IRIS plus

# Les données à caractère personnel sont-elles vraiment privées ?

2013-6

ARTICLE DE FOND

## Droit d'auteur et droit applicable à la protection des données à caractère personnel

**Les intermédiaires pris dans la zone de conflit entre ces deux domaines juridiques**

- Fondements juridiques au niveau européen
- Les zones de conflit dans la pratique

REPORTAGES

## Jurisprudence récente

- Allemagne
- Finlande
- France
- Royaume Uni
- Pays-Bas
- Fédération de Russie

ZOOM

## Le Patriot Act et le quatrième amendement

**Comment le Gouvernement américain étend secrètement son autorité pour s'engager dans la collecte des données personnelles de ses citoyens**

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**IRIS *plus* 2013-6**
**Les données à caractère personnel sont-elles vraiment privées ?**

ISBN (Version imprimée) : 978-92-871-7790-2
Prix : EUR 25,50
Observatoire européen de l'audiovisuel, Strasbourg 2013

ISBN (Version électronique PDF) : 978-92-871-7793-3
Prix : EUR 34,50

**La série IRIS *plus* 2013**
ISSN (Version imprimée) : 2078-9459
Prix : EUR 100

ISSN (Version électronique PDF) : 2079-1070
Prix : EUR 130

**Directeur de la publication :**
Susanne Nikoltchev, Directrice exécutive de l'Observatoire européen de l'audiovisuel
E-mail : susanne.nikoltchev@coe.int

**Éditrice et coordonnatrice :**
Susanne Nikoltchev

**Assistante éditoriale :**
Michelle Ganter
E-mail : michelle.ganter@coe.int

**Marketing :**
Markus Booms
E-mail : markus.booms@coe.int

**Photocomposition :**
Pointillés, Hoenheim (France)

**Impression :**
Pointillés, Hoenheim (France)
Conseil de l'Europe, Strasbourg (France)

**Maquette de couverture :**
Acom Europe, Paris (France)

**Éditeur :**
Observatoire européen de l'audiovisuel
76 Allée de la Robertsau
F-67000 Strasbourg
Tél. : +33 (0)3 90 21 60 00
Fax : +33 (0)3 90 21 60 19
E-mail : obs@obs.coe.int
www.obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**Organisations partenaires ayant contribué à l'ouvrage :**

**Institut du droit européen des médias (EMR)**
Franz-Mai-Straße 6
D-66121 Saarbrücken
Tél. : +49 (0) 681 99 275 11
Fax : +49 (0) 681 99 275 12
E-mail : emr@emr-sb.de
www.emr-sb.de

**Institut du droit de l'information (IViR)**
Kloveniersburgwal 48
NL-1012 CX Amsterdam
Tél. : +31 (0) 20 525 34 06
Fax : +31 (0) 20 525 30 33
E-mail : website@ivir.nl
www.ivir.nl

**Centre de droit et de politique des médias de Moscou**
Moscow State University
ul. Mokhovaya, 9 - Room 338
125009 Moscow
Fédération russe
Tél. : +7 495 629 3804
Fax : +7 495 629 3804
www.medialaw.ru

***Veuillez citer cette publication comme suit :***
IRIS *plus* 2013-6, Les données à caractère personnel sont-elles vraiment privées ?,
Susanne Nikoltchev (Ed.), Observatoire européen de l'audiovisuel, Strasbourg 2013

IRIS plus
2013-6 p.1

# Les données à caractère personnel sont-elles vraiment privées ?

# Avant-propos

En 2010, Mark Zuckerberg, co-fondateur et PDG de Facebook, déclarait : « Les gens sont désormais parfaitement à l'aise non seulement à l'idée d'échanger une multitude d'informations diverses, mais aussi de le faire plus ouvertement et avec davantage de monde. Cette norme sociale est un phénomène qui a tout simplement évolué au fil du temps. » En effet, beaucoup de choses semblent avoir changé depuis l'apparition de l'internet, notamment la façon dont les informations sont mises à la disposition du public. Parallèlement, de nouvelles attentes ont émergé concernant ce qui devrait être librement accessible à tous. Certains affirment même que ces changements devraient être relayés par la législation.

Il est clair que la législation suit l'évolution de la société à un rythme plus lent, de sorte qu'elle semble souvent décalée par rapport à des attitudes et des comportements qui se sont généralisés. Mais cela signifie-t-il pour autant que la législation doit toujours se conformer aux normes sociales ? Même si un courant majoritaire semble de cet avis, il n'en reste pas moins que la loi procède de la recherche d'un juste équilibre entre les différents droits et intérêts (y compris ceux des groupes minoritaires), qui doivent être scrupuleusement pondérés et mis en balance les uns par rapport aux autres. D'ailleurs, qui décide de ce qui est une norme sociale ? Certainement pas M. Zuckerberg à lui seul...

D'un point de vue général, on peut dire que la vie privée est le droit d'une personne de ne pas rendre publics certains renseignements personnels la concernant. Que ce droit soit applicable ou non dans un environnement en ligne est un sujet de préoccupation pour beaucoup de gens, et pas seulement pour les utilisateurs de Facebook. L'activité de chaque internaute en ligne laisse une trace numérique qui fournit des indices sur sa vie. Ces indices peuvent être collectés et utilisés par des tiers de façons diverses et rentables. Ces informations ont parfois été fournies par l'internaute volontairement, d'autres fois par inadvertance. Mais dans certains cas, des tiers requièrent un accès à l'intimité d'un internaute qui va bien au-delà de ce que l'internaute est prêt à accepter. Deux exemples de ce genre ont suscité dernièrement beaucoup d'attention. Le premier concerne les titulaires de droits qui cherchent à se renseigner sur l'identité et les coordonnées des internautes en vue de les poursuivre en justice pour violation de droit d'auteur. Le second met en cause les écoutes des agences de renseignement nationales dans le but de protéger leurs concitoyens contre des activités terroristes ou criminelles. Dans les deux cas, le fait que ces tiers ont besoin de ces données ne signifie pas qu'ils soient légalement autorisés à en disposer.

Ce numéro d'IRIS *plus* analyse les limites de la vie privée et ses liens avec d'autres droits fondamentaux. L'article de fond traite des relations quelque peu tendues entre le droit d'auteur et la protection des données personnelles. La section Reportages présente la jurisprudence récente en rapport avec les questions soulevées par l'article de fond. Enfin, la section Zoom revient sur le récent scandale provoqué par la publication dans la presse de fuites concernant les programmes de surveillance menés clandestinement par les agences américaines.

Strasbourg, novembre 2013.

**Susanne Nikoltchev**
*Directrice exécutive*
*Observatoire européen de l'audiovisuel*

# TABLE DES MATIÈRES

## ARTICLE DE FOND



## REPORTAGES

## ZOOM

IRIS plus
2013-6 p.7

# Droit d'auteur et droit applicable à la protection des données à caractère personnel

## *Les intermédiaires pris dans la zone de conflit entre ces deux domaines juridiques*

*Martin Rupp et Peter Matzneller,*
*Institut du droit européen des médias (EMR), Sarrebruck/Bruxelles*

## I. Introduction

La relation entre le droit d'auteur et la protection des données est de nature conflictuelle. Ceci s'explique en premier lieu par le fait que ces deux dispositifs juridiques reposent sur un concept virtuellement contradictoire. Il existe un conflit d'objectif entre le droit d'auteur et le droit de la protection des données. Or, ce conflit n'apparaît pas, à première vue, lors de l'examen comparatif des intentions respectives du législateur.

Le *droit d'auteur* protège la propriété intellectuelle de l'auteur d'un point de vue immatériel, mais aussi et surtout, d'un point de vue matériel. Les dispositions concernant le contenu, la portée, la transférabilité, les conséquences d'une violation du droit d'auteur et l'application des prérogatives découlant du droit d'auteur visent à permettre à l'auteur d'exploiter économiquement son travail.

Le *droit de la protection des données*, en revanche, donne à chacun la possibilité de décider fondamentalement de la communication et de l'utilisation des informations personnelles le concernant.

De prime abord, on ne voit pas forcément en quoi la « coexistence pacifique » des deux dispositifs juridiques peut s'avérer problématique. Pourtant, un conflit d'objectif apparaît dès lors qu'un ayant droit entend poursuivre les auteurs d'une violation de ses droits. En ce cas, l'ayant droit s'efforce de faire valoir ses droits découlant du droit d'auteur à l'encontre du contrevenant. Cette procédure peut porter sur une injonction en abstention, des dommages et intérêts, la destruction d'une copie ou toute autre requête. Pour faire valoir ses droits, l'ayant droit doit tout d'abord identifier le contrevenant. En vue de cette identification, le droit d'auteur confère à l'ayant droit des droits spécifiques pour obtenir des renseignements - droits qu'il peut également faire valoir contre des tiers.

C'est justement sur ce point que le droit de la protection des données et le droit d'auteur entrent en conflit. Le droit de la protection des données fixe des limites au « flux illimité de renseignements ». Le contrevenant au droit d'auteur - ou même simplement l'auteur potentiel d'un délit - jouit des droits que lui garantit la loi relative à la protection des données pour protéger son autodétermination informationnelle. Le système juridique a donc pour tâche de réglementer

cette zone sensible. D'une part, l'ayant droit a besoin de certaines informations pour faire valoir ses droits de façon efficace. D'autre part, la législation en matière de protection des données exige d'endiguer tout débordement de ces informations. C'est sur ce lien antagonique que se penche la présente contribution.

Pour étudier ces liens conflictuels, nous présenterons tout d'abord les sources juridiques en matière de droit d'auteur et de protection des données de l'Union européenne et du Conseil de l'Europe. Ces outils trouvent leur fondement dans les traités fondateurs[1] de l'Union européenne et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[2] (CEDH) du Conseil de l'Europe, dans lesquels sont définis les libertés fondamentales et les droits des citoyens. Toutefois, nous porterons une attention toute particulière à la conception du droit dérivé du droit d'auteur et de la protection des données. Ces deux domaines juridiques ont été marqués de façon significative par diverses directives de l'Union européenne.

Nous examinerons ensuite certaines zones de conflit spécifiques. Quelques exemples récents, issus notamment de la jurisprudence de la Cour de justice de l'Union européenne (CJUE), illustrent concrètement la problématique étudiée et les conflits d'intérêts. Un aperçu des différents systèmes juridiques nationaux nous permettra de mettre en lumière les modèles alternatifs d'une application du droit d'auteur qui « préserve les données ».

## II. Fondements juridiques au niveau européen

Les fondements juridiques au niveau européen sont ancrés essentiellement dans le droit de l'Union européenne. Des dispositions importantes figurent également dans les instruments juridiques du Conseil de l'Europe.

### 1. Aspects juridiques fondamentaux

*1.1. Charte des droits fondamentaux de l'Union européenne*

Concernant la zone de conflit entre les intérêts du droit d'auteur et la protection des données, la Charte des droits fondamentaux de l'Union européenne[3] joue un rôle particulièrement important.

Dans la situation présente, le droit d'auteur et l'ayant droit sont toujours protégés par le droit de propriété visé à l'article 17 de la Charte européenne des droits fondamentaux, dont le paragraphe 2 protège expressément la propriété intellectuelle. Cet article est en opposition avec l'article 8 de la Charte européenne des droits fondamentaux qui établit la protection des données personnelles comme un droit fondamental. Dans certains cas, il faut également faire intervenir la liberté professionnelle et la liberté d'entreprise, conformément aux articles 15 et 16 de la Charte. Dès lors qu'on a recours à des systèmes de filtres pour empêcher la violation du droit d'auteur, la liberté d'information visée à l'article 11 de la Charte se trouve mise en cause[4]. En cas de conflit, la Cour de justice de l'Union européenne procède souvent à la pondération des intérêts en jeu en vue de concilier les intérêts contradictoires.

1) Il s'agit en particulier du Traité sur l'Union européenne dans sa version modifiée par le Traité de Lisbonne (TUE) du 13 décembre 2007 ( JO 2007/ C 306, p. 1, et JO 2008/C 111, p. 56, JO 2009/C 290 p. 1, JO 2011/C 378, p. 3) et le Traité sur le fonctionnement de l'Union européenne (TFUE), dans sa version publiée le 9 mai 2008 ( JO 2008/ C 115, p. 47)).
2) Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, UNTS volume 213, p. 221.
3) Charte des droits fondamentaux de l'Union européenne du 12 décembre 2007, JO n° C 303 p. 1.
4) Voir Angelopoulos C, Filtrage des contenus protégés par le droit d'auteur sur Internet en Europe, IRIS *plus* 2009-4, Observatoire européen de l'audiovisuel, Strasbourg 2009.

*1.2. Convention de sauvegarde des droits de l'homme et des libertés fondamentales*

D'autre part, la protection des données ainsi que la protection des droits d'auteur sont également des droits reconnus dans les normes juridiques adoptées par le Conseil de l'Europe. L'article 8 de la CEDH garantit le droit au respect de la vie privée et familiale. L'article 1 du premier protocole additionnel à la CEDH prévoit la protection de la propriété. Si l'on considère la diffusion d'œuvres protégées par le droit d'auteur du point de vue de la diffusion d'informations et d'opinions, il faut également tenir compte de l'article 10 de la CEDH garantissant le droit à la liberté d'expression et d'information[5]. La Cour européenne des droits de l'homme rappelle qu'en cas de conflit d'objectifs entre le droit d'auteur et d'autres intérêts, une pondération est nécessaire.

Dans le cadre de sa jurisprudence, la Cour européenne des droits de l'homme n'a traité que rarement ce conflit spécifique entre droit d'auteur et vie privée. La jurisprudence « classique » de la Cour relative au droit des médias porte sur le conflit entre l'article 8 et l'article 10 de la CEDH. Il s'agit le plus souvent de cas où la couverture médiatique porte atteinte à la vie privée d'un individu. Le droit d'auteur a été pour l'instant relativement « peu affecté » par la jurisprudence de la Cour européenne des droits de l'homme. Deux arrêts récents ont retenu l'attention. Il s'agit, tout d'abord, de l'affaire *Ashby Donald et autres c. France*[6], dans laquelle le droit d'auteur est entré en conflit avec l'article 10 de la CEDH. En l'espèce, des photographes avaient publié des photos de défilés de mode protégées par le droit d'auteur sans le consentement des maisons de couture. Les juridictions nationales françaises ont condamné les photographes à des amendes et dommages-intérêts pour violation du droit d'auteur. La Cour européenne des droits de l'homme a confirmé la primauté du droit d'auteur dans cette situation. Elle a établi que les amendes et les dommages-intérêts n'étaient pas excessifs et que la décision de la juridiction nationale pouvait être considérée comme une pondération raisonnable des intérêts contradictoires.

En ce qui concerne le rôle des intermédiaires, l'arrêt du 19 février 2013 de la Cour européenne des droits de l'homme dans l'affaire *Neij et Sunde Kolmisoppi c. Suède*[7] revêt un intérêt particulier. Les requérants étaient des développeurs et représentants de The Pirate Bay, l'un des plus grands services de partage de fichiers du monde sur internet (« BitTorrent Tracker »)[8]. Bien que l'échange de fichiers n'ait pas eu lieu sur le serveur du fournisseur de services, ils ont été condamnés dans le cadre d'une procédure nationale devant les tribunaux suédois pour complicité d'infraction à la loi relative au droit d'auteur à une peine de huit et dix mois d'emprisonnement et 5 millions d'euros de dommages-intérêts.

La Cour a estimé que le service The Pirate Bay relevait de la protection de l'article 10 de la CEDH et que, par conséquent, le jugement des tribunaux suédois constituait une ingérence dans le droit à la liberté d'expression. Après quoi, l'élément déterminant consistait donc à établir si cette ingérence était « nécessaire dans une société démocratique », selon la formulation de l'article 10, paragraphe 2 de la CEDH. La Cour a conclu que c'était le cas et qu'il n'y a pas eu violation de l'article 10 de la Convention. En raison de l'intérêt majeur du Gouvernement suédois à protéger la propriété relevant du droit d'auteur, on ne saurait contester que les services fournis par The Pirate Bay soient considérés comme passibles de sanctions tout en engageant la responsabilité des prestataires en qualité de complices. A cet égard, la Cour a tenu compte du fait que les opérateurs avaient refusé de façon réitérée de supprimer les fichiers torrent alors qu'ils y avaient été invités à plusieurs reprises.

5) Conformément à l'article 11 de la Charte des droits fondamentaux de l'Union européenne.
6) Arrêt du 10 janvier 2013, requête n° 36769/08, disponible en français sur http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115845 ; voir également Voorhoof D., IRIS 2013-3/1.
7) Requête n° 40397/12, disponible en anglais sur : http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-117513, voir également Voorhoof D., IRIS 2013-5/2.
8) Un « BitTorrent-Tracker » ne procède pas lui-même à l'échange de fichiers mais aide ceux qui recherchent certains fichiers et ceux qui les proposent à se retrouver. Ces derniers échangent ensuite les fichiers directement sans avoir recours au Tracker.

Au-delà de la jurisprudence de la Cour, la CEDH est également pertinente au niveau national. La Convention est appliquée dans tous les Etats membres du Conseil de l'Europe sous la forme du droit national direct, que ce soit en la classant au-dessus du droit commun[9] ou en lui conférant une valeur constitutionnelle[10]. En outre, en vertu de l'article 6, paragraphes 2 et 3 du TUE, les droits fondamentaux de la CEDH font également partie du droit de l'Union européenne.

## 2. Le droit primaire

L'importance du droit d'auteur et de la protection des données pour la législation des organes de l'Union européenne apparaît clairement au niveau du droit primaire, qui constitue la base d'action de l'Union européenne.

### *2.1. Droit d'auteur*

Le droit d'auteur présente une forte dimension économique qui revêt une importance significative pour la libre circulation des biens et des services et pour la libre concurrence. La création, l'exploitation et l'exécution des œuvres relevant du droit d'auteur n'est pas un processus purement national, mais qui traverse allègrement les frontières[11] - notamment en raison de la diversité des ressources techniques. Ceci est particulièrement vrai pour la diffusion de ces œuvres par les services de médias audiovisuels[12].

L'Union européenne s'est engagée en vertu de l'article 26 du TFUE à créer un marché unique sans frontières intérieures au sein duquel sont garanties la libre circulation des marchandises (articles 28 et suivants du TFUE) et des services (article 56 et suivants du TFUE) et une concurrence libre et loyale (article 101 et suivants du TFUE). Les efforts d'harmonisation du système juridique au sein de l'Union européenne s'inscrivent dans la même optique. A cet égard, l'article 114 du TFUE impose expressément un rapprochement des législations. Le Traité de Lisbonne instaure une base de compétence formelle pour le droit d'auteur avec l'article 118 du TFUE. En vertu de cet article, l'Union européenne doit « assurer une protection uniforme des droits de propriété intellectuelle dans l'Union. » De même, suite à l'adoption du Traité de Lisbonne, la propriété intellectuelle est reconnue à l'article 207, paragraphe 1, phrase 1 du TFUE comme faisant partie de la politique commerciale commune.

L'Union européenne a adopté sur cette base un certain nombre de directives relatives au droit d'auteur, qui ont une nette incidence sur les systèmes juridiques nationaux des Etats membres (nous reviendrons sur ce point par la suite).

### *2.2. Droit de la protection des données*

A l'instar des œuvres protégées par le droit d'auteur, les données à caractère personnel ont souvent une valeur économique. Les informations sont utilisées pour effectuer des opérations commerciales et - comme dans le cas présent - revêtent une importance particulière lorsqu'il s'agit, le cas échéant, de faire valoir par la contrainte la reconnaissance des droits d'auteur. Par conséquent, l'Union européenne se sent tenue d'intervenir en tant que régulateur, en vue de répondre aux mêmes exigences du marché intérieur que pour le droit d'auteur. Le TFUE comporte également un

9) Comme dans la plupart des Etats, notamment en Belgique, en France, au Portugal, en Suisse, en Espagne, en Grèce.
10) C'est le cas en Autriche. En Allemagne, en Italie et au Royaume-Uni, la CEDH a le statut d'une simple loi tout en étant spécifiquement prise en compte dans ces mêmes Etats pour l'interprétation des autres lois, ce qui revient à la placer au-dessus du droit commun.
11) Voir à ce sujet la communication de la Commission « Renforcer l'application des droits de propriété intellectuelle sur le marché intérieur » du 11 septembre 2009, COM(2009) 467 final, et la Communication de la Commission sur le contenu dans le marché unique numérique du 18 décembre 2012, COM(2012) 789 final.
12) Yliniva-Hoffman A. et Matzneller P., Protection juridique des organismes de radiodiffusion dans : IRIS *plus* 2010-5, Les nouveaux services et la protection des radiodiffuseurs en droit d'auteur, Susanne Nikoltchev (ed.), Observatoire européen de l'audiovisuel, Strasbourg 2010. Tous les articles d'IRIS *plus* cités ici sont disponibles sur : www.obs.coe.int/oea_publ/iris/iris_plus/index.html

régime spécial pour la protection des données. L'article 16, paragraphe 1, du TFUE établit en premier lieu le droit de protéger ses propres données personnelles. En outre, l'article 16, paragraphe 2, du TFUE en lien avec l'article 39 du TUE donne mandat à l'Union européenne et aux Etats membres pour légiférer en matière de la protection des données. Ce mandat ne concerne pas uniquement la protection des données, mais aussi la garantie d'une libre circulation des données[13].

### 3. Le droit secondaire

Le droit d'auteur et le droit de la protection des données font l'objet d'une définition détaillée, notamment dans les directives et règlements pertinents de l'Union européenne.

*3.1. Droit d'auteur*

Le droit d'auteur de l'Union européenne est composé de nombreuses directives et autres actes juridiques. La Directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins de la société de l'information (2001/29/CE) revêt une importance majeure en ce qui concerne les conflits entre protection des données et droit d'auteur[14]. Cette directive a pour vocation d'adapter à l'échelle européenne le droit d'auteur au monde numérique et au commerce électronique. A cette fin, les droits d'auteur, tels que droit de reproduction, droit de communication au public et de mise à disposition, sont aménagés, notamment en fonction du secteur des activités en ligne, en vue de renforcer le statut des auteurs. L'article 8, paragraphe 3 de la directive prévoit des ordonnances judiciaires à l'encontre des intermédiaires lorsque leurs services sont utilisés par un tiers en violation du droit d'auteur[15]. La Directive 2001/29/CE est étroitement liée à la Directive sur le commerce électronique (2000/31/CE[16]). Les articles 12, 13 et 14 de cette dernière prévoient des exonérations de responsabilité importantes pour le prestataire intermédiaire. En sa qualité de fournisseur de services, il n'est en principe pas responsable des informations et des contenus :

- dont il assure uniquement la transmission (article 12 : Simple transport) ;
- qu'il stocke de façon automatique et temporaire (article 13 : « Caching ») et
- qui lui sont fournis par un utilisateur et stockés par ses soins à la demande de l'utilisateur (article 14 : Hébergement).

Cependant, ces exonérations de responsabilité n'affectent pas l'obligation du prestataire de services de mettre fin à une violation ou de prévenir une violation, et les Etats membres sont expressément invités à permettre aux tribunaux et aux autorités administratives de prendre les dispositions appropriées.

