

Valérie Dussex
Collaboratrice Notariat
Yann Jodry
Collaborateur Barreau

Recommandé
Tribunal fédéral
À l'att. du Président de la
Cour de droit public
Avenue du Tribunal fédéral 29
1005 Lausanne

Sion, le 29 juin 2009/sf

**Cause A-3144/2008 ; Logistep AG ; décision du Tribunal administratif fédéral du 27 mai 2009 ;
Association Razorback**

Monsieur le Président de la Cour de droit public du Tribunal fédéral, Mesdames, Messieurs les
Juges fédéraux, Mesdames, Messieurs les Greffiers,

Agissant au nom et pour le compte de l'Association Razorback, association de droit suisse (au sens
des articles 60 et suivants) dont le siège est à Sion, agissant en qualité de dénonciateur dans le cadre
du dossier cité en exergue, j'ai mandat de déposer le présent :

RECOURS EN MATIÈRE DE DROIT PUBLIC

relativement à la décision du Tribunal administratif fédéral du 27 mai 2009, rendue suite à la
recommandation établie le 9 janvier 2007 par le Préposé fédéral à la protection des données et à la
transparence à l'attention de la société Logistep AG, valablement représentée par Me Ursula Sury,
Alpenquai 4, 6005 Lucerne,

ce, à raison des faits, motifs et moyens de preuve suivants :

I. PROCÉDURE : COMPÉTENCE, POUVOIR D'EXAMEN, GRIEFS INVOCABLES, DÉLAI

Le recours est formé en temps utile contre un arrêt du TAF rendu dans une cause de droit public. Il est recevable au sens des articles 82 let. a, 86 al. 1 let. a et 100 al. 1 LTF. La décision n'est en effet parvenue à la connaissance du recourant qu'après que les médias en eurent fait état, soit au plus tôt le 29 mai 2009. Le délai de recours ne pourrait au demeurant être inférieur à celui dont dispose le Préposé à la protection des données, lequel échoit ce jour, le 29 juin 2009.

La qualité pour recourir se détermine à l'aune de l'article 89 LTF. L'Association Razorback a agi comme dénonciateur en saisissant le 20 avril 2007 les services du Préposé fédéral à la protection des données. Il entre manifestement dans son but de défendre les réseaux P2P principalement concernés par la décision du TAF. De surcroît, Monsieur XXX, membre fondateur de l'Association n'a pas obtenu de réponse de Logistep à ses légitimes interrogations. La qualité pour recourir est donc donnée en l'espèce.

Le Tribunal fédéral statue en principe sur la base des faits établis par l'autorité précédente (art. 105 al. 1 LTF), sous réserve des cas prévus à l'art. 105 al. 2 LTF. Cette disposition lui donne la faculté de rectifier ou compléter d'office l'état de fait de l'arrêt attaqué dans la mesure où des lacunes ou erreurs dans l'établissement de celui-ci lui apparaîtraient d'emblée comme manifestes.

Quant au recourant, il ne peut critiquer la constatation de faits importants pour le jugement de la cause que si ceux-ci ont été constatés en violation du droit au sens de l'art. 95 LTF ou de manière manifestement inexacte (art. 97 al. 1 LTF), c'est-à-dire arbitraire, ce qu'il lui appartient de démontrer par une argumentation répondant aux exigences de l'art. 42 al. 2 LTF, respectivement de l'art. 106 al. 2 LTF.

En outre, l'existence de faits constatés de manière inexacte ou en violation du droit n'est pas une condition suffisante pour conduire à l'annulation ou la modification de la décision attaquée. Il faut encore qu'elle soit susceptible d'avoir une influence déterminante sur l'issue de la procédure (art. 97 al. 1 in fine LTF).



II. FAITS PERTINENTS DE LA CAUSE ET EXPOSÉ DU DÉROULEMENT DE LA PROCÉDURE DEVANT LES INSTANCES INFÉRIEURES :

1. Par courrier du 20 avril 2007, l'Association Razorback a soumis la problématique d'une collecte des adresses IP par la société Logistep au Préposé fédéral à la protection des données et à la transparence (ci-après le Préposé).
2. L'Association Razorback est une association de droit suisse fondée en 2004 dont le but est le suivant :
 - encourager le partage d'œuvres libres et légales en favorisant leur distribution sur le réseau de P2P eDonkey ;
 - administrer un serveur eDonkey du nom de Razorback2.
3. En bref, dite association croit et défend un réseau P2P libre et légal.
4. Monsieur XXX est l'un des membres fondateurs de dite association.
5. Par correspondance du 4 avril 2007, Monsieur XXX s'est adressé (en substance en ces termes à la société Logistep :

Demande de renseignements

Madame, Monsieur,

Selon les informations contenues sur votre site web et d'autres trouvées sur Internet, votre société collecterait des données relatives aux échanges sur les réseaux de p2p. Bien que la lutte contre les échanges illicites soit une cause noble, votre activité pourrait porter atteinte à ma vie privée.

