- Abschrift -

513 C 7733/20 -

Amtsgericht Hannover

- Zivilabteilung -

09.09.2021

Öffentliche Sitzung des Amtsgerichts

Gegenwärtig:
Richter am Amtsgericht Knepper

- ohne Protokollführer/in -

Das Speichermedium, auf dem dieses Protokoll diktiert ist, wird einen Monat nach Zugang der Protokollabschriften an die Parteivertreter gelöscht. Nach diesem Zeitpunkt können Beanstandungen nicht mehr entgegengenommen werden.

in dem Rechtsstreit

Warner Bros. Entertainment GmbH, vertreten durch den Geschäftsführer [redacted] Humboldtstr. 62, 22083 Hamburg

Klägerin

Prozessbevolimächtigte: Rechtsanwälte Waldorf pp., Beethovenstr. 12, 80336 München
Geschäftszeichen: 17PP045807

gegen

Frau [redacted]

Beklagte

Prozessbevoilmächtigter: Rechtsanwalt Egbert Wöbbecke, Würzburger Straße 13, 30880 Laatzen
Geschäftszeichen: [redacted] vs Warner Bros.

erschienen bei Aufruf der Sache:

1) für die Klägerin Herr Rechtsanwalt [redacted]
2) mit der Beklagten in Person Herr Rechtsanwalt Wöbbecke.

Ferner war der geladene Zeuge [redacted] erschienen. Der Zeuge nahm im Zeugenstand Platz.

Beschlossen und verkündet:

Der prozessleitend geladene Zeuge soll zu den sein Wissen gestellten Tatsachenbehauptungen {behauptete Urheberrechtsverletzung durch Filesharing des Films „Collateral Beauty“ über den Internetanschluss der Beklagten IP-Adresse [redacted] am 02.04.2017: 18:26 Uhr bis 19:04:46 Uhr vernommen werden.

Der Zeuge wurde zur Wahrheit ermahnt, auf die Strafbarkeit einer falschen eidlichen und uneidlichen Aussage hingewiesen, sodann wie folgt vernommen:

1.
Zur Person:

Ich heiße [redacted], bin 49 Jahre alt, von Beruf Dipl.-Kaufmann, wohnhaft in [redacted]

Mit den Parteien des Rechtsstreits nicht verwandt und nicht verschwägert.

Die Abkürzung „PFS“ steht für peer to peer forensic System. Ich habe da ein Handout mitgebracht, das ich sowohl dem Gericht als auch den Parteivertretern zur Einsichtnahme aushändige. Es handelt sich um dezidiertes System mit verschiedenen Servern, das dazu gebaut ist, in peer to peer Netzwerken Urheberrechtsverletzungen festzustellen. Das Ganze läuft regelmäßig so ab, dass wir von dem Kunden, hier also von der Kanzlei Waldorf, Frommer, den Auftrag bekommen und auch die Informationen, wonach zu suchen ist. Wir bekommen dabei z. B. den Namen der Kopie und des Werkes, sowie entweder den torrent oder den filehash mitgeteilt. Dabei handelt es sich um solche Daten, die bereits beim Kunden validiert worden sind. Darauf lege ich besonderen Wert, das wird nicht von uns vorgenommen. Beim Kunden, also im Team von Waldorf, Frommer, gibt es dann jemanden, der die entsprechenden urheberrechtlichen Werke aus dem Tauschbörsennetzwerk herunterlädt und überprüft, ob es sich dabei tatsächlich um urheberrechtlich geschütztes Film- oder anderes Werkgut handelt. Nach dieser Validierung bekommen wir dann diese Daten mitgeteilt.