Par ailleurs, l'article 15, paragraphe 1 de la directive sur le commerce électronique dispose que les intermédiaires ne sont pas tenus de surveiller les données qu'ils transmettent ou stockent, ni de rechercher activement des faits ou des circonstances révélant des activités illicites. En revanche, le paragraphe 2, prévoit la possibilité pour chaque Etat membre d'obliger les intermédiaires à informer

13) La protection des données garantie par l'article 16, paragraphe 2 du TFUE engage en premier lieu les institutions, organes et agences de l'Union européenne et les Etats membres dans la mesure où ils se livrent à des activités qui relèvent du champ d'application du droit de l'Union.
14) Directive 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 information (Directive sur le droit d'auteur ), JO. L 167 du 22 juin 2001, p. 10 à 19.
15) Voir également le 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 œuvre protégée ou d'un autre objet protégé.[…]. Les conditions et modalités concernant une telle ordonnance sur requête devraient relever du droit interne des Etats membres.»
16) Directive 2000/31/CE du Parlement européen et du Conseil 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), JO L 178 du 17 juillet 2000, p. 1–16.

les autorités compétentes de tout contenu présumé illicite. En outre, les dispositifs juridiques nationaux peuvent conférer aux autorités de contrôle compétentes le droit d'obtenir de la part des intermédiaires des informations relatives aux utilisateurs. On peut ainsi envisager des cas de procédures pénales en matière de droit d'auteur dans lesquelles les autorités chargées de l'enquête, notamment les procureurs, s'adressent aux intermédiaires pour obtenir des renseignements.

Le droit d'obtenir des informations visé à l'article 15 de la directive sur le commerce électronique est bien entendu la prérogative des « autorités compétentes ». Or, cela ne recouvre pas les ayants droit, qui ont généralement un intérêt majeur à faire valoir leurs droits en cas de violations du droit d'auteur, qui sont justement monnaie courante dans le secteur des activités en ligne[17]. La responsabilité des intermédiaires au titre de tiers ou de « fauteurs de troubles » est exclue en vertu des articles 12 à 14 de la directive sur le commerce électronique. Par conséquent, les ayants droit doivent se limiter aux contrevenants principaux. Toutefois, pour connaître leur identité, ils ont besoin d'un droit d'information, tel qu'il est accordé aux autorités par l'article 15 de la directive sur le commerce électronique.

Un tel droit d'information des ayants droit - qui à l'heure actuelle n'existe toujours pas dans certains Etats membres - est garanti par la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle[18]. Ce droit, inscrit à l'article 8 de la Directive 2004/48/CE[19], a été créé en vue de réduire les disparités concernant les modalités d'application des mesures provisoires qui sont utilisées notamment pour sauvegarder les éléments de preuve ou initier des procédures en cessation des atteintes aux droits de propriété intellectuelle[20].

Conformément à l'article 8, les Etats membres doivent veiller à ce que, dans le cadre d'une action relative à une violation du droit d'auteur et en réponse à une demande du requérant, les autorités judiciaires puissent demander des informations à des tiers (ce qui englobe également les intermédiaires) dès lors que certaines conditions sont réunies, telles que par exemple une violation pratiquée à l'échelle commerciale. Cette demande d'information peut porter sur l'origine et les réseaux de distribution des activités contrefaisantes. Le cas échéant, la demande peut également s'étendre aux noms et adresses des personnes impliquées dans l'infraction. L'article 8 de la Directive 2004/48/CE énonce un droit d'information « assoupli ». comparativement aux projets antérieurs de la Commission européenne.

En effet, l'article 9 de la proposition initiale de la Commission pour une directive relative aux mesures et procédures visant à assurer le respect de la propriété intellectuelle[21] prévoyait un droit d'information élargi, permettant d'adresser une demande de renseignement « à toute personne » sur la base d'une simple présomption d'infraction. Cette disposition a été vivement critiquée par les défenseurs de la confidentialité des données, car cette formulation aurait étendu le droit à l'information au-delà du cadre d'une procédure en cours. Le droit d'information aurait ainsi pu être introduit dans une procédure de droit civil « contre X »[22]. Dans ce contexte, une implication des fournisseurs d'accès sur un simple soupçon était à craindre. D'autre part, la proposition de directive étendait le droit d'information à tous les particuliers, sans limitation aux contrevenants à l'échelle commerciale. En outre, en vertu de l'article 9, paragraphe 4 de la proposition de directive, les

17) Le « détour » par le procureur pour connaître l'identité du contrevenant est souvent nécessaire lorsque le système juridique national ne prévoit pas un droit d'information direct de l'ayant droit à l'encontre du fournisseur d'accès.
18) Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle dans la version rectificative du 30 avril 2004 JO L 157 du 30 avril 2004, p. 45-86.
19) L'article 8 de la Directive relative au respect des droits de propriété intellectuelle 2004/48/CE concrétise le recours juridique généralement défini dans l'article 8, paragraphe 3 de la Directive sur le droit d'auteur 2001/29/CE.
20) Voir le considérant 7 de la Directive relative au respect des droits de propriété intellectuelle(2004/48/CE).
21) COM/2003/0046 final – COD 2003/0024 ; la Directive relative au respect des droits de propriété intellectuelle (2004/48/CE) est basée sur cette proposition.
22) Cf. le commissaire fédéral chargé de la protection des données et de la liberté d'expression en Allemagne dans un communiqué de presse du 10 mars 2004 : « *Schaar begrüßt Stärkung des Datenschutzes bei der IPR-Enforcement-Richtlinie* », disponible en allemand sur : www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/Archiv/06-04StaerkungDesDatenschutzesBeiDerIPR-Enforcement-Richtlinie.html?nn=409394

services douaniers et policiers devaient transmettre systématiquement aux ayants droit les données dont ils avaient connaissance en lien avec une violation du droit d'auteur. Cette disposition n'a pas non plus été retenue dans la version finale de la directive relative au respect des droits de propriété intellectuelle.

*3.2. Droit de la protection des données*

La législation secondaire en matière de droit d'auteur est presque entièrement soumise aux dispositions du droit de l'Union européenne en matière de protection des données. Conformément à l'article 2, paragraphe 3, alinéa a) de la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle, les dispositions de ladite directive n'affectent pas la Directive 95/46/CE relative à la protection des données[23]. Le droit relatif à la protection des données est donc fondamentalement prioritaire sur les dispositions en matière de droit d'auteur, puisque les autres directives pertinentes en la matière sont applicables sous réserve des dispositions contraires prévues dans la directive relative à la protection des données ou, tout au moins, requiert de tenir compte des règles de protection des données pour l'application du droit d'auteur[24]. Concernant le domaine du commerce électronique, le considérant 14 de la directive sur le commerce électronique se réfère intégralement à la directive relative à la protection de données. Celle-ci est fondamentalement prioritaire - notamment en ce qui concerne le droit d'information conformément à la directive sur le commerce électronique[25].

La directive relative à la protection des données comprend les dispositions et les principes de base de la législation secondaire de l'Union européenne en matière de protection des données à caractère personnel, qui sont transposés dans la législation correspondante de tous les Etats membres. Parmi ces principes figure la règle d'interdiction sous réserve d'autorisation : conformément à l'article 7 de la directive relative à la protection des données, les données à caractère personnel ne doivent en principe être collectées ou traitées que si la personne concernée y consent expressément[26]. Toutefois, l'article 7 prévoit une exception dans plusieurs cas:

alinéa c) si le traitement des données à caractère personnel est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis[27] »

alinéa f) si le traitement des données à caractère personnel est « nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

23) Directive 95/46/CE du Parlement européen 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, JO L 281 du 23 novembre 1995, p. 31-50.

24) Voir les considérants 57 et 60 de la Directive sur le droit d'auteur (2001/29/CE) ; l'article 1, paragraphe 5, alinéa b et le considérant 14 de la Directive sur le commerce électronique (2000/31/CE) ; concernant le conflit entre le droit de la protection des données et les libertés des médias, voir Scheuer A. et Schweda S., La protection des données à caractère personnel et les médias, dans : Les limites à l'utilisation des données personnelles, IRIS *plus* 2011-6, Susanne Nikoltchev (ed.),Observatoire européen de l'audiovisuel, Strasbourg 2011, p. 7-29.

25) Considérant 14 de la Directive sur le commerce électronique (2000/31/CE) : « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est uniquement régie par la Directive 95/46/CE […] [Cette directive établit] d'ores et déjà un cadre juridique communautaire dans le domaine des données à caractère personnel et, par conséquent, il n'est pas nécessaire de traiter cette question dans la présente directive […] La mise en œuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel, notamment pour ce qui est des communications commerciales non sollicitées et de la responsabilité des intermédiaires. »

26) Cf. article 6 de la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (règlement d'application de la protection des données) du 25 janvier 2012.

27) Tel est le cas, notamment, lorsqu'un intermédiaire est tenu de divulguer les coordonnées de ses clients en vertu du droit d'information d'un tiers.

*3.3. Actes juridiques du Conseil de l'Europe*

Dans le domaine de la protection des données, le Conseil de l'Europe joue un rôle moteur dans la création de normes européennes en matière de confidentialité des données par le biais de la Convention du 28 janvier 1981 sur la protection des données[28]. Dans la pratique juridique, cependant, le droit européen en matière de protection des données a désormais davantage de poids que la convention.

Le Conseil de l'Europe s'est également penché sur la question du droit d'auteur dans le secteur des activités en ligne en reconnaissant l'existence d'un conflit au niveau des intérêts des utilisateurs.

Le 12 mars 2010, l'Assemblée parlementaire du Conseil de l'Europe (APCE) a adopté la Recommandation 1906 (2010), qui traite des droits de propriété intellectuelle dans la société numérique[29]. Le débat devait donc être lancé sur la base d'un modèle susceptible d'harmoniser les droits des auteurs d'œuvres de l'esprit, des investisseurs et du grand public. L'APCE considère que l'équilibre entre ces différents acteurs eu égard au développement de la société numérique est fortement perturbé : les instruments internationaux ne sont plus adaptés pour garantir aux auteurs une rémunération adéquate pour leurs œuvres tout en assurant la protection des données à caractère personnel. Selon la recommandation, la survie des métiers créatifs est menacée par le risque d'un contrôle sur Internet.

L'APCE estime en premier lieu qu'il incombe aux Etats membres d'instaurer un équilibre entre les droits. Mais elle considère également que le Conseil de l'Europe est tenu de contribuer à la réalisation de cet objectif. Le point 8.4 de la recommandation fait référence au rôle particulier des intermédiaires (« access providers, content-sharing platforms, search engine » - fournisseurs d'accès, plateformes d'échange de contenus, moteurs de recherche).

Le Conseil de l'Europe avait déjà réagi sur la question il y a dix ans, même s'il est vrai qu'à cette époque la priorité était clairement orientée vers la protection du droit d'auteur et moins axée sur la recherche d'un équilibre avec la protection des données personnelles. Dans la Recommandation Rec (2001) 7 sur des mesures visant à protéger le droit d'auteur et les droits voisins et à combattre le piratage, en particulier dans l'environnement numérique[30], le Comité des Ministres se penche sur l'émergence de nouvelles formes de piratage[31]. En ce qui concerne les instruments de droit civil, la recommandation préconise d'autoriser les autorités judiciaires à imposer des mesures provisoires pour la prévention et la poursuite des violations, mesures pouvant, le cas échéant, être prises même sans entendre l'autre partie. La recommandation prévoit également une obligation de coopération de la part du contrevenant pour l'obtention de preuves. De même, le contrevenant est tenu de divulguer l'identité de tiers dès lors qu'ils sont impliqués dans la violation. Toutefois, la recommandation ne prévoit pas de recours contre l'intermédiaire à cet égard.

La Convention sur la cybercriminalité, qui date également de 2001[32], adopte toutefois une approche clairement pénale de la question, ne traitant pas spécifiquement de la question du droit d'information des ayants droit à l'encontre des intermédiaires. « Conscients […] du droit à la protection des données personnelles » et en s'appuyant sur la Convention de 1981[33] sur la

28) Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) du 28 janvier 1981.
29) Recommandation 1906 (2010), Repenser les droits des créateurs à l'ère d'internet, disponible sur : http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta10/FREC1906.htm ; voir également Breemen V., IRIS 2010-10/4.
30) Recommandation Rec(2001)7 du Comité des Ministres aux Etats membres sur des mesures visant à protéger le droit d'auteur et les droits voisins et à combattre la piraterie, en particulier dans l'environnement numérique : https://wcd.coe.int/ViewDoc.jsp?id=220473&Site=CM ; voir également Thórhallsson P., IRIS 2001-9/7.
31) La recommandation est basée sur des recommandations antérieures de 1988 à 1995.
32) Convention sur la cybercriminalité en date du 23 novembre 2001, ETS n°185, disponible sur : http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm; voir également Asscher L. et McGonagle T., IRIS 2001-5/2 ; Gentile I. ; IRIS 2001-7/2.
33) Voir le préambule de la Convention sur la cybercriminalité.

protection des données, les rédacteurs prévoient en tout état de cause une obligation de la part des intermédiaires de communiquer des renseignements aux autorités compétentes[34]. En vertu de cette disposition, ces dernières peuvent exiger des fournisseurs de services la communication des données de base en leur possession concernant leurs clients. Au sens de cette convention, les données de base recouvrent notamment le type et la durée du service souscrit et l'identité de l'utilisateur (par ex. adresse postale, numéro de téléphone). Toute situation où les institutions publiques sollicitent ce genre de renseignements relève clairement de la protection juridique des données à caractère personnel. Toutefois, la présente contribution est axée en premier lieu sur la relation entre les trois parties prenantes que sont les ayants droit, les intermédiaires et les utilisateurs finaux. Les « détours » par le droit pénal procédural peuvent être un moyen pour les ayants droit d'identifier le contrevenant. Cependant, cette méthode s'avère généralement moins efficace.

Par conséquent, la Convention à dominante pénale sur la cybercriminalité reconnaît d'autres instruments juridiques civils : en vertu de l'article 10, paragraphe 3, une partie peut se réserver le droit de ne pas imposer de responsabilité pénale « à condition que d'autres recours efficaces soient disponibles ». On peut considérer le fait que l'ayant droit dispose de moyens de droit civils efficaces pour faire valoir ses droits comme un « autre recours efficace ».

## III. Les zones de conflit dans la pratique

Pour faire valoir ses droits d'auteur ou ses droits voisins, l'ayant droit, qu'il s'agisse d'une société de gestion collective des droits, du titulaire d'une licence exclusive ou de l'auteur lui-même, a besoin d'un minimum de renseignements personnels concernant la partie adverse. Pour pouvoir entrer en contact avec lui, mais aussi, le cas échéant, pour faire valoir ses droits en justice, il lui faut connaître au moins le nom et l'adresse de la personne concernée. En outre, il est souvent très utile de connaitre la nature et la portée de l'infraction commise. Même ces dernières informations sont considérées comme des données à caractère personnel conformément à la loi sur la protection des données[35], dont le but fondamental est d'endiguer un flux incontrôlé d'informations à caractère personnel. Le droit de l'ayant droit d'exploiter une œuvre se heurte donc toujours au droit à la vie privée de la personne concernée.

### 1. Le droit d'information à l'encontre du contrevenant

En matière de conflit entre droit d'auteur et protection des données, la situation la plus courante est celle où l'ayant droit fait valoir directement son droit d'information à l'encontre du contrevenant. Un tel droit d'information est prévu à l'article 8, paragraphe 1 de la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle. Ce droit à l'information ne porte pas sur l'identité du contrevenant (celle-ci doit être *de facto* connue préalablement). Cette information sert davantage à fournir des éléments sur l'origine des services contrefaisants, les canaux de distribution et l'identité des parties impliquées dans la violation du droit d'auteur. Cette information relative à des tiers permet, selon le considérant 21 de la Directive 2004/48/CE, d'assurer un niveau élevé de protection du droit d'auteur, car elle permet de poursuivre d'autres violations connexes.

Toutefois, ce droit est susceptible de se révéler inefficace chaque fois que l'ayant droit ignore l'identité du contrevenant. C'est là que les intermédiaires entrent dans le viseur des ayants droit.

### 2. Le droit d'information à l'encontre des intermédiaires

Le conflit entre droit d'auteur et vie privée prend une tournure plus concrète lorsque les ayants droit veulent obtenir, aux fins de poursuites pour violation du droit d'auteur sur internet, les

34) Article 18 de la Convention sur la cybercriminalité.
35) Les données à caractère personnel désignent toute information concernant une personne physique identifiée ou identifiable, article 2, alinéa a) de la Directive 95/46/CE sur la protection des données.

données relatives à des clients détenues par un fournisseur d'accès internet ou un prestataire de services dans le cadre de la fourniture de leurs services.

*2.1. Identification du contrevenant*

Le contrevenant au droit d'auteur, qui peut tout d'abord naviguer sur internet de façon anonyme, est généralement identifiable simplement par l'adresse IP qui lui a été assignée à un moment donné - le plus souvent une information dont dispose uniquement le fournisseur d'accès, qui peut faire le lien entre les données des clients et leur adresse IP respective[36]. Il en va de même avec les fournisseurs de services internet (par exemple, les réseaux sociaux ou « sharehoster ») dans la mesure où ils demandent à leurs clients de s'enregistrer à l'aide de données à caractère personnel.

Lorsqu'un ayant droit constate une infraction sur internet portant sur une œuvre protégée, il n'a tout d'abord que l'adresse IP à sa disposition. Par conséquent, il est plus intéressant pour l'ayant droit en général de s'adresser directement à l'intermédiaire et d'être ainsi couvert à cet égard. L'intermédiaire, toutefois, est à son tour protégé par les exonérations de responsabilité visées aux articles 12 à 15 de la Directive 2000/31/CE sur le commerce électronique, et n'est en principe pas responsable des infractions commises par le biais du service[37] qu'il fournit. Sa responsabilité n'est concevable que dans des cas exceptionnels et uniquement si l'intermédiaire est impliqué d'une quelconque façon dans la violation, la tolère ou l'encourage[38]. Dans ce cas-là, la procédure de l'ayant droit contre l'intermédiaire est facilitée par l'obligation faite à ce dernier de communiquer ses coordonnées de contact en vertu de l'article 5, paragraphe 1 de la directive sur le commerce électronique. Cette disposition impose à l'intermédiaire d'assurer un accès facile, direct et permanent à ses informations personnelles sur son site internet. Par conséquent, le fournisseur de services internet n'a pas - contrairement à l'utilisateur final - le droit de naviguer en ligne anonymement. L'ayant droit peut exiger du fournisseur de services non seulement des dommages-intérêts pour des infractions déjà commises[39], mais engager également une action contre lui à titre préventif pour des violations futures présumées[40].

Cependant, l'ayant droit sera principalement intéressé par une procédure de droit civil à l'encontre du contrevenant, procédure pour laquelle il a besoin des renseignements personnels qui se cachent derrière l'adresse IP (essentiellement nom et adresse). A cet égard, il peut s'appuyer sur le droit d'information à l'encontre de l'intermédiaire tel qu'il est visé à l'article 8, paragraphe 3 de la Directive 2001/29/CE sur le droit d'auteur et à l'article 8 de la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle. A défaut de ce droit d'information, il ne reste plus à l'ayant droit que la possibilité d'engager une procédure « contre X ». Dans le cadre d'une procédure pénale, le droit d'information peut également être exercé par les autorités chargées de l'enquête pour obtenir auprès de l'intermédiaire des informations sur l'identité du contrevenant[41]. Grâce à son droit d'accès aux documents des autorités chargées de l'enquête, l'ayant droit pourrait finalement avoir connaissance de l'identité du contrevenant. Le droit d'information allège ce parcours incertain et tortueux par une mise à contribution directe de l'intermédiaire.

*2.2. Limites du droit d'information*

Pour faire valoir le droit d'information, il convient toutefois de tenir compte de certains aspects du droit de la protection des données. Même en cas de violation (alléguée) du droit d'auteur, l'identité du contrevenant est protégée par la législation relative aux données à caractère personnel. Dans une telle situation, il est réaliste de supposer qu'il n'y aura pas de consentement portant sur

36) Cela implique que l'utilisateur n'utilise pas de dispositifs de camouflage (tels que les logiciels Tor), ni un serveur Proxy.
37) Voir plus haut paragraphe II.3.1.
38) Pour concrétiser la présomption d'une telle implication, tolérance ou incitation, l'Union européenne prévoit de réviser l'article 14 de la Directive sur le commerce électronique. La consultation correspondante a pris fin le 11 septembre 2012, www.ec.europa.eu/internal_market/e-commerce/notice-and-action/index_de.htm
39) Voir l'article 13 de la Directive relative au respect des droits de propriété intellectuelle2004/48/CE.
40) Voir les articles 9 à 11 de la Directive relative au respect des droits de propriété intellectuelle2004/48/CE ; par ex. sous la forme d'une suspension de l'accès au site internet concerné, cf. Karl H., IRIS 2011-7/8.
41) Voir l'article 15 de la Directive sur le commerce électronique 2000/31/CE.

la divulgation de l'identité, de sorte qu'en vertu de l'article 7, paragraphes b) à d) de la Directive 95/46/CE sur la protection des données, il faut pouvoir faire intervenir une exception particulière justifiant le traitement des données sans consentement. Conformément à l'article 13, paragraphe 1, alinéa g, des restrictions de la protection des données ne sont possibles que si elles sont nécessaires à la protection « des droits et libertés d'autrui. » Cette formulation vague est une « porte ouverte » aux controverses en faveur du droit d'auteur. C'est pourquoi en cas de conflit, l'arbitrage se fait toujours sur la base de la pondération des intérêts.

A cet égard, les intérêts des intermédiaires sont également pertinents. Du fait du droit d'information, ces derniers se trouvent exposés à de lourdes tâches et à des frais excessifs. A cela vient s'ajouter le souci de trahir la confiance qu'ont les clients dans l'anonymat de l'utilisation du service, ce qui peut entraîner une perte de clients et un manque à gagner pour les intermédiaires. C'est pourquoi le débat politique concernant les obligations des intermédiaires insiste toujours sur la nécessité d'aménager des exonérations de responsabilité, comme le prévoit la directive sur le commerce électronique. Plus la responsabilité des intermédiaires est engagée, plus il leur sera difficile de fournir des services abordables et attrayants. Les intermédiaires forment ainsi un « troisième camp » dans la zone de conflit entre vie privée et droit d'auteur[42].

*2.3. Le droit d'information dans la jurisprudence de la CJUE*

Plusieurs arrêts de la CJUE illustrent la manière dont elle définit et pondère les conflits d'intérêts et quels sont les critères appliqués pour évaluer la légitimité des mesures respectives. On peut observer que la CJUE s'appuie de plus en plus sur la Charte des droits fondamentaux de l'Union européenne lors de son analyse et procède à la pondération des droits fondamentaux concernés.