Dès lors, selon l'« Ordonnance relative à la loi fédérale sur la protection des données » du 14 juin 1993 article 1er, je vous prie de m'informer si vous détenez des informations concernant :

- *mon IP fixe n° 213.XXX.XXX.XXX détenue depuis 2002*
- *à mon nom personnel susmentionné*

Je vous serai gré de me transmettre toutes les informations concernant d'éventuelles données collectées. Selon ce même article, vous disposez d'un délai de 30 jours pour me renseigner.

Je tiens également à savoir si vous avez transmis des informations me concernant à l'étranger et si c'est le cas, auprès de quelle société ou personne.

Dans l'attente d'une réponse, je vous transmets mes salutations.

6. Aucune réponse ne lui parvient de la société Logistep, de sorte qu'un deuxième courrier fut adressé, courrier dont la teneur est *in parte qua* la suivante :



« ...Selon les informations contenues sur votre site web et d'autres trouvées sur Internet, votre société collecterait des données relatives aux échanges sur les réseaux de p2p. Bien que la lutte contre les échanges illicites soit compréhensible, votre activité pourrait porter atteinte à ma vie privée.

Me fondant sur l'art. 8 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD), je vous prie de bien vouloir me donner, dans un délai de 30 jours, des renseignements par écrit sur les points suivants:

- 1. toutes les données me concernant qui sont contenues dans votre (vos) fichier(s)*
- 2. le but et, le cas échéant, la base juridique du traitement des données*
- 3. les catégories de données personnelles traitées*
- 4. les catégories de participants au(x) fichier(s)*
- 5. les catégories de destinataires des données.*

Les recherches doivent porter sur mon nom susmentionné et sur mon adresse IP fixe (selon contrat annexé) n° 213.221.132.121 détenue depuis 2002.

Par ailleurs, je vous signale qu'il s'agit de mon 2^{ème} courrier et qu'au 1^{er}, vous n'avez pas daigné me répondre...

7. Le 7 août 2007 à 17h41, le courriel suivant parvient à Monsieur XXX :

Monsieur,

Faisant référence à votre lettre datée du 6 juillet 2007, veuillez trouver ci-joint une copie de notre réponse d'aujourd'hui.

Salutations distingués.

Logistep AG

M. R. Sundkvist

Sennweidstrasse 45

CH - 6312 Steinhausen

Switzerland

Tel +41 (0)41 790 88 44

www.logistepag.com »



8. Y était jointe une lettre dont voici le contenu (partiel) :

« Steinhausen, 07.08.2007

Monsieur,

Nous vous remercions pour votre lettre datée du 6 juillet 2007.

Bien que nous comprenons vos soucis en ce qui concerne la confidentialité de vos données personnelles dans la société actuelle, veuillez noter que nous travaillons de manière entièrement ciblée et recherchons des preuves électroniques des actes de téléchargement illégal de logiciel propriétaire bien précisés et définies sur les réseaux de partage de fichiers ("peertopeer"). Ainsi, nous exécutons ses tâches exclusivement selon les instructions/mandats que nous ont été confiés par les propriétaires des droits d'auteur.

Les protocoles qui en résultent ne portent en rein sur des données personnelles, mais contient essentiellement les adresses IP, avec quelques autres données non nominative.

Concernant ce qui signifie une adresse IP, nous sommes d'ailleurs du même avis que les juges et les récentes jugements (deux à Paris auprès de la cour d'appel et une à Montauban), où est constatés que l'adresse IP n'est pas une donnée indirectement nominative http://www.legalis.net/jurisprudence-decision.php3?id_article=1954 Si, et dans la mesure où les propriétaires des droits d'auteur ensuite décident de procéder juridiquement contre les abonnés de accès Internet concernés; (supposés d'avoir commis des contrefaçons des droits d'auteur), c'est aux cabinets des avocats à procéder; enter autre avec la tâche de demander et obtenir les noms et adresses des personnes concernés auprès des fournisseurs d'accès à Internet.

