



**Fundstelle:** CRi 2011, 28 (*Weber*) = JurPC Web-Dok 203/2010 = jusIT 2011/8, 12 (*Staudegger*)

- 1. Grundsätzlich können IP-Adressen als „Personendaten“ iS von Art 3 lit a schwDSG qualifiziert werden. Dies trifft sowohl auf statische als auch unter bestimmten Umständen auf dynamische IP-Adressen zu.**
- 2. Personendaten sind geschützt. Ihre Verarbeitung darf nach Art 12 Abs 1 schwDSG die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Personendaten dürfen insbesondere ohne Rechtfertigungsgrund weder ermittelt noch Dritten bekanntgegeben werden.**
- 3. Der Einsatz einer sog. „p2p-Monitorsoftware“ (Trackingsoftware) zur Erfassung von Daten für die Identifizierung der Nutzer von Filesharingsystemen und deren Weiterleitung an die Rechteinhaber verstößt gegen Art 12 und 13 schwDSG.**
- 4. Die Interessen des Entwicklers der Monitorsoftware sind keine allgemeinen oder privaten, sondern eigene, wirtschaftliche zur Verfolgung eines Geschäftsmodells. Sie wiegen nicht schwerer als die datenschutzrechtlichen Interessen der betroffenen Personen.**

Leitsätze verfasst von Dr. *Clemens Thiele*, LL.M.

Die Bundesrichter Féraud, Präsident, Bundesrichter Reeb, Raselli, Fonjallaz, Eusebio, Gerichtsschreiber Dold sowie Verfahrensbeteiligte Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, als Beschwerdeführer, gegen Logistep AG, als Beschwerdegegnerin, vertreten durch Rechtsanwältin Ursula Sury, zum Gegenstand einer Umsetzung einer Empfehlung des EDÖB, über die Beschwerde gegen den Entscheid vom 27. Mai 2009 des Bundesverwaltungsgerichts, Abteilung I, erkennen als Bundesgericht:

1. Die Beschwerde wird gutgeheissen und das Urteil des Bundesverwaltungsgerichts vom 27. Mai 2009 aufgehoben.
2. Die Beschwerdegegnerin wird angewiesen, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und es wird ihr untersagt, die bereits beschafften Daten den betroffenen Urheberrechtsinhabern weiterzuleiten.
3.
  - 3.1 Die Gerichtskosten von Fr. 3.000.-- werden der Beschwerdegegnerin auferlegt.
  - 3.2 Für das bundesgerichtliche Verfahren werden keine Parteientschädigungen zugesprochen.
  - 3.3 Die Sache geht zur Regelung der Kosten- und Entschädigungsfrage für das vorinstanzliche Verfahren an das Bundesverwaltungsgericht zurück.
4. Dieses Urteil wird den Parteien und dem Bundesverwaltungsgericht, Abteilung I, schriftlich mitgeteilt.

#### **Sachverhalt:**

A.

Am 9. Januar 2008 erliess der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eine Empfehlung an die Adresse der Logistep AG. Er hielt fest, die Logistep AG suche mittels der von ihr entwickelten Software in verschiedenen Peer-to-Peer-Netzwerken (auch P2P-Netzwerke genannt) nach angebotenen urheberrechtlich geschützten Werken. Beim Herunterladen dieser Werke würden folgende Übermittlungsdaten aufgezeichnet und in einer Datenbank abgespeichert:

- der Benutzername des Nutzers des P2P-Netzwerks;
- die IP-Adresse (Internetworking Protocol Address) des verwendeten Internetanschlusses;
- die GUID (eine Identifikationsnummer der vom Anbieter des urheberrechtlich geschützten Werks verwendeten Software);

- das verwendete P2P-Netzwerkprotokoll;
- der Name und elektronische Fingerabdruck (Hashcode) des urheberrechtlich geschützten Werks;
- das Datum, die Uhrzeit und der Zeitraum der Verbindung zwischen der Software der Logistep AG und der Software des Anbieters des jeweiligen urheberrechtlich geschützten Werks.

Die so erhobenen Daten würden anschließend an die Urheberrechtsinhaber weitergegeben und von diesen zur Identifikation des Inhabers des Internetanschlusses verwendet. Zu diesem Zweck reichten die Urheberrechtsinhaber unter anderem Strafanzeige gegen Unbekannt ein und verschafften sich die Identitätsdaten im Rahmen des Akteneinsichtsrechts. Diese Daten würden sodann zur Geltendmachung von Schadenersatzforderungen verwendet. Der EDÖB gelangte zum Schluss, dass die Bearbeitungsmethoden der Logistep AG geeignet seien, die Persönlichkeit einer größeren Anzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz [DSG; SR 235.1]). Daher empfahl er dieser mit Schreiben vom 9. Januar 2008 gestützt auf Art. 29 Abs. 3 DSG, die Datenbearbeitung unverzüglich einzustellen, solange keine ausreichende gesetzliche Grundlage für eine zivilrechtliche Nutzung der durch sie erhobenen Daten bestehe.

Nachdem die Logistep AG die Empfehlung mit Schreiben vom 14. Februar 2008 abgelehnt hatte, legte der EDÖB die Angelegenheit mit Klage vom 13. Mai 2008 dem Bundesverwaltungsgericht zum Entscheid vor. Er beantragte in erster Linie, die Logistep AG sei aufzufordern, die von ihr praktizierte Datenbearbeitung (inklusive der Weitergabe an die Urheberrechtsinhaber) unverzüglich einzustellen, solange keine ausreichende gesetzliche Grundlage für eine generelle Überwachung von Peer-to-Peer-Netzwerken bestehe. Die Logistep AG ihrerseits beantragte in ihrer Klageantwort, die Eingabe des Klägers sei infolge gravierender formeller Mängel zur befristeten Nachbesserung zurückzuweisen und ihr selbst sei anschließend neu Frist zur Einreichung einer Klageantwort anzusetzen. Eventualiter seien die Anträge des Klägers abzuweisen, soweit darauf überhaupt einzutreten sei. Der Kläger sei zu verpflichten, seine Empfehlung zurückzuziehen, subeventualiter im Sinne der Erwägungen des Bundesverwaltungsgerichts anzupassen. Zudem sei der Kläger zu verpflichten, die schweizerische Presse und Öffentlichkeit umfassend und aktiv hinsichtlich des Urteils des Bundesverwaltungsgerichts zu orientieren; dies alles unter Kosten- und Entschädigungsfolgen zu Lasten des Klägers.

Mit Urteil vom 27. Mai 2009 wies das Bundesverwaltungsgericht die Klage ab und hob die Empfehlung des EDÖB vom 9. Januar 2008 auf. Im Übrigen wies es die Begehren der Beklagten ab, soweit es darauf eintrat.

#### B.

Mit Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht vom 26. Juni 2009 beantragt der EDÖB, die Logistep AG sei anzuweisen, ihre Datenbearbeitung unverzüglich einzustellen. Ihr sei jegliche Weitergabe von gesammelten Peer-to-Peer-Daten an die Urheberrechtsinhaber zu untersagen. Die Kosten- und Entschädigungsfolgen seien zu Lasten der Beschwerdegegnerin festzulegen.

In seiner Vernehmlassung vom 17. Juli 2009 beantragt das Bundesverwaltungsgericht die Abweisung der Beschwerde, soweit darauf einzutreten sei. Die Beschwerdegegnerin beantragt in ihrer Stellungnahme vom 23. September 2009 in erster Linie, die Beschwerde sei abzuweisen und der Beschwerdeführer sei zu verpflichten, die schweizerische Presse und Öffentlichkeit umfassend und aktiv hinsichtlich des Urteils des Bundesgerichts in der vorliegenden Beschwerdesache zu orientieren.

