PROTECTION DES DONNÉES. Atteinte inadmissible à la personnalité par le traitement de données sur des utilisateurs de réseaux *peer-to-peer*.

Art. 82 ss LTF; art. 3 let. a, 4 al. 3 et 4, 12 al. 2 let. a, 13 LPD.

Une recommandation dans le secteur privé selon l'art. 29 LPD, émise par le Préposé fédéral à la protection des données et à la transparence, se rapporte à une cause de droit public au sens des art. 82 ss LTF (c. 1.1).

Conditions pour qualifier les adresses IP de données personnelles au sens de l'art. 3 let. a LPD (c. 3).

Si la collecte de données les concernant n'est pas reconnaissable par les utilisateurs de réseaux *peer-to-peer*, elle viole les principes de la finalité et de la reconnaissabilité selon l'art. 4 al. 3 et 4 LPD (c. 4).

Malgré sa lettre, l'art. 12 al. 2 let. a LPD permet les motifs justificatifs (comme dans les let. b et c); ceux-ci ne peuvent toutefois être admis qu'avec une grande retenue (c. 5).

L'atteinte à la personnalité que l'intimée a commise avec son traitement de données ne peut pas être justifiée par un intérêt privé ou public prépondérant (c. 6).

Préposé fédéral à la protection des données et à la transparence c. Logistep AG (recours en matière civile), 8 septembre 2010; 1C_285/2009; ATF 136 II 508.

Le 9 janvier 2008, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a émis une recommandation à l'adresse de Logistep AG. Il y retenait que Logistep AG recherchait, au moyen d'un logiciel développé par elle, des œuvres protégées par le droit d'auteur offertes sur divers réseaux *peer-to-peer* (aussi dits réseaux P2P). En cas de téléchargement desdites œuvres, les informations suivantes relatives à la transmission étaient enregistrées et stockées dans une base de données:

le nom ou pseudonyme de l'utilisateur du réseau P2P;

l'adresse IP (*Internetworking Protocol Address*) de la connexion Internet utilisée;

le GUID (un numéro d'identification du logiciel utilisé par la personne offrant au téléchargement l'œuvre protégée par le droit d'auteur);

le protocole du réseau P2P utilisé;

le nom et l'empreinte digitale électronique (*Hashcode*) de l'œuvre protégée par le droit d'auteur;

la date, l'heure et la durée de la connexion entre le logiciel de Logistep AG et le logiciel de la personne offrant au téléchargement l'œuvre concernée protégée par le droit d'auteur.

Les données ainsi obtenues étaient ensuite transmises aux titulaires du droit d'auteur et utilisées par ceux-ci pour identifier le détenteur de la connexion Internet. A ces fins et entre autres mesures, les titulaires du droit d'auteur déposaient plainte pénale contre inconnu et se procuraient les données relatives à l'identité de l'intéressé en faisant usage de leur droit de consulter le dossier. Ces données étaient ensuite utilisées pour mettre en œuvre des prétentions en dommages-intérêts. Le PFPDT est parvenu à la conclusion que les méthodes de traitement de Logistep AG étaient susceptibles de porter atteinte à la personnalité d'un nombre important de personnes (art. 29 al. 1er let. a de la loi fédérale du 19 juin 1992 sur la protection des données [LPD; RS 235.1]). Pour cette raison, dans sa lettre du 9 janvier 2008, en application de l'art. 29 al. 3 LPD, il a recommandé à Logistep AG de cesser immédiatement le traitement concerné de données, aussi longtemps que n'existerait pas une base légale suffisante pour l'utilisation des données collectées par elle à l'appui de prétentions civiles.

Après que Logistep AG a rejeté sa recommandation par courrier du 14 février 2008, le PFPDT a, dans une écriture du 13 mai 2008, porté l'affaire devant le TAF pour décision. Il a conclu principalement à ce qu'il soit ordonné à Logistep AG de cesser immédiatement le traitement de données pratiqué (y compris la remise des données aux titulaires du droit d'auteur), aussi longtemps que n'existerait pas une base légale suffisante pour une surveillance générale des réseaux *peer to peer*. (...) Par jugement du 27 mai 2009, le TAF a rejeté la requête et a annulé la recommandation du PFPDT du 9 janvier 2008. (...)

Le 26 juin 2009, le PFPDT a saisi le TF d'un recours en matière de droit public, dans lequel il a conclu à ce qu'il soit ordonné à Logistep AG de cesser immédiatement le traitement de données litigieux et à ce que toute remise des données collectées aux titulaires du droit d'auteur lui soit interdite. (...)