Notre seuls intérêts et devoir est à fournir les propriétaires des droits d'auteur avec des protocoles catégorique afin de leur permettre à prendre des décisions de comment traité les contrefaçons.

Dès que nous avons délivré nos protocoles aux cabinets d'avocats, notre travaille est accompli.

Nous pouvons ajouter que nous ne traitons pas de cas de téléchargements illégaux sur territoire suisse.

Nous espérons avoir répondu à vos questions et nous restons à votre disposition pour des renseignements supplémentaires.

Salutations distinguées.

Logistep AG

M. R. Sundkvist

Marketing & PR ».

9. Il n'était ainsi pas répondu à la question de savoir si l'adresse IP de Monsieur XXX figurait ou non dans les bases de données détenues par Logistep.
10. En substance dans la dénonciation au Préposé subséquente, il était fait grief à dite société de collecter des adresses IP et de porter ainsi à la vie privée des internautes.



11. Après avoir instruit le dossier, le Préposé établit le 9 janvier 2007 une recommandation à l'intention de la société Logistep.
12. Une correspondance informant l'Association Razorback a été adressée au soussigné par courrier du 21 janvier 2008, reçu le 24 janvier 2008.
13. Dans sa recommandation datée du 8 janvier 2008, le Préposé fédéral à la protection des données a considéré que le détenteur d'informations IP ne pouvait les transmettre à des tiers sans l'accord préalable des personnes concernées¹.
14. Pour le Préposé, le traitement des données doit être effectué conformément au principe de la bonne foi.
15. Les données de connexion entre les différents logiciels d'échange de fichiers étant échangées sans que les utilisateurs n'en prennent connaissance, et le détenteur d'accès Internet n'étant pas impliqué dans le processus d'échange, la société Logistep, selon le Préposé, ne respectait pas le principe de la transparence.
16. À ses yeux, la collection de telles informations constitue une atteinte à la personnalité au sens de l'article 12 de la loi fédérale sur la protection des données (abrévée ci-après LPD) et ne repose sur aucun motif justificatif au sens de l'article 13 LPD.
17. Concrètement, le traitement de données suivi d'une plainte pénale déposée en vue de prétentions civiles serait contraire au principe de la bonne foi et abusif au sens de l'article 2 du Code civil.
18. Pour le Préposé fédéral, de telles méthodes ne sont justifiées d'aucune manière.
19. Sous l'angle des motifs justificatifs de l'article 13 LPD, le Préposé a considéré qu'il y avait conflit entre deux intérêts opposés, soit l'intérêt des détenteurs des droits d'auteur à poursuivre en justice les personnes violant leurs droits et en exiger des dommages et intérêts, et les droits de la personnalité, notamment le droit à l'auto-détermination informationnelle des personnes concernées, en particulier du détenteur de l'accès Internet de bonne foi.

¹ Décision du Préposé fédéral à la protection des données et à la transparence du 8 janvier 2008, consultable notamment sur le site www.edoeb.admin.ch.



20. En résumé, pour le Préposé, les données collectées par la société Logistep, par le biais du droit d'accès au dossier, sont utilisées de façon abusive pour engager des actions civiles contre les détenteurs de l'accès Internet de bonne foi.
21. À ses yeux, cette démarche constitue en fin de compte un contournement du secret des télécommunications dans le domaine civil.
22. L'engagement d'une procédure pénale ne peut dans ce contexte pas être considéré comme un motif justificatif suffisant, tant qu'il n'est pas garanti que l'identité des détenteurs d'accès Internet qui sont de bonne foi soit protégée dans le cadre d'une procédure pénale.
23. Contre cette recommandation, Logistep a recouru auprès du Tribunal administratif fédéral.
24. Selon décision du 27 mai 2009², la position du Préposé a été infirmée.
25. Il est ainsi admis qu'une atteinte peut être considérée comme admissible si elle est destinée à récolter des preuves³.
26. Plus particulièrement, le TAF a considéré qu'il n'existait pas de loi interdisant la surveillance privée en droit suisse⁴.
27. Dans le cas particulier, l'attitude de Logistep, bien que discutable, serait compatible avec le principe de la bonne foi, dans la mesure où le but poursuivi est de traquer des données piratées.
28. Dès lors, il ne serait pas nécessaire de requérir le consentement des personnes concernées⁵.
29. En d'autres termes, l'intérêt public à collecter des données pour protéger la LCD, comme l'intérêt à traquer les fraudeurs, l'emportent sur l'intérêt privé à la protection de données secrètes⁶.
30. La décision du 27 mai 2009 a été adressée au Préposé à la protection des données et à la transparence le 29 mai 2009.

