La cour d'appel de Bruxelles, 9ème chambre,

après en avoir délibéré, prononce l'arrêt suivant :

R.G. : 2007/AR/2424

R. n° : 2010/ 790

N° : 192

Arrêt interlocutoire
Question préjudicielle à la C.J.U.E.

Droit d'auteur.
Internet.
Piratage d'œuvres musicales.
Logiciels "peer to peer".
Action en cessation.
Injonction à un Fournisseur d'Accès à Internet de mettre en place un système de blocage.
Conformité avec le droit communautaire ?

- art 1001 2° LRC

28-01-2010

EN CAUSE DE :

SCARLET EXTENDED, société anonyme dont le siège social est établi à 1800 Vilvoorde, Medialaan, 50, inscrite à la banque carrefour des entreprises sous le numéro 0463.815.792,

Appelante,
Intimée sur incident,

représentée par Maîtres Christoph De Preter et Thomas De Meese, avocats à 1000 Bruxelles, rue Royale, 71,

plaideur : Maître Th. De Meese,

CONTRE :

SOCIETE BELGE DES AUTEURS COMPOSITEURS ET EDITEURS, en abrégé SABAM, société civile à responsabilité limitée dont le siège est établi à 1040 Bruxelles, rue d'Arlon, 75-77, inscrite à la banque carrefour des entreprises sous le numéro 0402.989.270,

Intimée,
Appelante sur incident,

représentée par Maître Benoît Michaux, avocat à 1050 Bruxelles, avenue Louise, 149/20,

plaideurs : Maîtres B. Michaux, B. Docquir et Ph. Campolini,

EN PRESENCE DE :

1.- BELGIAN VIDEO FEDERATION, en abrégé BVF, actuellement dénommée BELGIAN ENTERTAINEMENT ASSOCIATION VIDEO,

en abrégé BEA Video, association sans but lucratif dont le siège social est établi à 1200 Bruxelles, place de l'Alma, 3/2, inscrite à la banque carrefour des entreprises sous le numéro 0427.838.294,

2.- IFPI BELGIUM, INDUSTRIE PHONOGRAPHIQUE BELGE – BELGISCHE FONOGRAFISCHE INDUSTRIE, en abrégé IFPI, actuellement dénommée BELGIAN ENTERTAINEMENT ASSOCIATION MUSIC, en abrégé BEA Music, association sans but lucratif dont le siège social est établi à 1200 Bruxelles, place de l'Alma, 3/B2,

Intervenantes volontaires,

représentées par Maître Benoît Michaux, avocat à 1050 Bruxelles, avenue Louise, 149/20,

plaideurs : Maîtres B. Michaux, B. Docquir et Ph. Campolini,

3.- INTERNET SERVICE PROVIDER ASSOCIATION, en abrégé ISPA, association sans lut lucratif dont le siège est établi à 1000 Bruxelles, rue Montoyer, 39/3, inscrite à la banque carrefour des entreprises sous le numéro 0461.515.409,

Intervenante volontaire,

représentée par Maîtres Geert Somers et Jos Dumortier, avocats à 1000 Bruxelles, rue du Congrès, 35,

plaideur : Maître G. Somers,

4.- BELGACOM, société anonyme de droit public dont le siège social est établi à 1030 Bruxelles, boulevard du Roi Albert II, 27, inscrite à la banque carrefour des entreprises sous le numéro 0202.239.951,

28 -01- 2010

Appelée en déclaration d'arrêt commun,

représentée par Maître Benoît Van Asbroeck, Laurent Masson et Maud Cock, avocats à 1040 Bruxelles, avenue d'Auderghem, 22-28/9.

****

I.- DECISION ENTREPRISE

L'appel est dirigé contre les jugements prononcés

contradictoirement les 26 novembre 2004 et 29 juin 2007 par le président du tribunal de première instance de Bruxelles.

Les parties ne produisent aucun acte de signification de ces jugements.

II.- PROCEDURE DEVANT LA COUR

L'appel principal est formé par requête, déposée par Scarlet Extended (dénommée ci-après Scarlet) au greffe de la cour, le 6 septembre 2007.

Par requêtes déposées au greffe de la cour le 13 décembre 2007, la BVF et l'IFPI interviennent volontairement pour prendre fait et cause pour la Sabam.

Par conclusions déposées au greffe de la cour le 14 décembre 2007, la Sabam introduit un appel incident.

Par requête déposée au greffe de la cour le 8 février 2008, l'ISPA intervient volontairement pour soutenir la thèse défendue par Scarlet.

Par exploit du 18 mars 2008, déposé le 5 mai 2008, la Sabam fait citer Belgacom en déclaration d'arrêt commun.

La procédure est contradictoire.

Il est fait application de l'article 24 de la loi du 15 juin 1935 sur l'emploi des langues en matière judiciaire.

28 -01- 2010

III.- FAITS ET ANTECEDENTS DE LA PROCEDURE

1. Par exploit du 24 juin 2004, la Sabam fait citer Scarlet devant le président du tribunal de première instance de Bruxelles, statuant comme en référé, en matière de cessation dans le cadre de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins.

   Elle se plaint que des internautes téléchargent illégalement des œuvres reprises dans son catalogue au moyen de logiciels dits « peer to peer » ou « P2P », sans acquitter de droits. Elle soutient que Scarlet, en sa qualité de fournisseur d'accès à Internet (en abrégé FAI ou ISP en anglais) en profite, dans la mesure où ce genre de pratiques est susceptible d'augmenter son volume de trafic

et, partant, la demande de ses services. Elle considère que les FAI sont idéalement placés pour prendre des mesures en vue de faire cesser les atteintes au droit d'auteur commises par leurs clients.

Elle demande qu'il soit constaté l'existence d'atteintes au droit d'auteur sur les œuvres musicales appartenant à son répertoire, en particulier au droit de reproduction et au droit de communication au public, consacrés par l'article 1er, paragraphe 1er de la LDA, du fait de l'échange non autorisé de fichiers électroniques musicaux réalisé grâce à des logiciels *peer to peer*, lesquelles atteintes sont commises au travers de l'utilisation des services de Scarlet.

Elle sollicite que Scarlet soit condamnée à faire cesser ces atteintes en rendant impossible ou en paralysant toute forme d'envoi ou de réception par ses clients de fichiers reprenant une œuvre musicale sans l'autorisation des ayants droit, au moyen d'un logiciel *peer to peer*, sous peine d'une astreinte de 25.000,00 € par jour ou partie de journée où Scarlet ne respecterait pas le jugement à intervenir. Elle demande également que Scarlet lui communique dans les huit jours de la signification le descriptif des mesures qu'elle appliquera en vue de respecter le jugement, sous peine d'une astreinte de 5.000,00€ par jour de retard. Elle postule enfin la publication d'un texte sur la page d'accueil du site Internet de Scarlet pendant une durée de trois mois, sous peine d'une astreinte de 5.000,00 € par jour de retard ainsi que la publication du jugement à intervenir dans deux quotidiens et un hebdomadaire de son choix.

2. Par jugement du 26 novembre 2004, le président du tribunal constate l'existence de l'atteinte au droit d'auteur dénoncée par la Sabam, mais, avant de statuer plus avant sur la demande de cessation, désigne M. Olivier Gerbehaye, en qualité d'expert, afin d'examiner si les solutions techniques proposées par la Sabam sont techniquement réalisables, si elles permettent de filtrer uniquement les échanges illicites de fichiers électroniques, s'il existe d'autres dispositifs susceptibles de contrôler l'usage de logiciels *peer to peer* et de déterminer le coût des dispositifs qui sont envisagés.