#### C.

Die I. öffentlich-rechtliche Abteilung des Bundesgerichts hat die Angelegenheit am 8. September

2010 an einer öffentlichen Sitzung beraten.

### **Erwägungen:**

1.

1.1 Angefochten ist ein Endentscheid des Bundesverwaltungsgerichts über eine Empfehlung des EDÖB (Art. 86 Abs. 1 lit. a und Art. 90 BGG). Gemäss Art. 29 Abs. 4 Satz 2 DSG i.V.m. Art. 89 Abs. 2 lit. d BGG ist der EDÖB berechtigt, gegen diesen Entscheid Beschwerde zu führen.

Der angefochtene Entscheid betrifft eine Empfehlung des EDÖB im Privatrechtsbereich (Art. 29 DSG). Es stellt sich die Frage, ob nicht statt der Beschwerde in öffentlich-rechtlichen Angelegenheiten nach Art. 82 ff. BGG die Beschwerde in Zivilsachen nach Art. 72 ff. BGG zu erheben gewesen wäre. Die Frage ist aus folgenden Gründen zu verneinen. Das Verfahren wurde vom der Bundesverwaltung angehörenden EDÖB eingeleitet und richtet sich gegen ein Privatrechtssubjekt. Die beiden stehen sich nicht als einander gleichgestellte Rechtssubjekte gegenüber. Zwar ist es dem EDÖB verwehrt, Verfügungen zu erlassen, doch sind private Personen unter Androhung der Busse verpflichtet, bei seinen Abklärungen mitzuwirken (Art. 34 Abs. 2 lit. b DSG). Zudem geht es gerade bei der Bestimmung von Art. 29 Abs. 1 lit. a DSG, auf die der EDÖB im vorliegenden Fall seine Empfehlung stützte, um Gefährdungen der Persönlichkeit, welche überindividuellen Charakter besitzen und damit öffentliche Interessen betreffen (vgl. Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz, BBl 1988 II 479 Ziff. 221.5; RENÉ HUBER, in: Basler Kommentar, Datenschutzgesetz, 2. Aufl. 2006, N. 7 zu Art. 29 DSG; DAVID ROSENTHAL, in: Handkommentar zum Datenschutzgesetz, 2008, N. 11 zu Art. 29 DSG). Der Entscheid des Bundesverwaltungsgerichts betrifft folglich eine Angelegenheit des öffentlichen Rechts, womit sich die Beschwerde in öffentlich-rechtlichen Angelegenheiten als das zutreffende Rechtsmittel erweist.

Die weiteren Sachurteilsvoraussetzungen geben zu keinen Bemerkungen Anlass. Auf die Beschwerde des EDÖB ist im Grundsatz einzutreten.

1.2 Das Bundesgericht legt seinem Urteil den von der Vorinstanz festgestellten Sachverhalt zugrunde (Art. 105 Abs. 1 BGG). Soweit die vorinstanzlichen Sachverhaltsfeststellungen beanstandet werden und eine mangelhafte Sachverhaltsfeststellung für den Ausgang des Verfahrens entscheidend ist, kann nur geltend gemacht werden, die Feststellungen seien offensichtlich unrichtig oder beruhten auf einer Rechtsverletzung im Sinne von Art. 95 BGG (Art. 97 Abs. 1 und Art. 105 Abs. 2 BGG). Eine entsprechende Rüge ist substantiiert vorzubringen (Art. 42 Abs. 2 BGG). Vorbehalten bleibt die Sachverhaltsberichtigung von Amtes wegen nach Art. 105 Abs. 2 BGG (BGE 135 III 127 E. 1.5 S. 129 f.; BGE 133 II 249E. 1.4.3 S. 254 f.; je mit Hinweisen).

Sowohl der Beschwerdeführer als auch die Beschwerdegegnerin stellen den Sachverhalt aus ihrer Sicht dar, jedoch ohne die diesbezüglichen Feststellungen des Bundesverwaltungsgerichts im vorangehend beschriebenen Sinne als fehlerhaft zu rügen. Soweit ihre Ausführungen von der Sachverhaltsfeststellung im angefochtenen Entscheid abweichen, ist darauf nicht einzutreten.

1.3 Die Beschwerdegegnerin hat gegen das Urteil des Bundesverwaltungsgerichts vom 27. Mai 2009 kein Rechtsmittel eingelegt. In ihrer Vernehmlassung zur vorliegenden Beschwerde beantragt sie, der Beschwerdeführer sei zu verpflichten, die schweizerische Presse und Öffentlichkeit umfassend und aktiv hinsichtlich des Urteils des Bundesgerichts in der vorliegenden Beschwerdesache zu orientieren. Damit geht sie über eine Stellungnahme zur Beschwerde der Gegenpartei hinaus. Dies ist unzulässig, denn das Bundesgerichtsgesetz sieht keine Anschlussbeschwerde vor (BGE 134 III 332 E. 2.5 S. 335 f. mit Hinweisen). Auf den Antrag ist nicht einzutreten.

2.

2.1 Der EDÖB wirft dem Bundesverwaltungsgericht vor, Art. 12 Abs. 2 lit. a DSG falsch ausgelegt zu haben. Diese Bestimmung lässt seiner Ansicht nach in ihrer aktuellen Fassung keine Rechtfertigungsgründe mehr zu. Stattdessen müsse geprüft werden, ob ein Grundsatz der Datenbearbeitung verletzt worden sei. Dies erfordere eine Verhältnismäßigkeitsprüfung, welche die bestehenden Rechtfertigungsgründe mitberücksichtige. Das Bundesverwaltungsgericht habe die dabei notwendige Interessenabwägung fehlerhaft vorgenommen, denn es bestünden keine überwiegenden privaten oder öffentlichen Interessen. Die Persönlichkeit der betroffenen Personen sei somit widerrechtlich verletzt worden. Indem die Vorinstanz dies verkannt habe, habe sie auch gegen das in Art. 4 Abs. 1 DSG verankerte Legalitätsprinzip verstoßen.

2.2 Die Beschwerdegegnerin hält dem entgegen, bei den von ihr bearbeiteten IP-Adressen handle es sich nicht um Personendaten im Sinne von Art. 3 lit. a DSG. Die Vorschriften des Datenschutzgesetzes fänden deshalb gar keine Anwendung. Im Übrigen wäre eine allfällige Verletzung der Persönlichkeit angesichts der überwiegenden privaten und öffentlichen Interessen nicht widerrechtlich. Entgegen der Ansicht des Beschwerdeführers müssten die in Art. 13 DSG genannten Rechtfertigungsgründe in jedem Fall berücksichtigt werden.

2.3 Das Bundesverwaltungsgericht ging von der Anwendbarkeit des Datenschutzgesetzes aus, wies die Klage des EDÖB indessen wegen des Vorliegens von Rechtfertigungsgründen ab. Da von einer Aufhebung seines Entscheids auch dann abzusehen wäre, wenn dessen Ergebnis mit einer alternativen Begründung aufrechterhalten werden könnte (Urteil des Bundesgerichts 2P.172/2005 vom 25. Oktober 2005 E. 2), ist im Folgenden vorab die von der Beschwerdegegnerin in Frage gestellte Anwendbarkeit des Datenschutzgesetzes zu untersuchen. In einem zweiten Schritt ist zu prüfen, ob eine widerrechtliche Persönlichkeitsverletzung vorliegt.

3.