² Arrêt du Tribunal administratif fédéral du 27 mai 2009, cause A-3144/2008, disponible sur le site Internet du TAF.

³ Arrêt précité cons. 3.2.3 p. 13.

⁴ Arrêt précité cons. 8.3.2 p. 18.

⁵ Arrêt précité cons. 9.3.4 p. 21.

⁶ Arrêt précité cons. 12.3.2 p. 26-27.



31. Dite décision a été publiée sur le site internet du Tribunal administratif à une date inconnue du soussigné.
32. Aucune notification n'est intervenue à l'adresse de l'Association Razorback, ni du soussigné.

III. MOTIFS :

A. LA SITUATION EN DROIT ÉTRANGER, EN PARTICULIER EN DROIT FRANÇAIS ET EN DROIT COMMUNAUTAIRE :

En droit français, la jurisprudence s'est montrée fluctuante sur ces questions. Dès 2004, la Commission nationale « *informatique et des libertés* » (CNIL) a assimilé les adresses IP à des adresses personnelles. Elle a rendu le 18 octobre 2005 trois décisions confirmant sa position⁷. Concrètement, cela signifie que toute organisation ou personne susceptible de recueillir ou de divulguer des données protégées doit recueillir l'autorisation préalable de la CNIL⁸. Cette position a été dans un premier temps contestée par les Tribunaux, en particulier par la Cour d'appel de Paris et par le Conseil d'État, dans deux arrêts rendus successivement les 23 avril 2007 et 23 mai 2007. Plus récemment, les Tribunaux considèrent que l'adresse IP est une donnée personnelle au sens de la loi DAVSI de 1978. La production d'adresses IP doit être validée par la CNIL, autorité administrative indépendante en France⁹. Cette solution va d'ailleurs dans le sens de la position des autorités européennes de protection des données, énoncée dans une résolution du 20 juin 2007 : le fait que l'adresse IP puisse être rapprochée des coordonnées du client sur la base d'une procédure relativement simple justifie une protection de celle-ci¹⁰.

⁷ Voir notamment <http://decryptages.wordpress.com>.

⁸ Ibidem.

⁹ Arrêt du Tribunal de Grande Instance de Paris du 25 juin 2007 dans l'affaire Techland/Logistep c/Neuf Cegetel/Orange, Télé2/Alice, consultable notamment sur le site www.nemerama.com/magazine.

¹⁰ Sur ces questions : voir <http://decryptages.wordpress.com>.



En droit communautaire, il importe de rappeler l'arrêt de la Cour de justice des Communautés européennes du 29 janvier 2008 dans l'affaire Promusicae/Telefonica¹¹. Interprétant plusieurs directives¹², la CJCE a clairement circonscrit le rôle et l'influence du droit communautaire sur celui des États membres.

Dans le cas particulier, la société Promusicae avait requis, du Juge civil, qu'il soit ordonné à la société Telefonica de révéler l'identité et l'adresse physique de certaines personnes auxquelles cette dernière fournissait un service d'accès Internet, à son adresse IP ainsi que la date et l'heure des connexions en cause. La question posée à la Cour était la suivante :

« le droit communautaire permet-il aux États membres de limiter au cadre d'une enquête criminelle ou aux impératifs de sauvegarde de la sécurité publique et de la défense nationale, et donc à l'exclusion des procédures civiles, l'obligation qui incombe aux opérateurs de réseaux et de services de communication électronique, aux fournisseurs d'accès à des réseaux de télécommunication et aux fournisseurs de services de stockage des données, de conserver et de mettre à disposition les données de connexion et de trafic engendré par des communications établies au cours de la prestation d'un service de la société de l'information ? ».

La Cour a répondu, de façon générale, comme il suit.

En premier lieu, s'il est vrai que les États membres doivent assurer, notamment dans la société de l'information, la protection effective de la propriété intellectuelle, en particulier le droit d'auteur, cette protection ne doit pas préjudicier aux exigences liées à la protection des données à caractère personnel¹³. Plus particulièrement, le droit communautaire n'impose pas aux États membres de pourvoir, en vue d'assurer la protection efficace du droit d'auteur, l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile¹⁴.

¹¹ Arrêt de la Cour de justice des Communautés européennes du 29 janvier 2008/demande de décision préjudicielle Juscado de Lo Mercantil n°5 de Madrid dans l'affaire Productores de Musica de Espana (Promusicae/Telefonica de Espana SAU SAU, affaire C.275/06, JOC 212 du 2.09.2006.