*Arrêt du 29 janvier 2008 (Promusicae)*

Une première décision rendue par la CJUE sur la base du dispositif normatif complexe des directives concernant le droit d'auteur (Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, Directive 2004/48/CE relative au respect des droits de propriété intellectuelle) et la Directive 2002/58/CE[43] (vie privée et communications électroniques) concerne l'affaire *Promusicae*[44]. Promusicae, une association de producteurs espagnols, demandait à Telefónica, un fournisseur d'accès espagnol, la divulgation des noms et adresses de différents clients qui violaient les droits d'auteur par le biais d'un site de partage de dossiers (« Shared Folder ») du programme KaZaA. En vue de l'examen de cette demande d'information, la juridiction nationale a saisi la Cour concernant l'interprétation des directives mentionnées ci-dessus. Il s'agit de savoir si le droit communautaire impose aux Etats membres de prévoir l'obligation de publier des données personnelles dans les procédures civiles aux fins d'assurer une protection efficace du droit d'auteur. Alors que la législation européenne prévoit expressément

42) Les exigences juridiques en matière de droit de la protection des données peuvent parfois avoir un impact négatif sur le consommateur lui-même, qui peut vouloir s'opposer à un avertissement par l'ayant droit et connaître dans quelles circonstances son fournisseur d'accès a transmis des informations à son sujet. Par exemple, en Allemagne, le *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (Commissaire fédéral à la protection des données et la liberté d'information - BfDI) déclare qu'un fournisseur d'accès n'est pas tenu d'informer ses clients sur la mise à disposition des informations les concernant. En particulier, le BfDI estime cependant qu'un fournisseur d'accès n'est pas autorisé à enregistrer le contenu transmis à un tiers, de sorte qu'il n'est pas possible de fournir de tels renseignements aux clients à leur demande ; voir le 23e rapport d'activité du BfDI 2009–2010, p. 52, disponible sur : www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile

43) 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 (Directive Vie privée et communications électroniques), JO L 201 du 31 juillet 2002, p. 37-47, dernièrement modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO L 337 du 18 décembre 2009, p. 11-36.

44) CJUE, affaire C-275/06, *Promusicae*, arrêt du 29 janvier 2008, rec. 2008, p. I-00271.

un droit d'information dans les procédures pénales, la situation juridique au niveau des actions civiles semblait moins claire. A partir d'un examen global des directives concernées, la Cour a conclu à l'absence d'une telle obligation. En vertu de l'article 8, paragraphe 1 de la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle, les Etats membres doivent veiller à ce que, dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle et en réponse à une demande justifiée et proportionnée du requérant, les autorités judiciaires compétentes *puissent* ordonner que des informations soient fournies par le contrevenant. L'article 8 ne comporte donc aucune obligation générale d'instaurer un tel droit d'information. L'article 8 est expressément limité dans sa portée par la directive relative à la protection des données[45]. La Cour souligne néanmoins qu'il n'est pas interdit aux Etats membres de prévoir de telles obligations lorsqu'il s'agit de trouver un équilibre raisonnable entre les différents droits fondamentaux[46] protégés par le droit de l'Union - en particulier le droit de propriété et le droit à la protection des données personnelles. Il convient toutefois de respecter le principe de proportionnalité dans la mise en œuvre de telles mesures.

*Ordonnance du 19 février 2009 (LSG)*

Environ un an plus tard, la CJUE a exprimé le même point de vue dans une ordonnance concernant l'affaire *LSG*[47]. Cette procédure portait également sur la communication des coordonnées d'utilisateurs par un fournisseur d'accès à internet. Dans l'affaire au principal, la société autrichienne de gestion collective Wahrnehmung von Leistungsschutzrechten GmbH (LSG) demandait à l'intermédiaire Tele 2 Telecommunication GmbH des informations sur les noms et adresses des personnes se cachant derrière des adresses IP dynamiques servant à pratiquer des échanges de fichiers illicites. L'angle d'attaque de la question préjudicielle posée par l'*Oberster Gerichtshof* (Cour suprême autrichienne) était différent dans cette affaire : la cour a explicitement demandé si le droit de l'Union européenne s'opposait à la communication des données dans le cadre de poursuites contre les atteintes au droit d'auteur devant les juridictions civiles. Etant donné que la CJUE avait déjà procédé à cette analyse dans le jugement précité, elle a pu traiter cette demande rapidement ; elle s'est donc contentée de rendre une ordonnance plutôt qu'un arrêt. La Cour a renouvelé dans cette ordonnance son injonction aux Etats membres de veiller, lors de la mise en place d'un droit d'information dans les actions de droit civil, à respecter les droits fondamentaux et autres principes généraux du droit de l'Union européenne. Cette recommandation concerne en particulier le principe de proportionnalité.

Le principe de proportionnalité qui, tout en étant systématiquement mis en avant, n'en reste pas moins très abstrait, ne contribue pourtant pas à renforcer la sécurité juridique. On peut tout au plus en conclure qu'un droit d'information exercé dans le cadre d'une action civile contre le fournisseur d'accès d'un utilisateur qui porte atteinte au droit d'auteur systématiquement et à grande échelle ne saurait être considéré comme contraire au droit communautaire. En revanche, la proportionnalité est plus difficile à justifier si le droit d'information d'un Etat membre était appliqué à la suite d'une seule atteinte présumée au droit d'auteur pour obtenir les données personnelles de l'utilisateur concerné[48].

*Arrêt du 19 avril 2012 (Bonnier Audio)*

L'arrêt de la CJUE dans l'affaire *Bonnier Audio*[49] marque la dernière étape sur cette question ; dans cette affaire, la panoplie des directives à prendre en considération s'est élargie à la Directive 2006/24/CE sur la conservation des données[50]. La situation initiale est la même que dans les deux affaires susmentionnées. Les détenteurs de droits suédois sur des livres audio ont adressé une

45) Voir l'article 8, paragraphe 3, alinéa e) de la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle.
46) Voir plus haut, paragraphe II. 1.
47) CJUE, affaire C-557/07, *LSG*, ordonnance du 19 février 2009, rec. 2009, p. I-01227 ; voir également Yliniva-Hoffmann A., IRIS 2009-9/7.
48) Le *Bundesgerichtshof* (cour fédérale de justice – BGH) a toutefois confirmé la proportionnalité en pareil cas, arrêt du 19 avril 2012, affaire I ZB 80/11, disponible sur http://lexetius.com/2012,3310
49) CJUE, affaire C-461/10, *Bonnier Audio*, arrêt du 19 avril 2012 ; voir Dohmen F., IRIS 2012-6/4.
50) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE, JO L 105 du 13 avril 2006, p. 54–63.

demande de renseignements au fournisseur d'accès dont le serveur était utilisé pour la diffusion illicite de leurs livres audio. La CJUE s'est livrée à un renvoi détaillé à sa jurisprudence antérieure dans les affaires *Promusicae* et *LSG* en aboutissant aux mêmes conclusions. Toutefois, elle précise clairement que la directive sur la conservation des données ne saurait intervenir en faveur des droits d'information dans les procédures civiles.

Pour bien comprendre cet arrêt, il faut connaître le rapport entre la Directive 2006/24/CE sur la conservation des données et la Directive 2002/58/CE sur la vie privée et les communications électroniques. Toutes deux abordent le stockage des données relatives au trafic[51] : d'une part, l'obligation de stocker sans motif aux fins de la recherche, la détection et la poursuite d'infractions graves ou d'actes de terrorisme et, d'autre part - comme faisant en quelque sorte exception aux considérations relatives à la protection des données - la possibilité pour les fournisseurs de conserver les données pendant une durée limitée, par exemple à des fins de comptabilité. En substance, l'arrêt *Bonnier Audio* peut se résumer de la façon suivante : les données qui ont été sauvegardées en vertu de la directive sur la conservation des données *ne peuvent pas* être utilisées pour répondre à des demandes d'informations dans le cadre d'infractions au droit d'auteur. Cette disposition est expressément formulée à l'article 4, phrase 1 de la directive sur la conservation des données : elle impose aux Etats membres de veiller à ce que les données conservées conformément à ladite directive ne soient transmises qu'aux *autorités* nationales compétentes, dans des cas précis. En revanche, les données relatives au trafic qui sont toujours stockées de façon licite par le fournisseur sur la base de la mise en œuvre de la Directive Vie privée et communications électroniques (2002/58/CE) peuvent tout à fait être utilisées à cette fin - toujours en tenant compte, bien entendu, du principe de proportionnalité et après pondération des droits fondamentaux en jeu.

Par conséquent, il est crucial de savoir si le législateur national a instauré une obligation de stockage ou une autorisation de stockage, en s'éloignant de la conservation des données telle qu'elle est visée par la Directive 2006/24/CE. L'autorisation de stockage des données aux fins de facturation est inscrite à l'article 6, paragraphe 2 de la Directive Vie privée et communications électroniques (2002/58/CE). A cet égard, on est en droit de s'interroger sur le fait que la forme actuelle la plus courante de règlement, à savoir les formules dites au forfait, ne requiert aucune donnée précise concernant les connexions pour facturer la consommation. Et même lorsqu'un traitement des données est nécessaire, l'article 6, paragraphe 2 de la Directive Vie privée et communications électroniques prescrit la suppression des données en mémoire dès lors que des actions sont engagées pour obtenir le paiement de la facture. Il résulte de ces deux aspects tout d'abord une réduction supplémentaire des données généralement disponibles pour un droit d'information, et ensuite se pose la question de savoir ce qui se passe si le fournisseur d'accès conserve malgré tout les données de connexion de manière illicite. Ces données ne peuvent pas non plus faire l'objet d'un droit d'information. L'*Oberster Gerichtshof* (cour suprême autrichienne) a également statué en ce sens dans son arrêt du 14 juillet 2009 en déclarant que les données relatives aux communications des usagers qui sont enregistrées à des fins légitimes doivent justement être utilisées à ces seules fins et être effacées par la suite[52]. Par conséquent, la Cour considère que la communication des données par le fournisseur d'accès est illégale, sauf si la loi prévoit expressément une obligation de divulgation de renseignements.

Les données doivent en principe être utilisées exclusivement dans le cadre des exceptions visées à l'article 15 de la Directive Vie privée et communications électroniques (2002/58/CE). Cet article prévoit une limitation de la confidentialité des données uniquement lorsqu'il s'agit d'une mesure proportionnée, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'Etat — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite

51) Conformément à l'article 2, paragraphe 2, alinéa b) de la Directive Vie privée et communications électroniques (2002/58/CE), les données relatives au trafic désignent toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation. En l'espèce, une donnée relative au trafic est l'information selon laquelle un certain fichier a été téléchargé à une certaine heure par une certaine adresse IP. Or, pour les ayants droit, ce sont les informations personnelles concernant l'utilisateur qui présentent un intérêt, car elles seules leur permettent de poursuivre un utilisateur pour violation du droit d'auteur.

52) Arrêt de la Cour suprême autrichienne du 14 juillet 2009, voir Yliniva-Hoffmann A., IRIS 2009-9/7.

d'infractions pénales. La liste des exceptions n'inclut pas d'éventuelles requêtes de dommages-intérêts introduites en droit civil par des ayants droit. Toutefois, les Etats membres sont libres de créer des droits d'information au niveau des procédures civiles. Cette possibilité est clairement énoncée à l'article 13, paragraphe 1, alinéa g) de la Directive 95/46/CE relative à la protection des données, qui permet d'assouplir le niveau de protection des données en vue de protéger les droits d'autrui. Les deux normes permettent ainsi une limitation des dispositions de protection des données en faveur de la protection des droits d'auteur. Par conséquent, le facteur déterminant est toujours le droit national de chaque Etat membre.

Nonobstant les dispositions de l'article 4, paragraphe 1 de la Directive 2006/24/CE sur la conservation des données, les médias rapportent que le ministère autrichien de la Justice a tenté de soumettre des données stockées sur la base de la conservation obligatoire des données à l'exercice d'un droit d'information de la part d'ayants droit[53]. La « conservation sans motif » des données relatives au trafic, mesure sujette à controverse du point de vue du droit de la protection des données, serait ainsi étendue en faveur des poursuites contre des infractions au droit d'auteur. Une telle extension entre en conflit avec l'article 4, phrase 1 de la Directive 2006/24/CE sur la conservation des données, qui prévoit la communication des données stockées aux autorités compétentes et non pas à des tiers privés. Nul doute qu'il sera intéressant de suivre l'évolution de la procédure législative. Celle-ci est pour l'instant au point mort - sans doute eu égard à la procédure pendante devant la CJUE visant à vérifier la compatibilité de la Directive sur la conservation des données[54] avec le droit de l'UE.

### 3. Proportionnalité du droit d'information national

Dans ses arrêts portant sur la zone de conflit entre protection des données et droit d'auteur, la CJUE a toujours insisté sur la nécessité de créer un juste équilibre entre les droits fondamentaux contradictoires. Pour garantir la proportionnalité d'un droit d'information, les Etats membres appliquent différents critères. En règle générale, il est nécessaire d'être en présence de circonstances particulières pour faire valoir un droit d'information à l'encontre des intermédiaires au préjudice des intérêts liés à la protection des données .

L'une des conditions fréquemment invoquée pour faire valoir un droit d'information est déjà inscrite dans la Directive 2004/48/CE relative au respect des droits de propriété intellectuelle. L'article 8 subordonne la reconnaissance d'un droit d'information à l'« échelle commerciale » d'une violation du droit d'auteur. L'action du contrevenant doit impérativement être motivée par des « bénéfices économiques ou commerciaux directs ou indirects » pour faire valoir un droit d'information. Cela permet d'exclure les infractions commises de bonne foi par un particulier[55].

On retrouve également cette idée dans les dispositifs juridiques nationaux. Le droit d'information allemand exige lui aussi une dimension commerciale de l'infraction[56] ainsi qu'un examen de la proportionnalité au cas par cas et une ordonnance systématique du tribunal[57]. Il en va de même en Autriche où, conformément à l'arrêt de l'*Oberster Gerichtshof* du 14 juillet 2009, le droit d'information[58] ne s'applique pas aux données qui sont soumises à une obligation de suppression. En outre, le droit d'information autrichien exige également une requête écrite et dûment motivée du droit d'information, en vue d'éviter un recours massif au droit d'information. La situation est

53) http://akvorrat.at/Ausweitung_der_Vorratsdatenspeicherung_BMJ_lehnt_Dialog_mit_BuergerInnen_ab
54) Demande de décision préjudicielle de la Haute cour d'Irlande introduite le 11 juin 2012, affaire C-293/12, pour une décision conjointe en lien avec la demande de décision préjudicielle déposée le 19 décembre 2012 par la cour constitutionnelle autrichienne dans l'affaire C-594/12.
55) Considérant 14 de la Directive 2004/48/CE relative au respect des droits de propriété.
56) Selon l'arrêt de la cour fédérale de justice allemande du 19 avril 2012 (affaire I ZB 80/11) il suffit aussi que le service utilisé pour l'acte de contrefaçon soit fourni par l'intermédiaire à l'échelle commerciale.
57) Article 101 de l'*Urheberrechtsgesetz* (loi allemande sur le droit d'auteur).
58) Article 87b de la loi autrichienne sur le droit d'auteur.

similaire concernant le droit d'information suédois[59] qui exige systématiquement une ordonnance du tribunal : outre une justification suffisante, il faut également exposer en quoi la poursuite en droit civil de l'atteinte au droit d'auteur sera considérablement facilitée par l'obtention des informations demandées. Tous les droits susmentionnés ont en commun l'article déjà mentionné à propos de l'Allemagne et portant sur l'examen au cas par cas de la proportionnalité des informations[60].

**4. L'obligation faite aux intermédiaires d'installer des filtres**

Le point de friction entre le droit d'auteur et la protection des données personnelles ne se limite pas à la question du droit d'information. Les systèmes juridiques nationaux ont créé des modèles alternatifs pour l'application du droit d'auteur dans le secteur en ligne. Dans deux affaires - toutes deux initiées par la société belge de gestion collective Société belge des Auteurs Compositeurs et Editeurs (SABAM) – la CJUE a dû se prononcer sur la compatibilité des ordonnances de filtres avec le droit de l'UE[61].

L'affaire *Scarlet Extended*[62] portait sur une ordonnance judiciaire obligeant de façon générale et préventive un fournisseur d'accès à internet à prévenir les infractions au droit d'auteur commises au moyen de ses services à l'aide de programmes *peer-to-peer* par la mise en place de systèmes de filtrage. L'affaire *Netlog NV*[63] concernait l'obligation faite à l'exploitant d'un réseau social d'empêcher les utilisateurs de ce réseau d'échanger des œuvres musicales et audiovisuelles sur leurs pages de profil.

Dans ces deux arrêts, la CJUE a établi que ces obligations contraignaient les opérateurs concernés à mettre en place un système de filtrage, ce qui implique une surveillance active de l'ensemble des données de chaque utilisateur. La Cour mentionne à cet égard plusieurs droits fondamentaux qui doivent être préservés lors de l'application d'un autre droit fondamental - notamment le droit de la propriété intellectuelle (article 17 de la Charte des droits fondamentaux) : il y a pour les différents fournisseurs de services des interférences avec la protection de la liberté d'entreprise (article 16 de la Charte) ; pour les utilisateurs, cela représente une ingérence dans la liberté de l'information (article 11), et – comme nous l'avons mentionné à plusieurs reprises – avec le droit de la protection des données à caractère personnel (article 8).

Dans les deux cas, la Cour s'est prononcée après un examen approfondi au détriment de la société de gestion collective. Elle considère qu'une obligation de surveillance déconnectée de contenus concrets n'est plus compatible avec l'article 15 de la Directive 2000/31/CE sur le commerce électronique. Du point de vue des fournisseurs de services, il est disproportionné de les obliger à mettre en place en permanence un dispositif de filtrage complexe, coûteux et à leur charge exclusive. Les droits fondamentaux des usagers doivent être placés plus haut en matière de protection des données, surtout si l'on considère la possibilité d'identifier les contrevenants au droit d'auteur par le repérage et le traitement des adresses IP ou les informations concernant les profils d'utilisateurs concernés. Avec les systèmes de filtration intégrés à titre préventif, cette analyse systématique des données personnelles a lieu pour chaque utilisateur, sans indice concret permettant de supposer une violation du droit d'auteur. En outre, la CJUE considère que la liberté de l'information est affectée par le fait qu'un tel système de filtrage risque de ne pas être en mesure de faire une distinction suffisante entre un contenu licite et un contenu non autorisé. Dans certaines circonstances, cela provoque le blocage de contenus licites : cela n'est pas sans évoquer les exceptions légales au droit

59) Article 53c de la *Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk* (loi suédoise sur les droits d'auteur des œuvres littéraires et artistiques).
60) Pour plus de détails sur les dispositions mentionnées et les dispositions correspondantes dans les autres Etats membres, voir Kuner C., Burton C., Hladjk J. et Proust O., Study on Online Copyright Enforcement and Data Protection in Selected Member States, novembre 2009, disponible sur : http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf
61) Voir le rapport détaillé de Angelopoulos C, Filtrage des contenus protégés par le droit d'auteur sur Internet en Europe, IRIS *plus* 2009-4,Observatoire européen de l'audiovisuel, Strasbourg 2009.
62) CJUE, affaire C-70/10, *Scarlet Extended*, arrêt du 24 novembre 2011 ; voir. Angelopoulos C., IRIS 2011-6/2; IRIS 2012-1/2.
63) CJUE, affaire C-360/10, *Netlog NV*, arrêt du 16 février 2012 ; voir Breemen K., IRIS 2012-3/3.

d'auteur telles que l'autorisation des copies à usage privé ainsi que les œuvres tombées dans le domaine public ou les œuvres orphelines.

## 5. Blocage de l'accès internet – dispositifs nationaux

Les Etats membres de l'Union européenne ont créé d'autres alternatives au droit d'information direct de l'ayant droit à l'encontre du fournisseur d'accès pour obtenir des informations personnelles sur le contrevenant. Du point de vue de la protection des données, ces modèles sont « plus respectueux des données », dans la mesure où l'ayant droit n'accède pas aussi facilement aux données personnelles du contrevenant présumé. L'alternative consiste à mettre en place des procédures dites de « riposte graduée » en réservant, d'une façon générale, le blocage temporaire de l'accès à internet en dernier recours. L'ampleur du traitement des données personnelles est sans doute moindre, mais les atteintes, notamment au droit à l'information et contre la liberté d'expression, sont nettement plus fortes[64].

### *5.1. France : HADOPI*

Depuis 2010, la France suit sa propre voie dans la poursuite des infractions au droit d'auteur et présente également un certain nombre de particularités en ce qui concerne la protection des données. Ainsi, elle a créé la Haute Autorité pour la diffusion des œuvres et la protection des droits sur l'Internet (HADOPI), un organisme indépendant employant environ 60 personnes et chargé de poursuivre les violations du droit d'auteur sur internet[65]. La HADOPI intervient soit sur une plainte déposée par un ayant droit (le plus souvent des représentants d'organisations professionnelles, des sociétés de gestion collective telles que la Société des auteurs, compositeurs et éditeurs de musique (SACEM), le Centre national de la cinématographie), soit à la demande du procureur. L'ayant droit transmet à la HADOPI la date et l'heure de la violation du droit d'auteur, l'adresse IP utilisée, des informations sur les œuvres protégées et sur le fournisseur d'accès Internet. La HADOPI peut alors exiger du fournisseur d'accès la transmission de données personnelles associées à l'adresse IP de l'utilisateur (nom, numéro de téléphone, adresse email, adresse postale).

Dans un premier temps, le contrevenant présumé reçoit un avertissement par e-mail avec une demande d'observations, puis dans un deuxième temps, il reçoit un courrier recommandé. Si la HADOPI épingle une troisième fois le même contrevenant, elle peut entamer une procédure judiciaire simplifiée assortie de sanctions telles que des amendes. Durant les trois premières années d'existence de cette autorité, le dispositif prévoyait en guise de sanction le blocage temporaire de l'accès internet, mesure très critiquée. La possibilité de bloquer l'accès à internet a été supprimée le 9 juillet 2013 - à la suite du changement de gouvernement en France[66]. Cette mesure avait préalablement fait l'objet de nombreuses procédures judiciaires. La compétence initiale de la HADOPI d'imposer elle-même des restrictions d'accès a été déclarée anticonstitutionnelle et annulée par le Conseil Constitutionnel français[67]. A la suite de quoi le législateur a remanié le dispositif de telle sorte que la loi subordonne l'application d'une restriction d'accès à la saisine d'un tribunal par la HADOPI[68].

---

64) L'Organisation pour la sécurité et la coopération en Europe (OSCE) est critique à cet égard ; voir Stone M., IRIS 2012-2/1.
65) Blocman A., IRIS 2010-9/24.
66) Décret nº 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle ; disponible sur http://de.scribd.com/doc/152648389/joe-20130709-0157-0060
67) Décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009 ; voir Blocman A., IRIS 2009-7/12 ; voir également IRIS 2010-9/24.
68) Le Conseil d'Etat tire de l'article 6 de la CEDH, qui établit le droit à une procédure équitable, la nécessité d'une ordonnance judiciaire. L'article 6 exige la tenue d'un procès pour toute sanction, quelle qu'en soit la nature. Alors que les premiers contacts de la HADOPI pour signaler une violation du droit d'auteur ne peuvent pas être considéré comme une sanction, ni même une accusation, l'application d'une suspension de l'accès à internet constitue indéniablement une sanction. La décision du 19 octobre 2011 est disponible sur : www.conseil-etat.fr/fr/communiques-de-presse/decrets_hadopi.html ; voir également Blocman A., IRIS 2011-10/15.