Le TF admet le recours et annule le jugement du TAF du 27 mai 2009. Il ordonne à Logistep AG de cesser tout traitement de données dans le domaine du droit d'auteur et lui interdit de remettre les données déjà collectées aux titulaires concernés du droit d'auteur.

(rés.)

Considérant en droit:

1.

1.1 L'objet du recours est une décision du TAF concernant une recommandation du PFPDT (art. 86 al. 1er let. a et art. 90 LTF). Conformément à l'art. 29 al. 4 2e phrase LPD, le PFPDT a qualité pour recourir contre cette décision.

La décision attaquée concerne une recommandation du PFPDT dans le secteur privé (art. 29 LPD). La question se pose de savoir si, au lieu du recours en matière de droit public au sens des art. 82 ss LTF, il n'y avait pas lieu de former un recours en matière civile au sens des art. 72 ss LTF. Pour les motifs suivants, il faut répondre à cette question par la négative. La procédure a été engagée par le PFPDT, organe de l'administration fédérale, et elle est dirigée contre un sujet de droit privé. Les parties ne sont pas entre elles dans un rapport d'égalité. Le PFPDT n'a certes pas le pouvoir de rendre des décisions, mais les personnes privées sont tenues, sous peine d'amende, de prêter leur collaboration dans l'établissement des faits par le préposé (art. 34 al. 2 let. b LPD). En outre, l'art. 29 al. 1er let. b LPD, sur lequel le PFPDT a

fondé sa recommandation en l'espèce, concerne précisément des cas de mise en danger de droits de la personnalité ayant un caractère excédant le cadre de la protection individuelle et qui relèvent ainsi de l'intérêt public (cf. Message du 23 mars 1988 concernant la loi fédérale sur la protection des données, FF 1988 II 485, ch. 221.5; *René Huber*, Basler Kommentar, Datenschutzgesetz, 2e éd. 2006, n° 7 ad art. 29 LPD; *David Rosenthal*, Handkommentar zum Datenschutzgesetz, 2008, n° 11 ad art. 29 LPD). La décision du TAF concerne par conséquent une cause de droit public, de sorte que la voie du recours en matière de droit public constitue la voie de droit correcte.

Les autres conditions relatives à la décision attaquée n'appellent pas de commentaires. Le recours du PFPDT est par principe recevable.

1.2(...)

1.3(...)

2.

2.1 Le PFPDT reproche au TAF d'avoir mal interprété l'art. 12 al. 2 LPD. De l'avis du recourant, dans sa teneur actuelle, cette disposition n'autoriserait plus de motifs justificatifs. En lieu et place, il y aurait lieu de déterminer si un principe de la protection des données a été violé. Cela requerrait un examen sous l'angle du principe de la proportionnalité prenant en considération les motifs justificatifs existants. Le TAF aurait procédé de manière incorrecte à la pesée des intérêts requise, dès lors qu'il n'existerait aucun intérêt prépondérant privé ou public. La personnalité des personnes concernées aurait donc été atteinte de manière illicite. En méconnaissant cela, les premiers juges auraient aussi contrevenu au principe de légalité ancré à l'art. 4 al. 1er LPD.

2.2 L'intimée considère au contraire que les adresses IP traitées par elle ne constitueraient pas des données personnelles au sens de l'art. 3 let. a LPD. Les dispositions de la loi sur la protection des données ne seraient par conséquent tout simplement pas susceptibles de s'appliquer. Pour le reste, une éventuelle atteinte à des droits de la personnalité ne serait pas illicite, au vu de l'existence d'intérêts prépondérants privés et publics. Contrairement à l'avis du recourant, les motifs justificatifs de l'art. 13 LPD devraient être pris en considération dans tous les cas.

2.3 Le TAF est parti du principe que la loi sur la protection des données est applicable, mais a rejeté la requête du PFPDT en raison de l'existence de motifs justificatifs. Dès lors qu'il y aurait lieu de s'abstenir d'annuler le jugement attaqué si le résultant pouvait en être maintenu sur la base d'une autre motivation (arrêt 2P.172/2005, du 25 octobre 2005), il y a lieu d'examiner en premier lieu l'applicabilité de principe de la loi sur la protection des données en l'espèce, dès lors que l'intimée la remet en question.

3.

3.1 En relation avec l'applicabilité de la loi sur la protection des données, l'avis a été exprimé en doctrine que les adresses IP tombent exclusivement dans le champ d'application de la loi du 30 avril 1997 sur les télécommunications (LTC; RS 784.10), qui contiendrait une réglementation exhaustive. Le motif en serait que les adresses IP constitueraient des paramètres de communication numériques et par conséquent des ressources d'adressage au sens de la législation sur les télécommunications, qui tomberaient ainsi sous le coup du secret des télécommunications prévu par l'art. 43 LTC (*Daniel Kettiger*, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, Jusletter du 9 août 2010, n. 20).

