

ANALYSES

- **SÉCURITÉ ET PERTINENCE DE LA BASE ÉLÈVES 1ER DEGRÉ , LES ASSOCIATIONS DÉNONCENT LES RISQUES**
Par M. Nicolas Samarcq et M. Luc Masson, Lexagone.fr
- **DÉTOURNEMENT DE MARQUE AU SEIN D'UN RÉSEAU DE FRANCHISE**
Par M. Benjamin Vitasse
- **LE PMU DEVRA T IL RENONCER À SON MONOPOLE SUR LES PARIS EN LIGNE?**
Par Me. Nicole Bondois et Melle Fanny Duban
- **TYPOSQUATTING : FOCUS SUR LES NOMS DE DOMAINE DES MOTEURS DE RECHERCHE**
Par M. Jean-François Poussard, Rédacteur en Chef MailClub.info
- **LES AGENCES DE SÉCURITÉ DOIVENT ÊTRE SOUMISES À UN CONTRÔLE DÉMOCRATIQUE**
Par M. Thomas Hammarberg, Commissioner for Human Rights

DOSSIER

- **TGI Paris, 3ème ch., 13 juillet 2007, CHRISTIAN C., NORD OUEST PRODUCTION / DAILYMOTION, UGC IMAGES**
- **AFFAIRE DAILYMOTION : LE TGI DE PARIS ÉCRIT LA LCEN 2.0**
Par I.R.I.S (Imaginons un Réseau Internet Solidaire)

AU JOURNAL OFFICIEL

- **Décret n°2007-1130 du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris, version consolidée au 25 juillet 2007, .0 n° 170 du 25 juillet 2007 page 12503.**
- **Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), J.O n° 113 du 16 mai 2007 page 9362.**

JURISPRUDENCE

- **Conseil d'Etat, 7 août 2007, AFA ET ALII**
- **Conseil d'Etat, 7 août 2007, ASSOCIATION FRANCAISE DES OPÉRATEURS DE RÉSEAUX ET DE SERVICES DE TÉLÉCOMMUNICATIONS (AFORS TELECOM) ET ALII**

RDTIC

REVUE DE DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

La revue de droit des techniques de l'information et de la communication (RDTIC) est un service proposé par DROIT-TIC - www.DROIT-TIC.com.

Elle vous propose une synthèse non exhaustive des informations juridiques mise en ligne sur le site DROIT-TIC durant le mois écoulé. Vous y trouverez non seulement des articles (actualités, analyses, synthèses, doctrines...), mais encore des décisions de justice, la doctrine de certaines autorités administratives indépendantes et des textes normatifs.

Conseil scientifique

- Julien Le Clainche, chercheur
- François-Xavier Boulin, avocat BCTG Associés
- Anthony Grevin, juriste M6 Web
- Vincent Duseauguey, juriste M6 Web
- Julien Linsolas, juriste SFR
- Olivier Gnos, architecte logiciel
- Marie-Alix Boussard, allocataire de recherche

Informations légales

La RDTIC est protégée par les normes nationales et internationales en vigueur, notamment celles relatives à la propriété intellectuelle.

Citation : RDTIC n° XX, mois année, DROIT-TIC, p. XX.

Les articles sont la propriété de leurs auteurs. Si vous souhaitez les contacter, rendez-vous sur le site DROIT-TIC.com, rubrique "DROIT-TIC et vous", "L'équipe de DROIT-TIC".

La lecture de la RDTIC emporte le respect des conditions d'utilisation du site DROIT-TIC qui sont disponibles à l'adresse : <http://www.droit-tic.com/index2.php?page=conditions.php>

Vous pouvez présenter vos observations, remarques, soutiens, encouragements et autres critiques constructives en écrivant à julien@droit-ntic.com.

DROIT-TIC / Julien Le Clainche, 5 rue des chênes verts, 34110 MIREVAL.

DOSSIER

■ TGI Paris, 3ème ch., 13 juillet 2007, CHRISTIAN C., NORD OUEST PRODUCTION / DAILYMOTION, UGC IMAGES

■ AFFAIRE DAILYMOTION : LE TGI DE PARIS ÉCRIT LA LCEN 2.0

Par I.R.I.S (Imaginons un Réseau Internet Solidaire)

ANALYSES

■ SÉCURITÉ ET PERTINENCE DE LA BASE ÉLÈVES 1ER DEGRÉ , LES ASSOCIATIONS DÉNONCENT LES RISQUES

Par M. Nicolas Samarcq et M. Luc Masson, Lexagone.Fr

■ DÉTOURNEMENT DE MARQUE AU SEIN D'UN RÉSEAU DE FRANCHISE

Par M. Benjamin Vitasse

■ LE PMU DEVRA T IL RENONCER À SON MONOPOLE SUR LES PARIS EN LIGNE?

Par Me. Nicole Bondois et Melle Fanny Duban, Juriste en propriété intellectuelle

■ TYPOSQUATTING : FOCUS SUR LES NOMS DE DOMAINE DES MOTEURS DE RECHERCHE

Par M. Jean-François Poussard, Rédacteur en Chef MailClub.info

■ LES AGENCES DE SÉCURITÉ DOIVENT ÊTRE SOUMISES À UN CONTRÔLE DÉMOCRATIQUE

Par M. Thomas Hammarberg, Commissioner for Human Rights

AU J.O

■ Décret n°2007-1130 du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris, version consolidée au 25 juillet 2007, .O n° 170 du 25 juillet 2007 page 12503.

■ Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), J.O n° 113 du 16 mai 2007 page 9362.

DÉCISIONS - JURISPRUDENCES

■ Conseil d'Etat, 7 août 2007, AFA ET ALII

■ Conseil d'Etat, 7 août 2007, ASSOCIATION FRANCAISE DES OPÉRATEURS DE RÉSEAUX ET DE SERVICES DE TÉLÉCOMMUNICATIONS (AFORS TELECOM) ET ALII

DOSSIER DAILYMOTION

**TGI de Paris, 3ème ch., 13
juillet 2007, CHRISTIAN C.,
NORD OUEST PRODUCTION /
DAILYMOTION, UGC IMAGES**

Thèmes

Propriétés intellectuelles, Informatique et libertés
qu'il lui incombe de procéder à un contrôle a priori

Résumé

Dailymotion n'a mis en œuvre aucun moyen propre à rendre impossible l'accès au film "Joyeux Noël", sinon après avoir été mise en demeure, soit à un moment où le dommage était déjà réalisé, alors qu'il lui incombe de procéder à un contrôle a priori

Décision

Christian C. est l'auteur du scénario et le réalisateur du film intitulé "Joyeux Noël", produit par la société Nord Ouest Production à laquelle il a cédé ses droits d'exploitation par contrats en date des 31 octobre 2001 et 28 mai 2004.

Ce film, sorti en salle le 9 novembre 2005, est distribué à titre exclusif par la société UGC Images. Il a connu un vif succès attirant plus de 2 millions de spectateurs.

Depuis le 17 mai 2006, il est commercialisé sous forme de DVD. Il a également été diffusé à la télévision, sur la chaîne Canal Plus et doit l'être sur la chaîne Ciné Cinéma à la fin de l'année 2007.

Le 30 janvier 2007, la société Nord Ouest Production a fait constater par huissier que ce film pouvait être visionné en "streaming" en deux parties sur le site internet www.dailymotion.fr et qu'il pouvait en outre être téléchargé par l'intermédiaire du site www.keepvid.com. Un second constat, dressé le 19 février 2007, ayant montré que le film était toujours accessible, la société Nord Ouest Production a mis en demeure la société Dailymotion de la retirer du site par lettre en date du 22 février 2007.