¹² Directive 2000/31/CE du Parlement européen du Conseil du 8 juin 2008, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur, JOL 178.1 ; Directive 2001/29/CE du Parlement européen du Conseil du 22 mai 2001, sur l'harmonisation de certains aspects de droits d'auteurs et de droits voisins de la société de l'information, JOL 167.10 ; Directive 2004/48/CE du Parlement européen du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle, JOL 157.45.

¹³ Arrêt précité, cons. 57.

¹⁴ Arrêt précité, cons. 58.



Dans le prolongement de cette dernière remarque, la Cour a considéré que les directives n'exigeaient pas davantage des États membres qu'ils prévoient de telles obligations sur le plan civil¹⁵. La Cour de justice des Communautés européennes a considéré que le droit d'auteur faisait partie du droit fondamental de propriété¹⁶. En ce sens, le droit d'auteur mérite le droit à une protection juridictionnelle effective. Ces principes constituent des principes généraux de droit communautaire¹⁷. Toutefois, selon la Cour, il importe de constater que la situation met en présence, en plus des deux droits susmentionnés, un droit supplémentaire fondamental, savoir la protection des données à caractère personnel et, partant, le droit au respect de la vie privée¹⁸.

En définitive, pour la CJCE, « les directives (...) n'imposent pas aux États membres de prévoir, dans une situation telle que celle de l'affaire au principal, l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile »¹⁹. Par ailleurs, et toujours selon la CJCE, « le droit communautaire exige des États que, lors de la transposition de ces directives, ils veillent à se fonder sur une intervention de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'Ordre juridique communautaire »²⁰. En définitive, la Cour a retenu que « lors de la mise en œuvre des mesures de transposition des dites directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national de manière conforme à ces mêmes directives, mais également de ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec les droits fondamentaux ou avec les autres principes généraux du droit communautaire, tel que le principe de la proportionnalité »²¹. En résumé, en droit communautaire, et en droit européen, le droit national doit respecter la vie privée, en particulier le secret des données protégées. Ainsi, le droit communautaire n'impose pas aux États membres de mettre en place un mécanisme permettant au Juge civil d'enjoindre le détenteur de données protégées de produire en procédure celles-ci.

¹⁵ Arrêt précité, cons. 59.

¹⁶ Voir notamment arrêt Laserdisken du 12 septembre 2006, cause C-479/04/REC p. I-8089.65.

¹⁷ Arrêt Alliance for Natural Health and consorts du 12 juillet 2005, cause C-154/04, C-155/04.REC.P.I-6451.126 ; arrêt Unibet du 13 mars 2007, cause C-432/05.REC.P.I-2271.37 et les références citées ; arrêt Promusicae précité, cause C-275/06 cons. 63.

¹⁸ Arrêt Promusicae précité, cons. 63.

¹⁹ Affaire Promusicae précitée, cons. 71.

²⁰ Ibidem.




²¹ Ibidem.



B. VIOLATION DES PRINCIPES FONDAMENTAUX (DROIT AU RESPECT DE LA VIE PRIVÉE, DROIT À LA PROPRIÉTÉ, DROIT AU RESPECT DU PRINCIPE DE LA PROPORTIONNALITÉ) TANT DU DROIT SUISSE QUE DU DROIT COMMUNAUTAIRE - VIOLATION DES ARTICLES 5, 13, 26, 36 CST. FÉD. & 8 CEDH AINSI QUE 1 DU PROTOCOLE N° 1 DE LA CEDH :

La décision du TAF, en ce sens qu'elle portait sur un cas d'espèce identique à celui qui a été soumis à la CJCE précitée, respecte-t-elle les principes fondamentaux du droit suisse ?

Qu'il s'agisse droit suisse ou de droit communautaire, les principaux fondamentaux sont les mêmes :

-  droit au respect de la vie privée (violation des articles 13 de la Constitution fédérale de la Confédération suisse et 8 de la CEDH),
-  droit à la propriété, englobant le droits d'auteur (violation des articles 26 Cst. féd. et article 1^{er} du Protocole n° 1 de la Convention européenne des Droits de l'Homme),
-  droit au respect du principe de la proportionnalité (violation des articles 5 et 36 Cst. féd., ainsi que 8 CEDH).