3.1 In Bezug auf die Anwendbarkeit des Datenschutzgesetzes ist in der Literatur die Meinung vertreten worden, dass IP-Adressen ausschließlich in den Anwendungsbereich des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10) fallen, welches eine abschließende Regelung enthalte. Dies wird damit begründet, dass es sich bei IP-Adressen um numerische Kommunikationsparameter und damit um Adressierungselemente im Sinne der Fernmeldegesetzgebung handle, die unter das Fernmeldegeheimnis gemäß Art. 43 FMG fielen (Daniel Kettiger, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, Jusletter vom 9. August 2010, Rz. 20).

Richtig ist, dass es sich bei den IP-Adressen um Adressierungselemente im Sinne der Fernmeldegesetzgebung handelt. Das Fernmeldegeheimnis gilt jedoch von vornherein nur für diejenigen, der mit fernmeldedienstlichen Aufgaben "betraut" ist (Art. 43 FMG; vgl. BGE 126 I 50 E. 6a S. 65 mit Hinweis). Dies trifft auf die Beschwerdegegnerin nicht zu. Das Fernmeldegesetz steht damit im vorliegenden Fall der Anwendbarkeit des Datenschutzgesetzes nicht entgegen.

3.2 Personendaten (bzw. "Daten" im Sinne des Datenschutzgesetzes) sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). Bei den betreffenden Informationen kann es sich sowohl um Tatsachenfeststellungen als auch um Werturteile handeln. Unerheblich ist, in welcher Form die Informationen auftreten (etwa als Zeichen, Wort, Bild, Ton oder eine Kombination davon) und wie der Datenträger beschaffen ist. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen (URS BELSER, in: Basler Kommentar, Datenschutzgesetz, 2. Aufl. 2006, N. 5 zu Art. 3 DSG).

Eine Person ist dann bestimmt, wenn sich aus der Information selbst ergibt, dass es sich genau um

diese Person handelt. Bestimmbar ist die Person, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor (BBl 1988 II 444 f. Ziff. 221.1). Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mit zu berücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuzuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat (BELSER, a.a.O., N. 6 zu Art. 3 DSG; ROSENTHAL, a.a.O., N. 24 f. zu Art. 3 DSG).

3.3 Bei den von der Beschwerdegegnerin bearbeiteten IP-Adressen handelt es sich um numerische Kommunikationsparameter, welche die Identifikation einer insbesondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglichen (so die Definition im Anhang der Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich [AEFV; SR 784.104]). Durch die IP-Adresse wird mit anderen Worten jeder an das Internet angeschlossene Computer identifiziert. Immer wenn im Internet Daten abgefragt werden, so zum Beispiel beim Aufrufen einer Website, übermittelt der Computer des Benutzers seine Anfrage verbunden mit der ihm zugewiesenen IP-Adresse (PER MEYERDIERKS, Sind IP-Adressen personenbezogene Daten? MultiMedia und Recht 1/2009 S. 8 f.). Auf diese Weise ermöglicht die IP-Adresse den Datenaustausch im Internet.

Wird einem Rechner eine IP-Adresse fest zugewiesen, spricht man von einer statischen IP-Adresse. Wählt sich ein Benutzer über einen Internet-Dienstanbieter (Provider) ins Internet ein, erhält er jedoch meist eine dynamische IP-Adresse, das heisst, seinem Computer wird bei jeder Verbindungsaufnahme neu irgendeine freie Adresse aus dem Pool des Providers zugewiesen. Die dynamische Adressierung wurde wegen der Knappheit der IP-Adressen entwickelt. Weil nach diesem System eine IP-Adresse nur für eine kurze Zeit einem Teilnehmer zugeteilt und nach dem Nutzungsvorgang wieder an einen anderen Teilnehmer vergeben wird, erfolgt die Identifikation des betreffenden Rechners durch diese IP-Adresse auch nur für die Zeit des einzelnen Nutzungsvorgangs. Aus diesem Grund ist die Identifikation des Inhabers der IP-Adresse bei der dynamischen Adressierung schwieriger als bei der statischen. Während statische IP-Adressen in zum Teil frei zugänglichen Verzeichnissen erfasst sind, ist der Inhaber einer dynamischen IP-Adresse in der Regel nur mit Hilfe des Providers, der die Adresse vergeben hat, eruierbar (ROLF H. WEBER/ORSOLYA FERCSIK SCHNYDER, "Was für 'ne Sorte von Geschöpf ist euer Krokodil?" - Zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic! 9/2009 S. 579 f.).

3.4 Ob eine Information aufgrund zusätzlicher Angaben mit einer Person in Verbindung gebracht werden kann, sich die Information mithin auf eine bestimmbare Person bezieht (Art. 3 lit. a DSG), beurteilt sich aus der Sicht des jeweiligen Inhabers der Information (ROSENTHAL, a.a.O., N. 20 zu Art. 3 DSG; WEBER/FERCSIK SCHNYDER, a.a.O., S. 583). Im Falle der Weitergabe von Informationen ist dabei ausreichend, wenn der Empfänger die betroffene Person zu identifizieren vermag. ROSENTHAL führt in diesem Zusammenhang das Beispiel einer Zeitungsmeldung über den Unfall eines nicht namentlich genannten Lokalpolitikers an. Sofern ein Teil der Leserschaft auf die betroffene Person (allenfalls anhand weiterer Recherchen) schließen könne, stelle aus ihrer Sicht die Publikation eine Bekanntgabe von Personendaten dar, so die überzeugende Argumentation des Autors (ROSENTHAL, a.a.O., N. 30 zu Art. 3 DSG; vgl. auch Art. 3 lit. e DSG). Dies bedeutet für den vorliegenden Fall, dass nicht vorausgesetzt ist, dass die Urheberrechtsverletzer bereits für die Beschwerdegegnerin bestimmbar sind. Vielmehr genügt es, wenn sie es nach Übergabe der entsprechenden Daten für die Urheberrechtinhaber werden. Trifft dies zu (dazu sogleich), so

gelangt das Datenschutzgesetz indessen auch auf die Beschwerdegegnerin selbst zur Anwendung. Anders zu entscheiden würde bedeuten, das Datenschutzgesetz nur auf die einzelnen Empfänger anzuwenden, nicht aber auf die Person, welche die betreffenden Daten beschafft und sie verbreitet. Dies würde dem Zweck des Gesetzes zuwiderlaufen.

3.5 Die Beschwerdegegnerin macht geltend, die Auftraggeber würden nur aufgrund des Tätigwerdens der Strafverfolgungsbehörden erfahren, wer die Inhaber der einzelnen IP-Adressen sind. Sie verkennt dabei, dass die Notwendigkeit des Tätigwerdens eines Dritten so lange unmaßgeblich ist, als insgesamt der Aufwand des Auftraggebers für die Bestimmung der betroffenen Person nicht derart groß ist, dass nach der allgemeinen Lebenserfahrung nicht mehr damit gerechnet werden könnte, dieser werde ihn auf sich nehmen (vgl. E. 3.1 hiavor). Solches ist vor dem Hintergrund der konkreten Umstände des Einzelfalls zu beurteilen. Eine abstrakte Feststellung, ob es sich (insbesondere bei dynamischen) IP-Adressen um Personendaten handelt oder nicht, ist somit nicht möglich (vgl. zum deutschen Recht ULRICH DAMMANN, in: Bundesdatenschutzgesetz, 6. Aufl. 2006, N. 20 zu § 3 BDSG; kritisch MEYERDIERKS, a.a.O., S. 10 ff.; vgl. zur datenschutzrechtlichen Qualifizierung von IP-Adressen im schweizerischen Recht ROSENTHAL, a.a.O., N. 27 zu Art. 3 DSG; WEBER/FERCSIK SCHNYDER, a.a.O., S. 588).