L'expert dépose son rapport le 29 janvier 2007. Il conclut de la manière suivante :

1. *Un réseau peer to peer est un moyen transparent de partage de contenu, indépendant, décentralisé et muni de fonctions de recherche et de téléchargement avancés.*
2. *A l'exception de la solution proposée par Audible Magic, toutes les solutions tentent d'empêcher l'utilisation des réseaux peer to peer, indépendamment du contenu qui y est véhiculé ;*
3. *Par ailleurs, la pérennité des solutions de filtrage d'application peer to peer est loin d'être assurée sur le*

moyen terme (2-3 ans) dû par l'utilisation grandissante du cryptage dans ce type d'application ;

4. *La solution proposée par la société Audible Magic est donc la seule à tenter de répondre à la problématique de manière spécifique. Cette solution, essentiellement destinée au monde éducatif, n'est cependant pas intrinsèquement dimensionnée pour répondre au volume de trafic d'un FAI. Le recours à cette technique dans le contexte FAI induit de ce fait un coût d'acquisition et d'exploitation élevé pour compenser ce sous-dimensionnement ;*
5. *Ce coût est à mettre en regard avec la période pendant laquelle cette solution sera efficace, le cryptage mentionné ci-dessus rendant cette solution également inefficace dans le cadre du filtrage en transit ;*
6. *Le recours aux méthodes d'investigations internes, entreprises par l'intérieur d'un réseau peer to peer sont plus complexes à mettre en œuvre, mais fournissent de meilleurs résultats. Ces méthodes ne visent en effet a priori que la partie répréhensible des échanges et sont capables de tenir compte du contexte dans lequel ces échanges se font ;*
7. *Ces méthodes ne sont par ailleurs pas ou nettement moins sensibles au cryptage et constituent selon nous la meilleure voie d'investissement sur le moyen et le long terme pour garantir le respect des droits d'auteur tout en respectant les droits de tous.*

Par le second jugement attaqué du 29 juin 2007, le président du tribunal condamne Scarlet *à faire cesser les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 en rendant impossible toute forme, au moyen d'un logiciel peer to peer, d'envoi ou de réception par ses clients de fichiers électroniques reprenant une œuvre musicale du répertoire de la Sabam sous peine d'une astreinte de 2.500,00 € par jour où Scarlet ne respecterait pas le jugement, après l'expiration d'un délai de six mois.*

28 -01- 2010

3. Scarlet interjette appel de cette décision.

Par exploit du 7 décembre 2007, Scarlet fait citer la Sabam devant le président du tribunal de première instance de Bruxelles. Elle expose qu'il lui est impossible d'exécuter le jugement du 29 juin 2007 dans la mesure où le système *Audible Magic* sur lequel cette décision s'est fondée ne fonctionne pas et qu'il n'est pas établi qu'il est techniquement faisable pour un FAI de réaliser un blocage ou un filtrage efficace du trafic *peer to peer*. Elle sollicite dès lors la suppression ou, à tout le moins, la suspension des astreintes vu l'impossibilité matérielle ou temporelle de se conformer à l'ordre de cessation.

Par son jugement du 22 octobre 2008, le président du tribunal rejette cette demande, considérant que l'effet dévolutif de l'appel s'oppose à ce que les parties replaident la cause devant lui, dès lors que sa décision a été précédée d'un débat fouillé sur les mesures techniques proposées par l'expert. Certes, il reconnaît que la solution *Audible Magic* n'a pu être implémentée avec succès, mais il constate que Scarlet n'a pas expérimenté d'autres solutions de blocage ou de filtrage, notamment celles mises en évidence par l'expert et que, partant, elle ne démontrait pas que l'ordre de cessation ne pouvait pas être respecté en recourant à ces mesures techniques. Afin de permettre à Scarlet d'explorer d'autres voies, le président suspend l'astreinte jusqu'au 31 octobre 2008.

Ce jugement est définitif, aucun recours n'ayant été introduit.

4. La BVF, l'IFPI et l'ISPA interviennent volontairement à la cause.

5. Aux termes de ses dernières conclusions, Scarlet demande à la cour de :

Réformer le jugement a quo et, statuant à nouveau sur la demande originaire:

A titre principal :

Déclarer celle-ci recevable mais non fondée;

A titre subsidiaire :

Préciser la mesure de cessation en définissant ce qu'il y a lieu d'entendre par « peer-to-peer » et en déterminant de manière concrète comment il peut être mis fin aux atteintes litigieuses ;

Constater que l'appelante ne peut en aucun cas être contrainte de bloquer purement et simplement l'accès par ses abonnés à l'utilisation d'un ou plusieurs logiciels « peer-to-peer » ;

Constater qu'aucune solution de filtrage existant actuellement n'est apte à assurer que tout échange de fichiers musicaux relevant du répertoire de la partie intimée via des logiciels « peer-to-peer » soit rendu impossible ;

Ordonner à la partie intimée de rembourser, à la première demande de l'appelante et dans les dix jours ouvrables après présentation d'une facture, même pro forma, tous les frais directs et indirects occasionnés par l'installation de dispositifs ou mesures tendant à faire respecter l'ordre de cessation

prononcé à charge de l'appelante ; à tout le moins imposer à la partie intimée de rembourser à l'appelante les frais supportés par celle-ci au fur et à mesure de l'augmentation des droits d'auteur qu'elle percevrait en raison du déploiement des mesures de cessation.

Ordonner que la partie intimée garantira l'appelante en justice concernant toute demande et tiendra l'appelante indemne de toute somme qu'elle devrait débourser à l'égard de tout abonné ou tout tiers quelconque en raison du préjudice qu'ils auraient respectivement directement ou indirectement subis en raison de la mise en œuvre de l'ordre de cessation et/ou que la partie appelante serait amenée à débourser en raison de la perte de son statut d'immunité de responsabilité sous l'article 18 de la Loi sur le commerce électronique.

6. La Sabam demande à la cour de :

Sur l'appel principal,

En ordre principal,

Le dire non fondé,

En ordre subsidiaire,

Au cas où la Cour déciderait que l'ordre de cessation doit faire référence à une liste de protocoles « Peer to Peer »,

Dire que l'ordre s'appliquera non seulement à la liste des protocoles actuellement identifiés par la SABAM à partir de la liste iPoque mais également aux protocoles que la SABAM identifiera à l'avenir à partir d'une liste similaire et qu'elle notifiera par courrier recommandé à SCARLET, sauf pour SCARLET à établir que les quantités de fichiers musicaux illicites véhiculés par les protocoles en cause seraient dérisoires.

28 -01- 2010

En débouter l'appelante,

Dire l'appel incident fondé,

Dès lors

(1) Fixer l'astreinte liée à l'ordre de faire cesser les atteintes au droit d'auteur à 25.000,00 EUR, au lieu de 2.500,00 EUR, par jour où SCARLET ne respecterait pas l'ordre de faire cesser.
(2) Prononcer une astreinte de 5.000,00 EUR par jour de

retard, au cas où SCARLET resterait en défaut de communiquer le descriptif des mesures appliquées en vue de respecter l'ordre de faire cesser.