Avant même l'adoption du Traité de Maastricht, la CJCE a admis que les droits fondamentaux faisaient partie intégrante des principes généraux du droit (communautaire). Ainsi, dans l'arrêt Nold de 1974²², la CJCE a reconnu que « *les instruments internationaux concernant la protection des droits de l'homme auxquels les États membres ont coopéré ou adhéré peuvent également fournir des indications dont il convient de tenir compte dans le cadre du droit communautaire* ».

Le Traité de Maastricht n'a rien changé au statut de la CEDH au sein de l'ordre juridique communautaire. L'article F § 2, devenu par la suite l'article 6 § 2 UE dans le Traité d'Amsterdam, a certes encré pour la première fois dans le droit primaire de l'Union européenne l'obligation de respecter les droits fondamentaux, tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire²³. Concrètement, la référence à la CEDH implique son respect dans tous les domaines d'activités de l'Union²⁴.

²² CJCE, arrêt du 14 mai 1974, aff. 4/73, REC.1974 p. 491 cons. 13.

²³ Sur ces questions, voir Christine Kaddous, Les droits de l'homme et les libertés de circulation en droit communautaire, in RSDIE 2007, p. 397ss, spéc. 401 et les références citées.

²⁴ Ibidem.



Ainsi, et conformément la jurisprudence de la CJCE, « *les droits fondamentaux font partie intégrante des principes généraux du droit dont le Juge communautaire assure le respect. À cet égard, le Juge communautaire s'inspire des traditions constitutionnelles communes aux États membres ainsi que des indications fournies par les instruments internationaux concernant la protection européenne des droits de l'homme auxquels les États membres ont coopéré ou adhéré* »²⁵. En définitive, l'on ne voit guère de différence entre les principes fondamentaux, tels que dégagés par le droit communautaire et le droit suisse. En particulier, le principe de la proportionnalité, tel que formulé dans l'arrêt CJCE du 27 janvier 2008 précité, n'est guère différent de celui que le droit suisse connaît. À l'aune du droit de l'UE, le principe de la proportionnalité est violé si les restrictions à une liberté fondamentale du Traité CE dépassent ce qui est nécessaire pour assurer la protection d'un droit fondamental²⁶.

En définitive, l'arrêt rendu par le Tribunal administratif fédéral du 27 mai 2009 précité, tranche singulièrement avec la solution retenue par la CJCE, dans son arrêt du 28 janvier 2008.

Fondamentalement, les principes qui gouvernent le droit suisse et le droit de l'UE sont identiques. On peut considérer que la protection des données personnelles, relevant du droit à la sphère privée, sont identiques en droit communautaire et en droit suisse. On peut s'étonner que l'arrêt du TAF du 27 mai 2009 ne contienne aucune référence à l'arrêt de la CJCE du 28 janvier 2008. Peut-être que les Juges suisses ignoraient cette décision. Il est incompréhensible que le TAF n'ait pas tenu compte d'une telle interprétation, par le droit communautaire, de la protection des données. Qui plus est, l'arrêt du TAF du 27 mai 2009 est en opposition avec les Accords bilatéraux signés entre l'Union et la Suisse. On pourrait imaginer, à la suite de cette décision, que des sociétés européennes viennent s'installer en Suisse pour récolter des données – en toute impunité – afin de les diffuser ensuite en territoire européen. On voit mal comment la décision du TAF du 27 mai 2009 puisse être justifiée, en pratique. Elle exposerait de surcroît la Suisse à des sanctions de ses voisins et partenaires européens qui seraient en droit de considérer que la Suisse n'offre plus de garantie suffisante en matière de protection des données. Pour les motifs qui précèdent, le Tribunal fédéral doit constater que l'arrêt rendu par le TAF le 27 mai 2009 est erroné, en ce sens qu'il ne tient pas compte de l'évolution du droit de l'Union européenne, viole les dispositions de la CEDH ainsi que du Protocole n° 1 et qu'il viole de surcroît les dispositions du droit constitutionnel suisse telles qu'évoquées ci-dessus.

²⁵ Ibidem.

²⁶ Christine Kaddous, op. cit. p. 410 et les références citées.



D'autre part, il ne paraît guère faire de doute que les données IP sont des données protégées considérant que, sous l'angle du droit suisse, la protection du droit d'auteur n'est pas absolue. La décision du 27 mai 2009 doit donc être annulée et il doit être fait droit à la recommandation du Préposé fédéral à la protection des données et à la transparence. Il existe également d'autres motifs qui postulent pour qu'il soit fait droit aux conclusions du présent recours.