Für den vorliegenden Fall ist die Bestimmbarkeit der betroffenen Personen grundsätzlich zu bejahen. Auf ihr beruht ganz eigentlich das Geschäftsmodell der Beschwerdegegnerin. Diese zeichnet nach eigenen Angaben dynamische IP-Adressen möglicher Urheberrechtsverletzer sowie weitere Daten auf, welche sie den Rechteinhabern weitergibt. Die Rechteinhaber ihrerseits können durch Strafanzeige auf die Einleitung eines Strafverfahrens hinwirken, um in dessen Rahmen Akteneinsicht zu nehmen und so den P2P-Teilnehmer ausfindig zu machen, welcher das urheberrechtlich geschützte Werk unrechtmäßig angeboten hat (vgl. Art. 67 ff. des Bundesgesetzes vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte [URG; SR 231.1] sowie Art. 5 und Art. 14 Abs. 4 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF; SR 780.1] i.V.m. Art. 43 FMG; BGE 126 I 50; Stéphane Bondallaz, La protection des personnes et de leurs données dans les télécommunications, 2007, Rz. 1086; Peter Schaar, Datenschutz im Internet, 2002, Rz. 175; vgl. auch Rosenthal, a.a.O., N. 27 zu Art. 3 DSG). Wohl ist davon auszugehen, dass in vielen Fällen der Urheberrechtsverletzer nicht ausfindig gemacht werden kann, so insbesondere dann, wenn verschiedene Personen zu einem Computer oder einem Netzwerk Zugang haben. Es ist jedoch ausreichend, dass die Bestimmbarkeit in Bezug auf einen Teil der von der Beschwerdegegnerin gespeicherten Informationen gegeben ist.

3.6 Diese Auslegung des Datenschutzgesetzes scheint im Übrigen in Einklang mit der Rechtslage in der Europäischen Union zu stehen. Mit dem Begriff der personenbezogenen Daten setzte sich dort die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten in ihrer Stellungnahme 4/2007 vom 20. Juni 2007 eingehend auseinander. Das unabhängige EU-Beratungsgremium für Datenschutzfragen stuft IP-Adressen als Daten ein, die sich auf eine bestimmbare Person beziehen. Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken könnten ohne großen Aufwand Internetnutzer identifizieren, denen sie IP-Adressen zugewiesen hätten, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internetnutzer zugeteilte dynamische IP-Adresse einfügen würden. Dasselbe lasse sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen würden. In diesen Fällen bestehe kein Zweifel, dass man von personenbezogenen Daten im Sinne von Art. 2 lit. a der Richtlinie 95/46/EG reden könne (Stellungnahme S. 19 f.; <[http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)> unter Documents adopted/2007 [besucht am 3. November 2010]).

3.7 Schließlich bringt die Beschwerdegegnerin vor, bei einer Qualifizierung der strittigen Angaben als Personendaten sei es ihr unmöglich, ihrer datenschutzrechtlichen Auskunftspflicht

nachzukommen. Dies ist unzutreffend. Zwar verlangt Art. 8 DSGVO, dass der Inhaber der Datensammlung der betroffenen Person alle über sie in der Datensammlung vorhandenen Daten mitteilt. Indessen beschränkt sich das Auskunftsrecht schon nach Gesetzeswortlaut auf die vorhandenen Daten (vgl. auch BBl 1988 II 453 Ziff. 221.2). Vom Inhaber einer Datensammlung können mithin keine Angaben gefordert werden, über die er gar nicht verfügt. Zudem können vom Auskunftsberechtigten allenfalls konkretisierende Angaben verlangt werden, wenn dies zum Auffinden der Daten notwendig oder hilfreich ist (VPB 65/2001 Nr. 49 E. 3b).

3.8 Zusammenfassend ist festzuhalten, dass das Bundesverwaltungsgericht die von der Beschwerdegegnerin bearbeiteten IP-Adressen zu Recht als Personendaten im Sinne von Art. 3 lit. a DSGVO qualifiziert hat.

4.

Die Beschwerdegegnerin bestreitet einen Verstoß gegen die Grundsätze der Zweckbindung und der Erkennbarkeit (Art. 4 Abs. 3 und 4 DSGVO). Die Bearbeitung der Daten erfolge zu einem im Voraus und für alle P2P-Nutzer erkennbaren Zweck, nämlich zur rechtmäßigen straf- sowie zivilrechtlichen Verfolgung von Urheberrechtsverletzungen.

Das Bundesverwaltungsgericht lege im angefochtenen Entscheid dar, die Beschwerdegegnerin sammle Daten über P2P-Netzwerkteilnehmer, die sie an ihre Auftraggeber weiterleite. Die Datenbeschaffung geschehe dabei im Regelfall ohne Wissen der betroffenen Personen und sei für diese auch nicht erkennbar. Das Vorgehen der Beschwerdegegnerin schließe zudem aus, dass dem IP-Adressinhaber im Moment der Beschaffung mitgeteilt werde, wozu seine Daten gespeichert würden. Selbst wenn es zutrefte, dass vereinzelt darauf aufmerksam gemacht werde, dass "Anti-P2P-Firmen Daten loggen", könne keineswegs von einer Angabe des Datenbeschaffungszwecks durch die Bearbeiterin gesprochen werden. Sowohl der Grundsatz der Zweckbindung wie auch der Grundsatz der Erkennbarkeit würden damit regelmäßig verletzt.

Die Beschwerdegegnerin geht auf die überzeugenden Ausführungen des Bundesverwaltungsgerichts nicht ein und beschränkt sich darauf, diese pauschal zu bestreiten. Auf ihre diesbezüglichen Vorbringen ist deshalb nicht einzutreten (vgl. Art. 42 Abs. 2 BGG).

5.

5.1 Art. 12 und 13 DSGVO legen die Voraussetzungen fest, nach welchen die Bearbeitung von Personendaten durch Private rechtmäßig ist.

Art. 12 Persönlichkeitsverletzungen

1 Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

2 Er darf insbesondere nicht:

- a. Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten;
- b. ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeiten;
- c. ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben.

3 In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Art. 13 Rechtfertigungsgründe

1 Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

2 Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese:

- a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;

- b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;
- c. zur Prüfung der Kreditwürdigkeit einer anderen Person weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet und Dritten nur Daten bekannt gibt, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen;
- d. beruflich Personendaten ausschließlich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet;
- e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind;
- f. Daten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Während auf die Rechtfertigungsgründe von Art. 13 DSG in Art. 12 Abs. 2 lit. b und c DSG ausdrücklich verwiesen wird, fehlt ein entsprechender Vorbehalt in der aktuellen Fassung von lit. a der letztgenannten Bestimmung. Der Beschwerdeführer schließt daraus, dass eine Verletzung der Grundsätze der Datenbearbeitung im Sinne von Art. 4 DSG, wozu auch die Grundsätze der Zweckbindung und der Erkennbarkeit gehören, nicht gerechtfertigt werden kann.

## 5.2

5.2.1 Es fragt sich, ob das Streichen des Vorbehalts in Art. 12 Abs. 2 lit. a DSG im Zuge der Gesetzesrevision vom 24. März 2006 ein qualifiziertes Schweigen zum Ausdruck bringt. Die Rechtfertigung einer gegen die Grundsätze der Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG verstoßenden Bearbeitung von Personendaten wäre diesfalls generell ausgeschlossen. In der Literatur gehen die Meinungen auseinander. Für die Möglichkeit, Rechtfertigungsgründe weiterhin zuzulassen, sprechen sich Stephan C. Brunner, Christian Drechsler und David Rosenthal aus (Stephan C. Brunner, Das revidierte Datenschutzgesetz und seine Auswirkungen im Gesundheits- und Versicherungswesen, in: Datenschutz im Gesundheits- und Versicherungswesen, 2008, S. 142 ff.; Christian Drechsler, Die Revision des Datenschutzrechts, AJP 2007 S. 1474; Rosenthal, a.a.O., N. 16 zu Art. 12 DSG). Anderer Ansicht ist, allerdings ohne dies näher zu begründen, René Huber (Die Teilrevision des Eidg. Datenschutzgesetzes - ungenügende Pinselrenovation, recht 24/2006 S. 214).