En dépit de l'assurance donnée par la société Dailymotion dans sa réponse en date du 26 février suivant, il était constaté le 26 mars qu'un long extrait du film était encore disponible.

Par assignation en date du 18 avril 2007, Christian C. et la société Nord Ouest Production ont, dûment autorisés à cette fin, assigné à jour fixe la société Dailymotion aux fins de voir juger qu'en reproduisant et en représentant sans autorisation préalable le film "Joyeux Noël", cette dernière a commis des actes de contrefaçon portant atteinte au droit moral de l'auteur et aux droits patrimoniaux de la société Nord Ouest Production et à ses droits de producteur de vidéogrammes, ainsi que des actes de parasitisme. Ils demandent en conséquence, la condamnation de la défenderesse à payer à Christian C. la somme de 1 € et à la société Nord Ouest Production la somme de 12 312 € en réparation de l'atteinte à ses droits patrimoniaux, celle de 7500 € en réparation de l'atteinte à ses droits voisins et celle de 10 000 € en réparation des actes de parasitisme.

Ils demandent en outre de prononcer une mesure d'interdiction sous astreinte et d'ordonner la publication du jugement sur la page d'accueil du site litigieux et dans la presse écrite, le tout sous le bénéfice de l'exécution provisoire.

La société Nord Ouest Production sollicite l'allocation de la somme de 9000 € sur le fondement des dispositions de l'article 700 du ncp.

La société UGC Images, appelée en cause par les demandeurs par actes en date des 12 et 18 avril 2007, se prévalant du contrat lui conférant l'exclusivité de la distribution pendant une durée de 15 ans selon contrat en date du 1er juillet 2004, reprenant les arguments des demandeurs quant à la qualité d'éditeur de la société Dailymotion et ajoutant que celle-ci ne respecte pas les obligations imparties aux prestataires techniques en ce qu'elle ne conserverait pas les données permettant l'identification de quiconque a contribué à la création de contenu illicite, demande la condamnation de la société défenderesse à lui payer la somme de 15 000 € du chef de contrefaçon et celle de 15 000 € en réparation d'actes de parasitisme commercial et de prononcer une mesure d'interdiction sous astreinte, le tribunal s'en réservant la liquidation. A titre subsidiaire, elle demande d'ordonner la communication des données d'identification de la personne qui a mis en ligne le film en cause. Elle sollicite en outre l'allocation de la somme de 6000 € sur le fondement des dispositions de l'article 700 du ncp, le tout sous le bénéfice de l'exécution provisoire, dépens inclus en application de l'article 515 modifié du même code.

La société Dailymotion expose que le service qu'elle met à disposition permet à tout internaute préalablement inscrit :

- de créer un espace personnel dans lequel il a la faculté de télécharger et de stocker des vidéogrammes personnels, soit pour les conserver, soit pour les partager avec un groupe plus ou moins étendu,

- d'accéder aux espaces personnels d'autres utilisateurs, de visionner les vidéos ainsi disponibles et de poster le cas échéant des commentaires. Elles souligne d'une part que le système ne permet qu'une visualisation grâce à une interface dénommée "Player" mais en aucun cas d'opérer un téléchargement par les autres utilisateurs et d'autre part, que l'utilisateur est le seul maître des choix qu'il entend opérer au sein de la plate forme (mise en ligne, étendue de celle-ci, retrait, critères d'identification au sein des groupes et rubriques proposées, mots clés permettant le référencement).

Elle soutient que son rôle est celui d'un prestataire technique tel que défini par l'article 6-1-2 de la loi du 21 juin 2004 de sorte que sa responsabilité civile ne peut être recherchée que ce soit du chef de contrefaçon ou du chef de concurrence déloyale dès lors qu'elle a respecté les obligations mises à sa charge à savoir : mise en œuvre de dispositifs d'information et d'alerte quant à tout contenu illicite incluant les contenus contrefaisants, retrait immédiat du contenu litigieux dès qu'il lui a été signalé et conservation des données disponibles permettant d'identifier l'utilisateur concerné, lequel n'a pas été mis en cause par les demandeurs.

Elle conclut au débouté de l'ensemble des demandes et sollicite l'allocation de la somme de 5000 € en réparation du caractère abusif de l'action engagée et de celle de 10 000 € au titre de ses frais irrépétibles.

Sur la nature de l'activité exercée par la société Dailymotion et sa responsabilité

Attendu que selon l'article 1er de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication, la communication au public par voie électronique est libre ;

Attendu que ce texte précise en préambule que l'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle ;

Attendu que selon les dispositions de l'article 6-1-7 de la loi du 21 juin 2004 modifiée par la loi du 23 janvier 2006, les prestataires techniques ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de

rechercher des faits ou circonstances révélant des activités illicites.

Attendu que se prévalant de ces dispositions, la société Dailymotion soutient qu'il appartient aux internautes qui se proposent de mettre des vidéogrammes en ligne de s'assurer de leur licéité au regard des droits d'auteur ; qu'elle précise et justifie diffuser sur son site une page de mise en garde à l'attention des destinataires du service en premier lieu dans la rubrique Conditions d'utilisation et en second lieu lors de toute mise en ligne, l'utilisateur ne pouvant accéder au service que s'il a expressément accepté ces conditions générales ; qu'elle ajoute avoir procédé au retrait immédiat du film concerné dès qu'elle a été informée de son utilisation illicite et ainsi respecté les dispositions de l'article 6-1-2 du texte susvisé ;

Attendu que cet article est ainsi libellé : "*Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public, par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère, ou si, dès le moment où elles en sont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible*" ;

Attendu que les demandeurs opposent que la défenderesse se prévaut indûment de l'exonération de responsabilité ainsi instaurée dans la mesure où l'activité qu'elle développe relève en réalité du domaine de l'édition de contenu ; qu'ils font savoir que :

- le phénomène dit de la "vidéo communautaire" ne génère aucun revenu au titre de l'activité de stockage de données,
- le modèle économique choisi repose sur une exploitation commerciale liée exclusivement à la vente d'espaces publicitaires,
- les annonceurs sont d'autant plus enclins à cette manière de promouvoir leurs produits que le nombre de visiteurs du site est important, élément déterminant des sommes qu'ils sont prêts à investir,

or, la fréquentation du site étant directement liée à la qualité des contenus proposés au public, seule la diffusion d'œuvres protégées et non celle de vidéos d'amateurs permet d'augmenter l'audience et de stimuler la vente d'espaces publicitaires ;

Qu'ils en concluent que la société Dailymotion a gagné sa position de leader sur le marché en développant une stratégie qui bafoue délibérément les droits d'auteur, la

valorisation du site reposant sur la diffusion et la commercialisation de contenus et non sur le stockage de données ;

Attendu cependant que la commercialisation d'espaces publicitaires ne permet pas de qualifier la société Dailymotion d'éditeur de contenu dès lors que lesdits contenus sont fournis par les utilisateurs eux-mêmes, situation qui distingue fondamentalement le prestataire technique de l'éditeur, lequel, par essence même, est personnellement à l'origine de la diffusion, raison pour laquelle il engage sa responsabilité.