(3) Condamner Scarlet à afficher dans les 24 heures de la signification de l'arrêt à intervenir le texte repris ci-après et sa traduction en néerlandais, allemand et anglais, sur la page d'accueil de son site Internet, en caractères gras, à un endroit visible et sous une forme lisible, de manière ininterrompue pendant trois mois, sous peine d'une astreinte de 5.000,00 € par jour ou partie d'une journée où la condamnation ne serait pas respectée:

> *"La Cour d'appel de Bruxelles a confirmé la décision condamnant SCARLET à rendre impossible toute forme d'envoi ou de réception, par sa clientèle, de fichiers reprenant la reproduction d'une œuvre musicale, sans l'autorisation des ayants droit, au moyen de logiciels "peer-to-peer". L'échange de fichiers musicaux illicites porte gravement atteinte aux droits des auteurs, compositeurs et éditeurs des œuvres musicales".*

(4) Ordonner la publication de l'arrêt à intervenir et de sa traduction en néerlandais dans deux quotidiens et un hebdomadaire au choix de la SABAM, aux frais de SCARLET, ces frais étant récupérables sur présentation d'une facture même pro-forma;

28 -01- 2010

7. Belgacom est citée en déclaration d'arrêt commun. Aux termes de ses dernières conclusions, elle demande à la cour de :

***Sur* [la demande en déclaration d'arrêt commun]**

A titre principal

De [la] *déclarer irrecevable ;*

A titre subsidiaire

De désigner avant dire droit un expert, lequel aura pour mission de reprendre la mission d'expertise ab initio, et en outre, de rendre un rapport sur les questions suivantes :

- dire en quoi le filtrage du peer-to-peer se différencie des dispositifs anti-spam et anti-virus ;

- dire si des technologies autres que le peer-to-peer permettent l'échange illicite de fichiers musicaux ;

- dire dans quelle mesure la pérennité de ladite solution peut-être assurée dans le temps;

- dire si la solution précitée est adaptée au volume d'un F.A.I. tel que BELGACOM ;

- dire si l'architecture de réseau des F.A.I. en Belgique, et plus précisément de SCARLET et de BELGACOM, permet le déploiement de ladite solution sans qu'aucune adaptation ne soit nécessaire ; dans la négative, déterminer le coût induit par l'adaptation du réseau au déploiement de ladite solution ;

- dire si le déploiement de ladite solution sur le réseau d'un F.A.I. est comparable à son utilisation par des hébergeurs, tels les exploitants de MySpace et Youtube;

- dire si ladite solution permet de traiter l'ensemble du trafic national de SCARLET et de BELGACOM et si elle est compatible avec le protocole ATM ;

- dire si ladite solution peut-être déployée simultanément sur l'ensemble des échanges peer-to-peer d'un F.A.I. ou si ladite solution est limitée à des « coups de sonde » ou « en interconnexion avec d'autres opérateurs » ;

- dire si il est techniquement possible pour les internautes d'ignorer l'ordre de « reset » envoyé par la dite solution, de procéder à du « tunneling » ou de mettre en œuvre quelque moyen susceptible de contrer le filtrage des échanges illicites de fichiers ;

28 -01- 2010

- dire si la base de données de ladite solution est exhaustive et mise à jour en temps réel ;

- dire si Audible Magic est en mesure de donner des garanties pour que ladite base de données reste mise à jour en temps réel et à long terme ;

- dire si l'encryptage des fichiers est utilisé à l'heure actuelle dans le cadre du peer-to-peer ; indiquer si cette tendance va à la hausse ou à la baisse ; dire quelles méthodes d'encryptage sont utilisées ; examiner dans quelle mesure les méthodes d'anonymisation se développent et dans quelle mesure elles mettent à mal le déploiement de l'application Copysense ;

- dire si l'encryptage des fichiers peut être considéré comme

temporaire ;

- dire si ladite solution s'avère efficace en cas d'encryptage et, dans l'affirmative, à l'égard de quelles formes d'encryptage;

- dire si les éditeurs de la solution disposent des ressources suffisantes en Europe et en Belgique pour assurer la maintenance et la continuité de la solution conformément aux meilleurs standards industriels ;

- dire si il y a d'autres applications autonomes ou combinées entre elles susceptibles de permettre la mise en œuvre de l'ordre de cessation sans nuance sollicité par la SABAM ;

- examiner dans quelle mesure tout ou partie des applications identifiées par l'expert qui permettraient, le cas échéant, de rencontrer sans faille l'ordre de cessation sollicité par la SABAM, peuvent être mises en œuvre par des tiers au F.A.I. et en particulier par la SABAM elle-même, le cas échéant assistée d'un expert technique ; identifier les tâches et actions qui doivent dans le cadre du déploiement nécessairement être exécutées par le F.A.I. ;

De surseoir à statuer pour le surplus, les parties pouvant reconclure après le dépôt du rapport d'expertise ;

De condamner la SABAM à provisionner l'expert et à en supporter seule les coûts ;

Sur l'appel principal

A titre principal

28-01-2010

De le déclarer recevable et fondé ;

En conséquence réformer le jugement a quo et débouter la SABAM de l'ensemble de ses demandes ;

A titre subsidiaire

D'adresser à la Cour de Justice des Communautés Européennes les questions préjudicielles suivantes :

Question 1

Une injonction, ordonnée sur base de l'article 8.3. de la directive 2001/29, imposant à un Fournisseur d'Accès Internet de déployer sur son réseau des mesures de filtrage non limitées dans le temps en vue de rendre impossible tout échange non autorisé par ses clients, par le biais d'un logiciel « peer-to-

peer », de tout fichier contenant toute œuvre faisant partie du répertoire d'une société de gestion collective et/ou de ses sociétés sœurs, peut-elle être interprétée comme l'imposition d'une mesure générale de surveillance au sens de l'article 15 de la directive 2000/31 et est-elle bien prohibée par cette disposition?

Question 2

Les mesures visées par l'article 8.3 de la directive 2001/29 peuvent-elles être préventives in abstracto (à l'égard de contrevenants potentiels non identifiés) ou doivent-elles se limiter à un ou plusieurs contrevenants identifiés ?

Question 3

L'article 8.3 de la directive 2001/29, d'une part, et l'exception au régime d'exonération de responsabilité des Fournisseurs d'Accès Internet prévue par l'article 12.3 de la directive 2000/31, d'autre part, peuvent-ils être interprétés de manière telle qu'ils justifient que soit ordonné à l'encontre d'un Fournisseur d'Accès Internet, par le biais d'une action en cessation, de déployer sur son réseau des mesures de filtrage non limitées dans le temps en vue de rendre impossible tout échange non autorisé par ses clients, par le biais d'un logiciel « peer-to-peer », de tout fichier contenant toute œuvre faisant partie du répertoire d'une société de gestion collective et/ou de ses sociétés sœurs ?

- *Dans l'affirmative, une telle mesure peut-elle être considérée comme une sélection au sens de l'article 12.1 de la directive 2000/31 et faire perdre au Fournisseur d'Accès Internet l'exonération de responsabilité prévue par cette disposition ?*

- *La réponse à cette question est-elle différente si l'efficacité des mesures de filtrage peut être mise en doute, et ce dans le cadre d'une injonction prononçant une obligation de résultat ?*

28 -01- 2010

Question 4

Etant donné que les titulaires de droits d'auteur peuvent demander, sur base de l'article 8.3 de la directive 2001/29, qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin, et ce en dehors de toute notion de faute des intermédiaires, les frais liés à l'injonction prononcée dans un tel cadre par le juge national incombent-ils aux demandeurs d'une telle injonction ?

A titre infiniment subsidiaire

Dire pour droit que le coût du déploiement d'un logiciel de filtrage tendant à faire respecter l'ordre de cessation ne peut être à charge de SCARLET.

IV.- DISCUSSION

1.- Sur la demande en déclaration d'arrêt commun dirigée contre Belgacom

8. L'article 812 alinéa 1er du Code judiciaire dispose que l'intervention peut avoir lieu devant toutes les juridictions, sans néanmoins que des actes d'instruction déjà ordonnés puissent nuire aux droits de la défense.

   Cette disposition permet à celui qui est appelé en intervention forcée de refuser le débat lorsque ses droits de défense ne sont pas saufs, notamment lorsque sa défense serait compromise en raison d'une décision déjà acquise (Cass., 25 novembre 1992, Pas., 1992, I, 1304).