5.2.2 Die Materialien bringen keine ausreichende Klarheit. Die Streichung des Vorbehalts geht auf einen Vorschlag der vorberatenden Kommission des Nationalrats zurück und war im Entwurf des Bundesrats noch nicht vorgesehen. Der Nationalrat genehmigte die Änderung diskussionslos (AB 2005 N 1450). Im Ständerat wurde sie vom Berichterstatter der Kommission in ausführlicher, jedoch auch widersprüchlicher Weise erläutert. Seine Äußerung, es ginge nicht an, dass man unrechtmäßig beschaffte Daten bei Vorliegen eines Rechtfertigungsgrunds bekannt geben dürfe, könnte in der Tat darauf schließen lassen, dass Rechtfertigungsgründe im Rahmen von Art. 12 Abs. 2 lit. a DSG generell ausgeschlossen sind. Der Berichterstatter erklärte indessen auch, dass es bei der vom Nationalrat beschlossenen Fassung im Grunde genommen nur um eine Klarstellung dessen gehe, was an sich heute schon bestehe, in der Praxis aber offenbar zu Problemen geführt habe. Wenn man diesen Rechtfertigungsumstand weglasse, so beschließe man keineswegs etwas völlig Neues, sondern übernehme im Prinzip das, was schon heute in der Rechtsprechung gelte (AB 2005 S 1159; vgl. dazu VPB 69/2005 Nr. 106 E. 5.2 und 5.8).

5.2.3 Nach Auffassung des Bundesamts für Justiz war kein Systemwechsel vorgesehen. Stattdessen habe mit der Neuformulierung von Art. 12 Abs. 2 lit. a DSG den Grundsätzen von Art. 4 DSG Nachachtung verschafft werden sollen, ohne an der früheren Rechtslage etwas zu ändern. Die textliche Änderung verdeutliche, dass eine Rechtfertigung nicht vorschnell angenommen werden dürfe (Bundesamt für Justiz, Änderung von Art. 12 Abs. 2 Bst. a DSG: Auslegungshilfe, 2006, <<http://www.edoeb.admin.ch/themen/00794/00819/01086/index.html?lang=de>> [besucht am 3. November 2010]). Diese Auslegung liegt auf einer Linie mit der Botschaft des Bundesrats zur ursprünglichen Fassung von Art. 12 Abs. 2 lit. a DSG, wonach die Grundsätze von Art. 4 DSG "das ethische und rechtspolitische Fundament des Datenschutzgesetzes" darstellen, weshalb "nicht ohne



zwingenden Grund gegen sie verstoßen werden können" solle (BBl 1988 II 458 f. Ziff. 221.3).

5.2.4 Würde man die Bearbeitung unrechtmäßig beschaffter Daten (Art. 4 Abs. 1 DSGVO) generell ausschließen, so wäre es beispielsweise einem Arbeitgeber, der von einem Mitarbeiter unrechtmäßig gespeicherte Personendaten entdeckt, nicht erlaubt, diese den Behörden zu übergeben. Auch wäre eine Verletzung der Grundsätze der Datenbearbeitung selbst bei Einwilligung des Verletzten widerrechtlich (Art. 13 Abs. 1 DSGVO; Rosenthal, a.a.O., N. 19 zu Art. 12 DSGVO). Dies kann jedoch nicht der Sinn des Gesetzes sein. Eine strikt systematische Auslegung, wonach lediglich bei lit. b und c, nicht aber bei lit. a von Art. 12 Abs. 2 DSGVO das Geltendmachen eines Rechtfertigungsgrunds zulässig sein soll, erweist sich als verfehlt, zumal in der aktuellen Fassung von lit. a Rechtfertigungsgründe zwar nicht mehr erwähnt, jedoch auch nicht ausdrücklich ausgeschlossen werden. Die Bestimmung ist daher so auszulegen, dass eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSGVO zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit großer Zurückhaltung bejaht werden können.

5.2.5 In Berücksichtigung des Bestrebens des Gesetzgebers, die Bedeutung der Grundsätze von Art. 4 DSGVO zu betonen, schlägt das Bundesamt für Justiz in seiner Auslegungshilfe zur Änderung von Art. 12 Abs. 2 lit. a DSGVO vor, künftig rechtfertigende Umstände primär bei der Auslegung der allgemeinen Grundsätze zu berücksichtigen (BUNDESAMT FÜR JUSTIZ, a.a.O., Ziff. 3.1). Ein derartiges Vorgehen erscheint etwa dort praktikabel, wo sich die Abgrenzung zwischen den Grundsätzen von Art. 4 DSGVO und den Rechtfertigungsgründen von Art. 13 DSGVO ohnehin als schwierig erweist, so beispielsweise beim Grundsatz der Verhältnismäßigkeit (vgl. CORRADO RAMPINI, in: Basler Kommentar, Datenschutzgesetz, 2. Aufl. 2006, N. 4 zu Art. 12 DSGVO). Indessen sind nicht alle Grundsätze der Datenbearbeitung einer Auslegung zugänglich, welche die Rechtfertigungsgründe von Art. 13 DSGVO bereits hinreichend berücksichtigt. Auch ist nicht zu übersehen, dass es im Ergebnis nicht von Belang ist, ob Rechtfertigungsgründe in einem zweiten Schritt selbständig geprüft werden oder bereits bei der Auslegung der Grundsätze der Datenbearbeitung berücksichtigt werden (vgl. zum Ganzen ROSENTHAL, a.a.O., N. 22 f. zu Art. 12 DSGVO).

5.2.6 Die Vorinstanz stellte in einem ersten Schritt eine Verletzung der Grundsätze der Zweckbindung und der Erkennbarkeit fest. Ob eine Verletzung des Verhältnismäßigkeitsprinzips vorliege, ließ sie zunächst offen. Bei der Prüfung der Frage, ob ein überwiegendes privates oder öffentliches Interesse die Persönlichkeitsverletzung rechtfertige, untersuchte sie indessen auch, ob die strittige Datenbearbeitung verhältnismäßig sei. Nach dem Gesagten ist an diesem Vorgehen nichts auszusetzen.

6.

6.1 Der Beschwerdeführer kritisiert die Interessenabwägung der Vorinstanz bei der Prüfung von Rechtfertigungsgründen gemäß Art. 13 DSGVO. Würde man ihr folgen, so wäre seiner Ansicht nach jegliche Art der Datenbearbeitung, auch eine zweckwidrige und heimliche, gerechtfertigt, der Zweck würde mithin die Mittel heiligen. Eine betroffene Person könnte sich gegen die Datenbearbeitung nicht einmal zur Wehr setzen, da sie über diese nicht oder nicht hinreichend informiert sei. Die Bürger in der Schweiz würden damit weitgehend ihrer Auskunftsrechte gemäß Art. 8 DSGVO beraubt. Die Vorinstanz blende zudem aus, dass der Inhaber der IP-Adresse nicht zwangsläufig identisch mit dem Verletzer des Urheberrechts sein müsse, da ein Internetanschluss zum Teil von mehreren Personen benutzt werde. Gutgläubige Inhaber von Internetanschlüssen würden so mit ungerechtfertigten Zivilforderungen konfrontiert. Das Vorgehen der Beschwerdegegnerin sei jenem eines verdeckten Ermittlers vergleichbar, dessen Einsatz jedoch an strenge Voraussetzungen geknüpft werde (Art. 4 des Bundesgesetzes vom 20. Juni 2003 über die verdeckte Ermittlung [BVE; SR 312]). Schließlich sei zu berücksichtigen, dass die Strafverfahren nur benützt würden, um das Fernmeldegeheimnis zu umgehen, und dass die Beschwerdegegnerin zusammen mit den Inhabern der Urheberrechte primär an der Geltendmachung von Zivilforderungen interessiert sei.