Il est exact que des adresses IP constituent des ressources d'adressage au sens de la législation sur les télécommunications. Le secret des télécommunications ne vaut toutefois que pour les personnes "chargées" d'assurer un service de télécommunication (art. 43 LTC; cf. ATF 126 I 50 c. 6a p. 65 et réf., JdT 2001 I 764). Tel n'est pas le cas de l'intimée. La loi sur les télécommunications ne s'oppose pas en l'espèce à l'application de la loi sur la protection des données.

3.2 Sont des données personnelles (ou "données" au sens de la loi sur la protection des données) toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 let. a LPD). Les informations concernées peuvent être aussi bien des constatations de fait que des jugements de valeur. La forme sous laquelle les informations se manifestent (par exemple signes, mots, images, sons ou combinaison de ces éléments) est sans pertinence, de même que la manière dont le support de données est obtenu. Est déterminant le fait que les indications puissent se rapporter à une ou plusieurs personnes (*Urs Belser*, Basler Kommentar, Datenschutzgesetz, 2e éd. 2006, n° 5 ad art. 3 LPD).

Une personne est identifiée lorsqu'il résulte de l'information elle-même qu'il s'agit précisément de cette personne. Une personne est identifiable lorsque l'on peut conclure à son identité sur la base d'informations supplémentaires. Pour qu'une personne soit identifiable, toute possibilité théorique d'identification ne suffit toutefois pas. Si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses1, aucun intéressé ne les mettra en œuvre, on ne peut guère parler de possibilité d'identification (FF 1998 II 452, ch. 221.1). La solution dépend des circonstances concrètes du cas d'espèce et il y a lieu en particulier de prendre en considération les possibilités offertes par la technique, par exemple les outils de recherche disponibles sur Internet. La mesure des efforts à consentir pour pouvoir rattacher les informations considérées à une personne déterminée n'est cependant pas seule déterminante; il faut aussi examiner l'intérêt de la personne qui traite les données (ou d'un tiers) à l'identification (*Belser*, n° 6 ad art. 3 LPD; *Rosenthal*, n° 24 ad art. 3 LPD).

3.3 Les adresses IP traitées par l'intimée sont des paramètres de communication numériques qui permettent d'identifier un domaine Internet composé notamment d'ordinateurs ou de serveurs de réseaux, ainsi que les ordinateurs des usagers qui participent aux relations de communication sur ce réseau (définition de l'annexe à l'ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications [ORAT; RS 784.104]). En d'autres termes, tout ordinateur se connectant à Internet est identifié par l'adresse IP. Chaque fois que des données sont appelées sur Internet, par exemple par la consultation d'un site web, l'ordinateur de l'utilisateur transmet sa requête en relation avec l'adresse IP qui lui est attribuée (*Per Meyerdierks*, Sind IP-Adressen personenbezogene Daten?, MultiMedia und Recht 1/2009 pp. 8 s.). C'est de cette manière que l'adresse IP rend l'échange de données possible sur Internet.

Si un ordinateur se voit attribuer une adresse IP de manière fixe, on parle d'adresse IP statique. Si un utilisateur a recours à un fournisseur d'accès Internet (provider) pour se connecter au réseau, il obtient en revanche dans la plupart des cas une adresse IP dynamique, ce qui signifie que son ordinateur se voit attribuer une nouvelle adresse IP lors de chaque

connexion, parmi celles qui sont disponibles dans le pool attribué à son fournisseur d'accès. L'adressage dynamique a été développé en raison du caractère limité des adresses IP. Parce que, dans ce système, une adresse IP n'est attribuée à un utilisateur que pour un temps limité et qu'elle est attribuée à un autre utilisateur après la fin de la connexion du premier, l'identification d'un ordinateur par une adresse IP déterminée n'est possible que pour la durée d'une connexion individuelle. Pour ce motif, l'identification du titulaire d'une adresse IP dynamique est plus difficile que celle du titulaire d'une adresse IP statique. Alors que les adresses IP statiques sont répertoriées dans des annuaires partiellement accessibles de manière libre, le titulaire d'une adresse IP dynamique ne peut en règle générale être identifié qu'avec l'assistance du provider qui a attribué l'adresse en question (*Rolf H. Weber/Orsolya Fercsik Schnyder*, "Was für 'ne Sorte von Geschöpf ist euer Krokodil?" - Zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic! 2009 pp. 579 s.).

