Protection des données et réseaux *peer-to-peer* : le Tribunal fédéral suisse considère que les activités d'une entreprise qui enregistre et transmet aux titulaires de droit d'auteur les adresses IP de raccordements utilisés pour offrir au téléchargement des œuvres protégées contrevient à la législation sur la protection des données
(arrêt du 8 septembre 2010 de la Première Cour de droit public, réf. 1C_285/2009, destiné à la publication officielle)

A. Résumé de l'arrêt

Le texte original allemand est joint. Pour les lecteurs de langue française, on le résumera ci-dessous.

1. Les faits

Logistep recherchait, au moyen d'un logiciel qu'elle a développé, l'offre d'œuvres protégées par le droit d'auteur dans les réseaux *peer-to-peer*, et enregistrait dans sa base de données :

- le nom d'utilisateur du réseau P2P
- l'adresse IP du raccordement Internet utilisé
- le GUID (n° d'identification du logiciel utilisé par celui qui offre au téléchargement l'œuvre)
- le protocole P2P utilisé
- le nom et la signature électronique (hashcode) de l'œuvre
- la date, l'heure et la durée de la liaison entre le logiciel de Logistep et le logiciel de celui qui offre l'œuvre au téléchargement.

Ces données étaient transmises aux titulaires des droits, qui déposaient plainte pénale contre inconnu et qui, après avoir obtenu son identité en accédant au dossier pénal, s'adressaient au prévenu pour lui réclamer une indemnité à titre de dommages-intérêts.

Le Préposé fédéral à la protection des données (autorité chargée de veiller au respect de la législation fédérale sur la protection des données) a considéré que les procédés de Logistep étaient susceptibles de porter atteinte à la personnalité d'un grand nombre de personnes et a émis une recommandation[1] à l'encontre de Logistep de cesser ses opérations aussi longtemps qu'il n'existait pas une base légale suffisante pour une exploitation civile des données ainsi collectées. Logistep ayant fait savoir qu'elle ne suivrait pas cette recommandation, le Préposé a saisi le Tribunal administratif fédéral (TAF). Ce dernier n'a pas suivi l'opinion du Préposé, et a rejeté sa demande. En substance, le TAF avait estimé que les adresses IP collectées constituaient bien des données personnelles, que les principes de la finalité et du caractère reconnaissable du traitement avaient été violés, mais que ces atteintes à la protection des données étaient justifiées par des intérêts prépondérants, tenant dans la nécessité de pouvoir identifier les violations du droit d'auteur commises au moyen de réseaux P2P.

Contre cet arrêt du TAF, le Tribunal fédéral (TF) a admis le recours du Préposé.

[1] Le Préposé n'a pas de pouvoir de décision en l'occurrence : il ne peut qu'émettre une recommandation ; si elle n'est pas acceptée, il lui appartient de saisir le Tribunal administratif fédéral, qui rend une décision selon sa propre appréciation.

2. Résumé des considérants

a) une adresse IP est-elle une donnée personnelle ?

Aux termes du texte légal, les données personnelles sont « *toutes les informations qui se rapportent à une personne identifiée ou identifiable* » (art. 3 litt. a de la loi fédérale sur la protection des données, ci-après LPD). Savoir si une personne est identifiable dépend du travail qui doit être effectué pour l'identification, et de l'intérêt de l'information pour celui qui traite les données ou pour un tiers. Peu importe que le détenteur de l'information doive ou non recourir aux services d'un tiers pour identifier la personne concernée. Ce qui est décisif, c'est de savoir si, dans le cas particulier, le travail d'identification serait tel que l'on devrait considérer, selon l'expérience générale, que le détenteur de l'information y renoncerait selon toute vraisemblance. C'est donc un examen au cas par cas qui permet de dire si une information se rapporte à une personne identifiable et s'il s'agit dès lors d'une donnée personnelle au sens de la loi.

Par conséquent, il n'est pas possible de dire de façon générale et abstraite si une adresse IP statique (adresse attribuée à un ordinateur) ou une adresse IP dynamique (adresse attribuée par le fournisseur de services par lequel passe l'internaute, et qui change lors de chaque connexion) constitue une donnée personnelle.