   Par ailleurs, la demande tendant à ce qu'une décision judiciaire à rendre soit déclarée commune a pour seul objet d'empêcher que le défendeur à cette demande puisse éventuellement, dans un litige subséquent l'opposant au demandeur, objecter que cette décision ne lui est pas opposable; l'existence de cette possibilité suffit pour que le demandeur établisse qu'il a un intérêt à ce que la décision soit déclarée commune au défendeur (Cass., 25 novembre 1996, C.94.0490.N). La déclaration de jugement ou d'arrêt commun confère, à l'égard du défendeur, l'autorité de la chose jugée de la décision en cause (Cass., 20 octobre 1988, Pas., 1989, I, 191). Dans le cadre d'un débat ultérieur, l'appelé en déclaration d'arrêt commun ne pourra soulever la fin de non-recevoir tirée de la relativité de l'autorité de la chose jugée (A. Fettweis, Manuel de procédure civile, p.421, n° 592).

9. En l'espèce, le litige dépasse de loin la seule revendication de la Sabam à l'encontre de Scarlet, mais concerne un grand débat de société, à savoir la lutte entreprise par les ayants-droit d'œuvres musicales, cinématographiques et audio-visuelles en vue d'enrayer le piratage de celles-ci par le téléchargement illégal de fichiers informatiques au moyen de logiciels *peer to peer*. Plutôt que de s'attaquer directement aux internautes contrefacteurs – comme cela se fait dans d'autres pays – la Sabam a choisi de mettre à la cause

les FAI qu'elle considère comme étant les mieux à même de rendre impossible, sur le plan technique, ce type de téléchargements.

Les interventions volontaires de la BVF, de l'IFPI et l'ISPA, associations professionnelles regroupant tous les acteurs du secteur, sont caractéristiques à cet égard et démontrent l'ampleur du débat. Il a d'ailleurs été plaidé que la présente procédure était une *première mondiale* et que le *monde attendait la décision de la cour d'appel de Bruxelles*. Il s'en déduit qu'il s'agit d'un *procès test*, susceptible d'être étendu à tous les FAI en cas de confirmation du jugement entrepris.

10. Outre la compatibilité de la mesure de cessation demandée avec les dispositions légales relatives à la protection des données à caractère personnel, le secret des communications et le commerce électronique, le débat est centré sur l'applicabilité technique des moyens à mettre en œuvre pour bloquer ou filtrer les transferts de fichiers contenant des œuvres protégées, effectués au moyen de logiciels *peer to peer*, débat auquel la cour ne pourra se soustraire au cas où il serait dit que l'ordre de cessation ne violerait pas d'autres droits fondamentaux.

A cet égard, la Sabam fait valoir que *l'expert désigné par le premier juge a confirmé l'existence de différentes solutions prêtes à l'usage permettant de se conformer à l'injonction* (point 6.3.1) et s'oppose à la demande d'expertise nouvelle sollicitée par Belgacom en soutenant qu'elle *n'aurait guère de sens* et que les questions qu'elle propose de poser à ce nouvel expert *sont sans pertinence* (point 6.7).

La Sabam considère donc que le rapport de l'expert désigné par le premier juge constitue un élément essentiel démontrant l'efficacité et la proportionnalité de l'ordre de cessation demandé, ce que conteste Belgacom.

Or, il est constant que Belgacom n'a pu participer à cette expertise, dès lors qu'elle n'a été appelée à la cause qu'en degré d'appel, après le dépôt du rapport définitif de l'expert.

Belgacom aborde sur plus de 60 pages (cf. point 4.2 de ses conclusions) les solutions techniques susceptibles ou non d'être efficaces dans le cas d'espèce. Elle n'a pu faire valoir son opinion devant l'expert ni obtenir de sa part de réponse aux dix-sept questions qu'elle aurait pu lui soumettre dans le cadre d'une note de faits directoires.

Il ne peut donc être sérieusement contesté que Belgacom n'a pu faire valoir ses droits de défense sur le plan technique au moment où elle a été citée en déclaration d'arrêt commun. Devant la cour,

l'égalité des armes est rompue en faveur de la Sabam qui entend s'appuyer sur le rapport d'expertise qui, s'il ne lie pas la cour, pourrait néanmoins avoir une influence déterminante sur sa décision dans le cadre de la demande principale.

Or, il n'est pas possible de tenir des raisonnements techniques différents selon que le FAI en cause est Scarlet ou Belgacom. Les demandes principale et en intervention sont intimement liées. Soit il existe un moyen fiable de blocage des fichiers illégaux soit il n'en existe pas et cette constatation s'impose à tous les FAI du monde. Belgacom n'est donc pas étrangère à la discussion principale entre la Sabam et Scarlet.

Eu égard à l'autorité de la chose jugée qui s'attachera à la décision de la cour sur la demande principale, et à supposer que celle-ci s'appuie sur le rapport de l'expert Gerbehaye, Belgacom se verra opposer, indirectement mais certainement dans un litige futur – qui ne fait aucun doute et qui est d'ailleurs annoncé en filigrane – les conclusions d'un rapport qui ne lui est pas opposable, ce qui est contraire aux principes du contradictoire et du respect des droits de la défense. Par ailleurs, dans la mesure où la Sabam tente de conférer au jugement du 22 octobre 2008 une force de chose jugée en ce qui concerne l'efficacité technique des mesures préconisées par l'expert, Belgacom risque d'être, en plus, confrontée aux effets d'une décision à laquelle elle n'a pas été partie.

11. Enfin, c'est en vain que la Sabam soutient qu'en se défendant et en proposant à la cour d'ordonner une nouvelle expertise ou de poser des questions préjudicielles à la Cour de justice de l'Union européenne, Belgacom devrait être considérée comme une intervenante volontaire.

Il résulte au contraire du dispositif de ses conclusions que ces moyens ne sont présentés qu'à titre subsidiaire et de défense, pour le cas où la cour déclarerait la demande en déclaration d'arrêt commun recevable.

12. Eu égard aux circonstances propres à l'espèce, il se déduit de ce qui précède que la citation en intervention forcée n'est pas recevable, dès lors que la mesure d'expertise déjà ordonnée et accomplie est, *in concreto*, de nature à porter préjudice à Belgacom et ainsi à nuire à ses droits de la défense.

C'est à tort cependant que Belgacom réclame une indemnité de procédure. En effet, aux termes de la loi du 21 avril 2007 sur la répétibilité des frais et honoraires d'avocat, le débiteur de l'indemnité de procédure est celui qui succombe à l'action ; le créancier est celui qui obtient gain de cause. Le lien d'instance entre

les parties doit s'entendre d'une manière restrictive : il faut qu'il y ait eu, entre les parties une demande de condamnation et que cette demande ait mené à la condamnation effective d'une d'entre elles. Il s'en déduit que la partie citée en déclaration de jugement ou d'arrêt commun ne peut prétendre à une indemnité de procédure pas plus qu'elle ne peut être condamnée à en payer une (cf. sur ce point, J.-F. Van Droogenbroeck et B. De Coninck, La loi du 21 avril 2007 sur la répétibilité des frais et honoraires d'avocat, J.T. 2008, p. 49, n° 51).

13. En revanche, les requêtes en intervention volontaire conservatoire de la BVF, de l'IFPI et de l'ISPA sont recevables, sans qu'elles ne donnent lieu, cependant, à l'octroi d'une indemnité de procédure.

2.- Sur l'ordre de cessation

a.- Le cadre juridique

14. La Sabam se fonde sur l'article 87 § 1er, premier et deuxième alinéas de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins qui dispose que :

> *Le président du tribunal de première instance (...) constate l'existence et ordonne la cessation de toute atteinte au droit d'auteur ou à un droit voisin.*
> *Il peut également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin.*

Le deuxième alinéa de cette disposition doit être interprété à la lumière des directives 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle qui disposent, notamment :

Directive 2001/29

> (considérant 59) :
> *Les services d'intermédiaires peuvent, en particulier dans un environnement numérique, être de plus en plus utilisés par des tiers pour porter atteinte à des droits. Dans de nombreux cas, ces intermédiaires sont les mieux à même de mettre fin à ces*

atteintes. Par conséquent, sans préjudice de toute autre sanction ou voie de recours dont ils peuvent se prévaloir, les titulaires de droits doivent avoir la possibilité de demander qu'une ordonnance sur requête soit rendue à l'encontre d'un intermédiaire qui transmet dans un réseau une contrefaçon commise par un tiers d'une oeuvre protégée ou d'un autre objet protégé. Cette possibilité doit être prévue même lorsque les actions de l'intermédiaire font l'objet d'une exception au titre de l'article 5. Les conditions et modalités concernant une telle ordonnance sur requête devraient relever du droit interne des États membres.