6.2 Die Vorinstanz erwog, ohne die Sammlung technischer Daten, wie insbesondere der IP-Adresse, wäre es für die in ihren Rechten verletzten Urheberrechtsinhaber nicht möglich, die Verletzer zu identifizieren und gegen diese Schadenersatz- und Unterlassungsansprüche geltend zu machen. Ein milderer, aber gleich geeignetes Mittel sei nicht ersichtlich. Demgegenüber erscheine der Eingriff in die Persönlichkeitsrechte der betroffenen Personen nicht ausgesprochen schwerwiegend. Sollten sich die Beweise nicht erhärten, würde ein Strafverfahren eingestellt und Zivilansprüche würden abgewiesen. Dabei sei zu beachten, dass es in der Regel der IP-Adressinhaber sei, der zumindest vermutungsweise gegen das Urheberrecht verstoßen habe.

### 6.3

6.3.1 Gemäß Art. 13 Abs. 2 BV hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Dieser Anspruch bildet Teil der verfassungsmäßigen Garantie der Privatsphäre und Kernbestandteil des Datenschutzgesetzes (Art. 1 DSG).

Das Vorgehen der Beschwerdegegnerin stellt eine Persönlichkeitsverletzung dar. Es verstößt gegen die Grundsätze der Zweckbindung und der Erkennbarkeit, mithin gegen Grundsätze, die für den Datenschutz von großer Wichtigkeit sind (Art. 4 Abs. 3 und 4 DSG). Im Folgenden ist zu prüfen, ob die Persönlichkeitsverletzung gerechtfertigt werden kann. Dabei kommt von vornherein nur ein überwiegendes privates oder öffentliches Interesse in Betracht; eine Einwilligung der Verletzten oder die Rechtfertigung durch Gesetz ist offensichtlich zu verneinen (Art. 13 Abs. 1 DSG). Wie bereits erwähnt, dürfen zudem Rechtfertigungsgründe beim Verstoß gegen die Grundsätze von Art. 4 DSG nur mit großer Zurückhaltung bejaht werden (E. 5.2.4 hiervor).

6.3.2 Das Datenschutzgesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1 DSG). Das Gesetz ergänzt und konkretisiert damit den bereits durch das Zivilgesetzbuch gewährleisteten Schutz (BGE 127 III 481 E. 3 a/bb S. 492 f. mit Hinweis). Art. 13 Abs. 1 DSG übernimmt in diesem Sinne den in Art. 28 Abs. 2 ZGB verankerten Grundsatz, wonach eine Persönlichkeitsverletzung widerrechtlich ist, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (BBl 1988 II 459 Ziff. 221.3). Trotz der identischen Formulierung der beiden Bestimmungen besteht in Bezug auf das Verfahren ein Unterschied. Während sich im Zivilprozess grundsätzlich zwei Parteien gegenüberstehen (der mutmaßlich in seiner Persönlichkeit Verletzte und der mutmaßliche Verletzer), geht es vorliegend darum zu prüfen, ob die Empfehlung des EDÖB, wonach die Beschwerdegegnerin ihre Datenbearbeitung unverzüglich einstellen solle, begründet ist (Art. 29 Abs. 3 DSG). Der EDÖB handelt dabei in einem Rahmen, welcher über das reine Zweiparteienverhältnis hinausgeht. Seine Empfehlung an die Adresse der Beschwerdegegnerin stützt sich auf Art. 29 Abs. 1 lit. a DSG. Danach klärt der Beauftragte den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer größeren Anzahl von Personen zu verletzen (Systemfehler). Seine Intervention bezweckt somit die Verteidigung einer Vielzahl von Personen und liegt damit letztlich im öffentlichen Interesse. Diese Bedeutung der Empfehlung des EDÖB ist bei der Interessenabwägung nach Art. 13 Abs. 1 DSG zu berücksichtigen. Im Übrigen zeitigt eine derartige (gegebenenfalls richterlich bestätigte) Empfehlung eine indirekte Wirkung für all jene Personen, die nach einer ähnlichen Methode vorgehen wie die Beschwerdeführerin, was zusätzlich Licht auf die Tragweite des vorliegenden Falls wirft (vgl. HUBER, Basler Kommentar, a.a.O., N. 37 zu Art. 29 DSG).

6.3.3 Wie die Vorinstanz dargelegt hat, kommen als überwiegende Bearbeitungsinteressen in erster Linie die Interessen der bearbeitenden Person, aber auch solche von Dritten in Frage.

Die Beschwerdegegnerin selbst verfolgt ein wirtschaftliches Interesse. Sie strebt eine Vergütung für ihre Tätigkeit an. Diese Tätigkeit besteht darin, mit Hilfe einer eigens dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken zu suchen und von deren Anbietern Daten zu speichern. Eine solche Methode führt allgemein - über den konkreten Fall hinaus - wegen fehlender gesetzlicher Reglementierung in diesem Bereich zu einer Unsicherheit in Bezug auf die

im Internet angewendeten Methoden wie auch in Bezug auf Art und Umfang der gesammelten Daten und deren Bearbeitung. Insbesondere sind die Speicherung und die mögliche Verwendung der Daten außerhalb eines ordentlichen Gerichtsverfahrens nicht klar bestimmt.

An dieser Einschätzung ändert auch das Interesse der Auftraggeber der Beschwerdegegnerin, welches in der Verwertung der Urheberrechte liegt, nichts (vgl. dazu MANFRED REHBINDER/ADRIANO VIGANÒ, URG, 3. Aufl. 2008, N. 3 f. zu Art. 1 URG). Mithin vermag auch das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse ist umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf.

Die Rüge des Beschwerdeführers erweist sich somit als begründet, was zur Gutheißung der Beschwerde führt. Unter diesen Umständen kann offengelassen werden, ob und inwiefern das Bundesgesetz über die verdeckte Ermittlung anwendbar ist, und insbesondere, ob die Strafverfolgungsbehörden die von der Beschwerdeführerin erlangten Daten verwenden dürften (vgl. dazu BGE 134 IV266 und Urteil 6B\_211/2009 vom 22. Juni 2009). Offengelassen werden kann zudem, ob auch das Verhältnismäßigkeitsprinzip für die Unterlassung der Datenbearbeitung spricht, zumal sich die Eruierung des Urheberrechtsverletzers in vielen Fällen als schwierig oder unmöglich erweisen würde, etwa wenn ein Drahtlosnetzwerk verwendet wird oder ein Computer mehreren Personen zur Verfügung steht.

6.4 Anzumerken ist, dass Gegenstand des vorliegenden Falls einzig die Datenbearbeitung durch die Beschwerdegegnerin ist und es nicht darum geht, dem Datenschutz generell den Vorrang gegenüber dem Schutz des Urheberrechts einzuräumen. Es ist Sache des Gesetzgebers und nicht des Richters, die allenfalls notwendigen Maßnahmen zu treffen, um einen den neuen Technologien entsprechenden Urheberrechtsschutz zu gewährleisten.

7.