C. VIOLATION DU PRINCIPE DE LA LÉGALITÉ CRIMINELLE (ABSENCE DE BASE LÉGALE) / VIOLATION DES ARTICLES 1, 3, 6, 7 LSCPT, 23 ET SUIVANTS OSCPT /VIOLATION DES ARTICLES 2, 3, 4, 12, 13 LPD / VIOLATION DE L'ARTICLE 8 CEDH :

Une surveillance en matière de communications n'est possible en droit suisse que moyennant le respect des conditions prévues par la loi fédérale sur la surveillance de la correspondance par poste et télécommunications du 6 octobre 2000 (LSCPT ; RS 780.1), entrée en vigueur le 1^{er} janvier 2002.

Aux termes de l'art. 1^{er} al. 1^{er} LSCPT, « [l]a présente loi s'applique à la surveillance de la correspondance par poste et télécommunication qui est ordonnée et mise en œuvre : (a) dans le cadre d'une procédure pénale fédérale ou cantonale ».

L'art. 1^{er} al. 2 LSCPT poursuit en disposant que « [e]lle [la loi] s'applique à tous les organismes étatiques, aux organismes soumis à concession ou à l'obligation d'annoncer qui fournissent des services postaux ou de télécommunication ainsi qu'aux fournisseurs d'accès à Internet ». Aux termes de l'art. 3 LSCPT, une telle surveillance n'est possible qu'à des conditions cumulatives restrictives, à savoir : (1) de graves soupçons reposant sur des faits déterminés pèsent sur la personne concernée quant à la commission de l'un des actes punissables visés à l'al. 2 ou 3, ou quant à sa participation à un tel acte ; (2) la gravité de l'acte justifie la surveillance et (3) les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance. La question de savoir si les deuxième et troisième conditions sont remplies peut être laissée ouverte, dans la mesure où la première ne l'est assurément pas s'agissant des infractions au droit d'auteur.

Ni l'article 3 al. 2 LSCPT, ni son alinéa 3 ne mentionnent les droits d'auteur comme infractions susceptibles d'entraîner une surveillance. La nouvelle entrée en vigueur le 1^{er} avril 2007 n'a pas modifié cette situation, seul un art. 3a ayant trait à la recherche d'une personne disparue ayant été ajouté comme circonstance permettant la surveillance en dehors d'une procédure pénale.



Aussi étrange cela puisse-t-il paraître, le législateur n'a donc pas jugé utile d'introduire une disposition permettant l'identification des utilisateurs en cas de soupçons d'infractions aux droits d'auteur. Partant, il s'agit là d'une lacune proprement dite qui, aussi regrettable soit-elle, oblige à en conclure que le droit suisse ne permet pas à l'heure actuelle d'identifier les utilisateurs échangeant des fichiers présumés illicites dans le cadre d'un réseau *peer-to-peer* si ces fichiers ne sont pas constitutifs d'une infraction tombant sous le coup de l'art. 3 al. 2 ou 3 LSCPT. Le fait que les recherches n'aient aucune chance d'aboutir ou soient excessivement difficiles en l'absence de surveillance au sens de l'art. 3 al. 1^{er} lit. c LSCPT ne permet malheureusement pas de pallier à cette lacune, puisque les trois conditions énoncées sont d'application cumulative. A supposer qu'à l'avenir le législateur revoie sa position et introduise une telle base légale, la surveillance ne pourra quoi qu'il en soit pas être le fait d'une société privée. Conformément à l'art. 6 lit. a LSCPT, une surveillance ne peut être ordonnée que par le procureur général de la Confédération, les juges d'instructions fédéraux ou par les autorités compétentes en vertu du droit cantonal. Une surveillance ordonnée par des entités privées est donc exclue. Qui plus est, l'art. 7 LSCPT précise que l'ordre de surveillance doit être transmis pour autorisation à certaines autorités suivant celle dont émane l'ordre de surveillance. Seule cette autorité peut ensuite accepter la surveillance si la mesure portant atteinte à la personnalité est justifiée. En matière d'Internet, seuls les fournisseurs d'accès sont au surplus habilités à récolter de telles informations pour le compte des autorités, étant précisé que l'ordre en question doit satisfaire aux conditions précitées, et que la récolte d'informations répond à des exigences particulières énoncées aux articles 23 et suivants de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT, RS 780.11). L'octroi de tels pouvoirs à une société privée comme Logistep est donc exclu. Cette conclusion est également celle à laquelle le Préposé fédéral à la protection des données et à la transparence a abouti dans sa recommandation du 9 janvier 2008, en considérant que la récolte de telles données par une société privée violait la loi fédérale sur la protection des données. Le Préposé relève dans sa recommandation que l'adresse IP de l'utilisateur constitue une donnée personnelle au sens de l'art. 3 lit. a LPD, soit une information qui se rapporte à une personne identifiée ou identifiable grâce au recoupement possible de l'adresse avec une identité que détient le fournisseur d'accès (BSK-BELSER, ad art. 3 N. 6 ; Groupe de travail Article 29 sur la protection des données²⁷).