Attendu que les récents accords passés entre la société Dailymotion et les sociétés Universal et Warner par lesquels ces dernières autorisent la diffusion des films de leur catalogue sur le site, aboutissent en effet à un changement de nature d'activité, le site Dailymotion devenant un éditeur voire un co-éditeur dès lors qu'il devient l'auteur de la mise en ligne des vidéos considérées ;

Attendu ceci étant posé que la société Dailymotion, prise en sa seule qualité d'hébergeur de contenu, engage sa responsabilité dans les termes de l'article 6-1-2 ci-dessus rappelés ;

Qu'en effet, ce texte n'instaure pas une exonération de responsabilité mais seulement une limitation de responsabilité restreinte aux cas où les prestataires techniques n'ont pas effectivement connaissance du caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;

Attendu qu'il ne peut être sérieusement prétendu que la vocation de l'architecture et les moyens techniques mis en place par la société Dailymotion ne tendaient qu'à permettre à tout à chacun de partager ses vidéos amateur avec ses amis ou la communauté des internautes selon l'option choisie, alors qu'ils visaient à démontrer une capacité à offrir à ladite communauté l'accès à tout type de vidéos sans distinction, tout en laissant le soin aux utilisateurs d'abonder le site dans des conditions telles qu'il était évident qu'ils le feraient avec des oeuvres protégées par le droit d'auteur ;

Qu'ainsi que le relèvent justement les demandeurs, le succès de l'entreprise supposait nécessairement la diffusion d'oeuvres connues du public, seules de nature à accroître l'audience et à assurer corrélativement des recettes publicitaires ;

Que si la loi a posé le principe de la liberté de la communication électronique, elle a également rappelé que cette liberté trouvait sa limite dans la mesure requise notamment par la propriété d'autrui ;

Que dans le contexte décrit, la société Dailymotion doit être considérée comme ayant connaissance à tout le moins de faits et circonstances laissant à penser que des vidéos illicites sont mises en ligne ; qu'il lui appartient donc d'en assumer la responsabilité, sans pouvoir rejeter la faute sur les seuls utilisateurs, dès lors qu'elle leur a fourni délibérément les moyens de la commettre ;

Attendu que si la loi n'impose pas aux prestataires techniques une obligation générale de rechercher les faits ou circonstances révélant des activités illicites, cette limite ne trouve pas à s'appliquer lorsque lesdites activités sont générées ou induites par le prestataire lui-même ;

Attendu que force est de constater en l'espèce que la société Dailymotion n'a mis en œuvre aucun moyen propre à rendre impossible l'accès au film "Joyeux Noël", sinon après avoir été mise en demeure, soit à un moment où le dommage était déjà réalisé, alors qu'il lui incombe de procéder à un contrôle a priori ;

Attendu en revanche qu'il ne saurait être imputé à la société Dailymotion d'avoir permis le téléchargement du film en cause dès lors que le site www.keepvid.com appartient à un tiers, lequel n'est pas dans la cause ;

Sur la contrefaçon et le parasitisme

Attendu que Christian C. déplore une atteinte à son droit de paternité ainsi qu'une atteinte à l'intégrité de l'oeuvre réalisée ;

Attendu que sur le premier chef, la demande n'est pas fondée dès lors qu'il résulte des constats que le générique du film diffusé fait mention du nom du réalisateur ; qu'il ne peut exister aucune confusion avec la mention du pseudonyme de l'internaute indiquant qu'il "présente Joyeux Noël" ;

Attendu en revanche que le mode de diffusion en "streaming" ne permet qu'une visualisation de mauvaise qualité du fait notamment d'un cadre très réduit, inadapté pour un film de long métrage, et de l'effet saccadé ; que l'unité du film est par ailleurs troublée par un découpage en deux parties ; Que l'atteinte à l'intégrité de l'oeuvre est donc constituée ;

Attendu que l'atteinte aux droits patrimoniaux sur l'oeuvre et aux droits de producteur de vidéogramme de la société Nord Ouest Production est pareillement constituée dès lors que la diffusion est intervenue sans leur accord ; qu'il en va de même en ce qui concerne l'atteinte aux droits exclusifs du distributeur dont le contrat a été régulièrement publié au Registre public de la cinématographie et de l'audiovisuel ;

Attendu que la faute imputée sous le grief de parasitisme, qui n'est pas distincte des actes de contrefaçon, s'agissant de la mise à disposition du public d'une œuvre protégée par le droit d'auteur en utilisant les investissements réalisés par autrui ; que ces demandes seront écartées.

Sur les mesures réparatrices

Attendu qu'il sera fait droit à la demande d'indemnisation symbolique formulée par Christian C. ;

Attendu que le préjudice de la société Nord Ouest Production sera intégralement réparé par l'allocation de la somme de 10 000 € au titre de l'atteinte à ses droits d'exploitation et de celle de 3000 € au titre de l'atteinte à ses droits voisins ;

Attendu qu'il sera alloué à la société UGC Images la somme de 10 000 € à titre de dommages-intérêts ;

Attendu que la mesure d'interdiction requise sera prononcée dans les termes précisés au dispositif ;

Attendu qu'il y a lieu par ailleurs d'ordonner à titre d'indemnisation complémentaire la publication du dispositif de la présente décision sur la page d'accueil du site www.dailymotion.com pendant un délai de huit jours et sous astreinte ; que la publication par voie de presse n'est pas justifiée ;

Sur les autres demandes

Attendu que la demande reconventionnelle est sans objet du fait des condamnations prononcées ;

Attendu que l'exécution provisoire sera prononcée en ce qui concerne la seule mesure d'interdiction sous astreinte ;

Attendu qu'il serait inéquitable que la société Nord Ouest Production supporte la charge de ses frais non compris dans les dépens ; qu'il lui sera alloué à ce titre la somme de 6000 € sur le fondement des dispositions de l'article 700 du ncp ;

Attendu que la société Dailymotion sera condamnée aux entiers dépens de l'instance.

Le tribunal, statuant en audience publique, par décision contradictoire et en premier ressort,

. Dit que la société Dailymotion, exploitant du site www.dailymotion.com développe une activité de

prestataire technique en ce qu'elle remet la mise en ligne de vidéogrammes par les internautes eux-mêmes,

. Dit que la société Dailymotion a effectivement connaissance de ce que le site considéré stocke en vue de la mise à disposition du public des contenus illicites en ce qu'ils sont protégés par le droit d'auteur, sans les retirer ou en rendre l'accès impossible,

. Dit qu'en acceptant la mise en ligne par un utilisateur de son service du film "Joyeux Noël" la société Dailymotion a commis une faute engageant sa responsabilité civile en fournissant audit utilisateur les moyens de réaliser une contrefaçon,

En conséquence,

. Condamne la société Dailymotion à payer à Christian C. la somme de un euro à titre de dommages-intérêts en réparation de l'atteinte portée à l'intégrité de son œuvre,

. La condamne à payer à la société Nord Ouest Production la somme de 10 000 € en réparation des atteintes portées à ses droits patrimoniaux et la somme de 3000 € en réparation des atteintes portées à ses droits de producteur de vidéogrammes,

. La condamne à payer à la société UGC Images la somme de 10 000 € à titre de dommages-intérêts en réparation des atteintes portées à son droit exclusif d'exploitation,

. Fait interdiction à la société Dailymotion de poursuivre les actes de contrefaçon ci-dessus relevés sous astreinte de 1500 € par infraction constatée à compter de la signification de la présente décision,

. Ordonne la publication du dispositif de la présente décision sur la page d'accueil du site www.dailymotion.com pendant une durée de huit jours sous astreinte de 10 000 € par jour de retard passé le délai de 15 jours suivant la date à laquelle la présente décision aura acquis un caractère définitif,

. Ordonne l'exécution provisoire de la présente décision en ce qui concerne la seule mesure d'interdiction sous astreinte,

. Déboute les parties de leurs demandes plus amples ou contraires,

. Condamne la société Dailymotion à payer à la société Nord Ouest Production la somme de 6000 € sur le fondement des dispositions de l'article 700 du ncpc,

. La condamne aux entiers dépens de l'instance.