Pendant toute la période où il était juridiquement possible de bloquer l'accès à internet, il n'y a eu qu'un seul cas où cette sanction a été appliquée[69]. En outre, certains fournisseurs d'accès ont exprimé dès le début des réserves concernant l'envoi des e-mails d'avertissement de la HADOPI et refusaient de les transmettre aux utilisateurs respectifs. En réaction, le législateur français a créé une obligation légale de transmettre les e-mails. Tout manquement à cette obligation peut désormais valoir au fournisseur d'accès une amende de 1 500 euros[70].

Concernant les exigences en matière de protection des données, la loi française prévoit que les données à caractère personnel ne soient connues que de la Commission de protection des droits, une instance au sein de la HADOPI qui vérifie les indications des ayants droit. A cet égard, la procédure HADOPI s'avère moins radicale, ne serait-ce que du point de vue du droit de la protection des données, qu'un droit d'information général à l'encontre des intermédiaires, puisque dans un premier temps les informations à caractère personnel sont uniquement à la disposition d'une partie d'un organisme gouvernemental. Dans le modèle prévoyant un droit d'accès direct vis-à-vis du fournisseur d'accès, chaque ayant droit privé a fondamentalement la possibilité d'accéder aux données personnelles des utilisateurs finaux. Lorsque l'ayant droit obtient ces données personnelles, l'utilisation de ces données par l'ayant droit est pour le moins incertaine. La procédure HADOPI laisse tout d'abord les données à caractère personnel entre les mains d'un organisme gouvernemental, qui les traite dans le cadre d'un processus institutionnalisé. La procédure HADOPI, critiquée à maints égards, s'avère donc plus efficace en matière de protection des données que l'instauration d'un droit d'information direct, d'autant plus que la HADOPI est légalement tenue de supprimer les données en fonction de certains délais[71].

La HADOPI devrait, sur la base de recommandations critiques, être dissoute en raison de son fonctionnement inefficace, mais le dispositif lui-même sera maintenu, avec de légères modifications, et confié au Conseil supérieur de l'audiovisuel (CSA), l'organe de régulation des médias[72].

Au niveau du droit de l'Union européenne, on retrouve des concepts similaires dans le rapport Gallo du Parlement européen[73]. Ce rapport réclame un renforcement des sanctions pour violation du droit d'auteur dans l'espace en ligne, car le système juridique n'est pas en mesure de maitriser la situation au moyen de simples recours de droit civil en dommages-intérêts[74]. Le rapport souligne néanmoins l'importance particulière de la protection des données, qu'il convient de prendre en compte lors de la mise en place de sanctions.

*5.2. Royaume-Uni : Digital Economy Act*

Un modèle similaire à celui de la France est également appliqué au Royaume-Uni. Les articles 124A à 124N de la *Communications Act* (loi sur les communications de 2003, introduite par la *Digital Economy Act* 2010 – loi de 2010 sur l'économie numérique ) prévoient une vaste procédure qui permet aux ayants droit d'informer les fournisseurs de services Internet ayant souscrit à l' « initial obligations code » (code des obligations initiales) élaboré par le régulateur britannique, l' *Office of Communications* (Ofcom)[75], sur la violation du droit d'auteur et de les inviter à informer leurs clients en conséquence. Dès lors que le nombre des messages adressés à un utilisateur donné atteint

69) Selon la presse ; voir www.pcinpact.com/news/80487-hadopi-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm
70) Blocman A., IRIS 2010-10/30.
71) Deux mois après le signalement fait par un ayant droit, etc. lorsqu'il n'y a pas d'avertissement. Au premier avertissement, 14 mois s'il n'y a pas de deuxième avertissement. Au deuxième avertissement, 20 mois si aucune autre violation n'a été commise.
72) Blocman A., IRIS 2013-6/19.
73) Résolution du Parlement européen du 22 septembre 2010 sur l'application des droits de propriété intellectuelle sur le marché intérieur (2009/2178(INI)) ; disponible sur : www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2010-0340+0+DOC+PDF+V0//FR
74) La proposition rejetée de directive du Parlement européen et du Conseil relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle suivait une orientation similaire, COM(2005)276 final, disponible sur : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276%2801%29:FR:HTML
75) L'Ofcom a publié un projet de code en juin 2012 et a lancé en même temps une procédure de concertation pendant un mois (disponible sur : http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf) ; le code n'est pas encore définitivement adopté.

un minimum fixé dans le code de conduite, les fournisseurs d'accès à Internet sont tenus de les consigner sur une liste anonyme (« copyright infringement list »)[76]. Sur demande, cette liste ou une partie de celle-ci peuvent être transmises aux ayants droit sous une forme anonyme conforme au droit de la protection des données.

Sur la base de cette liste, l'ayant droit peut exiger par le biais d'une ordonnance judiciaire la divulgation des informations personnelles pertinentes afin de poursuivre l'auteur de la contrefaçon en dommages-intérêts. Conformément aux paragraphes 33 à 35 des *Explanatory Notes* (notes explicatives), le secrétaire d'Etat peut imposer au fournisseur d'accès la mise en place de mesures techniques supplémentaires si la (seule) méthode de la liste s'avérait insuffisante[77]. Le blocage de l'accès à internet peut explicitement prendre la forme d'une limitation de la bande passante ou de la suspension totale provisoire du compte.

Les deux fournisseurs d'accès britanniques British Telecommunications Plc et TalkTalk Telecom Group Plc ont contesté ces dispositions en justice en faisant valoir d'importantes infractions au droit de l'UE[78]. Ils affirmaient, entre autres, que la *Digital Economy Act* était incompatible avec la Directive Vie privée et communications électroniques (2002/58/CE). L'*England and Wales High Court (Administrative Court) (*Haute Cour d'Angleterre et du Pays de Galles [tribunal administratif]) n' a toutefois pas retenu l'infraction au droit de la protection des données dans son arrêt du 20 avril 2011 au motif que le traitement des données personnelles est nécessaire pour remplir une obligation légale et faire respecter le droit de la propriété et qu'il sert la réalisation d'un intérêt légitime (en l'espèce, les intérêts économiques des ayants droit). Le traitement des données est ainsi couvert par l'article 7, paragraphes c), e) et f) et par les articles 8 et 15 de la Directive 95/46/CE relative à la protection des données.

D'autre part, la Haute Cour n'a pas retenu non plus l'infraction contre l'article 12 de la Directive 2000/31/CE sur le commerce électronique. Sur la base des dispositions contestées, les fournisseurs d'accès ne sont pas responsables des contenus, mais se limitent à documenter les violations et à informer les ayants droit. De même, il n'y a pas d'atteinte à l'interdiction d'une obligation de surveillance de la part des fournisseurs en vertu de l'article 15 de la Directive sur le commerce électronique, car le fournisseur d'accès ne surveille pas lui-même l'activité et se contente de documenter les signalements des ayants droit. Les requérants n'ont pas non plus obtenu gain de cause en appel devant la *England and Wales Court of Appeal (Civil Division)* (Cour d'appel d'Angleterre et du pays de Galles [Division droit civil]). Dans son arrêt du 6 mars 2012, la cour d'appel a repris en grande partie les considérants de la juridiction précédente[79].

La Haute Cour a également entrepris un examen détaillé des droits fondamentaux, mais a nié toute restriction excessive du droit à la protection des données personnelles par la *Digital Economy Act*, puisque le droit antagonique à la propriété est au moins aussi digne de protection. En outre, il n'existe pas de mesure aussi efficace pour protéger la propriété intellectuelle dans le secteur des activités en ligne qui serait plus souple du point de vue de la protection des données. Par conséquent, la conception adoptée dans la *Digital Economy Act* est proportionnel.

A l'instar du modèle HADOPI, ce système présente également l'avantage, en matière de protection des données, de ne pas placer d'emblée les données à caractère personnel du contrevenant (présumé) entre les mains de tierces personnes privées. Le système britannique va même jusqu'à ne pas permettre l'accès aux données par une quelconque autorité. Le dispositif prévoit simplement une consignation des faits de la part du fournisseur d'accès qui est publiée en préservant l'anonymat. Les informations à caractère personnel qui se cachent derrière les adresses IP ne sont accessibles aux ayants droit que dans le cadre d'une procédure judiciaire. En outre, la procédure se déroule en toute transparence pour l'utilisateur, car il est informé dès le premier signalement au fournisseur d'accès.

76) Articles 124A à 124N de la *Communication Act 2003*.
77) Les *Explanatory Notes* (notes explicatives) relatives à la *Digital Economy Act 2010* (loi sur l'économie numérique 2010) sont disponibles sur : www.legislation.gov.uk/ukpga/2010/24/notes/contents?view=plain
78) Voir sur ce point Prosser T., IRIS 2011-6/20.
79) Prosser T., IRIS 2012-5/22.

*5.3. Irlande : autorégulation*

Comparativement, l'Irlande utilise un modèle relativement indépendant de l'Etat en ce qui concerne l'implication des intermédiaires dans la poursuite des violations du droit d'auteur. Eircom, le principal opérateur irlandais de télécommunications et les représentants irlandais des quatre grandes maisons de disques EMI, Sony, Universal et Warner se sont mis d'accord sur un dispositif de riposte graduée à la suite d'un litige sur la divulgation de renseignements sur les clients[80]. Ce dispositif n'a pas de fondement légal et repose uniquement sur un compromis entre les parties[81].

Aux termes de ce compromis, Eircom intervient auprès de ses clients selon un processus à trois niveaux. A la première violation du droit d'auteur, le client reçoit un message d'*Eircom*. Au deuxième message, l'opérateur le menace d'un blocage de son accès internet et à la suite du troisième message, le blocage est appliqué[82]. Le commissaire irlandais chargé de la protection des données est intervenu lors du processus en émettant plusieurs réserves concernant les articles 8 et 6 de la CEDH : d'une part, le traitement des données personnelles selon le modèle de riposte graduée porte atteinte à la vie privée des utilisateurs. Par ailleurs, la procédure revient à supprimer une procédure équitable, puisque l'établissement du délit et l'application de la sanction sont pratiqués sans intervention judiciaire. Ces objections ont toutefois été rejetées par les tribunaux[83]. Le droit d'auteur est protégé en tant que tel par la Constitution irlandaise et mérite une protection appropriée. Lors de la procédure judiciaire, d'autres questions concernant la forme et la procédure ont été portées au premier plan, de sorte que les tribunaux se sont relativement peu penchés sur la question des rapports entre le droit d'auteur et le droit de la protection des données.

D'autre part, on peut voir dans la configuration du dispositif irlandais que la problématique se situe plutôt au niveau du droit à l'information : le blocage de l'accès à internet est appliqué sans fondement légal ni aucune participation d'une autorité.

*5.4. Espagne : Ley Sinde*

En Espagne, un modèle complètement différent a été mis en place. Les suspensions de l'accès internet ciblent davantage les plateformes par le biais desquelles ont été commises les violations au droit d'auteur que l'utilisateur final[84].

La *Ley Sinde*[85] instaure un processus permettant aux ayants droit de signaler les plateformes internet par le biais desquelles sont commises des infractions au droit d'auteur, notamment les réseaux *peer-to-peer*. Une commission gouvernementale examine ensuite les mesures à prendre contre l'opérateur de la plateforme. Si la Commission estime que la plainte est justifiée, elle transmet l'affaire au tribunal, qui peut ordonner la fermeture du site concerné.

80) McGonagle M., IRIS 2006-4/26.
81) En ce sens, le modèle irlandais est innovant au sens visé par la Communication de la Commission « Renforcer l'application des droits de propriété intellectuelle sur le marché intérieur » du 11 septembre 2009, COM(2009) 467 final, dans laquelle la Commission invite les parties intéressées à mettre en place des accords volontaires pour trouver des solutions pratiques permettant de concilier le droit d'auteur et la protection des données à caractère personnel, même si le groupe des utilisateurs était absent de ce compromis.
82) McGonagle M., IRIS 2010-6/34.
83) McGonagle M., IRIS 2012-8/29 ; ce qui a été confirmé récemment par la *Supreme Court*, (cour suprême irlandaise) dans un arrêt du 3 juillet 2013, disponible sur www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/c9861b9cda79509b80257b9d004e9a7a?OpenDocument
84) Letai P., IRIS 2012-7/18; 2012-4/22; 2012-2/18.
85) *Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual.*

Comparativement aux dispositifs nationaux présentés ci-dessus, la formule espagnole est certainement la forme plus clémente, du point de vue de la protection des données de l'utilisateur final, d'intervention pour la protection du droit d'auteur. Les sanctions ciblent uniquement le fournisseur de services internet. Des mesures préventives telles que le blocage d'un site impliquent nécessairement une intervention moins invasive auprès de l'utilisateur final, puisque aucune donnée personnelle n'est collectée en lien avec une violation concrète. Néanmoins - comme toujours avec ce genre de mesures préventives - ce dispositif met en cause la liberté d'information et d'expression des utilisateurs ainsi que les intérêts des intermédiaires concernés.

### 6. Problématique en cas d'utilisation payante

Tous les cas mentionnés précédemment concernent une utilisation en infraction avec le droit d'auteur et la procédure consécutive en dommages et intérêts. Toutefois, il existe également des conflits entre la vie privée et le droit d'auteur dans le cadre d'une utilisation légale. Ainsi, le droit de la protection des données exige qu'un fournisseur de vidéos à la demande ne collecte et n'utilise des renseignements personnels dans le cadre de son offre que si cela est *nécessaire* pour la gestion des relations contractuelles[86]. Il n'est pas nécessaire de fournir des informations relatives au sexe, au niveau universitaire, au numéro de téléphone ou autre. Un supplément d'information est possible, mais uniquement avec le consentement de l'utilisateur[87]. Le droit de la protection des données interdit, cependant, de subordonner l'accès à un service à l'autorisation de collecter et de traiter certaines données. Il est tout aussi difficile d'évaluer, du point de vue de la protection des données, le profilage en ligne qui permet, par exemple, de placer des cookies pour enregistrer le comportement de l'utilisateur et lui présenter des offres adaptées personnalisées. La Directive 2001/29/CE sur le droit d'auteur considère ce genre de systèmes d'information comme une opportunité pour la protection du droit d'auteur[88], mais exige que l'utilisation de ces systèmes respecte la vie privée du consommateur conformément à la Directive 95/46/CE sur la protection des données.

Il est donc très important, pour le consommateur et, partant, pour l'exploitation légale des droits d'auteur dans le secteur des activités en ligne, que la protection des données soit d'un haut niveau. Une étude menée par IBM révèle que 41 % des internautes au Royaume-Uni et 56 % en Allemagne s'abstiennent de tout achat en ligne en cas d'incertitude quant à l'utilisation de leurs données personnelles[89]. A cet égard, une offre garantissant la confidentialité des données peut s'avérer utile pour stimuler l'exploitation en ligne.

86) Voir l'article 7, alinéa b) de la Directive sur la protection des données 95/46/CE et l'article 6, paragraphe 1, alinéa b) de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).
87) C'est pourquoi la distinction est souvent faite entre champs obligatoires et facultatifs sur les pages d'enregistrement des fournisseurs d'accès.
88) Considérant 57 de la Directive sur le droit d'auteur 2001/29/CE.
89) IBM Multi-National Consumer Privacy Survey, 1999, p. 27, disponible sur : ftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf

## IV. Conclusion

Avec ses trois arrêts clés sur les liens entre droit d'auteur et droit de la protection des données (*Promusicae, LSG* et *Bonnier Audio*), la CJUE s'est penchée sur les conflits entre les intérêts des ayants droit en matière de droit d'auteur et les intérêts légitimes des utilisateurs en matière de protection des données. Du fait de la « généreuse référence» faite à l'importance du principe de proportionnalité, ces arrêts ne présentent que peu d'éléments tangibles en faveur du droit d'information. Force est de constater que la protection des données bénéficie d'une préférence en pratique sur les directives en matière de droit d'auteur et que la légitimité au regard du droit de l'Union européenne de la publication des données et de la création d'un droit d'information est toujours, en définitive, ancrée dans la pondération des intérêts en présence, c'est-à-dire d'une part, le droit de propriété et, d'autre part, le droit à la protection des données personnelles. Dans aucun arrêt pertinent la CJUE ne donne de directives précises pour ce processus de pondération. En outre, il reste à savoir comment le droit d'information, qui est défini de façon abstraite dans le droit de l'UE d'une part à l'article 8 de la Directive 2004/48/CE relative au respect des droits de propriété et à l'article 8 de la Directive 2001/29/CE sur le droit d'auteur, devrait être mis en pratique sans préjudice des normes établies par la Directive 95/46/CE sur la protection des données et la Directive Vie privée et communications électroniques (2002/58/CE), ainsi que des décharges de responsabilité prévues par la Directive 2000/31/CE sur le commerce électronique.

Dans son étude réalisée pour le compte de la DG Marché intérieur et services de la Commission européenne, le cabinet juridique belge Hunton & Williams constate qu'à bien des égards, ces questions restent sans réponse, tant au niveau européen qu'au niveau national. Par conséquent, le niveau d'harmonisation est très faible en matière de droit d'information à l'encontre des intermédiaires en cas de violation du droit d'auteur[90]. Actuellement, rien ne permet de penser que l'Union européenne vise à instaurer une plus grande harmonisation dans ce domaine. Les projets relatifs à un règlement de base en matière de protection des données et la proposition de directive sur les sociétés de gestion collective[91] permettent néanmoins d'espérer des efforts en faveur d'une réforme globale dans les différents domaines juridiques concernés. Toutefois, il semble que jusqu'à présent, ces réformes ne tiennent pas compte du conflit entre droit d'auteur et protection des données et, en particulier, qu'elles ne clarifient aucun point concernant la question du droit d'information des ayants droit à l'encontre les intermédiaires[92].

Les solutions alternatives au droit d'information, c'est-à-dire la possibilité de mettre en place des systèmes de filtrage et, surtout, la suspension de l'accès à internet, se révèlent parfois plus souples en matière de protection des données, mais impliquent souvent une ingérence massive dans d'autres droits des utilisateurs et, également, des intermédiaires. Les Etats membres envisagent d'ores et déjà des approches différentes ; il reste à voir si un système s'imposera à long terme - et si oui, lequel - pour l'application des droits d'auteur dans le secteur des activités en ligne.

90) Kuner C.,Burton C.,Hladjk J.et Proust O., Study on Online Copyright Enforcement and Data Protection in Selected Member States, novembre 2009, disponible sur : http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf

91) Proposition de directive du Parlement européen et du Conseil concernant la gestion collective des droits d'auteur et des droits voisins et la concession de licences multiterritoriales de droits portant sur des œuvres musicales en vue de leur utilisation en ligne dans le marché intérieur du 11 juillet 2012, COM(2012) 372 final.

92) Au contraire, on voit émerger de nouveaux champs conflictuels. Citons à titre d'exemple la surveillance automatisée de l'utilisation des œuvres protégées en conformité avec la licence, voir le considérant 27 et les articles 22 et suivants de la Proposition de directive sur les sociétés de gestion collective.

IRIS plus
2013-6 p.29

# Jurisprudence récente

Comme nous l'avons déjà mentionné, les relations entre le droit d'auteur, la liberté d'expression et la vie privée sont à ce point conflictuelles qu'il est souvent difficile de déterminer quel intérêt doit prévaloir sur l'autre. En ce cas, les tribunaux doivent manier le scalpel pour disséquer au plus près toutes les questions juridiques et techniques complexes avant de décider qui a raison. Cette section offre un aperçu des affaires récentes jugées par les tribunaux nationaux concernant, entre autres, des services internet bien connus tels que The Pirate Bay, VKontakte, YouTube ou Rapidshare. Ces décisions révèlent non seulement la complexité du problème, mais aussi le fait que ces affaires ne sont pas seulement tranchées au cas par cas, mais aussi en fonction des différents pays.

2013-6 p.30

# Allemagne

## Le BGH précise les obligations de surveillance de l'hébergeur *Rapidshare*

*Christian Lewke*
*Institut du droit européen des médias (EMR), Sarrebruck/Bruxelles*

Dans un arrêt du 15 août 2013, le *Bundesgerichtshof* (cour fédérale de justice - BGH) précise la portée de l'obligation de surveillance d'un prestataire de services d'hébergement de fichiers et, au-delà de l'exonération de responsabilité visée aux articles 7, paragraphe 2 et 10 de la *Telemediengesetz* (loi allemande sur les télémédias - TMG) ainsi qu'aux articles 14, paragraphe 1, et 15, paragraphe 1 de la Directive sur le commerce électronique (2000/31/CE), requiert une obligation de surveillance partiellement proactive de la part de l'hébergeur.

Cette décision fait suite à une plainte de *la Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte* (société allemande pour la protection des droits de représentation musicale et de reproduction mécanique - GEMA) contre l'hébergeur « Rapidshare ». La GEMA avait demandé le retrait de nombreux titres de musique enregistrés sur Rapidshare mais l'hébergeur ne les avait pas supprimés intégralement.

Dans son arrêt, le BGH confirme tout d'abord sa jurisprudence : en vertu de l'article 7, paragraphe 2 de la TMG, le fournisseur de service n'a pas d'obligation générale de surveiller les informations qui sont simplement stockées par ses soins. Mais, selon les circonstances, une telle obligation peut être envisagée au cas par cas.

Le BGH estime que les fournisseurs de services qui stockent des informations fournies par les utilisateurs doivent faire preuve de la diligence que l'on est raisonnablement en droit d'attendre d'elles pour détecter certains types d'activités illicites.

En l'espèce, le modèle économique de Rapidshare n'a pas été conçu initialement pour permettre des infractions, puisque le service permet également des modes d'utilisation licites. Il n'y a donc pas lieu de retenir une obligation de surveillance sans motif.

Cependant, pour plusieurs raisons, il existe une obligation de surveillance pour motif précis dès lors que l'hébergeur a connaissance d'une infraction ayant fait l'objet d'une intervention concrète de la part d'un ayant droit, sachant que Rapidshare renforce par ses propres mesures le risque d'un usage illicite de son service. Ainsi, le nombre de 100 000 téléchargements de certains fichiers, que l'hébergeur annonce pour faire la promotion de ses services, ne peut être atteint qu'avec des contenus très attrayants et illicites. L'attrait d'un usage illicite est renforcé par la possibilité d'utiliser les services de manière anonyme. En outre, l'attribution de points *premium* supplémentaires aux utilisateurs en fonction du nombre de téléchargements doit être considérée comme un autre indice révélateur d'une volonté de promouvoir la violation massive du droit d'auteur.

Ainsi se pose la question de la portée de l'obligation de surveillance de l'hébergeur pour un motif précis. Dans sa jurisprudence, le BGH estimait jusqu'à présent qu'on pouvait en principe attendre d'un fournisseur de services qu'il vérifie au moins un nombre réaliste de listes de liens vers certains contenus spécifiques. A présent, le BGH établit clairement que même avec une multitude d'œuvres musicales, à savoir plus de 4 800, on est en droit d'attendre de l'hébergeur un suivi régulier des listes de liens. Dans cette mesure, on peut exiger de la part de l'hébergeur qu'il utilise au moins un dispositif de filtrage de mots.