3.4 C'est du point de vue du détenteur concerné de l'information qu'il y a lieu de déterminer si celle-ci peut être associée à un individu sur la base d'indications complémentaires et se rapporte par conséquent à une personne déterminable (art. 3 let. a LPD) (*Rosenthal*, n° 20 ad art. 3 LPD; *Weber/Fercsik Schnyder*, p. 583).

En cas de transmission d'informations, il suffit que le destinataire soit en mesure d'identifier la personne concernée. *Rosenthal* donne à cet égard l'exemple d'une dépêche relatant l'accident d'un politicien local, sans désigner nommément celui-ci. A teneur de l'argumentation convaincante de cet auteur, dans la mesure où une partie du lectorat (le cas échéant sur la base de recherches complémentaires) peut identifier la personne concernée, la publication constitue une communication de données personnelles (*Rosenthal*, n° 30 ad art. 3 LPD; cf. aussi l'art. 3 let. e LPD). Cela signifie dans le cas d'espèce qu'il n'est pas nécessaire que les personnes ayant violé des droits d'auteur soient déjà identifiables par l'intimée. Il suffit au contraire qu'elles le soient par les titulaires de droits d'auteur concernés après la remise des données concernées. Si tel est le cas (point traité ci-dessous), la loi sur la protection des données s'applique déjà à l'intimée. Toute autre décision signifierait que la loi sur la protection des données ne s'applique qu'aux divers destinataires des données, non à la personne qui se procure les informations concernées et les leur remet. Cela serait en contradiction avec le but de la loi.

3.5 L'intimée fait valoir que ses mandants ne pourraient apprendre l'identité des titulaires des différentes adresses IP que sur la base des actes d'enquête des autorités de poursuite pénale. Elle méconnaît à cet égard que la nécessité de l'activité d'un tiers est pertinence dans la mesure où, dans l'ensemble, les moyens requis du mandant pour la détermination de l'identité des personnes concernées n'est pas si important que, selon le cours ordinaire des choses, aucun intéressé ne les mettrait en œuvre (cf. c. 3.1 ci-dessus). Ces moyens doivent être appréciés à la lumière des circonstances du cas d'espèce. Il n'est pas possible de constater de manière abstraite si des adresses IP (en particulier dynamiques) constituent ou non des données personnelles (cf. en droit allemand *Ulrich Dammann*, Bundesdatenschutzgesetz, 6e éd. 2006, n° 20 ad § 3 BDSG; critique *Meyerdierks*, pp. 10 ss; sur la qualification des adresses IP en droit suisse de la protection des données, *Rosenthal*, n° 27 ad art. 3 LPD; *Weber/Fercsik Schnyder*, p. 588).

Dans le cas d'espèce, il faut en principe considérer que les personnes concernées sont identifiables. C'est en fait exactement ce sur quoi repose le modèle d'affaires de l'intimée. Selon ses propres indications, celle-ci enregistre les adresses IP dynamiques relatives à des personnes susceptibles d'avoir violé des droits d'auteur, ainsi que d'autres données qu'elle transmet aux titulaires desdits droits. Ceux-ci, de leur côté, peuvent en portant plainte donner lieu à l'introduction d'une procédure pénale, dont ils ont le droit de consulter le dossier, ce qui leur permet d'identifier le participant d'un réseau P2P qui a mis à disposition l'œuvre protégée de manière illicite (cf. art. 67 ss de la loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins [LDA; RS 231.1], art. 5 et 14 al. 4 de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication [LSCPT; RS 780.1] en relation avec l'art. 43 LTC; ATF 126 I 50, JdT 2001 I 764; *Stéphane Bondallaz*, La protection des personnes et de leurs données dans les télécommunications, 2007, n. 1086; *Peter Schaar*, Datenschutz im Internet, 2002, n. 175; cf. également *Rosenthal*, n° 27 ad art. 3 LPD). Il y a certes lieu d'admettre que, dans de nombreux cas, la personne ayant violé des droits d'auteur ne peut être identifiée, en particulier lorsque plusieurs personnes ont accès à un ordinateur ou à un réseau. Il suffit toutefois qu'une partie des informations stockées par l'intimée permette une identification.