I.R.I.S (Imaginons un Réseau Internet Solidaire),
AFFAIRE DAILYMOTION : LE TGI DE PARIS ÉCRIT LA
LCEN 2.0; Droit-Tic, 20 juill. 2007

Référence : TGI de Paris, 3ème ch., 13 juillet 2007,
CHRISTIAN C., NORD OUEST PRODUCTION /
DAILYMOTION, UGC IMAGES, DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=104

AFFAIRE DAILYMOTION : LE TGI DE PARIS ÉCRIT LA LCEN 2.0

Par I.R.I.S (Imaginons un
Réseau Internet Solidaire)

La décision rendue en première instance le 13 juillet 2007 par le TGI de Paris, qui s'appuie sur la loi pour la confiance dans l'économie numérique (LCEN) de juin 2004, est susceptible de marquer un tournant pour la qualification juridique de plusieurs services du web2.0.

La société DailyMotion, deuxième après YouTube sur le marché mondial des plates-formes de stockage et d'échange de vidéos, vient d'être condamnée dans une affaire de contrefaçon. La décision rendue en première instance le 13 juillet 2007 par le TGI de Paris, qui s'appuie sur la loi pour la confiance dans l'économie numérique (LCEN) de juin 2004, est susceptible de marquer un tournant pour la qualification juridique de plusieurs services du web2.0.

Tout d'abord, la décision reconnaît à DailyMotion le statut d'hébergeur de contenus, au sens de l'article 6-1-2 de la LCEN. Elle réfute en cela les arguments des demandeurs, réalisateur, producteur et diffuseur du film rendu disponible en streaming sur la plate-forme par l'un de ses utilisateurs, qui soutenaient que DailyMotion avait la qualité d'éditeur. La nature de cette activité est reconnue sans ambiguïté : pour le tribunal, le simple fait de commercialiser des espaces publicitaires n'entraîne pas la qualité d'éditeur ; d'autre part, DailyMotion exerce par ailleurs l'activité d'éditeur ou de co-éditeur pour la diffusion des films des catalogues Universal et Warner, conformément aux accords passés avec ces sociétés ;

enfin, DailyMotion se conforme bien aux obligations que la LCEN impose aux hébergeurs, notamment la conservation des données d'identification de leurs abonnés.

Par conséquent, le tribunal reconnaît à DailyMotion, en tant qu'hébergeur, l'absence d'obligation générale de surveillance des contenus illégaux hébergés, ainsi que de recherche de faits ou circonstances révélant des activités illicites, garantie par la LCEN.

Pour autant, la condamnation résulte du fait que le tribunal considère que DailyMotion génère lui-même ou induit ces activités illicites, seules à même d'assurer la rentabilité de l'entreprise. En effet, la décision précise qu'« il ne peut être sérieusement prétendu que la vocation de l'architecture et les moyens techniques mis en place par la société DailyMotion ne tendaient qu'à permettre à tout un chacun de partager ses vidéos amateur avec ses amis ou la communauté des internautes selon l'option choisie, alors qu'ils visaient à démontrer une capacité à offrir à ladite communauté l'accès à tout type de vidéos sans distinction, laissant le soin aux utilisateurs d'abonder le site dans des conditions telles qu'ils le feraient avec des oeuvres protégées par le droit d'auteur ». Elle note de plus que « le succès de l'entreprise supposait nécessairement la diffusion d'oeuvres connues du public, seules de nature à accroître l'audience et à assurer corrélativement des recettes publicitaires ».

D'hébergeur n'ayant pas d'obligation générale de surveillance d'activités illicites, DailyMotion devient ainsi considéré comme hébergeur ayant une connaissance générale d'activités illicites, puisqu'il les induit, voire les génère lui-même, en tant que fondement de son modèle économique.

Cette qualification juridique est nouvelle, et en tout état de cause n'est pas inscrite dans la LCEN, ni dans la Directive européenne sur le commerce électronique. Elle va bien plus loin que les circonstances jugées, puisqu'elle s'applique à l'ensemble des activités de DailyMotion et, au-delà, à l'ensemble des services

marchands dits communautaires du web 2.0. Elle ne peut qu'imposer un contrôle a priori des contenus mis en ligne par ces services, c'est-à-dire en fin de compte une responsabilité éditoriale.

Cette décision pose plusieurs questions, juridiques, mais aussi économiques et sociologiques. Peut-on exercer une responsabilité éditoriale sans être éditeur ? Le modèle économique du « gratuit », en fait fondé sur les recettes publicitaires, est-il acceptable ou induit-il nécessairement la génération d'activités illégales ? Enfin, les usages dit communautaires de telles plates-formes d'échanges encouragent-ils vraiment l'autonomisation, la créativité, la participation, parfois même qualifiée de « démocratique » ou « citoyenne », ou bien ne sont-ils qu'un moyen, certes moderne, de conforter l'individualisme de masse et d'encourager la confusion des domaines public et privé ? La réponse à ces questions nécessiterait l'ouverture d'une réflexion et d'un débat public d'ampleur, avant toute modification législative.

DailyMotion annonce l'utilisation prochaine du système « Audible Magic », qui fonctionne comme un filtrage sur liste noire en empêchant la mise en ligne d'oeuvres audiovisuelles protégées par le droit d'auteur et listées dans une base de données. Mais la généralisation du contrôle a priori des contenus par les fournisseurs de plates-formes d'hébergement de vidéos n'est pas une solution, pas plus que le filtrage comme panacée en matière de lutte contre les contenus illégaux. Ces plates-formes doivent plutôt revenir à la seule et unique fonction d'hébergeur, dont le modèle économique consiste à générer des revenus au titre de la fourniture d'espace et de services associés pour le stockage d'informations sous la seule responsabilité des auteurs de leur mise en ligne. Le modèle du faux gratuit dénature aussi la répartition des responsabilités et, au final, fait obstacle à la préservation de la liberté d'expression, de communication et d'information.

Par I.R.I.S Imaginons un Réseau Internet Solidaire,
Association

Pour plus de détails, voir :

- La décision du TGI de Paris du 13 juillet 2007

http://www.droit-tic.com/juris/aff.php?id_juris=104
- Le dossier d'IRIS sur la LCEN
<http://www.iris.sgdg.org/actions/len/>

Contact IRIS :

iris-contact[AT]iris.sgdg.org - Tel : 0144749239



INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

SÉCURITÉ ET PERTINENCE DE LA BASE ÉLÈVES 1ER DEGRÉ , LES ASSOCIATIONS DÉNONCENT LES RISQUES

Par M. Nicolas Samarcq,
Juriste TIC et M. Luc Masson
Juriste TIC - Lexagon.Fr.

Depuis le mois de juin dernier, le développement de la « Base élèves 1er degré » (BE1D) suscite de nombreuses controverses tant au niveau de la sécurité que des données collectées et traitées par l'administration.

Le syndicat SNUIPP[1] de la Charente a saisi le 11 juin dernier le président de la CNIL pour dénoncer ces graves manquements à la loi. Parmi les informations collectées par l'éducation nationale pour alimenter le BE1D on retrouve la nationalité de l'élève, le pays d'origine et la date d'entrée en France.