En outre, le BGH précise que Rapidshare est également tenu de se renseigner sur d'autres liens illicites par le biais des moteurs de recherche courants. A cet égard, la seule mention des mesures générales de prévention (équipe «Abuse team» [détection des contrefaçons] de 17 personnes, filtre MD5, interfaces de suppression pour les ayants droit) ne suffit pas à décharger la défenderesse.

• *Urteil des BGH vom 15. August 2013 (Az. I ZR 79/12)* (Arrêt du BGH du 15 août 2013 (affaire I ZR 79/12))
http://merlin.obs.coe.int/redirect.php?id=16700

IRIS 2013-9/9

## L'OLG de la Hanse interdit à *Rapidshare* la mise à disposition de certains contenus

*Tobias Raab*
*Institut du droit européen des médias (EMR), Sarrebruck/Bruxelles*

Par arrêt du 14 mars 2012, le *Hanseatisches Oberlandesgericht* (tribunal régional supérieur de la Hanse - OLG) a interdit à l'hébergeur de fichiers Rapidshare de mettre à disposition certains contenus protégés par la loi sur le droit d'auteur.

Les juges se sont ainsi rangés à l'avis du *Landgericht* (tribunal régional - LG) de Hambourg qui avait adopté la requête des éditeurs Campus et De Gruyter de même que le point de vue juridique de la *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte* (société allemande pour la protection des droits de représentation musicale et de reproduction mécanique - GEMA) relatif à la responsabilité et aux obligations de Rapidshare. L'hébergeur a désormais interdiction de mettre les textes des éditeurs cités, de même que les œuvres musicales répertoriées par la GEMA, à la disposition de ses utilisateurs.

Afin d'établir la responsabilité secondaire se posait en l'occurrence la question de savoir dans quelle mesure Rapidshare pouvait être tenu responsable d'une utilisation illicite de ses services et si l'hébergeur prenait une « part active » au délit ou bien s'il se limitait à jouer un rôle « d'intermédiaire neutre ». L'OLG a estimé qu'à l'époque considérée, la nature même de Rapidshare encourageait implicitement ses utilisateurs à contrevenir à la loi et que l'hébergeur était responsable de la mise à disposition de ses capacités de sauvegarde comme de l'attribution de liens. Ces considérations ont mené à la question de la violation du droit d'auteur. Le tribunal a par ailleurs jugé que les mesures prises jusqu'alors par l'hébergeur contre l'utilisation illicite de son site n'étaient pas suffisantes et qu'il ne pouvait se contenter d'attendre les réactions d'un titulaire de droits pour agir contre la violation du droit d'auteur et effacer les liens incriminés. En cas de signalement d'un lien contraire à la loi, il convient de surveiller l'« environnement » des liens mis en cause en examinant toutes leurs pages ainsi que les liens similaires. Rapidshare doit donc suivre les derniers développements pour ne pas faillir à son « obligation de surveillance du marché », et ne pas se limiter aux listes de liens connus. C'est la seule façon d'éviter efficacement de nouvelles violations du droit. Rapidshare n'ayant pas tenu compte de ces aspects, l'OLG s'est rangé à l'avis des instances précédentes et a interdit à l'hébergeur de fichiers la mise à disposition des contenus incriminés.

Les magistrats se sont toutefois écartés de la jurisprudence sur deux points : ils ont corrigé le point de vue selon lequel une violation du droit d'auteur était constituée dès « l'upload », c'est-à-dire la mise à disposition des œuvres, considérant qu'à l'ère de l'informatique en nuage, des services de ce type sont de plus en plus utilisés pour la sauvegarde de copies autorisées ; les magistrats ont en outre observé qu'entre le dépôt de plainte et le jugement, Rapidshare avait fait preuve de plus en plus de sérieux dans l'exercice de son rôle de prestataire de services informatiques en nuage, se révélant dans une large mesure comme « un intermédiaire neutre ». L'ancien grief d'incitation implicite des utilisateurs à des actes illicites n'était donc plus pertinent. L'établissement d'une responsabilité secondaire de Rapidshare a été rendue possible par ces modifications, bien qu'il n'ait plus été question d'influence exercée sur les utilisateurs. Le motif retenu a été que Rapidshare donnait à ses utilisateurs la possibilité d'utiliser des services de manière anonyme, les incitant ainsi « activement » à violer le droit d'auteur. L'hébergeur ne

pouvait pas se référer à l'article 13 paragraphe 6 de la Telemediengesetz (loi sur les télémédias - TMG) qui prévoit que les utilisateurs puissent utiliser les services d'un fournisseur de manière anonyme ou sous le couvert d'un pseudonyme. Cette disposition est en effet applicable pour peu qu'elle soit « techniquement possible et réaliste », ce qui, en l'espèce « n'était manifestement pas le cas en considération de l'exposition du modèle d'entreprise du défendeur [au risque de violation du droit d'auteur] et justifie qu'à l'avenir soit potentiellement retenu le principe de responsabilité secondaire.

• *Pressemitteilung des Hanseatichen Oberlandesgerichts zum Urteil (Az. 5 U 87/09), 15. März 2012* (Communiqué de presse de l'Hanseatiches Oberlandesgericht sur l'arrêt (affaire 5 U 87/09), 15 mars 2012)
http://merlin.obs.coe.int/redirect.php?id=15787

IRIS 2012-5/12

## L'OLG de Munich dispense *YouTube* de fournir les données d'un utilisateur

*Anne Yliniva-Hoffmann*
*Institut du droit européen des médias (EMR), Sarrebruck/Bruxelles*

Selon les médias, l'*Oberlandesgericht* (tribunal régional supérieur - OLG) de Munich a décidé, lors d'une procédure d'urgence du 17 novembre 2011, que YouTube n'était pas tenu de divulguer à un ayant droit les données permettant d'identifier un utilisateur qui aurait mis en ligne des contenus piratés.

Dans cette affaire, un utilisateur de YouTube avait publié sur le portail vidéo des séquences de films qu'il avait manifestement réalisées en filmant un écran de cinéma. Se considérant lésée dans ses droits, la société de distribution concernée a exigé le retrait des séquences diffusées sur YouTube, ainsi que des informations sur l'identité de l'utilisateur. YouTube s'est exécuté sans délai sur le premier point, mais a refusé de fournir les données personnelles de l'utilisateur.

L'OLG de Munich a également rejeté cette requête d'informations, confirmant en appel la décision de la juridiction précédente. Même s'il y a effectivement une violation du droit d'auteur, la dimension commerciale du délit, telle qu'elle est requise par l'article 101 de la loi sur le droit d'auteur pour justifier une requête d'information, fait défaut. Les déclarations faites à cet égard par le requérant sont insuffisantes, d'autant plus qu'il n'existe aucun élément étayant l'hypothèse d'une quelconque intention lucrative de l'utilisateur.

Selon les médias, le distributeur du film envisage de poursuivre son action dans une procédure au principal.

• *Beschluss des Oberlandesgericht München vom 17. November 2011 (Az. 29 U 3496/11)* (Arrêt de l'*Oberlandesgericht* de Munich du 17 novembre 2011 (affaire 29 U 3496/11))

IRIS 2012-1/21

# Finlande

## Irrecevabilité d'un recours introduit par un fournisseur de services internet dans le cadre de l'affaire *The Pirate Bay*

*Anette Alén-Savikko*
*Institut de droit économique international,* Facing the Coordination Challenge,
*Centre de recherche et de communication, Université d'Helsinki*

Le 29 octobre 2012, la Cour suprême finlandaise a déclaré l'irrecevabilité du recours introduit par *Elisa Corporation*, un fournisseur de services de télécommunications et de technologies de l'information et de la communication (TIC), dans le cadre de l'affaire *The Pirate Bay*. A la suite de l'affaire suédoise relative à *The Pirate Bay* et au nom du Groupe national finlandais de la Fédération internationale de l'industrie phonographique (IFPI), le Centre d'information sur le droit d'auteur et de lutte contre le piratage (CIAPC) avait demandé en mai 2011 qu'une ordonnance provisoire soit prise contre *Elisa Corporation* afin de l'empêcher de poursuivre ses infractions au droit d'auteur.

Le recours se fondait sur l'article 60c de la loi finlandaise n° 404/1961 relative au droit d'auteur, dont l'alinéa 1 dispose qu'un juge peut, lorsqu'il instruit une affaire et à la demande du titulaire d'un droit, imposer à un intermédiaire d'interrompre la mise à disposition du public de tout contenu présumé en infraction avec le droit d'auteur (ordonnance de suspension). Cette mesure doit être proportionnée et raisonnable du point de vue à la fois du présumé contrevenant, de l'intermédiaire et du titulaire du droit d'auteur concerné. L'alinéa 2 précise les situations dans lesquelles aucune action en justice n'a encore été prise à l'encontre du prétendu contrevenant (réf. au § 60b). Un juge peut, avant même d'auditionner le présumé contrevenant, prendre une ordonnance provisoire dès lors qu'il estime que cette mesure s'avère nécessaire et urgente. Cette ordonnance reste en vigueur jusqu'à nouvel ordre. Le présumé contrevenant doit cependant conserver la possibilité d'être entendu sans délai et le juge doit décider du maintien ou de l'annulation de l'ordonnance en question (alinéa 3). L'ordonnance ne doit toutefois pas porter atteinte au droit d'un tiers à envoyer ou recevoir des messages et n'entrera en vigueur qu'une fois que le requérant aura apporté toutes ces garanties à l'agent chargé de faire exécuter l'ordonnance. En l'absence d'engagement de poursuites, l'ordonnance provisoire sera levée au plus tard un mois après avoir été prise (alinéa 4).

Le 26 octobre 2011, le tribunal d'instance d'Helsinki s'est prononcé en faveur de la requête de l'IFPI en Finlande et a rendu une ordonnance provisoire imposant à *Elisa Corporation*, sous peine de se voir infliger une amende de 100 000 EUR, de supprimer de son serveur l'ensemble des domaines du site *The Pirate Bay* et de bloquer l'accès aux adresses IP utilisées par ce dernier. Les mesures relatives aux abonnements ont été prises en janvier 2012, à la suite de l'exécution de cette ordonnance. *Elisa Corporation* a fait appel du jugement du tribunal d'instance, mais le 15 juin 2012, la Cour d'appel d'Helsinki a confirmé la décision rendue en première instance. Cette ordonnance provisoire a été jugée proportionnée au vu de l'efficacité des mesures juridiques et des conditions d'accessibilité du présumé contrevenant. La Cour a par ailleurs précisé que cette ordonnance provisoire pouvait être prolongée sur le long terme si les défendeurs au principal ne peuvent être auditionnés, sans pour autant que cette durée puisse être illimitée. *Elisa Corporation* a finalement demandé à la Cour suprême l'autorisation d'interjeter appel, de manière à ce que cet appel donne lieu à un précédent de la jurisprudence, mais sa requête a été déclarée irrecevable.

- *Helsingin käräjäoikeuden päätös, 26/10/2011, No 41552* (Décision n° 41552 du tribunal d'instance d'Helsinki, 26 octobre 2011)
  http://merlin.obs.coe.int/redirect.php?id=16227

- *Helsingin hovioikeuden päätös, 15/06/2012, No 1687* (Décision n° 1687 de la Cour d'appel d'Helsinki, 15 juin 2012)

• *Korkeimman oikeuden päätös, 29/10/2012, No 2187* (Décision n° 2187 de la Cour suprême, 29 octobre 2012)

IRIS 2013-1/18

## France

### Absence de responsabilité d'un site internet proposant l'accès à des programmes de TV de rattrapage via des liens hypertextes profonds

*Amélie Blocman*
*Légipresse*

Par arrêt du 31 octobre 2012, la Cour de cassation a rejeté le pourvoi formé par le groupe M6 à l'encontre de l'arrêt de la cour d'appel. En l'espèce, le groupe avait été intégralement débouté de ses demandes par la juridiction du fond dans le litige l'opposant à la société qui exploite le site TV-replay.fr, guide en ligne des sites de télévision de rattrapage (voir IRIS 2011-6/17). Le groupe de télévision, qui exploite notamment les chaînes M6 et W9 ainsi que leurs services de télévision de rattrapage M6replay et W9replay, reprochait notamment à TV-replay.fr de donner directement accès à ses programmes, par le biais de liens hypertextes dits « profonds », sans être préalablement dirigé sur les pages d'accueil de M6replay et W9replay. M6 se prévalait d'une violation des conditions générales d'utilisation de ses services de TV de rattrapage, d'une atteinte à ses droits d'auteur et de producteur de base de données, et estimait que le comportement de TV-replay était constitutif de concurrence déloyale et de parasitisme.

La Haute juridiction approuve tout d'abord la cour d'appel d'avoir retenu que la simple mise en ligne des conditions générales d'utilisation des sites M6 et W9, accessibles par un onglet à demi dissimulé en partie inférieure de l'écran, ne suffisait pas à mettre à la charge des utilisateurs des services proposés une obligation de nature contractuelle, et que la lettre de mise en demeure que le groupe M6 avait adressée à la société défenderesse, éditrice du site TV-replay.fr, d'avoir à respecter ces conditions générales d'utilisation, ne faisait pas naître à la charge de cette dernière une obligation contractuelle de s'y conformer.

En outre, la Cour de cassation juge que la cour d'appel a énoncé à bon droit que les sociétés de production du groupe M6 titulaires de droits sur les programmes diffusés ne pouvaient revendiquer collectivement une atteinte à des droits indifférenciés, et qu'elles n'établissaient pas les droits détenus par chacune d'elles sur les œuvres que la société défenderesse rendait accessibles sur son site tv-replay après leur diffusion sur les chaînes de télévision. La Cour rejette également le moyen fondé sur l'atteinte aux droits du groupe M6 en qualité de producteur de bases de données. Enfin, l'arrêt retient que l'utilisateur du site litigieux était dirigé vers le programme recherché qui lui était présenté, inséré dans une fenêtre de navigation des sites de TV de rattrapage des chaînes, laquelle donnait accès à toutes les fonctionnalités des sites et aux bannières publicitaires. La cour d'appel qui en a déduit que le grief allégué, tiré du contournement du processus normal de navigation, n'était pas démontré et que la preuve d'un comportement parasitaire n'était pas rapportée, a ainsi légalement justifié sa décision. Par cet arrêt est mis fin à ce contentieux qui pose toutefois la question des moyens dont disposent les titulaires de droits, pour s'opposer à l'accès à leurs contenus via des liens hypertextes.

• Cour de cassation (1re ch. civ.), 31 octobre 2012 - Société Métropole Télévision

IRIS 2013-1/19

# Pas d'obligation générale de surveillance du réseau, rappelle la Cour de cassation

*Amélie Blocman*
*Légipresse*

Le 12 juillet 2012, la 1re chambre civile de la Cour de cassation par trois arrêts importants a censuré la cour d'appel de Paris qui avait reproché à Google Images et Google Vidéo de ne pas avoir pris les mesures nécessaires pour rendre impossible la remise en ligne d'images et de films contrefaisants. Pour la juridiction suprême, une telle interdiction aboutit à soumettre Google à une obligation générale de surveillance et à lui prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps.

La Cour de cassation était appelée à se prononcer dans des litiges opposant des ayants droit (producteurs des films documentaires *Les Dissimulateurs* et *L'affaire Clearstream*, ainsi qu'un photographe) à Google, après avoir constaté la présence sur des sites accessibles via Google Images et Google Vidéo, de liens permettant aux internautes d'avoir accès gratuitement aux films dans leur intégralité, en streaming ou en téléchargement ainsi qu'à la photographie litigieuse. La cour d'appel avait jugé qu'en offrant la possibilité aux internautes de visionner directement sur les pages des sites Google Vidéo France et Google Images les vidéos et la photo litigieuses, mises en ligne sur des sites tiers, Google a commis des actes de contrefaçon donnant lieu à réparation. En outre, la cour a estimé que Google n'avait pas accompli les diligences nécessaires en vue de rendre impossible une nouvelle mise en ligne des films et de la photo, déjà signalées comme illicites. La société ne pouvait donc se prévaloir de la limitation de responsabilité prévue à l'article 6. I. 2 de la loi du 21 juin 2004 et avait donc engagé sa responsabilité à ce titre. Contestant ces arrêts d'appel, Google a donc formé un pourvoi devant la Cour de cassation. Dans un premier temps, la Haute juridiction souligne que Google, à partir des liens vers les autres sites, offre à l'internaute la possibilité de visionner les films d'une part, sur son propre site Google Vidéo, et la photographie d'autre part, sur Google Images. C'est à juste titre que la cour d'appel en a déduit que Google met alors en œuvre une fonction active qui lui permet de s'accaparer le contenu stocké sur des sites tiers afin d'en effectuer la représentation directe sur ses pages à l'intention de ses propres clients. La cour d'appel, qui a constaté que Google reproduisait ainsi le film sur ses sites, sans autorisation des titulaires des droits, ce qui caractérise la contrefaçon, allait ainsi au-delà de la mise en œuvre d'une simple fonctionnalité technique, et a légalement justifié sa décision.

Mais, dans un second temps, la Cour de cassation casse et annule, au visa de l'article 6, en ses dispositions I.2, I.5 et I.7 de la LCEN du 21 juin 2004, les arrêts d'appels en ce qu'ils ont refusé le bénéfice de ces dispositions et dit que les sociétés demanderesses n'avaient pas « pris les mesures utiles de nature à prévenir de nouvelles mises en ligne », peu importe que les films et la photo aient été accessibles à partir d'adresses différentes de celles portées dans les constats initiaux. Pour la Cour de cassation, cette décision, ainsi imposée à Google, en tant que prestataire de service de référencement, pour empêcher toute nouvelle mise en ligne des films et de l'image contrefaisants, sans même que la société en ait été avisée par une autre notification régulière pourtant requise par ladite loi, aboutit à soumettre Google « à une obligation générale de surveillance des images et des films qu'elle stocke, et de recherche des reproductions illicites, et à lui prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps ».

• Cour de cassation (1re ch. civ.), 12 juillet 2012 - *Google c. Bach Films et a.* (3 arrêts)

IRIS 2012-8/24

2013-6 p.36

# TF1 intégralement déboutée de ses demandes contre *YouTube*

*Amélie Blocman*
*Légipresse*

Le 29 mai 2012, aux termes d'un jugement de 34 pages, le tribunal de grande instance de Paris a débouté TF1 et ses filiales (la chaîne LCI, TF1 Vidéo et TF1 International, en charge de l'édition vidéo, de l'acquisition et de la distribution des droits) de ses poursuites contre YouTube pour contrefaçon, concurrence déloyale et parasitisme. Outre des mesures d'interdiction, la chaîne demandait réparation de son préjudice, qu'elle évaluait à 150 millions d'euros, en raison de la mise en ligne sur la plateforme de partage vidéo de toute une série de films, séries, événements sportifs, et émissions dont elle estimait avoir les droits, dont certains avant toute diffusion ou exploitation commerciale en France.

Dans un premier temps, le tribunal examine si les sociétés demanderesses ont suffisamment et correctement identifié les contenus litigieux. Il statue à cette fin selon les qualités desdites sociétés, et selon les fondements invoqués (droit d'auteur et droits voisins), et ce pour chaque contenu litigieux. Or, il est jugé que les sociétés demanderesses n'apportent pas la preuve de leurs droits invoqués. Ainsi, contrairement à ce que soutient TF1 Vidéo, elle n'est pas ayant droit des producteurs de vidéogrammes litigieux car elle n'a acquis qu'un droit d'exploitation, et ne démontre pas l'exclusivité dont elle se prévalait. De même, la société TF1 Droits audiovisuels, selon les œuvres, soit n'établit pas sa qualité de producteur d'œuvre audiovisuelle ou de vidéogramme, soit ne fait pas la preuve qu'elle a attrait les autres co-producteurs ou aurait leur autorisation d'agir seule. Ces deux sociétés sont donc irrecevables en leurs demandes. Par ailleurs, la reproduction et la mise à disposition du public des programmes des chaînes TF1 et LCI, qui sont elles-mêmes des entreprises de communication audiovisuelle, sont soumises à leur autorisation, conformément à l'article 216-1 du Code de la propriété intellectuelle (CPI). Mais le tribunal rappelle qu'aucune présomption de titularité n'est prévue pour bénéficier de cette protection. Il appartient à celui qui la réclame de démontrer l'existence du programme et la preuve de sa diffusion antérieure à la reprise sur YouTube alléguée. En l'espèce, les documents produits pour les chaînes (grilles de programmes, dossiers de presse…) sont jugés insuffisants au tribunal et les chaînes déclarées irrecevables en leurs demandes sur le fondement de l'article L. 216-1 du CPI, à l'exception de sept événements sportifs pour lesquels les éléments de preuves requis ont été apportés. De même, sur le fondement du droit d'auteur, les chaînes n'apportent pas la preuve de l'originalité des programmes (dont le Journal Télévisé) dont elles reprochaient la mise en ligne sur YouTube.

Une fois la titularité des droits examinée, le tribunal se penche sur le statut de la plateforme de partage vidéo. Dans un schéma désormais classique, les demanderesses soutenaient que la plateforme devait se voir appliquer le statut d'éditeur, en ce qu'elle jouerait un rôle actif sur les contenus mis en ligne par les utilisateurs. YouTube se prévalait de la qualité d'hébergeur, au sens de l'article 6-1-2 de la loi du 21 juin 2004, dite LCEN. Pour débouter TF1 et LCI de leur demande, et conforter le statut d'hébergeur de YouTube, le tribunal rappelle les dispositions de la LCEN, la position de la Cour de cassation dans la lignée de celle de la CJUE, examine les conditions d'utilisation du service en vigueur quand la procédure a été engagée, rappelle la licéité du recours à la publicité pour les hébergeurs, qui ne les prive pas de leur statut. En application des articles 6 et 7 de la LCEN, le tribunal examine ensuite les fautes reprochées à YouTube en sa qualité d'hébergeur et rappelle l'exigence de retirer promptement le contenu litigieux une fois qu'il lui est notifié. Or, en l'espèce, il juge que la plateforme a trop tardé en mettant « au mieux » cinq jours à supprimer les vidéos des sept événements sportifs en cause. Dans la mesure où ce délai « ne peut être qualifié de raisonnable », la plateforme est donc fautive. Cependant, dans une ultime observation sur ce point, le tribunal observe qu'en tout état de cause les conditions de l'article L. 216-1 du CPI ne sont pas remplies pour constater une faute de la part de YouTube, dès lors que la condition relative au paiement d'un droit d'entrée n'est pas remplie, puisque l'accès au site est gratuit. En conclusion, il est observé que la plateforme a conclu avec TF1 le 16 décembre 2011 un accord lui permettant d'accéder au service « Content ID » permettant aux titulaires de droits d'obtenir, après notification du contenu, le retrait définitif de la vidéo notifiée comme

litigieuse. Aucune atteinte n'a été déplorée par les requérantes depuis cette date. Le litige est-il pour autant clos ? Un appel est encore possible…

• TGI de Paris (3e ch. 1re sect.), 29 mai 2012 - *TF1, LCI et autres c/ Youtube*
http://merlin.obs.coe.int/redirect.php?id=15997

IRIS 2012-7/22

## Sanction de la contrefaçon de film sur une plateforme vidéo

*Amélie Blocman*
*Légipresse*

Le 9 mai 2012, la cour d'appel de Paris a rendu sa décision dans le litige opposant les producteurs du film Sheitan à la plateforme de partage vidéo Dailymotion. En effet, cinq vidéos, correspondant à l'intégralité du film découpé en cinq parties, pouvaient être visionnées en streaming sur la plateforme, et ce en dépit d'une ordonnance sur requête du TGI de Paris lui enjoignant de communiquer les données de nature à permettre l'identification de l'auteur des mises en ligne illicites.