(article 8) :
Sanctions et voies de recours
1. Les États membres prévoient des sanctions et des voies de recours appropriées contre les atteintes aux droits et obligations prévus par la présente directive et prennent toutes les mesures nécessaires pour en garantir l'application. Ces sanctions sont efficaces, proportionnées et dissuasives.
2. (...)
3. Les États membres veillent à ce que les titulaires de droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin.

Directive 2004/48

(article 3)
Obligation générale
1. Les États membres prévoient les mesures, procédures et réparations nécessaires pour assurer le respect des droits de propriété intellectuelle visés par la présente directive. Ces mesures, procédures et réparations doivent être loyales et équitables, ne doivent pas être inutilement complexes ou coûteuses et ne doivent pas comporter de délais déraisonnables ni entraîner de retards injustifiés.
2. Les mesures, procédures et réparations doivent également être effectives, proportionnées et dissuasives et être appliquées de manière à éviter la création d'obstacles au commerce légitime et à offrir des sauvegardes contre leur usage abusif.

28 -01- 2010

(article 9)
Mesures provisoires et conservatoires
1. Les États membres veillent à ce que les autorités judiciaires compétentes puissent, à la demande du requérant:
a) rendre à l'encontre du contrevenant supposé une ordonnance de référé visant à prévenir toute atteinte imminente à un droit de propriété intellectuelle, à interdire, à titre provisoire et sous

réserve, le cas échéant, du paiement d'une astreinte lorsque la législation nationale le prévoit, que les atteintes présumées à ce droit se poursuivent, ou à subordonner leur poursuite à la constitution de garanties destinées à assurer l'indemnisation du titulaire du droit; une ordonnance de référé peut également être rendue, dans les mêmes conditions, à l'encontre d'un intermédiaire dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle; les injonctions à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin sont couvertes par la directive 2001/29/CE.

(article 11)
Injonctions
Les États membres veillent à ce que, lorsqu'une décision judiciaire a été prise constatant une atteinte à un droit de propriété intellectuelle, les autorités judiciaires compétentes puissent rendre à l'encontre du contrevenant une injonction visant à interdire la poursuite de cette atteinte. Lorsque la législation nationale le prévoit, le non- respect d'une injonction est, le cas échéant, passible d'une astreinte, destinée à en assurer l'exécution. Les États membres veillent également à ce que les titulaires de droits puissent demander une injonction à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle, sans préjudice de l'article 8, paragraphe 3, de la directive 2001/29/CE.

15. Scarlet, quant à elle, met en exergue la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information et plus particulièrement ses articles 18 et 21 :

28 -01- 2010

(article 18)
En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services n'est pas responsable des informations transmises, s'il est satisfait à chacune des conditions suivantes :
1° il n'est pas à l'origine de la transmission;
2° il ne sélectionne pas le destinataire de la transmission;
3° il ne sélectionne, ni ne modifie, les informations faisant l'objet de la transmission ;
Les activités de transmission et de fourniture d'accès visées à l'alinéa 1er englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

(article 21)
§ 1er. Pour la fourniture des services visés aux articles 18, 19 et 20, les prestataires n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.
Le principe énoncé à l'alinéa 1er ne vaut que pour les obligations à caractère général. Il n'empêche pas les autorités judiciaires compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par une loi.
§ 2. Les prestataires visés au § 1er ont l'obligation d'informer sans délai les autorités judiciaires ou administratives compétentes des activités illicites alléguées qu'exerceraient les destinataires de leurs services ou des informations illicites alléguées que ces derniers fourniraient.
Sans préjudice d'autres dispositions légales ou réglementaires, les mêmes prestataires sont tenus de communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire.

Cette loi transpose la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, de laquelle il y a lieu de retenir les considérants et dispositions suivantes :

(considérant 9)
Dans bien des cas, la libre circulation des services de la société de l'information peut refléter spécifiquement, dans la législation communautaire, un principe plus général, à savoir la liberté d'expression, consacrée par l'article 10, paragraphe 1, de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui a été ratifiée par tous les États membres. Pour cette raison, les directives couvrant la fourniture de services de la société de l'information doivent assurer que cette activité peut être exercée librement en vertu de l'article précité, sous réserve uniquement des restrictions prévues au paragraphe 2 du même article et à l'article 46, paragraphe 1, du traité. La présente directive n'entend pas porter atteinte aux règles et principes fondamentaux nationaux en matière de liberté d'expression.

(considérant 42)
Les dérogations en matière de responsabilité prévues par la présente directive ne couvrent que les cas où l'activité du prestataire de services dans le cadre de la société de

l'information est limitée au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission. Cette activité revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées.

(considérant 45)
Les limitations de responsabilité des prestataires de services intermédiaires prévues dans la présente directive sont sans préjudice de la possibilité d'actions en cessation de différents types. Ces actions en cessation peuvent notamment revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible.

(considérant 46)
Afin de bénéficier d'une limitation de responsabilité, le prestataire d'un service de la société de l'information consistant dans le stockage d'informations doit, dès qu'il prend effectivement connaissance ou conscience du caractère illicite des activités, agir promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible. Il y a lieu de procéder à leur retrait ou de rendre leur accès impossible dans le respect du principe de la liberté d'expression et des procédures établies à cet effet au niveau national. La présente directive n'affecte pas la possibilité qu'ont les États membres de définir des exigences spécifiques auxquelles il doit être satisfait promptement avant de retirer des informations ou d'en rendre l'accès impossible.

28 -01- 2010

(considérant 47)
L'interdiction pour les États membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère général. Elle ne concerne pas les obligations de surveillance applicables à un cas spécifique et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale

(article 12)
1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas

responsable des informations transmises, à condition que le prestataire:
a) ne soit pas à l'origine de la transmission;
b) ne sélectionne pas le destinataire de la transmission
et
c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.
2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.
3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

(article 15)
Absence d'obligation générale en matière de surveillance
1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.
2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

28 -01- 2010

(article 18)
Recours juridictionnels
1. Les États membres veillent à ce que les recours juridictionnels disponibles dans le droit national portant sur les activités des services de la société de l'information permettent l'adoption rapide de mesures, y compris par voie de référé, visant à mettre un terme à toute violation alléguée et à prévenir toute nouvelle atteinte aux intérêts concernés.

16. Il convient aussi de prendre en considération la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des

traitements de données à caractère personnel et les articles suivants :

(article 1.)
§ 1. Pour l'application de la présente loi, on entend par "données à caractère personnel" toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "personne concernée"; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.
§ 2. Par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

(article 5)
Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :
a) lorsque la personne concernée a indubitablement donné son consentement;
b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance;
d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
e) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées;
f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.
Le Roi peut, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, préciser les cas où la condition mentionnée sous f) est considérée ne pas être remplie.