²⁷ Ce groupe a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive précitée et à l'article 15 de la directive 2002/58/CE.






Le Préposé les qualifie même de données sensibles au sens de l'art. 3 lit. c ch. 4 LPD, puisqu'elles peuvent conduire à l'ouverture d'une poursuite pénale. À juste titre, il relève que les principes fondamentaux de la protection des données ne sont pas respectés (art. 4 LPD), puisque l'utilisateur n'est évidemment pas informé de la collecte et que celle-ci n'est nullement conforme au but poursuivi par la publication de ces données de connexion, destinées à permettre l'échange de contenus.

Examinant la question de savoir si l'intérêt privé des titulaires de droits pourrait justifier une telle collecte (art. 13 LPD), en particulier dans l'optique de l'ouverture ultérieure d'une procédure pénale comme en l'espèce (la LPD ne s'appliquant pas aux procédures pénales soumises à des règles particulières, art. 2 al. 2 lit. c LPD), le Préposé répond par la négative, en considérant qu'un tel procédé tend à contourner le secret des télécommunications et porte atteinte aux droits de la personnalité d'un nombre indéfini d'utilisateurs de bonne foi, de sorte qu'aucun motif justificatif ne peut être invoqué. Le Groupe de travail « Article 29 » sur la protection des données a également eu l'occasion de dénoncer le traçage des utilisateurs par des gendarmes privés du réseau, dans un document du 18 janvier 2005 intitulé « Document de travail sur les questions de protection des données liées aux droits de propriété intellectuelle » (10092/05/FR WP 104, disponible sur : <http://www.europa.eu.int/comm/privacy>). C'est dire que la collecte de données personnelles, qui plus est sensibles, par une société privée viole non seulement la LSCPT, mais également la LPD, avis très largement partagé sur le plan international. C'est en effet à tort que le Préposé s'interroge sur la question de savoir si une telle collecte à des fins d'ouverture de poursuite pénale par une entité privée pourrait être licite puisque, nous l'avons vu, la LSCPT n'autorise pas la mise en place de mesures de surveillances pour des infractions au droit d'auteur quel que soit l'organisme qui s'en charge, réserve étant faite des fournisseurs d'accès à des conditions bien définies.

A fortiori, la décision du Tribunal administratif fédéral viole tant les dispositions de la LSCPT que celles de la LPD, la CEDH et le principe de légalité. En l'état aucune base légale n'autorise en effet une entité privée à collecter des adresses IP (lacune proprement dite). Ainsi, le Tribunal administratif fédéral aurait non seulement dû rejeter l'argumentaire de Logistep, mais également constater l'existence d'une lacune proprement dite laquelle, hormis l'hypothèse d'une modification législative, n'autorisait pas, dans notre pays, des privés à procéder à une collecte de données telle que celle relative aux adresses IP litigieuse. Partant, la décision doit être annulée avec suite de frais et dépens.



IV. MOYENS DE PREUVE :

-  Édition du dossier du Préposé fédéral à la protection des données – dossier A2008.01.21-0003/RO ;
-  Édition du dossier A-3144/2008 du Tribunal administratif fédéral ;
-  Décision querellée déposée en annexe à la présente.

V. CONCLUSIONS :

Fondé sur ce qui précède, plaise à la Cour de droit public du Tribunal fédéral dire et statuer :

1. Le recours en matière de droit public est admis et la décision du Tribunal administratif fédéral du 21 mai 2009 dans la cause A-3144/2008 est annulée.
2. Tous les frais sont mis à la charge de la société Logistep AG.
3. Il est alloué à l'Association Razorback une équitable indemnité pour ses dépens.

Veillez agréer, Monsieur le Président de la Cour de droit public du Tribunal fédéral, Mesdames, Messieurs les Juges fédéraux, Mesdames, Messieurs les Greffiers, l'expression de ma haute considération ainsi que mes respectueuses salutations.

SÉBASTIEN FANTI 

Annexe : décision querellée et lettre de Logistep.