Le tribunal de grande instance de Paris avait, le 11 juin 2010, condamné la plateforme pour contrefaçon à 15 000 EUR de dommages-intérêts (voir IRIS 2010-7/19), après avoir constaté la qualité de fournisseur d'hébergement de celle-ci, que lui déniait les producteurs du film. Il n'avait néanmoins pas reconnu à la société la possibilité de se prévaloir du régime de responsabilité limitée instauré par l'article 6-I-2 de la loi du 21 juin 2004 (LCEN), faute pour elle d'avoir « promptement » retiré le contenu contrefait que ces derniers lui avaient notifié. Rappelons qu'aux termes de ce texte, les personnes physiques ou morales qui exercent une activité de stockage de contenus ne peuvent voir leur responsabilité engagée que « si (…) dès le moment où elles ont eu connaissance du caractère illicite d'un contenu stocké, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ». La plateforme avait fait appel de sa condamnation. Dans son arrêt du 9 mai 2012, la cour constate que, contrairement à la première instance, et eu égard à une jurisprudence désormais bien établie, les parties s'accordent pour regarder Dailymotion comme répondant à la définition précitée du fournisseur d'hébergement, dès lors qu'elle met à la disposition du public un service de stockage de contenus audiovisuels (en l'espèce, des programmes personnels) fournis par les destinataires de ce service, sans avoir le pouvoir de sélectionner ces contenus. Les parties s'entendent en conséquence pour voir apprécier la responsabilité encourue par Dailymotion à l'aune des dispositions spécialement édictées par la LCEN à l'endroit du prestataire de stockage. En revanche, elles divergeaient sur le point de savoir si la plateforme avait satisfait aux obligations attachées à ce statut. Rappelant ces obligations, la cour va donc procéder en deux temps. Conformément à l'art. 6-I-2 de la LCEN, elle examine tout d'abord si la plateforme a retiré « promptement » les contenus attentatoires à des droits de propriété intellectuelle dès lors qu'elle en a eu effectivement connaissance. A cette fin, les juges relèvent que la plateforme avait, dès le jour de la signification de l'ordonnance sur requête, adressé par courrier au conseil de l'une des sociétés de production demanderesse à l'action, toutes les données et statistiques relatives aux cinq vidéos litigieuses (date de mise en ligne, adresse IP de l'auteur de celle-ci, statistiques). Elle est en conséquence mal fondée à prétendre, « non sans mauvaise foi » ajoute l'arrêt, que les éléments de l'ordonnance sur requête étaient insuffisants à lui permettre d'identifier et de localiser les contenus incriminés de contrefaçon. Or, elle a laissé s'écouler plus de trois mois entre la date à laquelle elle a eu effectivement connaissance des contenus contrefaits et celle à laquelle elle a procédé à leur retrait. Elle a ainsi manqué à l'obligation de prompt retrait qui incombe au prestataire de stockage.

Puis dans un second temps, la cour montre que la plateforme a failli à l'obligation qui lui est imposée par la LCEN de rendre impossible aux contenus précédemment retirés un nouvel accès à

la plateforme d'hébergement. En effet, contrairement à ce que soutenait Dailymotion en défense, les extraits du film disponibles sur le site après le premier retrait ne sauraient être regardés comme des contenus différents de ceux précédemment retirés. Ils réalisent donc une contrefaçon de la même œuvre et une atteinte des mêmes droits de propriété intellectuelle.

Si la cour confirme la responsabilité de Dailymotion, en revanche, elle considère que le préjudice subi par les sociétés de production demanderesses a été sous-estimé en première instance. Prenant acte de ce que les contenus illicites n'ont été retirés que plus de trois mois après avoir été signalés, qu'ils ont encore été rétablis après avoir été retirés et qu'ils ont fait l'objet, au moins jusqu'à leur retrait, de plus de 12 000 visionnages, elle condamne Dailymotion à leur verser 30 000 EUR à chacune des sociétés de production à titre de dommages-intérêts (contre 15 000 en première instance).

• Cour d'appel de Paris (pôle 5, ch. 1), 9 mai 2012 - *Dailymotion c. SARL 120 Films et La chauve-souris*

IRIS 2012-6/17

## Royaume Uni

### La Haute cour ordonne aux fournisseurs d'accès internet de bloquer l'accès aux sites de partage

*Tony Prosser*
*School of Law, Université de Bristol*

Dans sa décision du 28 février 2013, la Haute cour a ordonné à six fournisseurs d'accès internet de premier plan (représentant 94 % des internautes britanniques) de bloquer l'accès à trois sites de partage de fichiers en *peer-to-peer* appelés KAT, H33T et Fenopy. Cela fait suite à des décisions antérieures de la Haute cour exigeant le blocage d'autres sites (voir IRIS 2012-7/25 et IRIS 2011-9/21).

L'affaire a été portée par dix grandes maisons de disques en leur nom propre et en celui d'autres membres d'associations professionnelles de la musique enregistrée. Les trois sites génèrent chacun une activité lucrative substantielle dans le partage de fichiers, en particulier dans la musique. L'article 97A de la loi de 1988 relative au droit d'auteur, aux modèles et aux brevets, transposant la directive sur la société de l'information, habilite la Cour à rendre une ordonnance contre un fournisseur d'accès « dès lors que ce dernier a pleinement conscience du fait qu'un tiers utilise ses services pour enfreindre le droit d'auteur ». La Cour a considéré que les utilisateurs des sites web détenant des comptes auprès des défendeurs partageaient des enregistrements et, ainsi, en faisaient des copies non autorisées. Il s'agissait d'une pratique à grande échelle. Le matériel était également communiqué à un nouveau public et, bien que les sociétés aient été basées en dehors du Royaume-Uni, les sites web ciblaient le Royaume-Uni. Chaque site web visait simplement à rendre possibles les copies. Bien que les sites aient contenu des déclarations selon lesquelles leurs équipes étaient opposées au piratage, ces déclarations n'étaient pas convaincantes étant donnée la quantité de matériel mis à disposition en violation du droit d'auteur, l'inefficacité de leurs réponses aux demandes de suppression de contenu et les dispositions qu'ils avaient prises pour éviter les mesures d'exécution. Les utilisateurs et les exploitants des sites web utilisaient les services de fournisseurs d'accès pour enfreindre le droit d'auteur et les fournisseurs étaient informés chaque semaine des activités illicites, ils en avaient donc pleinement conscience ; aucun des fournisseurs n'a d'ailleurs nié ce fait.

La Cour a également considéré que les ordonnances établissaient un équilibre proportionné entre droits de propriété des requérants d'une part, et droit à la liberté d'expression d'autre part. Dans cette affaire, les fournisseurs d'accès ont accepté les ordonnances et n'ont pas cherché

à s'y opposer au motif qu'elles seraient excessivement coûteuses ou difficiles à mettre en œuvre. Bien que les mesures puissent être contournées, elles pouvaient être justifiées car elles empêchent l'accès d'une minorité d'utilisateurs seulement. Des données probantes suggèrent que ces ordonnances sont raisonnablement efficaces. Les ordonnances étaient restreintes et ciblées, et nécessaires et appropriées pour protéger les droits de propriété intellectuelle. Cela l'emporte nettement sur les droits à la liberté d'expression des utilisateurs qui peuvent obtenir le matériel auprès de sources légales, et des opérateurs de site qui profitaient de ces infractions.

- *Emi Records and others v. British Sky Broadcasting Ltd and others, [2013] EWHC 379 (Ch)* (Emi Records et autres c. British Sky Broadcasting Ltd et autres, [2013] Haute cour d'Angleterre et du pays de Galles 379 (Ch))
  http://merlin.obs.coe.int/redirect.php?id=16413

IRIS 2013-5/29

## La Haute Cour ordonne aux fournisseurs de services internet de bloquer l'accès au site *The Pirate Bay*

*Tony Prosser*
*School of Law, Université de Bristol*

Le 2 mai 2012, la Haute Cour britannique a rendu une ordonnance, en vertu de la loi relative au droit d'auteur, aux modèles et aux brevets de 1988, qui impose aux principaux fournisseurs de services internet de bloquer l'accès des internautes au site de partage de fichiers The Pirate Bay. La loi, telle que modifiée, transpose en droit interne la Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Les maisons de disques avaient engagé une action en justice en leur propre nom et pour le compte de British Recorded Music Industry and Phonographic Performance Ltd.

La loi permet à la Haute Cour de rendre une ordonnance contre un fournisseur de services dès lors que ce dernier a pleinement conscience du fait qu'un tiers utilise ses services pour enfreindre le droit d'auteur. La Cour avait déjà rendu une telle ordonnance à l'encontre du site Newzbin2 et avait conclu dans un précédent arrêt que les utilisateurs, ainsi que les exploitants du site The Pirate Bay avaient porté atteinte aux droits d'auteur dont les titulaires avaient engagé une action en justice (voir IRIS 2011-9/21 et IRIS 2012-4/28). En l'espèce, la Cour estime que les fournisseurs de services internet avaient connaissance de cette infraction, dans la mesure où les maisons de disques les en avaient déjà informés et qui avait par ailleurs été évoquée dans une précédente décision de justice. La Haute Cour estime que l'ordonnance n'est pas contraire à l'article 10 de la Convention européenne des droits de l'homme, ni à l'article 11 de la Charte des droits fondamentaux de l'Union européenne. Cette ordonnance est une réponse proportionnée, dans la mesure où sa teneur a en réalité été le fruit d'une négociation menée par des professionnels pour le compte des parties ; elle est par ailleurs proportionnée à l'égard des utilisateurs des services des fournisseurs de services internet pour les mêmes motifs que ceux qui avaient été retenus dans les précédentes affaires. L'ordonnance imposait en conséquence le blocage de l'adresse IP, ce qui était parfaitement réalisable dans la mesure où The Pirate Bay ne partageait son adresse avec personne.

- *Dramatico Entertainment et al v. Brisith Sky Broadcasting et al, [2012] EWHC 1152 (Ch)* (*Dramatico Entertainment et autres c. Brisith Sky Broadcasting et autres, [2012] EWHC 1152 (Ch)*)
  http://merlin.obs.coe.int/redirect.php?id=15944

IRIS 2012-7/25

2013-6 p.40

# La Haute cour ordonne à un fournisseur d'accès internet de communiquer les données à caractère personnel de clients à des producteurs de films pornographiques alléguant une violation du droit d'auteur

*Tony Prosser*
*School of Law, Université de Bristol*

La Haute cour d'Angleterre a ordonné au fournisseur d'accès internet O2 de communiquer les données à caractère personnel de plus de 9 000 clients à une société agissant pour le compte de titulaires de droit d'auteur et à une société de production de films pornographiques, tout en rejetant les demandes similaires déposées par 12 autres titulaires de droit d'auteur.

Golden Eye International Limited, organisation agissant pour le compte de titulaires de droit d'auteur, et 13 producteurs de films pornographiques ont demandé que soit prononcée une « ordonnance Norwich Pharmacal » pour contraindre O2 à leur communiquer les données à caractère personnel de 9 124 de ses clients afin de leur réclamer à chacun 700 GBP à titre de dommages et intérêts pour une présumée violation du droit d'auteur, et à les menacer d'intenter une action en justice et/ou de ralentir ou couper leur accès internet s'ils ne payaient pas. Les lettres proposées affirmaient également à tort que la personne qui paie la facture est responsable de toute violation du droit d'auteur commise sur sa connexion internet, qu'elle ait ou non commis l'infraction. Cette tactique est appelée « facturation spéculative » et vise à intimider les consommateurs afin qu'ils paient sans qu'il soit nécessaire d'aller devant les tribunaux. La requête a été renvoyée devant la Haute cour, qui craignait que les consommateurs dont les informations seraient communiquées ne soient pas en mesure de contester l'infraction. La Haute cour a demandé à l'association de défense des consommateurs Consumer Focus de représenter leurs intérêts devant les tribunaux.

La Haute cour a examiné les intérêts opposés des titulaires de droit d'auteur et du droit du client au respect de sa vie privée et à la protection de ses données à caractère personnel. En ce qui concerne Golden Eye et 12 titulaires de droit d'auteur, elle a conclu que l'ordonnance ne devait pas être prononcée car elle « équivaudrait pour la Cour à autoriser la vente des droits de protection des données et de la vie privée des défendeurs au plus offrant ». Cette décision est motivée par le fait que les titulaires ont confié la gestion du contentieux à Golden Eye, contre environ 75 % des sommes récupérées. En ce qui concerne Golden Eye et un producteur, Ben Dover Productions, qui présentaient le litige conjointement, la Cour a jugé qu'il serait proportionné d'ordonner la divulgation des données à caractère personnel des personnes payant la facture, car le dossier établissant que de nombreux défendeurs avaient violé le droit d'auteur était solide et défendable. Toutefois, l'ordonnance et la lettre qu'il est proposé d'adresser aux clients doivent être rédigées de manière à dûment préserver les intérêts légitimes des consommateurs, en particulier de ceux qui n'ont pas commis les présumées violations du droit d'auteur. Les lettres proposées étaient contestables à plusieurs égards ; elles auraient plutôt dû demander aux clients qui reconnaissaient une violation du droit d'auteur, les détails de leurs partages de fichiers P2P avant de négocier individuellement un règlement approprié. La Cour tiendra une seconde audience pour imposer des conditions quant au libellé des lettres et de l'ordonnance.

- *High Court (Chancery Division), Golden Eye (International) and another v. Telefonica UK Ltd [2012] EWHC 723 (Ch), 26 March 2012* (High Court (Chancery Division), Golden Eye (International) et autre c. Telefonica UK Ltd [2012] EWHC 723 (Ch), 26 mars 2012)
  http://merlin.obs.coe.int/redirect.php?id=15817

IRIS 2012-6/21

# La Cour d'appel déboute les fournisseurs de services internet de leur appel contre des dispositions de la loi relative à l'économie numérique

*Tony Prosser*
*School of Law, Université de Bristol*

Les fournisseurs de services internet BT et TalkTalk ont été déboutés par la Cour d'appel de l'appel qu'ils avaient interjeté contre la décision rendue par la Haute Cour l'an dernier, qui avait conclu que les dispositions de la loi relative à l'économie numérique de 2010 n'étaient pas contraires au droit de l'Union européenne (voir IRIS 2011-6/20).

Les dispositions en question imposent aux fournisseurs de services internet (FSI), d'une part, d'informer leurs abonnés lorsque leurs adresses IP (*Internet Protocol*) sont signalées par les ayants droits comme ayant été utilisées pour porter atteinte au droit d'auteur et, d'autre part, de conserver une trace du nombre de rapports sur chaque abonné et de compiler, anonymement, la liste de ces derniers. Après avoir obtenu du juge une injonction de divulgation des renseignements personnels des abonnés, les ayants droit auront la possibilité d'engager une action en justice à l'encontre des abonnés qui figurent sur ces listes. Ces obligations prendront uniquement effet une fois que le « code initial d'obligations » de l'Ofcom, le régulateur des communications, sera adopté par le Parlement et entrera en vigueur. Les FSI soutenaient que ces exigences auraient dû être notifiées à la Commission européenne en vertu de la directive « normes et techniques » ; qu'elles étaient incompatibles avec les dispositions de la directive « commerce électronique »; qu'elles étaient contraires à la directive « protection des données à caractère personnel » et à la directive « vie privée et communications électroniques » et, enfin, qu'elles étaient incompatibles avec la directive « autorisation ».

La Cour d'appel a estimé que les dispositions de la loi n'imposaient pas de notification dans la mesure où elles n'ont pas d'effet légal en soi puisque leur mise en œuvre est subordonnée à l'application du code. Elles ne sont par conséquent pas contraires à la directive « commerce électronique » dans la mesure où elles n'engagent pas la responsabilité des FSI et, pour ce qui est du droit d'auteur, elles ne relèvent pas du « domaine coordonné » couvert par la directive dans lequel les restrictions à la liberté de fournir des services de la société de l'information sont interdites. Ces dispositions légales ne sont pas contraires à la directive « protection des données à caractère personnel » dans la mesure où le traitement des données s'effectue dans le cadre d'une action en justice, ni à la directive « vie privée et communications électroniques » puisque les restrictions en matière de confidentialité des données à caractère personnel sont destinées à la protection des droits de propriété intellectuelle. Enfin, la directive « autorisation » n'exige pas que l'ensemble des règles spécifiques au secteur soient contenues dans une autorisation générale plutôt que dans une législation distincte. La Cour a par ailleurs estimé qu'il n'était pas disproportionné d'exclure de ce régime les petits FSI et les opérateurs de réseaux mobiles.

Les FSI contestaient également l'ordonnance de répartition des coûts de fonctionnement de ce régime. La Haute Cour avait estimé qu'imposer aux FSI une participation aux frais de mise en œuvre du régime était contraire à la directive « autorisation » et ce point n'a fait l'objet d'aucun appel. La Cour d'appel a en outre conclu que les « frais de justice » destinés à couvrir les frais d'appel étaient incompatibles avec la directive.

- *R (on the application of British Telecommunications and TalkTalk Telecom Group) v. Secretary of State for Culture, Media, Olympics and Sport [2012] EWCA Civ 232, 6 March 2012* (Affaire *British Telecommunications* et *TalkTalk Telecom Group* c. Secrétariat d'Etat à la Culture, aux Médias, aux Sports et aux Jeux olympiques [2012] EWCA Civ 232), 6 mars 2012)
  http://merlin.obs.coe.int/redirect.php?id=15770

IRIS 2012-5/22

2013-6 p.42

# Les exploitants de « The Pirate Bay » violent le droit d'auteur

*Tony Prosser*
*School of Law, Université de Bristol*

La Haute cour a décidé que les exploitants du site web The Pirate Bay et ses utilisateurs sont coupables de violation du droit d'auteur des ayants droit dans l'industrie musicale. Autrement dit, les fournisseurs d'accès internet peuvent désormais être obligés de bloquer l'accès de leurs clients au site.

La procédure a été intentée par une grande maison de disques contre les six principaux fournisseurs d'accès internet britanniques. The Pirate Bay est un site qui permet aux utilisateurs de rechercher et de télécharger du matériel protégé par droit d'auteur, notamment de la musique et des films. Les maisons de disques ont demandé une injonction de la cour pour forcer les fournisseurs d'accès à empêcher leurs clients d'accéder au site. En vertu de la loi de 1988 relative au droit d'auteur, aux modèles et aux brevets (telle que modifiée pour mettre en œuvre la directive de l'UE sur la société de l'information), une telle injonction peut être accordée contre un fournisseur d'accès internet s'il a « effectivement connaissance » du fait que son service est utilisé pour violer le droit d'auteur. Cette audience portait sur la question préliminaire de savoir si les utilisateurs et les exploitants du site avaient enfreint le droit d'auteur.

La cour a estimé que les utilisateurs de The Pirate Bay enfreignaient le droit d'auteur en raison de la façon dont ils partagent des fichiers musicaux ; cela équivalait à communiquer les enregistrements à un nouveau public, comme estimé par la Cour de justice de l'Union européenne dans l'affaire C-306/05 *Sociedad General de Autores c. Editores de España (SGAE) c. Rafael Hoteles SA* [2006] ECR I-11519 (voir IRIS 2007-2/3). Ces violations du droit d'auteur ont été permises par les exploitants de The Pirate Bay qui étaient solidairement responsables à cet égard ; le nom du site et son financement par une organisation suédoise opposée au droit d'auteur ayant contribué à la conclusion de la Cour selon laquelle une telle violation faisait partie de « l'objectif et de l'intention » des exploitants. L'affaire a ainsi ouvert la voie à une décision lors d'une future audience pour accorder une injonction, à la suite du précédent de l'affaire Newzbin2 dans laquelle une telle injonction a été accordée pour forcer un fournisseur d'accès internet à bloquer l'accès à un site violant le droit d'auteur de six grands studios de cinéma (voir IRIS 2011-9/21).

- *Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd [2012] EWHC 268 (Ch), 20 February 2012* (*Dramatico Entertainment Ltd c. British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch), 20 février 2012)
  http://merlin.obs.coe.int/redirect.php?id=15726

IRIS 2012-4/28

## Pays-Bas

# Un tribunal de district néerlandais ordonne à des fournisseurs d'accès à internet de bloquer l'accès au site *The Pirate Bay* aux utilisateurs finaux

*Axel M. Arnbak*
*Institut du droit de l'information (IViR), Université d'Amsterdam*

Le 11 janvier 2012, le tribunal de district de La Haye a ordonné à deux fournisseurs d'accès internet (FAI) néerlandais de bloquer l'accès au site de partage de fichiers The Pirate Bay. Par ailleurs, Stichting BREIN, une fondation protégeant les droits de l'industrie néerlandaise du divertissement, s'est vu accorder le droit de demander directement aux FAI de bloquer toutes les nouvelles adresses IP et les noms de (sous-)domaines qui pourraient faire référence à The Pirate Bay. Les FAI en question, Ziggo et XS4ALL, ont déjà annoncé qu'ils allaient faire appel de cette décision. La fondation BREIN, de son côté, a annoncé que d'autres FAI seront concernés par ces mesures.

Pour établir ce jugement, le tribunal de district s'est fondé sur la transposition en droit interne de l'article 11 de la Directive 2004/48/CE relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle, de l'article 8, paragraphe 3, de la Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et du récent arrêt de la Cour de justice de l'Union européenne dans l'affaire *L'Oréal SA et autres contre eBay* (C-324/09). Dans cette affaire, la Cour de justice avait estimé que lorsque les services d'un intermédiaire tel qu'un exploitant de site internet ont été utilisés par un tiers pour porter atteinte aux droits de propriété intellectuelle, une injonction à l'encontre de cet intermédiaire devrait empêcher de nouvelles atteintes à ces droits. The Pirate Bay avait déjà fait l'objet d'autres procès aux Pays-Bas et il avait été ordonné au site de mettre un terme à toute violation des droits d'auteur sur le marché néerlandais. The Pirate Bay ayant continué à fonctionner de la même manière, le tribunal a estimé que, dans le cadre de cette affaire en particulier, la demande d'injonction de la BREIN à l'encontre du site, agissant comme intermédiaire dont les services sont utilisés par des tiers pour porter atteinte aux droits de propriété intellectuelle, était légitime.