Dans le cas particulier, le TF a admis (comme le TAF d'ailleurs) que les données se rapportaient à une personne identifiable : le but des services fournis par Logistep était précisément de permettre à ses clients d'avoir connaissance des atteintes portées au droit d'auteur, et de leur communiquer les données permettant l'ouverture d'une enquête pénale, et ses clients pouvaient ensuite obtenir l'identité de la personne concernée en accédant au dossier pénal. Même si l'identité de l'auteur de la violation demeure souvent inconnue, en particulier lorsque plusieurs personnes partagent le même accès à Internet, cela ne change rien au fait que l'identification des personnes concernées est en partie possible grâce aux informations collectées par Logistep, ce qui est suffisant.

b) violation des principes de la finalité et du caractère reconnaissable du traitement des données

Selon les al. 3 et 4 de l'art. 4 LPD, « *les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* » (principe de la finalité du traitement), et « *la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée* » (principe du caractère reconnaissable du traitement). En l'espèce, rien n'étant indiqué ni reconnaissable pour les personnes concernées, il fallait admettre que ces principes étaient violés. Il existait donc en soi une atteinte à la personnalité des personnes concernées (art. 12 LPD).

c) possibilité de faire valoir un motif justificatif

Toutefois, l'art. 13 réserve la possibilité, pour celui qui traite des données en violation des principes posés par la loi, d'invoquer un motif justificatif : « *une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi* » (art. 13 al. 1 ; son alinéa 2 donne une liste d'exemples de motifs justificatifs).

Une révision de la LPD, en 2006, pouvait donner à penser que les violations des principes de l'art. 4 LPD seraient systématiquement illicites (l'art. 12 al. 2 litt. a ne réserve plus l'existence de motifs justificatifs). Toutefois, et contre l'avis du Préposé, le TF a admis que cette modification ne devait pas être comprise ainsi, et que le législateur n'avait pas eu l'intention de changer le système existant, qui permet d'invoquer un motif justificatif notamment en cas de violation de l'art. 4 LPD. Le texte révisé devait simplement faire ressortir l'idée qu'un motif justificatif ne devait pas être admis à la légère – ce qui ressortait déjà des travaux préparatoires de la loi, lors desquels le Conseil fédéral avait déclaré que les atteintes aux principes fondamentaux de l'art. 4 LPD ne pouvaient être justifiées en l'absence de motifs impérieux. Le TF en a déduit que de tels motifs justificatifs ne devaient être admis qu'avec une grande retenue.

d) motif justificatif tiré d'un intérêt privé ou public prépondérant

La LPD concrétise la protection de la personnalité contre les atteintes portées à la sphère privée par le traitement abusif de données personnelles. En matière de protection générale de la personnalité, l'art. 28 du Code civil (CC) permet aussi une atteinte à la personnalité, lorsqu'elle est « *justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi* ». Selon le TF toutefois, malgré l'identité de formulation du texte légal aux art. 28 CC et 13 LPD, il existerait une différence entre la situation visée à l'art. 28 CC, dans laquelle deux personnes sont opposés, et celle visée à l'art. 13 LPD lorsqu'il s'agit de savoir si une recommandation du Préposé est fondée ou non : le Préposé agit dans l'intérêt public, pour protéger un grand nombre de personnes contre une atteinte, ce dont il y aurait lieu de tenir compte dans la pesée des intérêts prescrite par l'art. 13 LPD.

Concernant la pesée des intérêts prévue à l'art. 13 LPD, les seuls considérants du TF sont les suivants (TdA) :

« *Logistep poursuit quant à elle des intérêts économiques. Elle déploie une activité contre rémunération. Cette activité consiste à rechercher des œuvres protégées dans les réseaux P2P, au moyen du logiciel qu'elle a développé et à enregistrer les données de ceux qui offrent de telles œuvres. Une telle méthode conduit généralement – indépendamment du cas d'espèce – à une incertitude en relation avec les méthodes utilisées sur Internet, le type et l'étendue des données collectées, ainsi que leur traitement, ceci à cause d'une absence de réglementation légale en la matière. En particulier, l'enregistrement et les utilisations possibles des données en dehors d'une procédure judiciaires ne sont pas clarifiés.*