Le système scolaire français est conçu comme un parcours, de l'entrée à la maternelle à la sortie du lycée[2]. Les informations concernant les élèves sont donc collectées et agrégées en flux à l'entrée dans chaque classe et à chaque changement d'établissement. Les finalités de cette « traçabilité éducative » sont d'assurer un suivi social, pédagogique, éducatif[3], médical, mais également de permettre aux Recteurs et aux chefs d'établissement de mieux faire coïncider besoins et ressources.

Ces dernières années, les données collectées ont également permis la mise en place de la suspension des

allocations familiales pour les familles qui ne satisfont pas à leurs obligations éducatives. Les dernières évolutions de la collecte de données personnelles dans l'éducation nationale démontrent un renforcement de la politique d'immigration, c'est du moins la dérive potentielle dénoncée par un grand nombre de personnels de l'éducation nationale, de parents d'élèves et de syndicats.

Rappelons pour mémoire qu'en application de la Convention Internationale des Droits de l'enfant ratifiée par la France en 1990, les enfants de moins de 16 ans, nés hors de France de parents étrangers ont le droit d'être scolarisé[4]. L'article L131-1 du Code de l'éducation nationale rappelle cette obligation publique[5].

C'est en 2004 que le Ministère de l'Education nationale a déclaré à la Commission Nationale Informatique et Libertés (CNIL) la mise en œuvre d'un traitement de données à caractère personnel dénommée « Base élèves 1er degré » (BE1D).

Finalités et personnes concernées par le BE1D

La BE1D a pour finalités :

- la gestion administrative des élèves (inscription, admission, non fréquentation, répartition dans les classes, suivi des effectifs et de la scolarité),
- le pilotage pédagogique,
- le suivi des parcours scolaires de la maternelle à l'entrée en 6^{ème},
- l'élaboration de statistiques académiques et nationales.

Ce traitement concerne donc tous les élèves des écoles maternelles et élémentaires, privées et publiques, y compris les enfants recevant une instruction dispensée en dehors de l'école[6].

Les parents ne peuvent s'opposer à la collecte de ces données personnelles concernant leurs enfants, puisque l'inscription scolaire est obligatoire jusqu'à 16 ans.

Destinataires des données traitées

Outre l'éducation nationale^[7], les maires sont habilités à accéder aux données relatives à l'identité de l'enfant (nom, prénoms, sexe, date et lieu de naissance, adresse) et de son responsable légal (nom, prénom, adresse, téléphone, lien avec l'enfant) résidants dans leur commune, dans la mesure où ils sont chargés du contrôle de l'obligation scolaire et de la gestion des inscriptions. Cette disposition n'est pas nouvelle, depuis 1991, une norme simplifiée adoptée par la CNIL prévoit la collecte de ces catégories d'informations à leur bénéfice.

Le Ministère de l'Education nationale traite, uniquement à des fins de statistiques anonymes, également les données relatives à la nationalité, à l'année d'arrivée en France de l'enfant et aux coordonnées de l'employeur des parents. Ces données ne sont pas transmises aux maires.

Seuls le directeur de l'école d'affectation de l'élève, l'inspecteur d'académie chargé de circonscription, l'inspecteur d'académie et le directeur des services départementaux de l'éducation nationale sont destinataires des données sur les élèves en difficulté relatives à un besoin éducatif particulier, tels que le bénéfice d'un dispositif d'accueil individualisé (PAI), d'assistance pédagogique à domicile (SAPAD) ou d'un dispositif réseau d'aide aux élèves en difficultés (RASED).

On notera toutefois quelques interconnexions malencontreuses.

Comme vous avez pu le lire ci-dessus, la totalité des données n'est pas accessible à tous les personnels et à tous les interlocuteurs de l'éducation nationale, du moins cela devrait-il être le cas.

Or, il n'est pas rare qu'un chef d'établissement ou un enseignant, soit à la fois présent dans l'établissement où est scolarisé un élève et accessoire d'un juge pour enfant dans la même commune ou circonscription, voire

membre du conseil municipal de la commune dans laquelle réside l'élève en question. Le cloisonnement des accès aux données apparaît alors immédiatement illusoire.

Conservation des données

Concernant le suivi de la scolarité, seules les données factuelles du cursus scolaire de l'élève sont conservées (école, classe, niveau (9 niveaux), apprentissages suivis) et non ses notes ou évaluations.

Toutefois, il est à remarquer qu'une circulaire du 26 juin 1968 prévoit que lors de son inscription l'élève fournira les bulletins trimestriels des deux dernières années, bulletins dans lesquels on retrouve notes et appréciations. Le même principe prévaut lors d'une inscription post-baccalauréat en section de technicien supérieur.

Informations des parents

La CNIL a précisé que le dossier déposé par le Ministère indique que la fiche de renseignements individuels adressée par le directeur d'école aux parents ou à la personne responsable de l'élève porte mention des dispositions de la loi Informatique et Libertés relatives aux droits d'accès, de rectification et d'opposition sur certaines données non strictement nécessaires à la gestion administrative et au suivi pédagogique de l'élève.

Il faudrait toutefois préciser que les parents ont droit d'accès à l'ensemble de fichiers concernés, qu'ils soient informatisés ou non car bon nombre d'établissements scolaires utilisent encore des fichiers papiers non informatisés.

La « Base élèves 1er degré » est actuellement en phase de déploiement. Elle devrait être généralisée pour la rentrée 2009.

Luc Masson, chargé d'enseignement en droit
Nicolas Samarcq consultant et juriste TIC
www.lexagone.fr

Par M. Nicolas Samarcq, Juriste TIC et M. Luc Masson Juriste TIC

[1] Le Syndicat National Unitaire des Instituteurs,
Professeurs des écoles et Pegc

[2] Lycée d'enseignement général ou professionnel.

[3] Eu égard, entre autres choses, à la discipline.

[4] Article 28. Les Etats parties reconnaissent le **droit de l'enfant à l'éducation**, et en particulier, en vue d'assurer l'exercice de ce droit progressivement et sur la base de l'égalité des chances.

[5] Voir également la circulaire n° 68-265 du 26 juin 1968 relative au dossier d'inscription des élèves dans les établissements du second degré (RLR-522.0) et circulaire n° 84-246 du 16 juillet 1984 relative à l'inscription d'élèves étrangers dans le premier et le second degré.

[6] Un traitement identique de gestion et de pilotage, intitulé « Scolarité », existe depuis 1995 pour les élèves du second degré.

[7] Directeurs d'écoles, les inspecteurs de l'éducation nationale, les inspecteurs d'Académie.

ADRESSAGE, NOMS DE DOMAINE ET LIENS HYPERTEXTES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

DÉTOURNEMENT DE MARQUE AU SEIN D'UN RÉSEAU DE FRANCHISE

Par M. Benjamin Vitasse,
Juriste - Consultant noms de
domaine, MailClub.info

Faute de dispositions contractuelles contraires, le franchisé devient titulaire du nom de domaine identique à la marque de son franchiseur. Un montage juridique à risque...

Faute de dispositions contractuelles contraires, le franchisé devient titulaire du nom de domaine identique à la marque de son franchiseur. Un montage juridique à risque, notamment lorsque le franchisé indélicat décide de commercialiser des produits concurrents sous le nom de son patron ...

Le litige oppose la société Allemande Refill24 GmbH, spécialisée dans la commercialisation de systèmes de remplissage de cartouches d'encre pour imprimantes (le Requéant), à la société Française Reset Multiservices (le Défendeur).