28 -01- 2010

ainsi que la directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et plus particulièrement son article 13 qui dispose que :

> *Exceptions et limitations*
> *1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:*
> *a) la sûreté de l'État;*
> *b) la défense;*
> *c) la sécurité publique;*
> *d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;*
> *e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;*
> *f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);*
> *g) la protection de la personne concernée ou des droits et libertés d'autrui.*

17. Enfin, pour être complet, il y a lieu de retenir la loi du 13 juin 2005 relative aux communications électroniques qui dispose que :

> (article 124)
> *S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut:*
> *1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement;*
> *2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;*
> *3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne;*
> *4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non.*

et l'article 5 § 1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques qui prévoit que :

> *Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.*

ainsi que la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques de laquelle il faut extraire les articles suivants :

> (article 2)
> *Les définitions suivantes sont aussi applicables:*
> *[...]*
> *b) 'données relatives au trafic': toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;*
> *[...]*
> *d) 'communication': toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.*
>
> (article 5)
> *1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En*

28 -01- 2010

particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

(article 15)
Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

28 -01- 2010

b.- Position de la Sabam

18. Au regard des dispositions, tant de droit interne que de droit communautaire, rappelées ci-dessus, les moyens de la Sabam peuvent être résumés comme suit :

    1. Tant la loi belge que le droit communautaire prévoient une injonction de cessation à l'encontre des intermédiaires tels que Scarlet dont les services sont utilisés par les internautes pour commettre des atteintes au droit d'auteur, sans qu'il soit nécessaire de mettre en cause les contrefacteurs eux-mêmes ni, a fortiori, d'agir préalablement contre ces derniers.

    2. Sous l'empire de la loi belge sur le droit d'auteur (article 87, par.1er), l'injonction de cessation revêt un caractère

obligatoire et inconditionnel: le juge est obligé, lorsqu'il constate l'existence d'une atteinte, d'en ordonner la cessation ; seul l'abus de droit peut justifier que l'ordre soit refusé.

L'ordre de cessation est impératif et inconditionnel qu'il soit prononcé à l'encontre du contrevenant lui-même ou de l'intermédiaire dont les services sont utilisés pour commettre la contrefaçon.

Les directives 2001/29 et 2004/48 n'affectent nullement le caractère impératif et inconditionnel de l'ordre de cessation régi par la loi belge. Inversement, le caractère impératif et inconditionnel de l'ordre en droit belge n'empêche pas le juge de prendre en compte le critère de proportionnalité dans le cadre de l'examen d'un abus de droit éventuel, conformément aux principes généraux de droit national et de droit communautaire.

Dès lors que la loi a fait de l'ordre une mesure impérative et inconditionnelle, il n'appartient plus au juge de dire le contraire au motif qu'il ne constituerait soi-disant pas une mesure efficace et dissuasive. Le juge conserve le pouvoir de prendre en compte le défaut de toute efficacité et de tout caractère dissuasif dans l'examen d'un abus de droit éventuel. Cependant, en l'espèce, on ne saurait raisonnablement prétendre que l'ordre serait dénué de tout caractère efficace et dissuasif. Il est en effet incontestablement de nature à assurer un niveau de protection adéquat du droit d'auteur dès lors qu'il vise l'intégralité du répertoire musical de la Sabam et le canal spécifique par lequel les violations sont commises de manière massive (les échanges peer-to-peer non autorisés sur le réseau de Scarlet). L'ordre ne se voit pas privé de toute efficacité et de tout caractère dissuasif sous prétexte qu'on ne pourrait exclure l'hypothèse que, dans le futur, la partie condamnée se retrouve dans l'impossibilité d'empêcher une partie des échanges non autorisés.

La seule exception à la règle du caractère obligatoire et inconditionnel de l'ordre de cessation est le cas de l'abus de droit. Les conditions d'application de cette exception – qui correspondent au principe général de proportionnalité en droit communautaire – sont très strictes et Scarlet qui supporte la charge de la preuve de l'abus de droit ne démontre pas qu'elles seraient remplies. Aucun des arguments avancés par Scarlet ne permet de dire que le préjudice que lui causerait prétendument le respect de l'injonction serait considérablement plus grand que le bénéfice qu'en retirerait la Sabam, ce bénéfice étant

constitué de la cessation du dommage que lui cause le nombre étourdissant de fichiers musicaux continuellement échangés sur le réseau de Scarlet. L'ordre de cessation n'est contraire à aucune des dispositions légales mentionnées par Scarlet, contrairement à ce que celle-ci argumente. Par ailleurs, même si la Sabam disposait d'autres moyens de protection équivalents (ce qui n'est pas le cas), cette circonstance ne rendrait pas l'ordre abusif pour autant. De même, l'ordre n'est pas manifestement disproportionné au regard de l'intérêt qu'a la Sabam à l'obtenir, sous prétexte qu'on ne pourrait exclure qu'à l'avenir la partie condamnée se retrouve dans l'impossibilité d'empêcher certains des échanges non autorisés ou qu'il contraindrait soi-disant à empêcher certains échanges licites ou qu'il causerait des charges financières prétendument excessives.

3. La finalité de l'action en cessation est à la fois de mettre fin à des atteintes existantes et de prévenir des atteintes futures. L'ordre de cessation permet de protéger l'intégralité d'un répertoire à l'égard de la menace d'atteintes futures. Dès lors que l'ordre de cessation remplit une fonction préventive et que les échanges non autorisés peuvent être réalisés à tout moment par n'importe quel internaute potentiel via n'importe quel logiciel peer-to-peer, il n'aurait aucun sens de limiter l'ordre aux seuls échanges pratiqués par certains internautes déterminés ou via certains logiciels ou protocoles peer-to-peer déterminés.

4. Scarlet prétend qu'il lui serait soi-disant impossible de se conformer à l'injonction. Il appartient à Scarlet de démontrer l'impossibilité qu'elle prétend, d'autant que le législateur part du principe qu'elle est précisément la plus à même d'empêcher la contrefaçon, qu'une décision judicaire d'octobre 2008 coulée en force de chose jugée a déjà constaté qu'elle ne prouvait pas l'impossibilité et qu'elle est la partie la plus apte à fournir la preuve.

En outre, Scarlet doit démontrer que l'impossibilité qu'elle prétend est totale et définitive, car une simple impossibilité temporaire ou partielle ne suffit pas à faire obstacle à l'ordre de cessation.

5. Scarlet prétend à tort que l'ordre de cessation violerait les règles en matière de vie privée et de télécommunications. Tant la législation en matière de vie privée que la jurisprudence de la C.J.C.E en matière de télécommunications établissent clairement le principe selon lequel le droit à la vie privée peut connaître des restrictions justifiées par la nécessité de protéger les droits et libertés d'autrui. La loi belge sur le droit d'auteur offre elle-même

une base légale qui permet de limiter le droit à la vie privée des internautes dans la mesure où elle prévoit expressément la possibilité de s'adresser aux fournisseurs de services Internet afin de mettre fin aux atteintes commises par les internautes. Scarlet ne peut reprocher au législateur de n'avoir pas réglé lui-même dans le détail l'étendue de la restriction du droit à la vie privée, car c'est la tâche du juge. C'est à Scarlet de prouver que l'ordre de cessation l'obligerait soi-disant à violer les dispositions légales en matière de vie privée ou de secret des télécommunications. Le juge du droit d'auteur a l'obligation d'interpréter les règles relatives à la vie privée et aux télécommunications. Scarlet n'identifie pas le traitement de données à caractère personnel auquel elle devrait prétendument recourir afin de se conformer à l'ordre de cessation. L'ordre de cessation n'exige nullement l'identification des personnes concernées par les transmissions illicites. L'opération de filtrage n'impose pas à Scarlet le traitement d'adresses IP, mais se limite à empêcher la transmission de certaines informations par la délivrance de messages "time-out" indiquant l'impossibilité de procéder à la transmission. Dans la présente affaire, les adresses IP ne peuvent par ailleurs pas être qualifiées de données à caractère personnel puisqu'elles ne permettent pas d'identifier les utilisateurs des appareils auxquels se rapportent les adresses IP. Même à considérer que l'ordre de cessation imposerait le traitement de données à caractère personnel, celui-ci serait admissible en vertu de la loi belge sur la protection de la vie privée puisque nécessaire au respect par Scarlet d'une obligation légale, à savoir l'exécution d'un ordre judiciaire. Par ailleurs, à supposer même que les adresses IP soient à considérer comme des données judicaires (quod non) et qu'elles fassent l'objet d'un traitement (quod non), ce soi-disant « traitement » servirait un intérêt légitime.