L'intérêt des mandants de l'intimée, qui tient dans l'exploitation des droits d'auteur, ne modifie en rien cette appréciation (cf. à ce propos Manfred Rehbinder/Adriano Viganò, URG, 3ème éd. 2008, N. 3 s. ad art. 1). L'intérêt à pouvoir lutter de manière efficace à l'encontre des violations du droit d'auteur ne peut non plus l'emporter sur l'étendue de l'atteinte à la personnalité et des incertitudes engendrées par les procédés litigieux en relation avec le traitement des données sur Internet. Un intérêt privé prépondérant ou public doit être dénié d'autant plus qu'un tel intérêt ne peut être admis qu'avec retenue ».

Le TF a cependant ajouté que ce cas ne concernait que les activités de Logistep et qu'il ne s'agissait pas de consacrer de manière générale une prééminence de la protection des données sur le droit d'auteur, et qu'il appartenait au législateur et non au juge de prendre les mesures

éventuellement nécessaires pour garantir une protection du droit d'auteur qui corresponde aux nouvelles technologies.

B. Remarques critiques

La notion de donnée personnelle est si large (« *toutes les informations qui se rapportent à une personne identifiée ou identifiable* ») qu'il n'est guère possible de contester la « qualité » de donnée personnelle à une adresse IP.

Cette qualification entraîne l'application de la LPD, et en particulier de son art. 4, qui prévoit que « *les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* » (principe de la finalité du traitement), et « *la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée* » (principe du caractère reconnaissable du traitement). Puisque les activités de Logistep se déroulaient à l'insu des personnes concernées, ces principes étaient violés.

Toutefois, la LPD réserve la possibilité, comme en droit général de la personnalité, d'invoquer un motif justificatif : une atteinte à la personnalité n'est illicite que si elle n'est pas justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. Et pour déterminer si un intérêt privé ou public est prépondérant, il y a lieu de procéder à une pesée des intérêts en présence.

L'instance précédente, le Tribunal administratif fédéral, avait admis que les atteintes à la protection des données étaient en l'espèce justifiées par des intérêts prépondérants, tenant dans la nécessité de pouvoir identifier les violations du droit d'auteur commises au moyen de réseaux P2P : sans disposer des données collectées par Logistep, les auteurs et leurs ayants droit ne peuvent identifier ceux qui portent atteinte à leurs droits (intérêt privé) ; en outre, il existe aussi un intérêt public à ce que les violations du droit d'auteur puissent être poursuivies.

Le raisonnement suivi par le TF ne convainc guère. Tout d'abord, la thèse selon laquelle les motifs justificatifs (un intérêt privé ou public prépondérant, le consentement de la victime, ou la loi) ne devraient être admis qu'avec retenue est contraire au système légal. Selon l'art. 13 LPD, une atteinte n'est pas illicite si elle est justifiée par un intérêt prépondérant privé ou public (les autres motifs justificatifs — n'entrent pas en ligne de compte ici). Dès lors, en présence d'un intérêt privé ou public prépondérant, l'atteinte est justifiée, et n'est donc pas illicite. La seule question est celle de savoir si l'intérêt mis en balance est prépondérant ou non. S'il est prépondérant, l'atteinte à la personnalité n'est pas illicite, sans qu'il y ait lieu de se demander en plus si des motifs impérieux commandent que la violation de la LPD soit justifiée.

Sur ce point, le TF croit voir une différence entre le droit général de la personnalité et la LPD : l'art. 28 CC (qui prévoit aussi qu'une atteinte à la personnalité n'est pas illicite si elle est justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi) s'inscrit dans un pur rapport de droit privé entre l'auteur de l'atteinte à la personnalité et la victime de cette atteinte, tandis que le Préposé fédéral émet des recommandations dans l'intérêt public. Toutefois, dans un cas comme dans l'autre, c'est une atteinte à la personnalité qui est en cause, et la loi prévoit exactement le même mécanisme qui en permet la justification (un intérêt prépondérant). De plus, en présence d'une violation de la