Le Requéant exploite son réseau de franchise sous le nom refill24 dont il est titulaire à la fois du nom de domaine refill24.com et de la marque communautaire Refill24, enregistrée le 3 décembre 2004 auprès de l'OHMI et dont la protection lui est accordée notamment sur le territoire français.

Le Défendeur intègre le réseau de franchise du Requéant lors de la signature d'un contrat en date du 2

décembre 2003 et enregistre le nom de domaine refill24.fr le 17 juin 2005.

Très vite, les relations commerciales se dégradent entre les parties. Le franchisé ne commande plus de marchandise auprès de son franchiseur alors qu'il y est tenu contractuellement ; Pire encore, ce dernier découvre que son franchisé commercialise directement des produits concurrents via le site refill24.fr.

Après avoir mis fin au contrat de franchise, le Requéant engage une PARL aux fins de récupérer le nom de domaine litigieux.

Pour ordonner le transfert du nom au profit du Requéant, l'expert retient simplement que « *l'utilisation du nom de domaine par le Défendeur, du fait de la résiliation du contrat de franchise, constitue une violation des droits du Requéant sur la marque communautaire REFILL24 dont il est titulaire* ».

Sur la question de savoir si le franchisé était en droit d'enregistrer le nom de domaine litigieux, l'expert ne peut se prononcer. En effet, le contrat de franchise ne précise pas l'étendue des droits du franchisé dans le cadre de l'utilisation de la marque du franchiseur ni ses éventuelles limitations. Par ailleurs, le Requéant n'a jamais contesté ni remis en cause cet enregistrement.

Une lacune contractuelle qui aujourd'hui encore porte préjudice au Requéant. En effet, à ce jour (et en dépit de la PARL rendue le 19 juin 2007) le nom de domaine refill24.fr pointe toujours sur le site du Défendeur et entretient donc la plus grande confusion pour le public.

La décision Refill24 GmbH contre Reset Multiservices,
Litige n° DFR2007-0019



ECONOMIE NUMÉRIQUE, LOI APPLICABLE ET JURIDICTION COMPÉTENTE

LE PMU DEVRA T IL RENONCER À SON MONOPOLE SUR LES PARIS EN LIGNE?

Par Me. Nicole Bondoïs,
Avocate et Melle Fanny Duban,
Juriste en propriété
intellectuelle.

La loi du 2 juin 1891 apparaissait pourtant limpide : hormis les autorisations délivrées par le Ministère de l'Agriculture, la prise de paris sur les courses hippiques françaises est interdite.

La loi du 2 juin 1891 apparaissait pourtant limpide : hormis les autorisations délivrées par le Ministère de l'Agriculture, la prise de paris sur les courses hippiques françaises est interdite. Seul le PMU bénéficie d'un monopole et ce depuis sa création en 1930.

Dans ce contexte, la société Zeturf s'engage pourtant le 17 juin 2005, dans une activité d'organisation et d'exploitation de paris hippiques en ligne sur des courses se déroulant notamment en France, et ce avec le concours de la société française Eturf.

Le groupement d'intérêt économique PMU, qui ne l'entend pas ainsi, assigne les deux sociétés Zeturf et Eturf en référé devant le Tribunal de Grande Instance de Paris aux fins d'obtenir la cessation de leur activité.

Le président du TGI, saisi du litige, considère que cette activité cause effectivement un trouble manifestement illicite au PMU, en ce qu'elle porte atteinte à son droit exclusif réservé par la loi pour organiser des paris sur les courses de chevaux, et rend une ordonnance en ce sens.

Celle ci se voit confirmée par la Cour d'Appel de Paris..

Or, la Cour de Cassation, dans un arrêt en date du 10 juillet 2007, opte pour l'annulation de la décision d'appel. S'appuyant sur la jurisprudence de la CJCE et notamment sur les décisions Zenatti (21 octobre 1999), Gambelli (6 novembre 2003) et Placanica (6 mars 2007), elle reconnaît que les activités de paris sont assimilables à des services et qu'en tant que tels, ils sont soumis aux principes communautaires de liberté d'établissement et de libre prestation de services.

En un mot, elle semble indiquer que le droit national qui a instauré le monopole du PMU est contraire au droit communautaire.

Le monopole du PMU est il pour autant remis en cause ? Il semble que non. En effet, la jurisprudence communautaire admet une exception aux principes de liberté.

Une restriction à la libre prestation de services peut ainsi être justifiée « soit au regard de l'objectif consistant à prévenir l'exploitation des jeux de hasard à des fins frauduleuses (...) en les canalisant dans des circuits contrôlables, soit au regard de l'objectif tenant à la réduction des occasions de jeux (...) ».

La Cour de Cassation ne se prononce pas, dans cet arrêt, sur le fait de savoir si le PMU répond ou non à ces objectifs mais renvoie à la Cour d'Appel de Paris. Le PMU devra donc prouver qu'il concourt bel et bien à la diminution du marché des paris en ligne, et qu'il remplit en quelque sorte une mesure d'utilité publique.

Pari cette fois ci difficile à tenir pour le PMU dont la prospérité insolente s'accorde mal avec une diminution des marchés qu'il est censé favoriser. On attend avec impatience les arguments qu'il avancera dans un contexte qui ne lui est pas favorable.

En effet, la Cour de Cassation n'a pas hésité à montrer du doigt l'Etat français en énonçant que « la seule circonstance que l'Etat retire des bénéfices de l'activité des jeux en ligne n'est pas en tant que tel une justification des restrictions à la libre prestations de services ».

« L'Etat croupier » au sens du rapport Trucy est ici clairement dénoncé avec audace par la Cour suprême.

ADRESSAGE, NOMS DE DOMAINE ET LIENS HYPERTEXTES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

TYPOSQUATTING : FOCUS SUR LES NOMS DE DOMAINE DES MOTEURS DE RECHERCHE

Par M. Jean-François
Poussard, Rédacteur en Chef
MailClub.info

Respectivement, premier et troisième site les plus visités au monde, Yahoo et Google sont les cibles privilégiées des typosquatteurs qui tentent de détourner le trafic généré par ces deux mastodontes. Confirmation avec notre [étude spéciale typosquatting](#) sur les noms de domaine des principaux moteurs de recherche.

Depuis l'émergence des noms de domaine, on a connu les phénomènes de « cybersquatting ». L'enregistrement abusif et spéculatif d'un nom de domaine à l'identique a connu ses heures de gloire avant que les ayants-droits se réveillent. Ces derniers ont alors utilisé les procédures alternatives de litiges (essentiellement les procédures UDRP de l'OMPI ; 25 000 litiges tranchés en octobre 2006) pour récupérer leurs noms de domaine. De ce fait, la majorité des sociétés notoires sont désormais quasiment toutes titulaires de leurs .com et de leurs extensions nationales. Les « cybersquatteurs » ne se sont pas laissés démonter et ont décidé d'enregistrer des noms de domaine connus avec des fautes

d'orthographe.

Des fautes d'orthographe à foison

La pratique du typosquatting consiste à l'enregistrement de noms de domaine similaires à des droits antérieurs : nom de domaine, marque, signe distinctif, dénomination sociale, nom de personne physique... Letyposquatting joue sur l'inversion de caractères, les modifications de lettre ou les variantes phonétiques, en espérant que certains internautes commettront une faute d'orthographe ou une faute de frappe. Ces enregistrements sont majoritairement effectués par des tiers mal intentionnés, bien que de nombreuses sociétés se prémunissent désormais de ce type de comportement en déposant elles-mêmes ces noms de domaine.