Cependant, le tribunal de district a souligné que, dans le cadre du blocage d'un site internet, la protection de la propriété intellectuelle ne doit pas faire obstacle à la liberté d'expression protégée par l'article 10 de la Convention européenne des droits de l'homme et que, dans cette affaire, le tribunal devait exercer une certaine retenue judiciaire. Le tribunal de district a estimé également que, dans cette affaire, la procédure d'injonction ordonnant aux deux FAI de bloquer l'accès au site web respectait les principes de proportionnalité et de subsidiarité et que cette injonction était justifiée. Dans le cadre de l'examen de la proportionnalité, les décisions judiciaires précédentes à l'encontre du site n'ayant eu qu'un impact limité sur son mode de fonctionnement, le tribunal s'est fondé sur les preuves fournies par la fondation BREIN. Le tribunal a fait valoir que le nombre d'utilisateurs ayant utilisé The Pirate Bay pour télécharger des films néerlandais était suffisamment important. Par ailleurs, même si l'accès au site The Pirate Bay est bloqué, le partage de contenus autorisés reste possible en passant par d'autres sites web. Il ne devrait donc pas y avoir d'obstacle à la liberté d'expression dans cette affaire. Enfin, le tribunal a estimé que le blocage du serveur DNS et de l'adresse IP d'un site web particulier permet d'éviter d'avoir recours au Deep Packet Inspection (DPI), une technologie destinée à surveiller le contenu des fichiers ou « paquets » envoyés par tous les utilisateurs finaux sur internet, ce que la Cour de justice de l'Union européenne a jugé illégal dans l'affaire *Scarlet contre Sabam* (C-70/10).

Le 20 décembre 2011, dans une résolution, les parlementaires néerlandais se sont prononcés à une large majorité contre le blocage des communications électroniques sous prétexte de faire respecter la législation sur le droit d'auteur. Les juges ont pris en considération l'initiative prise par le législateur néerlandais mais ont estimé qu'il était trop tôt pour que cela influence leur

décision. Il sera donc intéressant de voir, dans les semaines qui viennent, si le législateur poursuit son action et si cette initiative peut influencer l'issue du procès en appel des fournisseurs d'accès internet.

- *Rechtbank 's-Gravenhage, 11 januari 2012, LJN: BV0549, Stichting BREIN tegen Ziggo B.V. & XS4All Internet B.V.* (Tribunal de district de La Haye, 11 janvier 2012, LJN: BV0549, Stichting BREIN c. Ziggo B.V. & XS4All Internet B.V.)
  http://merlin.obs.coe.int/redirect.php?id=15624

- *Tweede Kamer, 29 838 Auteursrechtbeleid, Nr. 35 Motie van het Lid Verhoeven* (Deuxième chambre, 29838, politique en matière de droit d'auteur, n°35, motion déposée par le député Verhoeven)
  http://merlin.obs.coe.int/redirect.php?id=15645

IRIS 2012-2/31

## Fédération de Russie

### Amende infligée au réseau social *VKontakte* pour piratage

*Dmitry Golovanov*
*Centre de droit et de politique des médias de Moscou*

Le 25 mai 2012, la treizième cour arbitrale d'appel de Saint-Pétersbourg (tribunal de commerce de deuxième instance) a confirmé le jugement rendu par le tribunal de première instance selon lequel le célèbre réseau social VKontakte avait porté atteinte aux droits de propriété intellectuelle de deux maisons d'édition (S.B.A. Music Publishing et S.B.A. Production). Une amende de 210 000 RUB (environ 5 000 EUR) avait été infligée à VKontakte pour avoir mis à la disposition des internautes sur son site web 17 œuvres musicales des groupes russes de musique pop « Maksim » et « Infinity ».

Ni les requérants, ni par la partie défenderesse n'ont nié le fait que le contenu a été publié sans l'autorisation préalable des titulaires des droits sur le site web VKontake.ru. Cependant, la Cour n'a pas réussi à déterminer précisément si le contenu en question avait été publié illégalement sur le site par l'administration de VKontakte ou par un utilisateur du réseau social. La principale question reste donc de définir si l'administration de VKontake doit être tenue responsable ou non d'avoir mis à la disposition du public des contenus illicites en vertu des définitions du Code civil russe.

La Cour d'appel a fondé sa décision conformément aux principes directeurs formulés dans la Résolution du 1er novembre 2011 de la plus haute instance d'arbitrage, le Présidium de la Cour suprême d'arbitrage. Cette dernière décision a déterminé quels éléments essentiels devaient être pris en compte par les juridictions ordinaires d'arbitrage lorsqu'elles doivent se prononcer sur la responsabilité de sites web qui hébergent des vidéos sur internet.

En l'espèce, la Cour d'appel a formulé diverses positions de principe en faveur de l'engagement de la responsabilité de l'administration de VKontakte. Elle a tout d'abord déclaré que le contenu avait été mis à la disposition du grand public et non à un groupe précis de personnes comme le soutenait la partie défenderesse. La procédure d'enregistrement payante, obligatoire pour les utilisateurs de vkontakte.ru, est disponible et accessible à tous et ne précise aucun groupe spécifique ou restreint qui serait considéré comme étant le groupe cible d'un contenu précis. La Cour a ensuite examiné la politique de téléchargement de contenu du site VKontakte et a constaté que même si les utilisateurs du réseau social vkontake.ru sont parfaitement informés des modalités d'utilisation du site et de l'obligation de s'assurer de la légalité des contenus qu'ils

téléchargent, VKontakte met à leur disposition un certain nombre de dispositifs techniques qui permettent le téléchargement de contenus illicites. L'existence de ces dispositifs constitue une preuve de la responsabilité de VKontakte. La Cour a également fait remarquer que ces dispositifs rendent le site vkontakte.ru plus attrayant pour les annonceurs qui proposent des contenus publicitaires sur le web et représentent à ce jour une augmentation potentielle des revenus de VKontakte. La Cour a par ailleurs souligné que l'existence d'avantages (même éventuels) résultant de la violation du droit de propriété intellectuelle devait être considérée comme un élément de preuve de la responsabilité de VKontakte.

La Cour a finalement conclu que VKontakte avait fait preuve de passivité et d'une efficacité toute relative face aux demandes des requérants de mettre un terme à ces pratiques illicites. VKontakte soutenait que les plaintes officielles qui lui avaient été adressées ne contenaient aucune information susceptible d'affirmer que les requérants étaient réellement les titulaires des droits en question. La Cour a rejeté cet argument et a fait valoir que VKontakte pouvait parfaitement vérifier le statut juridique des requérants (en demandant par exemple des copies des licences et autres documents nécessaires). VKontakte ne pouvait par ailleurs pas prétendre ne pas être au courant du caractère illicite de l'utilisation du contenu en question, dans la mesure où la diffusion de contenus illicites sur le réseau social VKontakte avait fait l'objet d'un grand débat public, y compris dans les médias de masse.

La décision de la treizième cour arbitrale d'appel de Saint-Pétersbourg peut faire l'objet d'un appel devant les juridictions supérieures de grande instance.

- *Постановление Тринадцатого арбитражного апелляционного суда 25 мая 2012 года по делу № А56-57884/2010* (Décision du 25 mai 2012 rendue par la treizième cour arbitrale d'appel (affaire n° A56-57884/2010))
  http://merlin.obs.coe.int/redirect.php?id=15989

IRIS 2012-7/36

# Le Patriot Act et le quatrième amendement

## *Comment le Gouvernement américain étend secrètement son autorité pour s'engager dans la collecte des données personnelles de ses citoyens*

*Jonathan Perl*
*Locus Telecommunications, Inc.**

## I. Introduction

En 2001, le Congrès américain a adopté le *USA Patriot Act* (ci-après « la loi »), en réponse aux attaques du 11 septembre et en vue de prévenir de nouvelles attaques[1]. En modifiant considérablement les lois régissant les perquisitions et la surveillance, cette loi clé a donné au Gouvernement fédéral (ci-après « le Gouvernement ») une autorité sans précédent en matière de collecte de données. Bien qu'elle ait été mise en œuvre de façon très discrète, l'étendue de l'usage qu'en a fait le Gouvernement en vue de collecter les données personnelles des citoyens américains commence à apparaître au grand jour, à la suite des révélations du lanceur d'alerte de la NSA Edward Snowden. Les enquêtes menées par le Congrès et l'importante couverture médiatique ont permis de révéler que le Gouvernement était en train d'étendre en secret son autorité pour recueillir les données personnelles de ses citoyens, de manière massive et non ciblée, et sans que ceux-ci ne soient nécessairement l'objet de soupçons.

## II. Les limites juridiques imposées au Gouvernement américain en matière de collecte de données

La capacité du Gouvernement à recueillir des données personnelles est limitée principalement par le quatrième amendement de la Constitution américaine, qui prévoit que : « Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse [...] ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir[2] ». Il repose sur un principe selon lequel « les agents de la force publique peuvent observer votre maison depuis la rue, mais dans la plupart des cas ils ne peuvent y faire irruption que lorsqu'ils ont convaincu un juge de la nécessité d'une telle mesure[3] ».

---

* Jonathan D. Perl travaille en qualité de conseiller pour les affaires réglementaires chez Locus Telecommunications, Inc. Les opinions exprimées dans cet article sont celles de l'auteur et ne peuvent en aucun cas être considérées comme représentatives, ni être attribuées, à Locus Telecommunications, Inc.

1) Voir *USA Patriot Act* de 2001, Pub. Law 107-56, 115 Stat. 272 (2001).

2) Constitution américaine, amendement IV.

3) Bob Sullivan, « Big Brother may not be listening, but he's watching: Why metadata snooping is legal », *NBC News*, 15 juin 2013, disponible sur : www.nbcnews.com/technology/big-brother-may-not-be-listening-hes-watching-why-metadata-6C10334990

La Cour suprême américaine (ci-après « la Cour ») a appliqué pour la première fois le quatrième amendement aux données téléphoniques – ce qu'on appelle aujourd'hui les métadonnées – dans une affaire célèbre de 1979[4]. En l'espèce, la Cour avait jugé que les métadonnées téléphoniques n'étaient pas protégées par le quatrième amendement, contrairement au contenu de la conversation téléphonique, pour lequel un mandat était nécessaire. La Cour avait retenu la doctrine de la « tierce partie », selon laquelle un individu renonce à la protection de ses données personnelles quand il fournit une information volontairement à une tierce partie. Elle avait donc estimé que les numéros de téléphones n'étaient pas protégés, dans la mesure où ils avaient été communiqués volontairement à la compagnie téléphonique lors de la composition du numéro.

Le Congrès a codifié cette approche en 1986 avec l'adoption de la loi sur la protection des données des communications électroniques (*Electronic Communications Privacy Act* – ECPA[5]). En vertu de cette loi, les agents de la force publique peuvent accéder aux informations relatives à un appel via un « pen register[6] » (registre des appels) et un « trap and trace device[7] » (dispositif de traçage), dans le cadre d'une assignation qui n'est pas soumise à un contrôle juridictionnel. Le « pen register » est « un dispositif ou un procédé qui enregistre ou décode les informations relatives à la composition d'un numéro, le routage, la destination, le signal transmis par un instrument ou un appareil permettant la transmission d'une communication électronique ou filaire, sous réserve que ces informations n'incluent pas le contenu de la communication ». Un « trap and trace device » est un « dispositif ou un procédé qui capte les impulsions entrantes, électroniques ou autres, en vue d'identifier le numéro appelant ou d'autres informations portant sur le numéro composé, le routage, la destination ou le signal transmis, susceptibles de permettre d'identifier la source de la communication électronique ou filaire, sous réserve que ces informations n'incluent pas le contenu de la communication ». Les auteurs de la loi ont indiqué dans un rapport au Sénat américain annexé à la ECPA qu'ils ne prévoyaient pas de dispositif de contrôle juridictionnel indépendant portant sur le critère de « pertinence » de la demande, les juges pouvant seulement se prononcer sur le caractère complet de la demande déposée[8]. Cet aspect a été réaffirmé par une cour d'appel fédérale, qui a indiqué que « le rôle judiciaire était [...] fondamentalement administratif[9] ». De nombreux juges ont par conséquent conclu qu'ils ne disposaient quasiment d'aucun fondement pour refuser l'accès aux « pen registers », ce qui a conduit un magistrat fédéral de Floride à déplorer qu'en application de la ECPA, « la Cour n'était qu'une simple chambre d'enregistrement[10] ».

En revanche, le Gouvernement est autorisé par la loi de surveillance et de renseignement extérieurs de 1978 (*Foreign Intelligence Surveillance Act* – loi FISA)[11] et par le décret 12333[12] à recueillir les données portant sur des citoyens non américains à l'étranger. La loi FISA exclut leurs communications du champ d'application de la protection du quatrième amendement et autorise le Gouvernement à recueillir des informations sur toutes leurs communications, tant qu'il existe un motif raisonnable de penser que l'une des parties est un citoyen non américain sur sol étranger. Il n'est alors pas tenu d'identifier ces cibles ou les dispositifs surveillés. La loi permet au Gouvernement d'obtenir, sur la base d'une ordonnance unique délivrée par le tribunal de surveillance et de renseignement extérieurs (*Foreign Intelligence Surveillance Court* – tribunal FISA), l'autorisation de mettre en place la surveillance de milliers, voire de millions de personnes, y compris celle, « fortuite », de citoyens américains[13]. Les travaux du tribunal FISA

4) *Smith c. Maryland*, 442 U.S. 735 (1979).
5) *Electronic Communications Privacy Act* de 1986, 18 U.S.C. §§ 2510-2522.
6) 18 USC § 3127 (3).
7) 18 USC § 3127 (4).
8) Declan McCullag, « Feds tell Web firms to turn over user account passwords », *CNET* (25 juillet 2013) disponible sur : http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/
9) *United States c. Fregoso*, Cour d'appel américaine, 8e Circuit (1995).
10) Voir *supra* note 8.
11) *Foreign Intelligence Surveillance Act* de 1978, Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. 36 (loi « FISA »).
12) 46 FR 59941, 3 CFR, 1981, disponible sur : www.archives.gov/federal-register/codification/executive-order/12333.html
13) Margot Kaminskijun, « PRISM's Legal Basis: How We Got Here, and What We Can Do to Get Back, A privacy scholar explains the recent news about government surveillance », *The Atlantic* (7 juin 2013), disponible sur : www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/

sont moins connus du fait de leur caractère confidentiel, néanmoins un ancien juge fédéral qui avait fait partie de cette instance, James Robertson, a récemment expliqué qu'il estimait que ce système était « déficient », dans la mesure où il ne permet pas aux parties concernées de mettre en cause les actions du Gouvernement. Selon lui, le tribunal était devenu « une sorte d'agence administrative[14] ». Le décret 12333 permet au Gouvernement de recueillir, de conserver, d'analyser et de transmettre les informations de renseignement extérieur provenant de systèmes de communications partout dans monde[15].

Le Congrès s'est appuyé sur ces distinctions lorsqu'il a élaboré trois nouveaux outils visant au recueil de données dans le cadre du *Patriot Act* : (1) les demandes de registres commerciaux (section 215), (2) « Sneak and Peek Warrants » (mandats d'enquête furtive), et (3), les lettres de sécurité nationale (LSN)[16]. Des demandes ont été effectuées dans le cadre de la section 215 pour obtenir des informations relatives à la clientèle, comme la liste de titulaires des permis de conduire, des registres d'hôtels, de location de voiture, et de location d'appartement, ainsi que des relevés de cartes bancaires ou de comptabilité. Ces demandes sont assorties d'une obligation de confidentialité, qui interdit au destinataire de la demande d'en informer qui que ce soit. La loi permet aussi au Gouvernement de demander un « Sneak and Peek Warrant » qui lui permet de consulter brièvement un certain nombre de registres pouvant contenir des relevés d'appels téléphoniques et des informations bancaires. Une LSN permet en outre aux agents de la force publique de s'introduire au domicile d'un suspect et de saisir des informations, y compris dans ses ordinateurs, sans l'en informer pendant plusieurs mois. L'Agence nationale de sécurité (*National Security Agency* – NSA) est l'agence gouvernementale qui « recueille, examine, et diffuse les informations transmises via les signaux électroniques étrangers, dans un objectif de renseignement et de contre-renseignement extérieurs et de soutien aux opérations militaires[17] ». Cette agence appuie principalement son action sur les dispositions de la section 215, lui permettant de recueillir « tout élément tangible » en lien avec une investigation autorisée aux fins de lutte contre le terrorisme international ou des activités de renseignement clandestines, s'il « existe des motifs raisonnables de penser que les éléments tangibles recherchés sont pertinents dans le cadre d'une investigation autorisée » par une ordonnance secrète délivrée par le tribunal FISA. Une analyse de l'Association américaine des libertés civiles (American Civil Liberties Union – ACLU) estime qu'environ 192 000 LSN ont été délivrées entre 2003 et 2006, et qu'elles ont donné lieu à une seule condamnation pour terrorisme. L'ACLU souligne également que moins d'1 % des 3 970 « Sneak and Peek Warrants » délivrés en 2010, étaient en lien avec une activité terroriste.[18]

## III. L'étendue de la collecte des données

Le 6 juin 2013, le *Guardian* a publié cinq pages d'une présentation PowerPoint de la NSA décrivant PRISM, un programme top secret de renseignement intérieur[19]. La parution de ce document top secret a entraîné la divulgation d'une avalanche d'autres documents montrant l'étendue des activités du Gouvernement en matière d'accès, de collecte et d'utilisation des données personnelles.

14) Associated Press, « Former judge admits flaws with secret FISA court », *CBS News*, (9 juillet 2013), disponible sur : www.cbsnews.com/8301-250_162-57592836/former-judge-admits-flaws-with-secret-fisa-court/
15) *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, Agence nationale de sécurité (9 août 2013), disponible sur : http://i2.cdn.turner.com/cnn/2013/images/08/09/2013_08_09_the_nsa_story1.pdf
16) *Reclaiming Patriotism, A Call to Reconsider the Patriot Act*, Association américaine des libertés civiles, (mars 2009), disponible sur : www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf
17) *Frequently Asked Questions* (Questions fréquemment posées), Agence nationale de sécurité, disponible sur : www.nsa.gov/about/faqs/index.shtml
18) *Surveillance Under the Patriot Act*, American Civil Liberties Union, ( Octobre2011) disponible sur : https://www.aclu.org/national-security/surveillance-under-patriot-act.
Voir également *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, Office of the Inspector General, U.S. Department of Justice, (Mars 2008).
19) Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian* (6 Juin 2013), disponible sur: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Ces révélations ont mis en lumière le fait que le public américain n'était au courant ni de l'étendue des activités de surveillance et de collecte de données, ni des douzaines d'avis juridiques – certains de plusieurs centaines de pages – justifiant ces activités. Selon les estimations de la NSA elle-même, on comptait en 2012 117 675 cibles de surveillance active dans la base de données anti-terroriste de PRISM, qui avaient donné lieu à 24 005 rapports, soit « plus de 2 000 rapports fondés sur PRISM » chaque mois[20], plus de 77 000 rapports de renseignements qui citaient le programme PRISM, 850 milliards de « données d'appels » rassemblées et stockées dans les bases de données de la NSA, près de 150 milliards de données internet, chiffre qui augmente de 1 à 2 milliards par jour. Encore plus effrayant, la NSA a récemment admis qu'elle « touchait » environ 1.6 % des données internet et qu'elle en sélectionnait 0.025% pour examen[21].

**a. PRISM**

Les documents top secret fournis par Snowden révèlent que PRISM « permet à un analyste d'examiner, de collecter et de mettre en lien le contenu de courriers électroniques, de conversations par voix ou vidéo, de vidéos, de photos, de communications sur IP (par Skype par exemple), de chats, de dossiers transférés et de détails de réseaux sociaux[22] » c'est-à-dire de n'importe quelle donnée à laquelle il a été accédé via des serveurs Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, et Apple[23], et qui est « pertinente » pour le renseignement extérieur. Après avoir accédé à ces données des serveurs, les analystes de la NSA peuvent ouvrir une investigation portant sur un individu en présentant un rapport à un supérieur. La demande sera approuvée s'il existe des « motifs raisonnables » de penser que la cible en question est un citoyen étranger qui se trouve hors du territoire américain au moment du recueil des données. Le caractère raisonnable est défini par une certitude de 51 %[24].

Le Directeur du renseignement national a admis que des interprétations larges de la NSA résultait l' « acquisition fortuite de données[25] » portant sur des citoyens américains, alors que PRISM ne *cible* que « les personnes non-américaines situées en dehors des Etats-Unis ». Mais il a aussi souligné que la NSA avait mis en place des « procédures de minimisation », en vertu desquelles PRISM identifie ces données comme des données auxiliaires collectées de manière fortuite et les efface du poste de travail de l'analyste, l'analyste étant tenu de les mettre à part lorsque cela ne se fait pas automatiquement[26]. Cependant, le Directeur a également admis dans une lettre au sénateur Ron Wyden qu' « au moins une fois », le tribunal FISA avait jugé que les « procédures de minimisation » utilisées par le Gouvernement n'étaient « pas raisonnables au regard du quatrième amendement[27] ». Cette position reflète la crainte que ces données restent en possession du Gouvernement même si elles ne font pas l'objet « de fichages, d'indexations ou de mentions dans un rapport[28] ». En outre, des problèmes liés à la manière dont les données sont partagées se posent. Lorsqu'un analyste estime qu'un citoyen se rend coupable d'activités criminelles ou d'intentions criminelles, il lance une procedure visant à transmettre ces informations au Bureau fédéral d'enquête (Federal Bureau of Investigation – FBI). Ce dernier commence alors ses propres investigations, en s'appuyant sur les données de la NSA comme

20) Ibid.
21) Voir *supra* note 15.
22) Voir *supra* note 19
23) Voir « NSA slides explain the PRISM data-collection program », *The Washington Post* (6 juin 2013), disponible sur : www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
24) Voir *supra* note 15 (les lignes directrices de la NSA qui ont fait l'objet de fuites sont disponibles sur : www.documentcloud.org/documents/727943-exhibit-a.html).
25) Voir *supra* note 11.
26) Marc Ambinder, « Solving the mystery of PRISM », *The Week* (7 juin 2013), disponible sur : http://theweek.com/article/index/245360/solving-the-mystery-of-prism
27) Spencer Ackerman, « U.S. Admits Surveillance Violated Constitution At Least Once », *Wired* (20 juillet 2012), disponible sur : www.wired.com/dangerroom/2012/07/surveillance-spirit-law/; voir aussi http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/ .
28) Eli Lake, «THE SURVEILLANCE SCANDALS, Former NSA Director Michael Hayden Responds to Edward Snowden Claim », *The Daily Beast* (12 juin 2013) (Citant l'affaire *U.S. c. Sattar,* dans laquelle le Gouvernement avait produit des milliers d'heures de communications interceptées qui avaient fait l'objet d'une « minimisation » mais qui n'avaient pas été détruites).

cause probable[29]. Mais il appartient à chaque analyste de faire une distinction subjective entre communications pertinentes ou non et de déchiffrer les intentions d'un citoyen sur la base de peu d'éléments de contexte. De plus, ces informations peuvent être partagées avec toutes sortes d'agences fédérales, dont certaines demandent de plus en plus de données à la NSA.