28 -01- 2010

6. Scarlet ne prouve pas que l'ordre de cessation impliquerait une violation du secret des communications électroniques. En vertu des principes fondamentaux du droit pénal, des faits en principe punissables ne constituent pas des infractions pénales dans la mesure où ils sont ordonnés par la loi. Ceci est confirmé par la législation en matière de communications électroniques. La disposition légale selon laquelle l'emploi de la cryptographie est libre est dépourvue de toute incidence en l'espèce, de même que la disposition légale prévoyant que le Gouvernement est l'autorité en charge de la détermination des exigences techniques en matière d'équipements permettant de réaliser des communications électroniques.

7. En tout état de cause, conformément à la jurisprudence de la

CJCE, même dans l'hypothèse où l'ordre de cessation impliquerait une violation des règles en matière de vie privée ou de secret des communications, celui-ci ne pourrait être refusé que si Scarlet prouve que la violation en question est disproportionnée, ce qu'elle reste en défaut de faire.

8. L'ordre de cessation est parfaitement conforme à la législation sur le commerce électronique qui prévoit expressément la possibilité pour le juge de prononcer des injonctions à l'encontre des intermédiaires, notamment les fournisseurs d'accès à l'Internet. Il est vrai que cette législation prévoit par ailleurs un privilège de non-responsabilité au profit de ces intermédiaires, mais tant la directive 2000/31 que la directive 2001/29 confirment que ce privilège n'affecte en rien la possibilité d'actions en cessation, qui est totalement indépendante de la question de la responsabilité éventuelle des intermédiaires. La règle selon laquelle les intermédiaires ne peuvent se voir imposer une obligation générale de surveillance ne peut limiter en aucune manière la liberté du juge de prononcer un ordre de cessation destiné à prévenir toute nouvelle atteinte aux intérêts concernés. Un tel ordre n'implique pas une obligation générale de surveillance. Il est faux de prétendre que le respect de l'ordre de cessation entraînerait une perte du privilège de responsabilité.

9. Scarlet invoque encore la hauteur des coûts qu'elle subirait si elle devait se conformer à l'ordre de cessation. Les coûts d'exécution d'une décision judiciaire ne peuvent cependant ni constituer une cause d'impossibilité d'exécution de cette décision, ni empêcher le juge de prononcer la décision en question. Il serait par ailleurs contraire à la loi d'imputer ces coûts à la Sabam, comme le réclame Scarlet.

c.- Position de Scarlet et de l'ISPA

19. Scarlet et l'ISPA (qui déclarent reprendre par ailleurs à leur compte les moyens développés à titre subsidiaire par Belgacom, pour autant qu'elles ne les soulèvent pas elles-mêmes) soutiennent quant à elles que :

    1. Il existe une multitude de systèmes fonctionnant selon le modèle « peer-to-peer ». Ce modèle est en effet utilisé pour de multiples applications. La téléphonie par Internet, le *chat*, la diffusion d'émissions radio, la distribution de logiciels et l'échange de fichiers entre internautes n'en sont que quelques exemples parmi d'autres. Très souvent, un

même logiciel « peer-to-peer » sera en outre utilisé pour plusieurs de ces applications. Il n'existe donc pas un mais plusieurs phénomènes « peer-to-peer ».

Le « peer-to-peer » est par ailleurs caractérisé par une faculté d'adaptation hors du commun. Cela explique pourquoi toute tentative de blocage ou de filtrage est, au mieux, vouée à l'échec à très court terme. Il existe à l'heure actuelle plusieurs logiciels « peer-to-peer » très répandus qui (i) fonctionnent de manière décentralisée; (ii) garantissent l'anonymat des pairs ou (iii) prévoient l'encryptage des fichiers échangés ce qui rend impossible la vérification de leur contenu par des tiers.

Tout dispositif de blocage ou de filtrage du trafic « peer to peer » suppose nécessairement une surveillance généralisée/ « écoute » préalable de toutes les communications passant sur le réseau. La mise en œuvre de tels dispositifs se heurte en outre à de nombreux obstacles pratiques (problèmes de capacité, impact sur le réseau, ...).

Enfin, au moins l'efficacité, mais également la pérennité de ces systèmes n'est pas du tout prouvée. Des experts *et* des fournisseurs de solutions s'accordent sur le fait que toute tentative de filtrage est nécessairement vouée à l'échec suite à l'avènement de logiciels 'peer-to-peer' de la troisième génération qui ont recours à la technologie de l'encryptage. Les tentatives d'emploi de technologies de filtrage ou de blocage par certains autres prestataires et sur base volontaire ne changent rien à ce constat.

28 -01- 2010

2. Le jugement a quo impose de facto une obligation générale de surveillance des communications sur le réseau de Scarlet. Le fait que cette obligation soit mise en œuvre de manière (partiellement) automatisée n'y change rien.
   Cette obligation générale de surveillance est contraire à l'article 21 de la LCE et met en péril le délicat équilibre mis en place par les législateurs belges et communautaires. La loi ne permet l'imposition d'une obligation de surveillance générale à un prestataire intermédiaire que pour autant que cette obligation soit (i) temporaire ; (ii) spécifique; (iii) prévue par la loi et (iv) clairement définie. L'obligation générale de surveillance imposée par le jugement *a quo* ne répond à aucune de ces exigences.

3. L'ordre de cessation est incompatible avec l'article 18 de la LCE puisqu'il fait supporter à Scarlet les conséquences des atteintes au droit d'auteur commises par ses clients et, ce faisant, la rend de facto responsable de celles-ci.

4. Le juge a quo a outrepassé les compétences que lui confèrent l'ancien article 87 §1 LDA en imposant un ordre de cessation à Scarlet alors que cette dernière n'est pas l'auteur des infractions litigieuses. La référence à l'article 8.3 de la Directive 2001/29 n'y change rien dès lors que cette disposition n'autorise que les mesures provisoires alors que l'action en cessation est une procédure au fond. Pour les mêmes raisons le nouvel article 87 §1 LDA viole le droit communautaire et ne justifie pas les actions au fond contre des intermédiaires.

5. Dans le contexte d'une action en cessation dirigée contre un tiers, il appartient au juge des cessations d'analyser s'il est possible, opportun, raisonnable et proportionné d'exiger une contribution de ce tiers nonobstant le fait que celui-ci n'est pas l'auteur de la contrefaçon.

   Il n'est en l'espèce pas opportun, raisonnable et proportionné d'imposer un ordre de cessation à Scarlet dès lors que :

   - l'ordre de cessation impose à Scarlet une charge opérationnelle et financière considérable liée à des activités illégales dont elle n'est pas responsable *alors que* le succès des mesures à prendre n'est même pas garanti puisque l'efficacité et la pérennité des dispositifs de blocage ou de filtrage est plus que douteuse.
   - le strict respect de l'ordre de cessation est matériellement impossible ou à tout le moins impossible : (i) sans se mettre en porte-à-faux par rapport à diverses obligations légales qui incombent à Scarlet ; et/ou (ii) sans rendre impossible toute une série d'utilisations parfaitement légitimes des logiciels « peer-to-peer » et dès lors pénaliser bon nombre d'internautes qui n'ont rien à se reprocher.
   - la Sabam dispose d'autres moyens plus proportionnés pour atteindre ses objectifs.