Des sites parking complaisants

La plupart du temps, les typosquatteurs redirigent ces noms de domaines vers des sites dits « parking » qui renvoient vers des liens sponsorisés. Ils captent ainsi l'internaute étourdi qui a mal saisi le nom de domaine du site qu'il comptait visiter. Arrivé malgré lui sur ce site parking, le visiteur va se voir proposer des liens correspondant au site typosquatté, des liens vers des concurrents directs, voir même des liens vers son propre site ! Ce système permet au typosquatteur de rentabiliser l'achat de son nom de domaine frauduleux. Le principe est simple : il est rémunéré à chaque clic de l'internaute vers un des liens sponsorisés. Ce mode de revenu particulier est nommé Pay Per Click (paiement au clic). Comme il n'y a pas de petites économies, le nom de domaine typosquatté est également mis à la vente.

Afin de mesurer le potentiel de visites (et donc d'euros) du nom de domaine litigieux, les fraudeurs utilisent une méthode particulière : le « domain tasting » ou « cybersquatting furtif ». Chaque jour, plusieurs

millions de noms de domaine sont enregistrés et testés en usurpant des milliers de marques de notoriété mondiale. Le titulaire est en effet autorisé à supprimer ces noms de domaines après cinq jours d'activité grâce à « l' Add Grace Period ». Chose qu'il fait pour les noms non rentables tout en obtenant de l'ICANN le remboursement total des frais d'enregistrement. Les noms intéressants sont eux conservés par le typosquatteur. Cette technique permet **decapter un maximum de trafic Internet, de mesurer le potentiel commercial des domaines squattés** et de ne conserver que ceux susceptibles de rembourser au minimum leurs frais d'enregistrement définitif. L'objectif étant bien sûr de générer un maximum d'euros.

MailClub.info a réalisé son étude spéciale avec l'outil exclusif anti-typosquatting du MailClub ([disponible en cliquant ici](#)). Ce système générateur de « typos » teste les combinaisons d'écritures d'un nom de domaine, tout en vérifiant sa disponibilité. Plus un nom de domaine est long (altavista), plus le nombre de combinaisons possibles augmente.

MailClub.info a reporté les résultats suivants lors de ses tests : nombre de combinaisons testées, nombre de noms de domaine typosquattés, le nombre de noms de domaine enregistrés par la société titulaire et enfin le pourcentage de noms de domaine pris par des tiers.

Enregistrements records

Trois moteurs (Google, Yahoo et Lycos) ont été testés sur les extensions .fr et .com, Voila en .fr, Copernic et Altavista sur leurs .com. Première conclusion, le nombre très élevé de noms enregistrés par rapport au nombre de combinaisons testées. **Les noms de domaines typosquatables de Google.com (76 combinaisons testées), Yahoo.com, Lycos.com sont enregistrés à 100 %.** Altavista.com n'est pas loin avec 96 % et 112

noms de domaine. Google.fr suit (84 %) avec copernic.com (75 %), yahoo.fr (70 %), voila.fr (56 %) et lycos.fr (30 %). La quasi-totalité des noms de domaine enregistrés le sont par des tiers : 98 % pour google.fr et lycos.com, 97 % pour copernic.com, 94 % pour lycos.fr... Entre 70 et 80 % pour yahoo.fr, altavista.com, google.com et voila.fr. Il s'agit principalement de sites parkings divers et variés, parfois de sites pornographiques. On notera les cas particuliers de www.lyc0s.com qui renvoi sur Google et de altaviista.com qui conduit chez yahoo.com !

Rayon extensions, **les noms de domaine typosquattés en .fr sont moins nombreux que ceux en .com, mais ceux qui le sont, font l'objet de dépôts beaucoup plus litigieux.**

Yahoo en pointe dans sa lutte

Google et Lycos semblent laisser faire ces enregistrements frauduleux alors que Yahoo est entré en guerre, tout du moins sur son .com. Si 78 % de ces noms de domaine sont pris par des tiers en .fr, seulement 42 % le sont sur yahoo.com.

Le premier site visité dans le monde, n'a pas obtenu ces noms de domaine sans effort. Il a mené une lutte acharnée contre les typosquatteurs en envoyant fin juin 2006 **plus de 1 700 lettres de mises en demeure à des titulaires de noms de domaine typosquattant sa marque phare : Yahoo.** Cette lettre signale que la société américaine a déposé une plainte le 12 décembre 2005, à la cour des Etats-Unis pour violations de l'acte de protection des consommateurs d'anti-cybersquatting de 1999. Le courrier de Yahoo propose aux titulaires de « résoudre ce problème officiellement et d'arrêter les réclamations contre le propriétaire résultant de l'utilisation du nom de domaine, y compris écarter le préjudice, sur le transfert du (des) noms de domaine à Yahoo ». Pour cela, Yahoo joint un accord de

consentement à sa lettre. En utilisant ce procédé à l'amiable de façon massive, Yahoo contourne les résolutions de litiges de l'OMPI (Organisation Mondiale de la Propriété Intellectuelle). Le géant américain est pourtant un habitué des procédures UDRP. Plus de 700 décisions concernent ses noms de domaine !

Une stratégie qui permet à Yahoo, d'être le moteur de recherche maîtrisant le mieux le phénomène du typosquatting.



INFORMATIQUE ET LIBERTÉS, VIE PRIVÉE

LES AGENCES DE SÉCURITÉ DOIVENT ÊTRE SOUMISES À UN CONTRÔLE DÉMOCRATIQUE

Par M. Thomas Hammarberg,
Commissioner for Human Rights

Nous savons que les services de sécurité nationaux d'Europe ont participé à la "guerre contre la terreur" menée par les USA. Ils ont participé à des opérations qui ont constitué des violations flagrantes des droits de l'homme

Nous savons que les services de sécurité nationaux d'Europe ont participé à la "guerre contre la terreur" menée par les USA. Ils ont participé à des opérations qui ont constitué des violations flagrantes des droits de l'homme. La CIA des USA a certes assuré la direction et la coordination des opérations, mais les services de renseignements d'Europe doivent accepter leur part de responsabilité pour les enlèvements, les "restitutions", les détentions secrètes et les interrogatoires illégaux.

Certains ont remis des suspects à la CIA ou fermé les yeux sur des enlèvements secrets de personnes. Ils ont facilité l'organisation d'avions transportant des prisonniers et fourni des informations à la CIA.

Le Sénateur Dick Marty a indiqué à l'Assemblée parlementaire du Conseil de l'Europe que deux de ses Etats membres ont même mis à disposition pendant quelques années des installations pénitentiaires

destinées aux détentions secrètes.

Il faut à tout prix faire un bilan complet de ce qui s'est produit après le "onze septembre" et tirer les leçons des erreurs commises. Il faut rétablir les normes en matière de droits de l'homme qui ont été adultérées. Une telle démarche s'impose également pour protéger la crédibilité de la lutte contre le terrorisme à l'avenir.

Le retard considérable qu'a pris cette évaluation vitale est partiellement imputable aux intimidations politiques et autres menaces de l'administration Bush. De plus, l'on estime généralement en Europe que les questions de sécurité nationale ne peuvent être discutées ouvertement. Les gouvernements ont craint que leurs efforts de transparence ne bloquent leur collaboration avec d'autres agences de sécurité et ne compromettent les échanges d'informations.