Die Ermittlungen laufen dann dergestalt, dass wir selbst an dem peer to peer Netzwerken teilnehmen, wie das oben links auf der von mir ausgeteilten Grafik ersichtlich ist. Dabei nehmen wir „fast ganz normal“ daran teil, dass bedeutet, dass wir dem Netzwerk quasi mitteilen, dass wir dem Netzwerk quasi mitteilen, dass wir „neu sind“, also selbst keine eigenen Inhalte zum Hochladen zur Verfügung stellen, und gleichzeitig auch den Quellcode der Filesharingsoftware dergestalt verändert haben, dass wir den Quellcode herausgelöscht haben, der für den Upload zuständig wäre, so dass wir sicherstellen können, dass von unseren Rechnern aus selbst keine Dateien zur Verfügung gestellt werden. Die Programme nehmen dann ganz automatisch am peer to peer Netzwerk teil, da sind keine Menschen mehr beteiligt. Der gesamte Datenverkehr, der in diesem Zusammenhang mit dem Internet passiert, wird dann über einen sogenannten traffic-Monitor, wie er oben mittig in der Grafik zu sehen ist, mitgeschnitten. Damit sind also sämtliche Datenpakete, die dort hin- und hergeschickt werden, als „noch Rohdaten“ gesichert. Diese werden mit einem Zeitstempel versehen, der aufgrund des sogenannten MTP-Protokolls mit Zeitangaben versehen wird, nach der Deutschen Standardzeit. Dabei handelt es sich um die gesetzliche Zeit. Auf Basis dieser Rohdaten finden dann die weiteren Ermittlungsschritte statt. Das Ganze läuft dann über eine sogenannte deep packet inspection, wie sie auf dem linken unteren Teil des Schaubildes zu sehen ist. Dabei werden dann über die Investition in die „investigation database“ die Daten reingeschrieben, dabei sind das pro Paket die fünf Informationen unserer IP-Adresse, die IP-Adresse der Gegenseite, unsere Ports, die Ports der Gegenseite und das Transportprotokoll. Dazu werden weitere Informationen festgestellt, und ob es sich z. B. um einen handshake handelt, um eine Zuweisung in der Warteschlange oder tatsächlich um einen Transfer. Sollte es sich um einen Transfer handeln, wird dann im Vergleich mit dem vom Kunden zur Verfügung gestellten validierten Taten festgestellt, ob es Bit für Bit um die gleiche Kopie handelt, die der Kunde uns zur Verfügung gestellt hatte.

Der Vorgang geht dann so weiter, dass etwa jeden Werktag über den „Reportgenerator“ die Daten gefiltert werden können. Der Kunde gibt dabei an, nach welchen Kriterien er gefiltert haben will, beispielsweise nach Zeitraumwerken oder nach Providern. Der Kunde gibt diese Sachen vor, und bekommt dann einen entsprechenden Report, in dem dann die entsprechenden Daten vorhanden sind. Der Kunde kann dann anhand der Zeitstempel, die die gesetzliche Zeit beinhalten, die ja auch bei den Internetprovidern maßgeblich ist, entsprechende Auskunftsverfahren über die IP-Adressen führen. Das machen dann auch nicht mehr wir.

Zusätzlich speichern wir die Rohdaten, wie unten rechts auf dem Schaubild ersichtlich, auf Magnetbändern und zwar zweifach redundant, diese werden auch signiert, um die Datenintegrität festzustellen. Dies geschieht deshalb, damit auch ggf. Jahre später sachverständige Dritte sich diese Rohdaten anschauen können und dann unsere Ermittlungsergebnisse nachvollziehen können. Das ist bereits auch schon mehrfach geschehen. Ich würde schätzen, dass es dazu vielleicht 100 Gerichtsgutachten schon zu unseren Daten gibt.

Der Zeuge ergänzt:

Das System funktioniert vollautomatisch. Da gibt also nirgendwo ein Mensch Zahlen ein. Natürlich wird das System laufend durch unser Team verbessert und überwacht, der eigentliche Ermittlungsvorgang funktioniert aber ohne menschliche Eingriffe statt.

Der Zeuge überreicht zur Erläuterung der konkreten Ermittlungen im vorliegenden Einzelfall ein weiteres handout, das als Anlage zu Protokoll genommen wird.

Der Zeuge erklärt hierzu:

Auf dem handout ist ganz oben der Clientname zu sehen. Dieser wird von der Tauschbörsensoftware vergeben, der kann z. B. aus der Versionsnummer und einer eindeutigen Zuordnung zu einem bestimmten Client bestehen, muss dies aber nicht. Die Idee dahinter ist, dass jede Clientbezeichnung nur einmal vergeben wird. Dann ist ersichtlich, dass die Verbindung über die IP-Adresse [redacted] im Zeitraum 02.04.2017 von 7:18:26 Uhr bis 19:04:46 Uhr gedauert hat. Weiter ist ersichtlich, dass es um den Film „Collateral Beauty“ geht, jedenfalls ist dieser Titel dort angegeben. Für die Technik entscheidend ist jedoch der sogenannte „Filehash“, der hier mit den der Zahlen-/ Ziffernfolge 164E83 usw. beginnt. Aus den weiteren Daten ist ersichtlich, dass insgesamt 4 Transfers stattgefunden haben, die insgesamt ca. 1,9 Millionen Bits uns versandt worden sind. Diese Bits, multipliziert mit 8, ergibt die Anzahl an Bits, die jeweils mit der Originaldatei, wie sie uns von Waldorf, Frommer zur Verfügung gestellt worden ist, verglichen worden ist. Sämtliche dieser Bits sind verifiziert worden, also waren übereinstimmend mit der uns gegebenen Vorlage.

Auf Frage des Beklagtenvertreters:

Es ist richtig, dass wir eine Kopie der Datei von Waldorf, Frommer bekommen. Mit dem aus der Datei ersichtlichen Hashwert nehmen wir dann an der Tauschbörse teil. Dabei handelt es sich nicht um einen klassischen „Honeypot“ im forensischen Sinne, wir also quasi eine Falle aufstellen und die inkriminierten Sachen anbieten, sondern wir äußern den Bedarf und die anderen bieten uns dann eben diese Dateien oder die jeweilige Datei nach dem Hashwert aus an. Allgemein ist es so, dass Tauschbörsensoftware so funktioniert, dass derjenige, der an der Tauschbörsensoftware teilnimmt, Inhalte bekommt und diese auch gleichzeitig weiterverteilt. Er bekommt die Dateien, die Inhalte von vielen anderen und gibt diese auch an viele andere weiter. Es ist also eine End-zu-End-Verbindung.

Unsere Software stellt nur fest, dass die Datei über eine bestimmte IP-Adresse unserem Client angeboten worden ist. Mehr können wir technisch nicht feststellen.

Auf Frage der Beklagten:

Ich bin für die Datenbanken zuständig, ich bin der Geschäftsführer und Produktmanager. Die anderen Angestellten bei mir in der Firma sind Informatiker. Man kann die Rohdaten nicht einfach so öffnen, das muss ein Sachverständiger machen.

Auf weitere Frage der Beklagten, ob der hier streitgegenständliche Film „Collateral Beauty“ auch mit anderen Filmen vermischt gewesen sein könnte, erklärt der Zeuge:

Das ist ausgeschlossen. Anhand des Filehashwertes kann man die Datei eindeutig zuordnen. Weshalb jetzt ein Nutzer nach diesem Film sucht und ob den auch tatsächlich anschauen will, oder ob er sich dabei vielleicht vertippt hat oder ähnliches, das kann ich natürlich nicht sagen.

Laut diktiert und genehmigt; auf erneutes Vorspielen wurde allseits verzichtet.

Der Zeuge wurde im allseitigen Einvernehmen unbeeidigt um 14.45 Uhr entlassen.

Der Zeuge machte Auslagenersatz geltend.

Die Beklagte überreicht ein Schreiben, dass sie im November 2020 an Vodafone gesandt hatte wegen der Auskunft, wonach keine Daten über ihren Anschluss herausgegeben worden seien und die entsprechende Antwort der Firma Vodafone vom 22.12.2020. Beide Schriftstücke werden dem Klägervertreter mit der Gelegenheit zur Kenntnisnahme ausgehändigt und sodann als Anlage zum Protokoll genommen.

Die Parteivertreter verhandeln streitig zum Ergebnis der Beweisaufnahme mit den Anträgen wie zu Protokoll vom 19.11.2020 (Bl. 155 d. A.).

Beschlossen und verkündet:

1. **Beide Parteien erhalten Gelegenheit, zum Ergebnis der bisherigen Beweisaufnahme mittels Schriftsatz an das Gericht bis zum 07.10.2021 (bei Gericht eingehend) schriftsätzlich Stellung zu nehmen,**

2. **Termin zur Verkündung einer Entscheidung wird im Hinblick auf die gewährte Stellungnahmefrist bestimmt auf:**

   <u>Donnerstag, den 28.10.2021, 08.45 Uhr,</u>
   <u>Geschäftsstelle der Abt. 513.</u>

Für die Richtigkeit der Übertragung vom Speichermedium:

Knepper
Richter am Amtsgericht

Chadwick
Justizangestellte