3.6 Cette interprétation de la loi sur la protection des données semble du reste correspondre à la situation juridique qui prévaut dans l'Union Européenne. Le concept de données à caractère personnel y a été analysé de manière détaillée par le groupe de protection des personnes à l'égard du traitement des données à caractère personnel dans son avis 4/2007 du 20 juin 2007. Cette commission consultative indépendante en matière de protection des données, instituée par l'Union Européenne, considère les adresses IP comme des données concernant une personne identifiable. Selon le groupe de travail, les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP donnée à l'utilisateur Internet et il en va de même pour les fournisseurs de services Internet qui conservent un fichier-registre sur le serveur http, de sorte que, dans ces cas, on peut parler, sans l'ombre d'un doute, de données à caractère personnel au sens de l'art. 2, point a), de l'art. 2 let. a de la directive 95/46/CE (avis 4/2007, p. 18, disponible sur le site internet <http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/2007/wp136_fr.pdf> [dernière consultation de contrôle, par le traducteur, le 12 novembre 2011]).

3.7 Enfin, l'intimée fait valoir que, s'il fallait qualifier les informations litigieuses de données personnelles, il lui serait impossible de se conformer aux obligations que la loi sur la protection des données lui imposerait en relation avec le droit d'accès. L'art. 8 LPD exige certes que le maître du fichier communique, à la personne qui fait valoir ce droit, toutes les données la concernant qui sont contenues dans le fichier. Cependant, à teneur du texte même de la loi, le droit d'accès est limité aux données *disponibles* (cf. également FF 1988 II 460 s., ch. 221.2)2. Il n'est pas possible de demander au maître du fichier des indications dont il ne dispose pas. En outre, il est permis de demander à la personne qui exerce son droit d'accès de fournir des indications complémentaires si cela est nécessaire ou utile à la recherche des données qui la concernent (JAAC 65 [2001], n° 49 c. 3b).

3.8 En résumé, c'est à juste titre que le TAF a qualifié de données personnelles au sens de l'art. 3 let. a LPD les adresses IP traitées par l'intimée.

4. L'intimée conteste avoir contrevenu aux principes de la finalité et de la reconnaissabilité (art. 4 al. 3 et 4 LPD). Le traitement des données aurait lieu dans un but reconnaissable à l'avance pour tous les utilisateurs de réseaux P2P, soit la poursuite légitime, au pénal comme au civil, de violations de droits d'auteur.

Le TAF a constaté, dans le jugement attaqué, que l'intimée collecte des données relatives à des utilisateurs de réseaux P2P, qu'elle remet ensuite à ses mandants. Ainsi, l'obtention des données interviendrait en règle générale à l'insu des personnes concernées et ne serait pas reconnaissable pour celles-ci. La façon de procéder de l'intimée exclurait en outre qu'au moment de la collecte, le titulaire de l'adresse IP soit informé du but dans lequel les données le concernant sont enregistrées. Même s'il était exact que, dans des cas isolés, l'utilisateur serait rendu attentif au fait que "des sociétés anti-P2P enregistrent des données", on ne saurait parler d'information sur le but de la collecte de données par la personne qui se charge du traitement de celles-ci. Aussi bien le principe de la finalité que celui du caractère reconnaissable de la collecte seraient ainsi régulièrement méconnus.

L'intimée n'aborde pas les considérations convaincantes du TAF à ce sujet et se contente de les contester en bloc. Il n'y a donc pas lieu d'entrer en matière sur cet argument (cf. art. 42 al. 2 LTF).

5.

5.1 Les art. 12 et 13 LPD fixent les conditions auxquelles le traitement de données par des personnes privées est licite.

(...)

Alors que les let. b et c de l'art. 12 al. 2 LPD se réfèrent expressément aux motifs justificatifs de l'art. 13 LPD, une telle réserve fait défaut dans la teneur actuelle de l'art. 12 al. 2 let. a LPD. Le recourant en déduit qu'une violation des principes définis à l'art. 4 LPD (auxquels appartiennent les principes de la finalité et du caractère reconnaissable de la collecte) ne peut pas être justifiée.

5.2 5.2.1 La question se pose de savoir si la suppression, dans le cadre de la révision législative du 24 mars 2006, de la réserve qui figurait précédemment à l'art. 12 al. 2 let. a LPD exprime un silence qualifié. La justification d'un traitement de données personnelles contrevenant aux principes des art. 4, 5 al. 1er et 7 al. 1er LPD serait dans ce cas exclue de manière générale. La doctrine est divisée à ce sujet. *Stephan C. Brunner*, *Christian Déchaler* et *David Rosenthal* s'expriment en faveur d'un maintien de la possibilité de faire valoir des motifs justificatifs (*Stephan C. Brunner*, Das revidierte Datenschutzgesetz und seine Auswirkungen im Gesundheits- und Versicherungswesen, in: Datenschutz im Gesundheits- und Versicherungswesen, 2008, pp. 142 ss; *Christian Drechsler*, Die Revision des Datenschutzrechts, PJA 2007 p. 1474; *Rosenthal*, n° 16 ad art. 12 LPD). *René Huber* exprime un avis différent, sans toutefois le motiver (*René Huber*, Die Teilrevision des Eidg. Datenschutzgesetzes - ungenügende Pinselrenovation, recht 24/2006 p. 214).