Es ergibt sich, dass die Beschwerde gutzuheissen und das angefochtene Urteil aufzuheben ist. Die Beschwerdegegnerin wird angewiesen, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und es wird ihr untersagt, die bereits beschafften Daten den betroffenen Urheberrechtinhabern weiterzuleiten (Art. 107 Abs. 2 BGG).

Diesem Ausgang entsprechend sind die Gerichtskosten des bundesgerichtlichen Verfahrens der unterliegenden Beschwerdegegnerin aufzuerlegen (Art. 66 Abs. 1 BGG). Weder der Beschwerdeführer noch die unterliegende Beschwerdegegnerin haben Anspruch auf eine Parteientschädigung (Art. 68 Abs. 1 und 3 BGG). Die Angelegenheit wird an das Bundesverwaltungsgericht zu neuem Entscheid über die Kosten- und Entschädigungsfolgen zurückgewiesen. [...]

## ***Anmerkung***\*

### **I. Das Problem**

Das Geschäftsmodell der Logistep AG, ein Schweizer Unternehmen, bestand darin für die Erhebung von IP-Adressen von Internetnutzern, die an Peer-to-Peer-Netzwerken (sog. Internet-Tauschbörsen) teilnehmen und dabei durch das Urheberrecht geschützte Tonwerke an Dritte zur Verfügung stellen,

---

\* RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), [Anwalt.Thiele@eurolawyer.at](mailto:Anwalt.Thiele@eurolawyer.at); Näheres unter <http://www.eurolawyer.at>.

durch sog. Trackingsoftware zu ermöglichen („p2p-Monitorsoftware“).<sup>1</sup> Die Logistep AG wirkte (zumindest indirekt) im Auftrag der Rechteinhaber daran mit, die jeweiligen IP-Adressen der Tauschbörsennutzer zu ermitteln, aufzuzeichnen und erklärend darzustellen. Die jeweiligen IP-Adressen wurden an die Staatsanwaltschaft bekannt gegeben, die dadurch gegenüber den Internet-Provider in die Lage versetzt wurden, eine Offenlegung der Namen der jeweiligen Internet-Nutzer bzw. Anschlussinhaber zu verlangen. Nach Schweizer Recht waren die Internet-Provider verpflichtet, die relevanten Daten für eine Dauer von 6 Monaten zu speichern. Im Rahmen des Strafverfahrens konnte die Identität der Anschlussinhaber und damit letztlich der p2p-Nutzer auch für Rechteinhaber wegen der Einleitung zivilrechtlicher Klagen auf Schadensersatz enthüllt werden.

Der Schweizer Datenschutzbeauftragte (EDÖB) qualifizierte diese Tätigkeit der Logistep AG als nicht in Übereinstimmung mit dem Schweizer Datenschutzgesetz (DSG). Daher forderte der EDÖB Logistep AG durch eine spezifische Anordnung, das Geschäftsmodell nicht weiter fortsetzen. Dagegen erhob Logistep AG eine Beschwerde an das Bundesverwaltungsgericht. Mit Entscheidung vom 27. Mai 2009 vertrat das Bundesverwaltungsgericht die Auffassung, dass IP-Adressen personenbezogene Daten darstellen, jedoch wäre im konkreten Fall das Sammeln und die Übermittlung der Daten an Dritte im übergeordnete Interesse der Urheberrechtsberechtigten und würde keine Gefährdung der Persönlichkeitsrechte der betroffenen Nutzer darstellen.

Der erhob gegen die Entscheidung des Bundesverwaltungsgerichts Beschwerde ab das oberste Schweizer Bundesgericht mit der Begründung, die Logistep AG suchte zu Erwerbszwecken mittels der von ihr entwickelten Software in Peer-to-Peer-Netzwerken nach unrechtmäßig angebotenen urheberrechtlich geschützten Werken. Beim Herunterladen dieser Werke würden verschiedene Übermittlungsdaten aufgezeichnet und in einer Datenbank abgespeichert. Die so erhobenen Daten würden anschließend entgeltlich an die Urheberrechtsinhaber weitergegeben und von diesen zur Identifikation des Inhabers des Internetanschlusses verwendet. Zu diesem Zweck reichten die Urheberrechtsinhaber unter anderem Strafanzeige gegen Unbekannt ein und verschafften sich die Identitätsdaten im Rahmen des Akteneinsichtsrechts. Diese Daten würden sodann zur Geltendmachung von Schadenersatzforderungen gegen die mutmaßlichen Urheberrechtsverletzer verwendet.

Das Schweizer Höchstgericht hatte sich daher letztlich mit der Frage zu befassen, ob das „Geschäftsmodell“ der Logistep AG gegen geltendes Datenschutzrecht verstieß oder rechtmäßig wäre?

## **II. Die Entscheidung des Gerichts**

Das Bundesgericht erachtete die Beschwerde als zulässig bejahte zunächst die Anwendbarkeit des Datenschutzgesetzes, da die von der beklagten AG bearbeiteten IP-Adressen Personendaten iS de Art 3 lit a schwDSG darstellten. Die Höchststrichter entschieden, dass das fragliche Vorgehen der AG nicht durch ein überwiegendes Interesse nach Art 12, 13 schwDSG gerechtfertigt wäre, zumal ein solches Interesse nur zurückhaltend bejaht werden durfte. Die Datenschutzverletzung lag im konkreten Fall darin begründet, dass das Bearbeiten der Daten durch die Logistep AG im Regelfall ohne Wissen der betroffenen Personen und in einer für diese nicht erkennbaren Weise erfolgt war.

Zwar erschwerte die Möglichkeit der digitalen Vervielfältigung die umfassende wirtschaftliche Verwertung von Urheberrechten erheblich, jedoch bedeutete das gewerbliche Vorgehen des Softwareherstellers einen bedeutsamen Eingriff in die Privatsphäre jedes betroffenen Benutzers. In einer an den gesetzlichen Aufgaben des EDÖB ausgerichteten Interessenabwägung qualifizierte das Bundesgericht die Ziele der Logistep AG als wirtschaftlicher und privater Natur während jene des Datenschutzbeauftragten im überwiegenden öffentlichen Interesse lagen. Nach Auffassung des BG erschien deshalb das Interesse der Logistep AG und ihrer Auftraggeber nicht überwiegend, zumal ein datenschutzrechtliches Rechtfertigungsinteresse nur zurückhaltend anzunehmen wäre.

---

<sup>1</sup> Zu den technischen Anforderungen einer IP-Adressen-Ermittlungssoftware vgl. instruktiv *Morgenstern*, Zuverlässigkeit von IP-Adressen-Ermittlungssoftware, CR 2011, 203 ff mwN.

### III. Kritische Würdigung und Ausblick

In seinem durchaus bemerkenswerten „Entscheid“ hat das Schweizer Bundesgericht letztlich dem Softwaredienstleister untersagt, IP-Adressen von Nutzern der p2p-Netzwerke zu sammeln, um diese später dann durch Leistungsschutzberechtigte oder Urheber abmahnen zu lassen. IP-Adressen unterliegen nämlich als sog. Personendaten<sup>2</sup> dem Bundesgesetz über den Datenschutz (DSG).<sup>3</sup> Wenn private Unternehmen IP-Adressen in P2P-Netzwerken sammeln, sind dadurch die schutzwürdigen Geheimhaltungsinteressen der Nutzer verletzt. Dem Unternehmen Logistep als Beschwerdegegnerin kommt kein Rechtfertigungsgrund zu gute.

