicht – wie bspw. in den Sachen *UPC Telekabel Wien* oder *L'Oréal* – um irgendwelche Inhalte, die jederzeit entfernt, gesperrt oder berichtigt werden können, was technisch mithilfe eines Algorithmus wesentlich einfacher machbar ist.

Zu den vorgeschlagenen Maßnahmen:

- a) Durch die **Stilllegung des Anschlusses** würde einem Internetnutzer jegliches Informationsmedium und Kommunikationsmedium abgeschnitten und ein gravierender Eingriff in seine Grundrechte vorgenommen werden.
- b) **Ein Passwortschutz**, d.h. das Verbot der Mitbenutzung durch Dritte, hätte zur Folge, dass sich jegliches öffentliches WLAN in öffentlichen Einrichtungen, Geschäftszentren, Beherbergungsbetrieben, Gaststätten, Museen in ein privates WLAN verwandeln würde. Auch im privaten Umfeld dürften zukünftig weder Ehepartner noch Kinder noch Mitbewohner noch Freunde das WLAN benutzen bzw. das Passwort erhalten, da man ansonsten mit einer Haftung rechnen müsste. Würde man hingegen einen Registrierungsprozess einrichten, würde im Endeffekt – entgegen dem Verbot der generellen Überwachung – jegliche Aktion des Nutzers überwacht, nämlich Einwahl, Abwahl und auch die jeweiligen Logdaten dazwischen. Im Übrigen hindern Anmeldepflichten ebenso wenig wie Hinweispflichten etwaige Rechtsverletzungen. Die von Sony angeführte Sicherung via WPA2 führt zu einer Zugangsbeschränkung, die bei einem offenen WLAN gerade nicht bezweckt sein soll. Soweit Sony hier eine Registrierungspflicht anführt, um Auskünfte zu erhalten, so geht dies an der Sache vorbei, da es streitgegenständliche nicht um die Gewährleistung von Auskünften, sondern um Schadensersatzansprüche und Unterlassungsansprüche geht. Im Übrigen kann auch mithilfe einer Speicherung der Nutzerdaten keine Aussage über einen etwaigen Täter getroffen werden, wenn mehrere Personen den Internetzugang gleichzeitig benutzen: Jeder Nutzer könnte der Täter sein. Des Weiteren käme eine Registrierung der Nutzer einer unzulässigen Vorratsdatenspeicherung gleich.
- c) Kostspielige, zeitraubende und aufwändige technische Vorkehrungen durch absolute **Überwachung sämtlicher elektronischer Kommunikation oder**, technische Blockaden würden zu einer unzulässigen Überwachung der Kommunikation des Einzelnen und damit einen Eingriff in den Schutz personenbezogener Daten führen.. Dies gilt umso mehr, als die Effektivität dieser Maßnahmen stark in Frage gestellt ist. Hinzukommend müsste eine Maßnahme einen Eingriff in die Rechte des anderen verhindern oder zumindest so erschweren, dass der Nutzer zuverlässig davon abgehalten wird, die Rechte des anderen zu verletzen. Bis heute sind aber keine solchen Maßnahmen bekannt. Hinzukommend – und das ist im Rahmen der Verhältnismäßigkeit zu berücksichtigen – handelt es sich bei dem Kläger des Ausgangsverfahrens um einen kleinen WLAN-Anbieter, ähnlich einem Hotel, einer Gaststätte, Ferienwohnungsbetreiber. Diesbezüglich dürfen die Kosten der Maßnahme erst recht nicht außer Betracht gelassen werden in Bezug auf das, was dem Access-Provider technisch zumutbar ist. Insbesondere ist auch hier zu berücksichtigen, dass die komplette Kostenübernahme für technische Maßnahmen, die sehr kostspielig sein können, zu einem

Quasi-Schadensersatz führt. Ein solcher wird durch Art. 12 der Richtlinie aber gerade nicht zugelassen.

Die von Sony vorgeschlagenen Möglichkeiten, einen Nutzer bzw. ein bestimmtes Endgerät von der Nutzung auszuschließen, würde nicht nur eine generelle, dauernde Überwachung der Verkehrsdaten, sondern auch der Inhaltsdaten bedeuten, was aber Art. 15 der RL 2000/31 nicht zulässig ist. Insbesondere stellen diese Maßnahmen ganz sicher keinen geringen Eingriff in die Informationsfreiheit oder gar den Datenschutz dar. Auch Portsperrern sind komplett wirkungslos, da hierdurch keine Rechtsverletzungen verhindert werden können: Mit Hilfe von Portsperrern kann nämlich nur das eigene WLAN-Netz vor Zugriffen von außen geschützt werden. Soweit Sony nun darauf abstellt, dass zumindest verhindert werden soll, dass bestimmte Werke rechtswidrig übermittelt werden sollen, wurde bis heute kein vernünftiger Vorschlag gemacht, wie dies ein Access-Provider technisch bewerkstelligen soll. Insbesondere ohne kostspielige Investitionen in mathematische Verfahren, die es noch gar nicht gibt.

Ferner ist es nicht mit dem allgemeinen Gleichbehandlungsgrundsatz vereinbar, von den großen Playern des Telekommunikationswesens keine Unterlassungspflichten zu verlangen, aber wohl von den kleinen Anbietern offener WLAN-Anschlüsse. Die großen Access Provider betreiben zahlreiche Hotspots im Flugzeug, Zug und an öffentlichen Plätzen bzw. gewähren Kunden gegen ein monatliches Entgelt die Möglichkeit, für das eigene Geschäft einen HotSpot einzurichten. Dasselbe gilt für andere Firmen, aber auch für die zwischenzeitlich vorhandenen Freifunk-Angebote.

Und was ist mit den sonstigen Access Providern: Bekannte Fastfood-Ketten haben zwischenzeitlich öffentliche Hotspots eingerichtet, wie bspw. McDonalds, Burger King, Starbucks. Der Bürgermeister von London hatte für die Olympischen Spiele 2012 die Vision, ganz London in einen riesigen WLAN-Hotspot zu verwandeln, was er auch geschafft hatte – mit Ausnahme des Olympiageländes, wo es durch das Olympische Komitee verboten wurde.

### c) Fazit

Bereits jetzt ist die Flut von Informationen im Internet und die Anzahl der Informationssuchenden so groß, dass die Mobilfunknetze überlastet sind. Von daher strebt insbesondere die Telekom eine bessere Netzabdeckung durch öffentliche Hotspots an, die die Mobilfunknetze entlasten sollen. Würde das Gericht eine Verantwortlichkeit eines Access-Provider annehmen, werden das Informationsrecht und das Informationsbedürfnis der Gesellschaft stark eingeschränkt.

Der deutsche Gesetzgeber bereitet daher derzeit eine Gesetzessänderung vor, wonach offenes WLAN zulässig sein soll – allerdings nur einhergehend mit zahlreichen Sicherungsmaßnahmen und Rechtstreuerklärungen. Die Kommission selbst hat in einer internen Stellungnahme an den deutschen Gesetzgeber deutlich gemacht, dass dieses Gesetz gegen Art. 12 der RL 2000/31 verstößt, da Access-Provider ohne weitere Voraussetzung von der Haftung für Rechtsverstöße Dritter freizustellen sind. Das angestrebte Gesetz würde letztlich zusätzliche Bedingungen zu den in Art. 12 genannten auferlegen, was so nicht zulässig wäre. Insbesondere bezweifelt die Kommission hierbei die Verhältnismäßigkeit der Maßnahmen.