5.2.2 Les travaux préparatoires n'apportent pas à ce sujet une clarté suffisante. La suppression de la réserve remonte à une proposition de la Commission du Conseil national et n'était pas prévue dans le projet du Conseil fédéral. Le Conseil national a approuvé cette modification sans discussion (BO 2005 N 1450). Au Conseil des Etats, le rapporteur l'a expliquée de manière plus détaillée, mais toutefois aussi contradictoire. Ses propos, selon lesquels il ne conviendrait pas que l'on puisse, en présence d'un motif justificatif, révéler des données collectées de manière illicite, laisse certes entendre que les motifs justificatifs sont exclus de manière générale dans le cadre de l'art. 12 al. 2 let. a LPD. Le rapporteur a toutefois aussi expliqué que la modification décidée par le Conseil national ne constituerait de manière générale qu'une clarification du texte qui était en vigueur à ce moment-là et qui avait apparemment donné lieu à des problèmes en pratique. En supprimant ces circonstances justificatives, il ne se serait pas agi de créer une situation entièrement nouvelle, mais seulement de codifier la jurisprudence de l'époque (BO 2005 E 1159; cf. à ce sujet JAAC 69 [2005], n° 106 c. 5.2 et 5.8).

5.2.3 De l'avis de l'Office fédéral de la justice, aucun changement de système n'était envisagé. La nouvelle formulation de l'art. 12 al. 2 let. a LPD n'avait pour objectif que de renforcer l'attention portée aux principes de l'art. 4 LPD, sans changer quoi que ce soit à la situation juridique prévalant précédemment. La reformulation du texte visait à mettre en évidence que les dérogations ne doivent pas être hâtivement justifiées (*Office fédéral de la justice*, Modification de l'art. 12 al. 2 let. a LPD: Notice interprétative, 2006, <http://www.edoeb.admin.ch/themen/00794/00819/01086/index.html?lang=fr> [dernière consultation de contrôle, par le traducteur, le 12 novembre 2011]). Cette interprétation s'inscrit dans la ligne de l'opinion exprimée dans le message du Conseil fédéral relatif à la version originale de l'art. 12 al. 2 let. a LPD, selon laquelle les principes généraux définis à l'art. 4 LPD "constituent la colonne vertébrale de la législation sur la protection des données", raison pour laquelle "ils ne peuvent être transgressées sans raison majeure" (FF 1988 II 465, ch. 221.3).

5.2.4 S'il s'agissait d'exclure de manière générale tout traitement de données collectées illicitement (art. 4 al. 1er LPD), il serait par exemple interdit à un employeur découvrant des données personnelles stockées illicitement par un travailleur de remettre celles-ci aux autorités. Une violation des principes applicables au traitement de données serait en outre illicite même en cas de consentement de la victime (art. 13 al. 1er LPD; *Rosenthal*, n° 19 ad art. 12 LPD). Cela ne peut toutefois pas être le sens de la loi. Une interprétation systématique stricte, au sens de laquelle un motif justificatif ne peut être invoqué que dans le cadre des let. b et c, mais non de la let. a, de l'art. 12 al. 1er LPD, s'avère ainsi erronée, ce d'autant que, si la version actuelle de la let. a ne réserve en effet plus les motifs justificatifs, elle ne les exclut pas non plus expressément. Cette disposition doit donc être interprétée en ce sens que la justification d'un traitement de données contrevenant aux principes des art. 4, 5 al. 1er et 7 al. 1er LPD n'est certes pas exclue de manière générale, mais ne peut être admise dans un cas d'espèce qu'avec grande retenue.

5.2.5 Eu égard à l'intention du législateur de souligner l'importance des principes de l'art. 4 LPD, l'Office fédéral de la justice propose, dans sa notice interprétative relative à la modification de l'art. 12 al. 1er LPD, de considérer qu'à l'avenir les motifs justificatifs soient pris en compte essentiellement au niveau de l'interprétation des principes généraux (*Office fédéral de la justice*, notice précitée, ch. 3.1). Une telle manière de procéder semble par exemple praticable dans les cas où la distinction entre les principes de l'art. 4 LPD et les motifs justificatifs de l'art. 13 LPD s'avère quoi qu'il en soit difficile, par exemple en relation avec le principe de la proportionnalité (cf. *Corrado Rampini*, Basler Kommentar, Daten, 2e éd. 2006, n° 4 ad art. 12 LPD). Cependant, tous les principes applicables au traitement de données ne sont pas susceptibles d'une interprétation qui permettrait de tenir compte des motifs justificatifs de l'art. 13 LPD de manière suffisante. Il ne faut pas non plus oublier qu'il est sans importance, du point de vue du résultat, de déterminer si l'existence de motifs justificatifs doit être examinée pour elle-même dans un second temps ou déjà au moment de l'interprétation des principes applicables au traitement de données (voir sur l'ensemble de cette question *Rosenthal*, nos 22 s. ad art. 12 LPD).