Microsoft, Yahoo, Google, Facebook et PalTalk ont nié « participer en connaissance de cause » à PRISM[30]. Mais il ne faut pas oublier la clause de confidentialité, selon laquelle il est interdit de reconnaître l'existence même du programme. Une telle coopération, si elle était avérée, ne contrasterait pas avec les pratiques passées de ces opérateurs puisqu'ils avaient reconnu en 2006 avoir volontairement participé à une version antérieure du programme, jusqu'à ce que son existence soit révélée par le *New York Times*[31], révélation qui avait été confirmée par la suite, quand le Congrès leur avait accordé l'immunité totale via des amendements de 2008 à la loi FISA[32].

**b. Accès en bloc aux journaux d'appels – « Personne n'écoute vos appels téléphoniques »**

Les fuites ont en outre révélé qu'en avril 2013, le tribunal FISA avait donné suite à une demande de la NSA d'accéder à tous les numéros de téléphone de Verizon – l'un des plus grands opérateurs de télécommunications aux Etats-Unis – de manière indiscriminée et en bloc, que les abonnés soient soupçonnés d'activités criminelles ou non. A la suite de cette requête, Verizon a été contraint de fournir à la NSA des copies électroniques de « tous les registres d'informations relatifs aux appels ou « métadonnées téléphoniques » créés par Verizon pour les communications entre les Etats-Unis et l'étranger » ou « entièrement à l'intérieur des Etats-Unis, y compris les appels locaux sur une base quotidienne » et ce depuis la date de la requête jusqu'au 19 juillet 2013[33]. Plus précisément, il était demandé à Verizon de fournir les « informations permettant d'identifier la session » telles que « les numéros d'origine et d'arrivée », la durée de chaque appel, les numéros des cartes d'appels, les identifiants de communications interurbaines, les numéros d'identité internationale d'abonné mobile (*International Mobile Subscriber Identity*), et les « informations exhaustives de routage de la communication ». Il est difficile de savoir si cette requête était unique en son genre ou si elle n'était que la dernière en date d'une série de demandes similaires. On ne sait pas non plus si Verizon a été le seul opérateur soumis à une telle demande. Néanmoins, un rapport de 2006 de *USA Today* révélait que la NSA avait mis en œuvre un programme de collecte en bloc de données intérieures portant sur les téléphones, internet et les registres de courriers électroniques des abonnés de AT&T, Verizon et BellSouth, qui avait été secrètement autorisé par le Président Bush, ce qui indique que la NSA aurait collecté des données relatives aux téléphones portables auprès de tous les principaux opérateurs de réseaux électroniques par le passé.

**c. XKeyscore**

Une autre révélation porte sur le programme de collecte de données de la NSA appelé XKeyscore, qui se targue d'être le système de « développement de renseignement à partir de

29) Voir *supra* note 27.
30) Chris Gayomali, « Here are the tech companies denying involvement with the NSA's PRISM program », *The Week* (7 juin 2013), disponible sur : http://theweek.com/article/index/245325/here-are-the-tech-companies-denying-involvement-with-the-nsas-prism-program
31) Barton Gellman, « U.S. surveillance architecture includes collection of revealing Internet, phone metadata », *The Washington Post* (12 mars 2004), disponible sur : www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html?hpid=z1
32) Amendements de 2008 à la loi FISA, Pub.L. 110–261, 122 Stat. 2436, H.R. 6304 (2008).
33) Glen Greenwald, « NSA collecting phone records of millions of Verizon customers daily », *The Guardian* (5 juin 2013), disponible sur : www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

réseaux d'ordinateurs[34] » avec « la portée la plus étendue ». Dans les supports de formation qui ont fait l'objet d'une fuite, la NSA explique que le programme couvre « à peu près tout ce qu'un usager lambda fait sur internet », notamment le contenu de ses courriers électroniques, les recherches effectuées et les sites visités, ainsi que leurs métadonnées, y compris l'interception « en temps réel » des activités d'un individu sur internet. Les analystes y ont recours pour exploiter les énormes bases de données de l'agence en se contentant de donner une justification assez large à la recherche sans autorisation préalable d'un juge ou d'un agent de la NSA. Un outil de la NSA appelé DNI Presenter permet en outre à un analyste qui utilise XKeyscore de lire le contenu de chats ou de messages privés. Le contenu est conservé dans le système de trois à cinq jours, tandis que les métadonnées sont stockées pendant 30 jours.

## IV. Les justifications juridiques du Gouvernement sur ses programmes secrets

L'importante attention médiatique et le débat public qui ont suivi les fuites ont amené le Président Obama à publier un livre blanc de 22 pages expliquant les fondements juridiques des divers programmes de surveillance de la NSA[35]. Ce document explique que ces programmes sont justifiés dans la mesure où ils répondent à une définition élargie de notion de« pertinence » introduite dans le cadre de la section 215. Il avance que la définition de la « pertinence » devrait être interprétée « de manière au moins aussi large » qu'elle l'a été dans une série d'affaires impliquant la découverte de documents dans le cadre « d'investigations ordinaires en matière administrative, civile et criminelle », parce que les « normes de « pertinence » offrent une latitude considérable lorsque cela est nécessaire et, selon le contexte, permettent de recueillir un volume d'informations important en vue de retrouver les éléments clés qu'elles contiennent ». Le rapport avance également que toutes les métadonnées téléphoniques sont importantes au regard de la section 215 parce que, quelque part dans ce vaste ensemble de données, se trouvent des éléments qui sont effectivement pertinents. Bien que le Gouvernement soit conscient que ces dispositifs semblent lui conférer une autorité extensive pour recueillir d'autres types de données, telles que des données médicales ou les registres de prêt des bibliothèques, il souligne qu'il s'abstient de rechercher ce type d'informations dans le cadre de ses activités anti-terroristes, parce que l'utilisation de ces données n'est en général pas équivalente à l'utilisation des métadonnées de communication, comme moyen d'identification d'agents ou des réseaux terroristes auparavant inconnus. Cette interprétation ne va pas sans poser de problème puisqu'il est essentiellement affirmé dans le livre blanc que « nous ne pensons pas que le recueil en bloc de données médicales soit nécessaire pour contrer le terrorisme, mais si c'était le cas, nous pourrions les collecter ». Auquel cas « le Gouvernement serait en droit de recueillir quasiment n'importe quelle donnée au motif qu'elle pourrait un jour s'avérer pertinente », par exemple « des milliards de dossiers médicaux et de registres de livres ou de prêts de bibliothèques, et cela sans mandat – en clair, un cas classique de chasse à l'information parfaitement anticonstitutionnelle[36] ».

Le Président Obama a promis de réformer la section 215 du *Patriot Act*. Plus précisément, il a indiqué que serait créé un nouveau site internet qui donnerait aux citoyens des Etats-Unis et du reste du monde plus d'explications sur les programmes de surveillance, qu'un panel consultatif externe serait mis en place pour examiner les programmes de surveillance, ainsi qu'un agent chargé de la protection de la vie privée à la NSA et un avocat indépendant pouvant contester devant les tribunaux les arguments et les politiques du Gouvernement[37]. Ces propositions ont été reçues avec scepticisme par des figures républicaines importantes du Congrès, qui craignent

34) Glen Greenwald, « XKeyscore: NSA tool collects "nearly everything a user does on the internet" », *The Guardian* (31 juillet 2013), disponible sur : www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

35) Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* (9 August 2013) (Livre blanc du gouvernement, *La collecte en bloc de métadonnées téléphoniques au regard de la section 215 du* USA Patriot Act , 9 août 2013), disponible sur : http://big.assets.huffingtonpost.com/Section215.pdf

36) Jeffrey Rosen, « The Lies Aren't What Make Obama's NSA Stance So Awful », *The New Republic* (12 août 2013), disponible sur : www.newrepublic.com/article/114276/obama-surveillance-comments-dishonesty-isnt-only-problem

37) Voir « Obama announces NSA surveillance reform », *RT* (9 août 2013), disponible sur : http://rt.com/usa/obama-nsa-statement-transparency-308/

que l'intervention d'un avocat dans les procédures du tribunal FISA qui supervise le recueil de données téléphoniques par l'agence ralentisse les efforts anti-terroristes, alors que le temps est un facteur particulièrement important dans ces affaires[38].

## V. Le Gouvernement reconnaît avoir outrepassé son autorité

En août 2013, la fuite d'un audit interne de la NSA a révélé que l'agence avait violé les règles relatives au respect de la vie privée et outrepassé son autorité légale des milliers de fois par an[39]. L'audit, datant de mai 2012, recensait 2 776 incidents portant sur le recueil, le stockage, l'accès et la transmission non autorisés de communications juridiquement protégées, pour les seuls 12 derniers mois. Bien que la plupart de ces cas ne fussent pas intentionnels, beaucoup impliquaient une mauvaise application des procédures de vérification et de traitement requises. Des exemples significatifs sont la violation de l'ordonnance d'une cour, l'utilisation non autorisée d'informations portant sur plus de 3 000 citoyens américains et détenteurs de la carte verte, des erreurs typographiques ayant entraîné l'interception involontaire de courriers électroniques et appels aux Etats-Unis, et même une décision selon laquelle il n'était pas nécessaire de rendre compte de cette surveillance involontaire. L'audit évoque aussi des violations remontant à l'année 2008, notamment l'interception d'un « grand nombre » d'appels passés depuis Washington lorsqu' à la suite d'une erreur de programmation, l'indicatif local américain 202 a été confondu avec 20, l'indicatif international de l'Egypte. Une autre violation a été révélée lorsque le tribunal FISA a conclu que la NSA avait agi au mépris de la Constitution en omettant d'informer le tribunal d'une nouvelle méthode de collecte des données utilisée depuis plusieurs mois. Un autre exemple a concerné le détournement d'un volume important de données internationales transitant via des câbles de fibre optique vers les Etats-Unis en vue de leur stockage temporaire pour examen et sélection. Le nombre de violations est probablement bien plus élevé, dans la mesure où l'audit ne portait que sur les incidents s'étant déroulés au sein du siège social de la NSA à Fort Meade, et n'incluait pas les autres unités opérationnelles et centres régionaux de collecte des données de la NSA.

## VI. Conclusion

Les partisans des programmes soutiennent qu'ils ne sont pas intrusifs dans la mesure où le Gouvernement ne consulte pas en pratique les contenus. Mais, même si cela était vrai de tous les programmes de la NSA, cette distinction est de moins en moins pertinente, puisque les métadonnées peuvent souvent, selon un expert, « être bien plus intrusives que le contenu lui-même[40] ». En pratique, elles permettent au Gouvernement « d'avoir connaissance d'une quantité immense d'informations commerciales[41] ». Par exemple, des données relatives aux appels entre dirigeants d'entreprise peuvent révéler l'imminence d'opérations de prise de contrôle sur des entreprises ; des appels à un gynécologue, un cancérologue, suivis d'appels à des parents proches peuvent révéler des informations médicales sensibles ; et des informations liées à l'usage de tel ou tel relais téléphonique peuvent renseigner sur les allées et venues d'un individu. Ces exemples sont confirmés par les conclusions de nombreuses études, qui indiquent qu'un individu peut être identifié simplement sur la base du lieu où il s'est trouvé en quatre occasions différentes[42], et que les préférences d'un individu, ses orientations politiques ainsi que de nombreux autres

38) Janet Hook et Sarah Portlock, « Republicans Warn on NSA Changes », *The Wall Street Journal* (11 août 2013), disponible sur : http://blogs.wsj.com/washwire/2013/08/11/republicans-warn-against-nsa-changes/?mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth

39) Voir http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/

40) Nidhi Subbaraman, « Facebook forensics? What the feds can learn from your digital crumbs », *NBC News* (8 juin 2013), www.nbcnews.com/technology/facebook-forensics-what-feds-can-learn-your-digital-crumbs-6C10240840

41) Bob Sullivan, « Big Brother may not be listening, but he's watching: Why metadata snooping is legal », *NBC News*, 15 juin 2013.

42) Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, « Unique in the Crowd: The privacy bounds of human mobility », Scientific Reports (25 March 2013).

aspects de son caractère peuvent être déduits simplement de ses « j'aime » sur Facebook[43]. Cette réalité nouvelle rend bien plus complexe la définition de la limite entre « frapper à votre porte et s'introduire par effraction[44] ».

Le type de remèdes auxquels le Congrès ou la Cour pourraient recourir n'est pas encore connu. Néanmoins, même les membres du Congrès favorables aux programmes ont fait part de leurs préoccupations. Certains déplorent ne pas avoir été suffisamment informés de cette rafle de données[45], tandis que d'autres, notamment l'un des auteurs du *Patriot Act* originel, regrettent que « l'interprétation secrète ne soit pas conforme aux objectifs initiaux de la législation ». Quatre projets de loi ont été introduits pour répondre à ce problème, chacun suivant une approche différente : renforcer les normes en exigeant que les faits soient « spécifiques et détaillés » et que « chacun des » registres commerciaux soit lié à une investigation[46] ; exiger que les registres constituent des éléments « probants » ou réellement pertinents pour une enquête donnée ; imposer que toute ordonnance explique pourquoi ces registres « se rapportent » à un individu donné ou sont « pertinents » pour une enquête donnée[47] ; et, projet de modification le plus récent à avoir été soumis au vote, l'exigence que la NSA ait une cible spécifique lorsqu'elle demande des relevés téléphoniques[48]. Alors que ce dernier a été rejeté par 217 votes contre 205, il a montré que les voix en faveur d'une limitation du pouvoir de la NSA gagnaient du terrain et que de telles dispositions étaient même susceptibles d'être approuvées prochainement, dans la mesure où les lignes partisanes traditionnelles ne sont pas nécessairement suivies sur cette question. Le soutien de membres conservateurs et libéraux, qui ont coparrainé la loi, et le résultat serré du vote sont particulièrement surprenants dans la mesure où les dirigeants des deux partis avaient pris position contre le projet de loi.

Des éléments récents permettent de penser que la Cour suprême américaine ne se prononcera peut-être pas sur la constitutionnalité de ces programmes. En février 2012, dans un procès portant sur la constitutionnalité de la loi autorisant PRISM, la Cour a estimé que les plaignants – des avocats, journalistes et avocats des droits de l'homme – n'avaient pas qualité à contester cette loi dans la mesure où ils n'en avaient pas été personnellement affectés[49]. La Cour a expliqué que les allégations de surveillance revêtaient un caractère trop spéculatif et que la surveillance des plaignants n'était pas « imminente de façon certaine ». Alors que les nouvelles révélations montrent que « la surveillance est peut-être « imminente de façon certaine » puisque nous connaissons l'existence du programme PRISM », cela ne peut suffire à démontrer que le Gouvernement a espionné ces plaignants « en particulier ».

Néanmoins, les demandes qui visent à mettre en place un comité spécial d'enquête du Congrès et à établir un cadre plus transparent dans lequel les responsabilités de chacun seraient clairement établies se font de plus en plus nombreuses. Le mouvement est porté par une coalition de plus de 100 groupes de défense des libertés individuelles.

---

43) Michal Kosinski, David Stillwell, et Thore Graepel, « Private traits and attributes are predictable from digital records of human behavior », Compte-rendu de l'Académie nationale américaine des sciences (12 février 2013).
44) Voir *supra* note 3.
45) Voir *supra* note 28.
46) Mark M. Jaycox, « Bills Introduced by Congress Fail to Fix Unconstitutional NSA Spying », *Electronic Frontier Foundation* (15 juillet 2013), disponible sur : www.eff.org/deeplinks/2013/07/bills-fail-fix-unconstitutional-nsa-spying
47) Amendements à la loi sur la protection des données des communications électroniques de 2013, Rapport du Sénat avec positions supplémentaires sur la loi de modification de 2013, annexé à S. 607, Comité sur le judiciaire (16 mai 2013), disponible sur : www.fas.org/irp/congress/2013_rpt/ecpa_amend.html https://ch1prd0410.outlook.com/owa/redir.aspx?C=dK0S0rt_d0CA0ZDdK7sVj-l6ELxxZdAIvCw0XqT_lixdcqPrgc_eWunRbfP2y9Qnf9ekwtnv7I0.&URL=https%3a%2f%2fwww.eff.org%2fdeeplinks%2f2013%2f07%2fbills-fail-fix-unconstitutional-nsa-spying
48) Ginger Gibson, « Justin Amash, John Conyers introduce NSA bill », *Politico* (18 juin 2013), disponible sur : www.politico.com/story/2013/06/justin-amash-john-conyers-nsa-bill-92982.html#ixzz2bUBXZXie
49) Cindy Cohn et Trevor Timm, « Supreme Court Dismisses Challenge to FISA Amendments Act; EFF's Lawsuit Over NSA Warrantless Wiretapping Remains », *Electronic Frontier Foundation*, (27 février 2013), disponible sur : www.eff.org/deeplinks/2013/02/supreme-court-dismisses-challenge-fisa-warrantless-wiretapping-law-effs-lawsuit

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

# Informations pour le secteur audiovisuel

L'Observatoire européen de l'audiovisuel a pour but d'assurer une plus grande transparence du secteur audiovisuel en Europe. Cette mission comporte la collecte, l'analyse et la publication d'informations actuelles et pertinentes sur les industries audiovisuelles.

L'Observatoire a adopté une définition pragmatique du secteur audiovisuel auquel il se consacre. Ses principaux domaines d'activité comprennent le cinéma, la télévision, la vidéo et le DVD, les services audiovisuels à la demande et les politiques publiques relatives au cinéma et à la télévision. Pour ces cinq domaines, l'Observatoire fournit des informations juridiques ainsi que des informations sur les marchés et les financements. Son champ d'activité géographique s'étend à ses Etats membres, pour lesquels l'Observatoire consigne et analyse les évolutions. Il couvre en outre, lorsque cela lui paraît opportun, d'autres Etats présentant une pertinence pour l'analyse de l'évolution en Europe. La mise à disposition de l'information implique diverses étapes, telles que la collecte systématique et le traitement des données ainsi que leur diffusion auprès des utilisateurs sous forme de publications, d'informations en ligne, de bases de données et répertoires et de présentations dans le cadre de conférences et d'ateliers. Le travail de l'Observatoire fait appel à des sources d'information internationales et nationales permettant de rassembler des données actuelles et pertinentes. Le réseau d'information de l'Observatoire a été constitué à cette fin. Il comprend des organismes et des institutions partenaires, des entreprises spécialisées dans la mise à disposition d'informations professionnelles ainsi que des correspondants spécialisés. Les principaux groupes cibles de l'Observatoire sont les professionnels du secteur audiovisuel : les producteurs, les distributeurs, les exploitants, les radiodiffuseurs et les autres fournisseurs de services audiovisuels, les organisations internationales du secteur, les décideurs au sein des organismes publics responsables des médias, les législateurs nationaux et européens, les journalistes, les chercheurs, les juristes, les investisseurs et les consultants.

L'Observatoire européen de l'audiovisuel a été créé en 1992 sous l'égide du Conseil de l'Europe dont il constitue un « Accord partiel et élargi ». Il a son siège en France, à Strasbourg. L'Observatoire se compose à l'heure actuelle de 39 Etats membres et de l'Union européenne, représentée par la Commission européenne. Chaque Etat membre désigne son représentant au Conseil exécutif de l'Observatoire. L'équipe internationale de l'Observatoire est dirigée par le Directeur exécutif.

**Les publications et services proposés par l'Observatoire sont classés en quatre catégories :**

- **Publications**
- **Informations en ligne**
- **Bases de données et répertoires**
- **Conférences et ateliers**

**Observatoire européen de l'audiovisuel**
76 Allée de la Robertsau – F-67000 Strasbourg – France
Tél.: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: obs@obs.coe.int

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# Services d'informations juridiques de l'Observatoire européen de l'audiovisuel

**Pour commander :**
- **en ligne sous http ://www.obs.coe.int/about/order**
- **par e-mail : orders-obs@coe.int**
- **par fax : +33 (0)3 90 21 60 19**

## Lettre d'information IRIS

*Observations juridiques de l'Observatoire européen de l'audiovisuel*

***Accès en ligne et gratuit !***

IRIS est un bulletin mensuel vous garantissant une information fiable et toujours à jour sur les évolutions les plus marquantes du droit dans le secteur de l'audiovisuel. IRIS couvre tous les domaines juridiques importants de l'industrie audiovisuelle et se concentre principalement sur la cinquantaine de pays qui composent l'Europe élargie. IRIS décrit la législation relative aux médias au sens le plus large, ainsi que les développements majeurs en matière de jurisprudence, les importantes décisions administratives et les décisions d'ordre politique pouvant avoir un impact sur la loi.
L'abonnement à IRIS est gratuit, les articles sont accessibles et téléchargeables sur le site internet : http://merlin.obs.coe.int/newsletter.php

## IRIS *plus*

*Un thème juridique brûlant examiné sous différents angles*

Les développements juridiques, technologiques et économiques dans le secteur audiovisuel génèrent pour les professionnels des besoins immédiats en informations. IRIS *plus* a pour but d'identifier ces nouveautés et de fournir leur contexte juridique. Sur la base d'un article de fond étayé par des exposés concis, suivi d'un zoom sur le sujet traité sous forme de tableaux synoptiques, de données de marché ou d'informations pratiques selon les cas, IRIS *plus* fournit à ses lecteurs la connaissance nécessaire pour suivre et prendre part aux dernières discussions très pertinentes concernant le secteur audiovisuel.
Pour plus d'informations : http://www.obs.coe.int/irisplus

## IRIS Merlin

*Base de données d'informations juridiques relatives au secteur audiovisuel en Europe*

La base de données IRIS Merlin vous permet d'accéder à plus de 6 500 articles présentant des informations juridiques en rapport avec l'industrie audiovisuelle. Ces articles relatent les lois, les arrêts des tribunaux, les décisions des administrations, ainsi que les documents de politique générale relatifs aux domaines intéressés, et ce pour plus d'une cinquantaine de pays. Ils portent également sur les instruments juridiques, les résolutions et les documents d'ordre politique émanant des principales institutions européennes et internationales. Accès gratuit au site : http://merlin.obs.coe.int

## IRIS *Spécial*

*Informations factuelles détaillées associées à une analyse approfondie*

Dans nos publications IRIS *Spécial*, tous les sujets d'actualité relatifs au droit des médias sont abordés et examinés d'un point de vue juridique. Les publications IRIS *Spécial* offrent des analyses détaillées de la législation nationale applicable, facilitant ainsi la comparaison entre les cadres juridiques de différents pays. Elles identifient et analysent en outre des questions très pertinentes et donnent un aperçu du contexte juridique, européen et international, ayant un impact sur la législation nationale. Les publications IRIS *Spécial* abordent ces thèmes juridiques de manière très accessible. Inutile d'être juriste pour les lire ! Chaque édition relève d'un niveau élevé de pertinence pratique combiné à la rigueur académique. Pour accéder à la liste de toutes les publications IRIS *Spécial*, visitez le site : http://www.obs.coe.int/oea_publ/iris_special/index.html

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**IRIS *plus* 2013-6**
**Les données à caractère personnel sont-elles vraiment privées?**
**25,50 € - ISBN 978-92-871-7790-2**