LPD par une personne privée (comme Logistep en l'espèce), c'est l'art. 13 LPD qui s'applique pour déterminer l'existence d'un éventuel motif justificatif, que ce soit dans le cadre d'un procès civil ou d'une procédure faisant suite à une action du Préposé. Or l'art. 13 LPD ne peut être appliqué différemment suivant qu'il est invoqué dans l'une ou l'autre de ces hypothèses. En particulier, si un internaute "piégé" avait ouvert action contre Logistep, il aurait fallu procéder à la pesée des intérêts prévue par cette disposition, et le juge civil aurait dû déterminer si l'atteinte à la personnalité était justifiée par un intérêt prépondérant (à faire respecter le droit d'auteur). La même atteinte, lorsqu'elle est visée par une recommandation du Préposé, doit être jugée en application des mêmes règles.

Quant aux deux paragraphes qui devraient traiter de la pesée des intérêts en présence, ils expriment plutôt le désarroi des juges face à un texte légal vague. On y lit que les méthodes telles que celles utilisées par Logistep conduiraient « *à une incertitude en relation avec les méthodes utilisées sur Internet, le type et l'étendue des données collectées, ainsi que leur traitement, ceci à cause d'une absence de réglementation légale en la matière* ». En particulier, « *l'enregistrement et les utilisations possibles des données en dehors d'une procédure judiciaires ne sont pas clarifiés* ».

Ainsi, plutôt que de mettre en balance l'intérêt à la protection de cette donnée personnelle qu'est l'adresse IP avec la protection du droit d'auteur, le TF a opposé les « *incertitudes engendrées par les procédés litigieux* » et « *l'étendue de l'atteinte à la personnalité* » (sans dire en quoi l'atteinte serait "étendue") d'une part, et « *l'intérêt à pouvoir lutter de manière efficace à l'encontre des violations du droit d'auteur* », d'autre part. Autrement dit, et ce point est encore confirmé par la suite de l'arrêt, à la place de peser les intérêts en présence, conformément à l'art. 13 LPD, le TF a estimé que le texte légal manquait de clarté : selon notre Haute Cour, il appartiendrait « *au législateur et non au juge de prendre les mesures éventuellement nécessaires pour garantir une protection du droit d'auteur qui corresponde aux nouvelles technologies* ».

Pourtant, en droit de la personnalité, le caractère vague de l'art. 28 CC, qui oblige le juge à peser les intérêts en présence, n'a jamais été mis en cause par la jurisprudence. Au contraire, il est admis en ce domaine qu'il appartient au juge de concrétiser la portée des droits de la personnalité, et que le système de la balance des intérêts permet de tenir compte de toutes les circonstances du cas d'espèce. Pourquoi devrait-il en aller différemment sur la base de l'art. 13 LPD, qui prescrit dans les mêmes termes le recours à une balance des intérêts en présence ?

Sans doute l'explication de cet arrêt doit-elle être recherchée dans le fait qu'il a été rendu par une Cour de droit *public*, habituée à exiger de l'Etat une base légale claire. Mais ici, il ne s'agissait pas d'une problématique de droit public, mais de droit privé : fallait-il faire triompher la protection de la sphère privée – dans la mesure où elle est mise en cause par une adresse IP – sur la nécessaire recherche de preuves pour identifier des atteintes au droit d'auteur dans des réseaux *peer-to-peer* ? Telle était la question, et il faut reconnaître qu'elle est à peine abordée dans l'arrêt.

Le TF se défend d'avoir voulu consacrer une prééminence de la protection des données sur le droit d'auteur. Pourtant, en renvoyant la question au législateur, il empêche désormais les ayants droit de rechercher les atteintes à leurs droits dans les réseaux *peer-to-peer*. En outre, et contrairement à ce que pense le TF, le législateur n'est pas mieux armé pour définir si, dans un cas tel que celui-ci, la protection de la donnée personnelle qu'est l'adresse IP doit être

préférée à la recherche des preuves de multiples violations du droit d'auteur. Il s'agit d'un cas typique de conflit entre droits subjectifs, en soi d'égale valeur, et la jurisprudence a toujours résolu ce genre de conflits par une pesée des intérêts en présence. Pourquoi devrait-il en aller différemment ici ?