5.2.6 L'autorité précédente a dans un premier temps constaté une violation des principes de la finalité et de la reconnaissabilité. Elle a ensuite laissé indécise la question de savoir si le principe de la proportionnalité avait été méconnu. En vérifiant l'existence d'un intérêt prépondérant privé ou public qui justifierait une atteinte aux droits de la personnalité, les premiers juges ont toutefois examiné si le traitement de données litigieux était conforme au principe de la proportionnalité. Il s'ensuit qu'il n'y a rien à redire à cette façon de procéder.

6.

6.1 Le recourant critique la pesée des intérêts opérée par les premiers juges dans l'analyse de l'existence de motifs justificatifs au sens de l'art. 13 LPD. S'il fallait suivre ceux-ci, tout type de traitement de données, même secret et contraire au but annoncé, serait justifié par la fin poursuivie. Une personne concernée ne pourrait même pas se défendre contre un tel traitement, dès lors qu'elle n'en serait pas ou pas suffisamment informée. Les citoyens suisses seraient ainsi privés de leur droit d'accès au sens de l'art. 8 LPD dans une large mesure. L'autorité précédente occulterait enfin le fait que le titulaire de l'adresse IP n'est pas nécessairement celui qui viole des droits d'auteur, dès lors qu'un raccordement Internet peut en partie être utilisé par plusieurs personnes. Des titulaires de bonne foi de raccordements Internet pourraient ainsi être confrontés à des prétentions civiles injustifiées. La manière de procéder de l'intimée s'apparenterait à une investigation secrète, dont la mise en œuvre est pourtant soumise à des conditions strictes (art. 4 de la loi fédérale du 20 juin 2003 sur l'investigation secrète [LFIS; RS 312]3). Enfin, il y aurait lieu de tenir compte du fait que les procédures pénales ne seraient engagées que pour contourner le secret des télécommunications et que l'intimée, avec les titulaires des droits d'auteur, serait principalement intéressée à faire valoir des prétentions civiles.

6.2 L'autorité précédente a considéré que, sans la collecte de données techniques, en particulier des adresses IP, il ne serait pas possible aux titulaires de droits d'auteurs lésés, d'identifier les auteurs de ces atteintes et de faire valoir à leur encontre des prétentions en dommages-intérêts et en cessation. Il n'existerait pas de moyen plus léger mais également propre à atteindre le but visé. En revanche, l'atteinte aux droits de la personnalité des personnes concernées ne serait pas particulièrement grave. Si les preuves ne devaient pas être corroborées, il serait mis un terme à la procédure pénale et les prétentions civiles seraient rejetées. Il y aurait lieu à cet égard de noter qu'en règle générale le titulaire de l'adresse IP pourrait, au moins présomptivement, être considéré comme l'auteur de l'atteinte au droit d'auteur.

6.3 6.3.1 A teneur de l'art. 13 al. 2 Cst., toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent. Ce droit est partie intégrante de la garantie constitutionnelle de la sphère privée et constitue un élément central de la loi sur la protection des données (art. 1er LPD).

Le procédé de l'intimée constitue une violation de droits de la personnalité. Il contrevient aux principes de la finalité et de la reconnaissabilité, soit de principes revêtant une grande importance dans le cadre de la protection des données (art. 4 al. 3 et 4 LPD). Il y a ainsi lieu d'examiner si cette atteinte à la personnalité peut être justifiée. A cet égard, il apparaît d'emblée que seul un intérêt prépondérant privé ou public peut entrer en ligne de compte; le consentement de la victime ainsi qu'un motif justificatif légal peuvent à l'évidence être écartés (art. 13 al. 1er LPD). Comme précédemment indiqué, des motifs justificatifs ne doivent être admis qu'avec grande retenue en présence de violations des principes de l'art. 4 LPD (c. 5.2.4 ci-dessus).