Bemerkenswert erscheinen aus rechtsvergleichender Perspektive die Ausführungen der Schweizer Höchststrichter zur **datenschutzrechtlichen Qualifikation der IP-Adressen**:

*"[3.2] Personendaten (bzw. "Daten" im Sinne des Datenschutzgesetzes) sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). [...] Eine Person ist dann **bestimmt**, wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt. **Bestimmbar** ist die Person, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor [...]"*

*[3.5] [...] Für den vorliegenden Fall ist die Bestimmbarkeit der betroffenen Personen grundsätzlich zu bejahen. Auf ihr beruht ganz eigentlich das Geschäftsmodell der Beschwerdegegnerin. Diese zeichnet nach eigenen Angaben dynamische IP-Adressen möglicher Urheberrechtsverletzer sowie weitere Daten auf, welche sie den Rechteinhabern weitergibt. Die Rechteinhaber ihrerseits können durch Strafanzeige auf die Einleitung eines Strafverfahrens hinwirken, um in dessen Rahmen Akteneinsicht zu nehmen und so den P2P-Teilnehmer ausfindig zu machen, welcher das urheberrechtlich geschützte Werk unrechtmäßig angeboten hat [...] Wohl ist davon auszugehen, dass in vielen Fällen der Urheberrechtsverletzer nicht ausfindig gemacht werden kann, so insbesondere dann, wenn verschiedene Personen zu einem Computer oder einem Netzwerk Zugang haben. Es ist jedoch ausreichend, dass die Bestimmbarkeit in Bezug auf einen Teil der von der Beschwerdegegnerin gespeicherten Informationen gegeben ist."*

Ebenso bemerkenswert für die österreichische Rechtslage erscheint auch der Hinweis der Schweizer Bundesrichter auf die **europäischen Datenschutzrechtsgrundlagen**.<sup>4</sup>

*"[3.6] Diese Auslegung des Datenschutzgesetzes scheint im Übrigen in Einklang mit der Rechtslage in der Europäischen Union zu stehen. [...] Das unabhängige EU-Beratungsgremium für Datenschutzfragen stuft IP-Adressen als Daten ein, die sich auf eine bestimmbare Person beziehen. Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken könnten ohne großen Aufwand Internetnutzer identifizieren [...] Dasselbe lasse sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen würden. In diesen Fällen bestehe kein Zweifel, dass man von personenbezogenen Daten im Sinne von Art. 2 lit. a der Richtlinie 95/46/EG reden könne [...]"*

**Die Frage, ob eine IP-Adresse ein personenbezogenes Datum darstellt, ist bis heute umstritten.** Das vorliegende Urteil bejaht dies mE grundsätzlich iS einer Bestimmbarkeit. In der Praxis gewinnt die zunächst als bloße Entscheidungsfrage anmutende Herausforderung rasch an Bedeutung, nicht nur z.B. bei der Speicherung, sondern auch wenn externe Dienste wie Statistik-Tools genutzt werden, in deren Rahmen dann die IP-Adressen an einen Dritten übermittelt werden. Hier besteht nicht nur eine große Gefahr für Webseiten-Betreiber, sondern auch für Agenturen, die

<sup>2</sup> Entspricht dem Begriff der „personenbezogenen Daten“ nach § 4 Z 1 DSG 2000.

<sup>3</sup> BG vom 19. Juni 1992, AS 1993 1945 (Stand 1. 1.2011), abrufbar unter <http://www.admin.ch> über die Suchfunktion Dokumentation (7.3.2011).

<sup>4</sup> Unter Zitierung der Art 29 Gruppe „Stellungnahme 4/2007 zum Begriff der „personenbezogenen Daten“ vom 20.6.2007, 19: Dynamische IP-Adressen, abrufbar unter [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf) (7.3.2011).

solche Tools (unwissentlich) in Seiten Ihrer Kunden einbauen, die dann eine (zumindest für die Agentur) peinliche Abmahnung erhalten.

Nach hA<sup>5</sup> stellen IP-Adressen, gleichgültig ob dynamischer oder statischer Art, dann bestimmbare personenbezogene Daten dar, wenn zu den gespeicherten Daten mit rechtlich zulässigen Mitteln ein Personenbezug herstellbar ist. Nur im Fall der Vergabe von IP-Adressen ohne rechtlich zulässigem Mittel der Zuordnung oder bei anonymisierten IP-Adressen kann kein Personenbezug hergestellt werden; im ersten Ausnahmefall liegen indirekt personenbezogene Daten vor; im zweiten Fall ist das Datenschutzrecht nicht anwendbar.<sup>6</sup>

**Ausblick:** Das Schweizer Bundesgericht weist abschließend darauf hin, dass eine Weitergabe von Daten durch die Logistep AG nicht mehr erlaubt sei: *„Die Beschwerdegegnerin wird angewiesen, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und es wird ihr untersagt, die bereits beschafften Daten den betroffenen Urheberrechtsinhabern weiterzuleiten.“* Demzufolge dürfte dieses Geschäftsmodell solange keine Daten mehr z.B. an Rechteinhaber oder deren Anwaltskanzleien weiterleiten, bis entsprechende Rechtsfertigungsgründe nach Art 13 schwDSG eintreten würden. Demgegenüber ist nach Ansicht deutscher Instanzgerichte<sup>7</sup> dadurch kein Beweisverwertungsverbot ausgesprochen, da *„keine Anhaltspunkte dafür [bestehen], dass ein Beweisverwertungsverbot vorliegen könnte, nur weil zwischenzeitlich ein Schweizerisches Bundesgericht die Tätigkeit des Dienstleisters Logistep nach dortigem Recht als datenschutzwidrig beurteilt hat“*.<sup>8</sup>

Für die rechtliche Bewertung, ob ein Beweisverwertungsverbot hinsichtlich der mittels p2p-Trackingssoftware ermittelter IP-Adressen vorliegt, ist nach österreichischem Recht festzuhalten, dass nach hM<sup>9</sup> ein sehr uneinheitliches Bild der Spruchpraxis zur Beantwortung dieser Frage je nach anzuwendendem Prozessrecht vorliegt. Als kleinster gemeinsamer Nenner ist vom Grundsatz auszugehen, dass die Berücksichtigung von Beweismitteln, die allenfalls auf gesetzwidrige Weise gewonnen wurden, nur dann unzulässig ist, wenn das Gesetz dies entweder anordnet oder wenn die Verwertung des betreffenden Beweisergebnisses dem Zweck des durch seine Gewinnung verletzten Verbotes widerspräche.<sup>10</sup>

#### **IV. Zusammenfassung**

Nach Auffassung des schweizerischen Höchstgerichts verstößt das Geschäftsmodell einer privaten AG, das darin besteht, im Auftrag von Urheberrechtsinhabern in Peer-to-Peer-Netzwerken nach dort illegal angebotenen urheberrechtlich geschützten Werken zu suchen, gegen das Schweizer Datenschutzgesetz. Die Begründung überzeugt und ist das Ergebnis bei der durchaus vergleichbaren Rechtslage in Österreich durchaus vertretbar.

---

<sup>5</sup> Statt vieler eingehend *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 4/53 ff mwN.

<sup>6</sup> Grundlegend bereits *Jahnel*, Datenschutz im Internet. Rechtsgrundlagen, Cookies und Web-Logs, *ecolex* 2001, 84, 85.

<sup>7</sup> Vgl. OLG Hamburg 3.11.2010, 5 W 126/10, CR 2011, 126 mwN.

<sup>8</sup> OLG Hamburg 3.11.2010, 5 W 126/10, CR 2011, 126, 127.

<sup>9</sup> Statt vieler eingehend *Jahnel*, Datenschutzrecht Rz 4/53 ff mwN.

<sup>10</sup> Vgl. *Jahnel*, Datenschutzrecht Rz 4/56.