C. Conclusions

L'arrêt ne manque pas de surprendre : les juges en appellent au législateur alors qu'ils auraient dû mettre en balance les intérêts en présence dans le cas particulier. Le législateur a pourtant voulu que les juges statuent au cas par cas, puisqu'il a prévu qu'une atteinte à la personnalité résultant d'une violation de la LPD pouvait être justifiée par un intérêt privé ou public prépondérant.

Le plus inquiétant réside toutefois dans la tendance, exprimée en particulier par le Préposé fédéral à la protection des données. S'il se défend de vouloir favoriser les atteintes aux droits d'auteur dans les réseaux *peer-to-peer*, sa décision à l'origine de cette affaire montre une tendance à la sacralisation des données personnelles.

Il est vrai aussi que le détenteur de l'adresse IP n'est pas nécessairement celui qui a commis l'infraction au droit d'auteur. Ce point avait considérablement ému le Préposé, qui estimait que les pratiques de Logistep portaient atteinte « *aux droits de la personnalité d'un nombre indéfini de détenteurs d'accès Internet qui sont de bonne foi* ». Ainsi, des personnes de bonne foi ont pu se voir confrontées à des demandes en dommages-intérêts injustifiées. On admettra volontiers qu'il n'est pas agréable, pour le détenteur d'une adresse IP, de se voir réclamer des dommages-intérêts alors que les téléchargements illicites auraient été effectués par un proche ou employé. Mais cette problématique n'a rien à voir avec la protection des données personnelles, et cette circonstance ne devrait donc pas avoir d'influence sur la question qui était soumise au Tribunal fédéral.

6.12.2010/IC

Tribunal fédéral

1C_285/2009

Urteil vom 8. September 2010
I. öffentlich-rechtliche Abteilung

Besetzung
Bundesrichter Féraud, Präsident,
Bundesrichter Reeb, Raselli, Fonjallaz, Eusebio,
Gerichtsschreiber Dold.

Verfahrensbeteiligte
Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter EDÖB,
Beschwerdeführer,

gegen

Logistep AG,
Beschwerdegegnerin,
vertreten durch Rechtsanwältin Ursula Sury.

Gegenstand
Umsetzung einer Empfehlung des EDÖB,

Beschwerde gegen den Entscheid vom 27. Mai 2009
des Bundesverwaltungsgerichts, Abteilung I.

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;
den Namen und elektronischen Fingerabdruck (Hashcode) des urheberrechtlich geschützten Werks;
das Datum, die Uhrzeit und den 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 substanziiert 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.; 133 II 249 E. 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 aufrecht erhalten 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 denjenigen, 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 mitzuberücksichtigen 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 zuordnen 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 Urheberrechteinhaber 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 solange 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 hiervor). 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-Dienstanbietern 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» 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 DSG, 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 DSG qualifiziert hat.

4.
Die Beschwerdegegnerin bestreitet einen Verstoss gegen die Grundsätze der Zweckbindung und der Erkennbarkeit (Art. 4 Abs. 3 und 4 DSG). 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 legte 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 zutreffe, 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 DSG 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 DSG) 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 DSG; Rosenthal, a.a.O., N. 19 zu Art. 12 DSG). 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 DSG 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 DSG 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 DSG zu betonen, schlägt das Bundesamt für Justiz in seiner Auslegungshilfe zur Änderung von Art. 12 Abs. 2 lit. a DSG 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 DSG und den Rechtfertigungsgründen von Art. 13 DSG 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 DSG). Indessen sind nicht alle Grundsätze der Datenbearbeitung einer Auslegung zugänglich, welche die Rechtfertigungsgründe von Art. 13 DSG 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 DSG).
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 DSG. 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 DSG 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 milderes, 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 gegenüber stehen (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 offen gelassen 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 IV 266 und Urteil 6B_211/2009 vom 22. Juni 2009). Offen gelassen 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 Urheberrechtsinhabern weiterzuleiten (Art. 107 Abs. 2 BGG).