6. La mise en place d'un système de filtrage ou de blocage de transfert de fichiers sur les réseaux *peer to peer* porte atteinte aux dispositions légales et communautaires sur la protection des données à caractère personnel et le secret des communications, dès lors qu'il implique le traitement des adresses *IP* qui sont des données personnelles. En effet, l'adresse IP est un format d'adresse numérique, comparable à un numéro de téléphone, qui permet aux appareils connectés au réseau, tels que des serveurs Web, des serveurs de courrier électronique ou des ordinateurs personnels, de communiquer sur l'Internet. Lorsqu'un utilisateur consulte

une page, l'adresse de l'ordinateur appelant est communiquée à l'ordinateur dans lequel la page est stockée, de sorte que les données peuvent être transférées d'un ordinateur à l'autre par le biais de l'Internet (Conclusions de l'Avocat Général. J. KOKOTT, 18 juillet 2007, Aff. C-275/06, Promusicae v. Telefónica de España SAU, www.curia.eu, cons. 30).

La Commission de la protection de la vie privée a également rappelé que les adresses *IP* des utilisateurs est une donnée à caractère personnel qui ne peut faire l'objet d'aucun traitement, sauf les exceptions prévues par la loi.

7. Le traitement des adresses *IP* pour les fins de filtrage ou de blocage manque de base légale.

   Il n'est en effet pas possible, dans le cas d'espèce, de recourir ni à l'article 5 b) de la loi du 8 décembre 1992 ni à l'article 5 f).

   Par ailleurs, il est interdit de traiter des données à caractère personnel relatives à des suspicions ou à des poursuites ayant trait à des infractions. Pour être légale, la surveillance des communications électroniques doit être limitée à des situations spécifiques, fondées sur les suspicions sérieuses d'infractions aux droits d'auteur, de préférence commerciale et non purement domestiques.

8. Le traitement d'adresses *IP* à des fins de blocage ou de filtrage contrevient en outre aux règles régissant le secret des communications.

   En effet, le filtrage des communications constitue une violation du droit à la vie privée et au secret des correspondances et manque de base légale.

28 -01- 2010

c.- Appréciation de la cour

20. Avant de vérifier si un mécanisme de filtrage et de blocage des fichiers *peer to peer* existe et peut être efficace, il convient de s'assurer que l'article 87 § 1er de la LDA, tel qu'il est interprété par la Sabam est conforme au droit communautaire, eu égard aux critiques formulées par Scarlet.

   Dans l'affaire *Promusicae* (C-275/06), qui voyait s'opposer une association regroupant des producteurs et des éditeurs d'enregistrements musicaux à un FAI, et où il était demandé à cet

FAI de révéler l'identité et l'adresse physique des personnes qui utilisaient des logiciels *peer to peer*, et ce afin de pouvoir engager des procédures civiles contre les intéressés, la CJCE a, dans son arrêt du 29 janvier 2008, répondu, en ces termes à une question préjudicielle qui demandait, en substance, si le droit communautaire et spécialement les directives 2000/31, 2001/29 et 2004/48, lues aussi à la lumière des articles 17 ainsi que 47 de la charte, devaient être interprétés en ce sens qu'ils imposent aux États membres de prévoir, en vue d'assurer la protection effective du droit d'auteur, l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile :

> *Les directives 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle, et 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), 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. Toutefois, le droit communautaire exige desdits États que, lors de la transposition de ces directives, ils veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, lors de la mise en œuvre des mesures de transposition desdites directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à ces mêmes directives, mais également de ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.*

Eu égard aux moyens développés par les parties, la même nécessité de la conciliation nécessaire des exigences liées à la protection de différents droits fondamentaux se pose dans la présente cause, à la différence que, dans le cas d'espèce, l'ingérence dans la vie privée interviendrait *a priori* en vue d'éviter une atteinte à un droit de propriété intellectuelle et pas *a posteriori*, comme ce fut le cas dans

l'affaire *Promusicae* en vue d'obtenir une indemnisation suite à une violation avérée de ce même droit. De plus, dans l'affaire *Promusicae*, le débat concernait une demande adressée à un FAI de révéler l'identité et l'adresse physique de certaines personnes auxquelles il fournit un service d'accès à l'Internet et dont l'adresse *IP* ainsi que la date et l'heure de connexion étaient connues, alors que dans la présente cause, il s'agit de mettre en place un système préventif de blocage et de filtrage de fichiers électroniques envoyés par un internaute à un autre, par l'intermédiaire d'un ou de plusieurs FAI.

Les enseignements que contient l'arrêt *Promusicae* ne sont donc pas suffisants pour permettre à la cour de statuer, comme le demande les parties, sur la compatibilité avec le droit communautaire de l'article 87 § 1er de la LDA, tel qu'il est interprété par la Sabam, et de vérifier s'il constitue une transposition adéquate de ces directives.

Il convient dès lors de poser à la CJUE les questions préjudicielles reprises au dispositif du présent arrêt.

3.- Sur les autres demandes et exceptions

21. Dans l'attente de l'arrêt de la CJUE, il y a lieu de surseoir à statuer sur les autres demandes, moyens et exceptions développés par les parties.

28 -01- 2010

V.- DISPOSITIF

Pour ces motifs, la cour,

1. **Dit la demande en déclaration d'arrêt commun dirigée contre Belgacom irrecevable et en déboute la Sabam.**

   Délaisse à la Sabam ses frais de citation en intervention forcée et dit la demande de Belgacom en paiement d'une indemnité de procédure non fondée.

2. **Dit les demandes en intervention volontaire conservatoire de la BFV, de l'IFPI et de l'ISPA recevables.**

3. **Avant dire droit et en application de l'article 234 du Traité instituant l'Union européenne, décide de poser à la Cour de justice de l'Union européenne les questions préjudicielles suivantes :**

1. ***Les directives 2001/29 et 2004/48, lues en combinaison avec les directives 95/46, 2000/31 et 2002/58, interprétées notamment au regard des articles 8 et 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, permettent-elles aux Etats membres d'autoriser un juge national, saisi dans le cadre d'une procédure au fond et sur la base de la seule disposition légale prévoyant que :*** « Ils [le juge national] peuvent également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin », ***à ordonner à un Fournisseur d'Accès à l'Internet (en abrégé FAI) de mettre en place, à l'égard de toute sa clientèle, in abstracto et à titre préventif, aux frais exclusifs de ce FAI et sans limitation dans le temps, un système de filtrage de toutes les communications électroniques, tant entrantes que sortantes, transitant par ses services, notamment par l'emploi de logiciels peer to peer, en vue d'identifier sur son réseau la circulation de fichiers électroniques contenant une œuvre musicale, cinématographique ou audio-visuelle sur laquelle le demandeur prétend détenir des droits et ensuite de bloquer le transfert de ceux-ci, soit au niveau de la requête soit à l'occasion de l'envoi ?***

2. ***En cas de réponse positive à la question sub.1., ces directives imposent-elles au juge national, appelé à statuer sur une demande d'injonction à l'égard d'un intermédiaire dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur, d'appliquer le principe de proportionnalité lorsqu'il est amené à se prononcer sur l'efficacité et l'effet dissuasif de la mesure demandée ?***

28 -01- 2010

4. Réserve les dépens.

Cet arrêt a été rendu par la 9ème chambre de la cour d'appel de Bruxelles, composée de M. Henry MACKELBERT, conseiller, président f.f. de la chambre et de Mmes Marie-Françoise CARLIER, conseiller et Marielle MORIS, conseiller, qui ont assisté à toutes les audiences et ont délibéré à propos de l'affaire.

Il a été prononcé en audience publique par M. Henry MACKELBERT, président f.f. de la chambre, assisté de Mme Patricia DELGUSTE, greffier, le 28 -01- 2010

P. DELGUSTE M. MORIS M.-F. CARLIER H. MACKELBERT