6.3.2 La loi sur la protection des données vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (art. 1er LPD). La loi complète et concrétise ainsi la protection déjà offerte par le Code civil (ATF 127 III 481 c. 3 a/bb p. 492 et réf., JdT 2002 I 426). L'art. 13 al. 1er LPD reprend en ce sens le principe ancré à l'art. 28 al. 2 CC, aux termes duquel une atteinte à la personnalité est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi (FF 1988 II 466 ch. 221.3). Malgré la formulation identique des deux dispositions, celles-ci se distinguent sous un angle procédural. Alors qu'un procès civil oppose en général deux parties (la personne qui se déclare victime d'une atteinte à sa personnalité et la personne désignée comme l'auteur de ladite atteinte), il s'agit en l'espèce principalement de déterminer si la recommandation du PFPDT, au sens de laquelle l'intimée devrait cesser immédiatement le traitement de données litigieux, est fondée (art. 29 al. 3 LPD). Le PFPDT agit à cet égard dans un cadre qui excède celui d'une pure contestation entre deux parties. Sa recommandation à l'adresse de l'intimée se fonde sur l'art. 29 al. 1er let. a LPD. Dans ce contexte, le préposé établit les faits lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système). Son intervention tend ainsi à défendre un grand nombre de personnes et poursuit donc en dernière analyse un intérêt public. Il faut tenir compte de cette portée de la recommandation du PFPDT dans la pesée des intérêts opérée aux fins de l'art. 13 al. 1er LPD. En outre, une telle recommandation (le cas échéant confirmée par la voie judiciaire) emporte un effet indirect pour toutes les personnes qui procèdent de la même manière que l'intimée, ce qui donne un éclairage supplémentaire sur la portée du présent cas (cf. *Huber*, n° 37 ad art. 29 LPD).

6.3.3 Comme l'autorité précédente l'a retenu, l'intérêt prépondérant est en première ligne celui de la personne qui traite les données, mais peut aussi être celui d'un tiers.

L'intimée poursuit un but économique propre. Elle cherche à se faire rémunérer pour son activité. Cette activité consiste à rechercher des œuvres protégées par le droit d'auteur sur des réseaux P2P, au moyen d'un logiciel que l'intimée a développé à cette fin, ainsi qu'à stocker des données sur les personnes qui en proposent ainsi. En raison du défaut de réglementation légale à ce sujet, un tel procédé conduit de façon générale - c'est-à-dire au-delà des circonstances concrètes du cas d'espèce - à une incertitude sur les méthodes en usage sur Internet, ainsi que sur la nature et l'étendue des données collectées et sur leur traitement. En particulier, le stockage et l'utilisation possible des données en dehors d'un procès civil ordinaire n'est pas clairement déterminé. L'intérêt des mandants de l'intimée à l'exploitation de leurs droits d'auteur (cf. à ce sujet *Manfred Rehbinder/Adriano Viganò*, URG, 3e éd. 2008, nos 3 s. ad art. 1er LDA) ne change rien à cette appréciation. Par conséquent, l'intérêt à une lutte efficace contre des violations du droit d'auteur ne parvient pas à contrebalancer l'étendue de l'atteinte à la personnalité et les incertitudes relatives au traitement de données sur Internet liées au procédé litigieux. Il se justifie d'autant plus de nier l'existence d'un intérêt prépondérant privé ou public qu'un tel intérêt ne peut être admis que restrictivement.

Le grief du recourant s'avère ainsi bien fondé, ce qui conduit à l'admission du recours. Dans ces circonstances, il n'est pas nécessaire de déterminer si et dans quelle mesure la loi fédérale sur l'investigation secrète4 est applicable, ni, en particulier, si les autorités de poursuite pénale peuvent utiliser les données obtenues par l'intimée (voir à ce sujet ATF 134 IV 266,

JdT 2008 IV 35 et l'arrêt 6B_211/2009, du 22 juin 2009). Il n'est pas nécessaire non plus de déterminer si la cessation du traitement de données litigieux peut être justifié également par le principe de la proportionnalité, d'autant plus que, dans de nombreux cas, l'identification des auteurs de violations du droit d'auteur se révélerait quoi qu'il en soit difficile, voire impossible, par exemple dans le cas où il serait fait usage d'un réseau sans fil ou dans celui où un ordinateur serait à disposition de plusieurs personnes.

6.4 Il faut noter que seul le traitement de données opéré par l'intimée est l'objet de la présente affaire, et qu'il ne s'agit pas de manière générale de donner à la protection des données la priorité sur celle du droit d'auteur. Il appartient le cas échéant au législateur, non au juge, de prendre les mesures nécessaires pour garantir une protection du droit d'auteur adaptée aux nouvelles technologies.

I^re^ Cour de droit public.

Trad. Ed. Ph.