Toutefois, l'exécutif ne doit pas échapper à ses responsabilités pour les violations des droits de l'homme sous prétexte du "secret d'Etat". Il est urgent d'organiser une discussion constructive et approfondie afin de définir des garde-fous dans ce domaine. S'il existe une volonté politique suffisante, ce sera possible sans divulguer des faits qui doivent rester confidentiels. Le gouvernement canadien a donné un excellent exemple en créant une [commission](#) pour l'affaire Arar.

Nous devons partir du constat que le terrorisme est une grave menace. Après le 11 septembre 2001, d'autres attentats effroyables ont été perpétrés à Beslan, à Istanbul, à Madrid, à Londres et en d'autres endroits. Il faut prendre des mesures afin de prévenir et d'empêcher de telles atrocités et d'en poursuivre les auteurs. Cela ne peut se faire sans le travail de surveillance et de collecte de données.

Il convient toutefois de fixer des limites claires aux activités des services de sécurité, y compris les organismes militaires. La torture et les autres traitements cruels, inhumains ou dégradants ne peuvent jamais être tolérés, les personnes privées de leur liberté doivent disposer d'une possibilité de contester leur détention

dans le cadre de procédures correctes, sans oublier les garanties contre l'exploitation illicite d'informations collectées sur les particuliers. Les normes du domaine des droits de l'homme doivent toujours être respectées, même en période de crise. Ce n'est pas un domaine sujet à des dérogations proportionnelles à un intérêt supérieur.

Quand une part aussi importante des activités des services de sécurité est classée secrète, il devient particulièrement important de veiller à la présence d'un système de contrôle démocratique. Il est apparu ces dernières années que même les chefs de gouvernement ne sont pas toujours impliqués. Le contrôle exercé par le Parlement et par les autorités judiciaires a été minime. Les services de renseignements ont mené leur collaboration avec d'autres agences sans grand contrôle.

L'année dernière, le Secrétaire général du Conseil de l'Europe, M. Terry Davis, a soulevé ce point en rapport avec la question de la détention illicite et du transport de détenus soupçonnés d'être impliqués dans des actes terroristes. Il a suggéré que l'on améliore la surveillance des activités des services secrets, tant étrangers que nationaux, sur le territoire des Etats membres.

La Commission de Venise a récemment publié un Rapport intéressant sur la manière dont un contrôle démocratique pourrait être organisé afin de garantir une responsabilité de l'Etat. Même si elle ne couvre pas les services de renseignements militaires et étrangers, l'analyse de la Commission est particulièrement utile. Elle aborde quatre types de responsabilité: les mécanismes parlementaires et judiciaires, les experts et les recours.

- L'autorité formelle des services de renseignements devrait reposer sur une tutelle parlementaire. Le Parlement pourrait lui-même mettre en place un organe de surveillance dont les membres seraient tenus de respecter la confidentialité nécessaire. Un tel mécanisme pourrait convaincre le grand public qu'il existe effectivement un contrôle permanent, même si les détails des diverses activités ne sont pas divulgués au public.

- Les décisions visant à autoriser des mesures spéciales d'enquête pourraient être confiées à l'appareil judiciaire. Celui-ci pourrait également jouer un rôle en jugeant ces méthodes par la suite. La Commission de Venise fait observer que l'extraction de données et d'autres méthodes de collecte d'informations échappent généralement au contrôle judiciaire.

- Des groupes d'experts pourraient être mis en place pour aider à contrôler les activités des services de sécurité. Cette option peut être préférée quand il est nécessaire de veiller à l'indépendance des membres, et parce que les experts disposent de davantage de temps que les parlementaires et les juges pour exercer un tel contrôle. Il existe également des modèles d'organes de contrôle qui combinent les experts et les parlementaires.

- Il faut mettre en place des mécanismes spécifiques offrant une possibilité de recours devant une instance indépendante aux particuliers qui prétendent avoir été victimes des services de sécurité. Cela peut renforcer la responsabilité et favoriser les améliorations du système dans son ensemble.

Les gouvernements pourraient utiliser le [Rapport de la Commission de Venise](#) comme un guide pratique pour faire le point sur les lacunes qui ont été si laborieusement révélées.

Thomas Hammarberg

Par **M. Thomas Hammarberg**, Commissioner for Human Rights

Liens

- ▶ [La Commission Arar](#)
- ▶ [Détentions secrètes et transferts illégaux de détenus impliquant des Etats membres du Conseil de l'Europe : second rapport](#)
- ▶ [Rapport de la Commission des questions juridiques et des droits de l'homme de l'APCE - Rapporteur Dick Marty \(doc. 11302 rev., 11/06/07\)](#)
- ▶ [Rapport de la Commission de Venise sur le contrôle démocratique des services de sécurité \(doc. CDL-AD \(2007\)016, 11/06/07, en anglais seulement\)](#)
- ▶ [Suivi des rapports du Secrétaire Général, établi en vertu de l'article 52 de la CEDH, sur la question de la](#)

détention et du transport secrets de détenus soupçonnés d'actes terroristes, notamment par des agences relevant d'autres Etats ou à leur instigation (SG/Inf(2006)5 et SG/Inf(2006)13) - Propositions du Secrétaire Général (SG/Inf(2006)01, 30/06/06)

« Également disponible sur le site du Commissaire, sur www.commissioner.coe.int ».

**Décret n°2007-1130 du 23 juillet 2007 relatif
à l'expérimentation du vote électronique
pour les élections prud'homales de 2008 à
Paris, version consolidée au 25 juillet 2007,
J.O n° 170 du 25 juillet 2007 page 12503**

Le Premier ministre,

Sur le rapport du ministre du travail, des relations
sociales et de la solidarité,

Vu le code du travail, notamment le chapitre III du titre Ier
du livre V ;

Vu le code électoral ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à
l'informatique, aux fichiers et aux libertés, notamment son
article 27 ;

Vu l'ordonnance n° 2004-603 du 24 juin 2004 relative
aux mesures de simplification dans le domaine des
élections prud'homales, notamment son article 9 ;

Vu l'avis de la Commission nationale de l'informatique et
des libertés en date du 9 novembre 2006 ;

Vu l'avis du Conseil supérieur de la prud'homie en date
du 26 janvier 2007 ;

Le Conseil d'Etat (section sociale) entendu,

Chapitre Ier : Dispositions générales.

Article 1

Conformément aux dispositions de l'article 9 de
l'ordonnance du 24 juin 2004 susvisée, le vote pour
l'élection des conseillers prud'hommes prévue en 2008
peut être émis, à Paris, par voie électronique, à distance,
dans les conditions et selon les modalités fixées par le
présent décret.

Article 2

L'électeur ayant exercé son droit de vote par voie
électronique n'est plus admis à voter, ni par
correspondance, ni à l'urne.

Article 3

Trois semaines au plus tard avant la date d'ouverture du
scrutin par voie électronique, le ministre chargé du travail
informe les électeurs des modalités d'accès à ce système
de vote.

Article 4

Le vote par voie électronique s'exerce pendant une
période définie par arrêté du ministre chargé du travail.
Cette période prend fin au moins cinq jours avant
l'ouverture du vote à l'urne.

**Chapitre II : Les conditions du vote par voie
électronique.**

Article 5

Ne peuvent voter par voie électronique que les électeurs
inscrits sur les listes électorales prud'homales pour
lesquelles sont connues les informations mentionnées au
I de l'article R. 513-11 du code du travail.

Article 6

L'électeur apte à voter par voie électronique en
application de l'article 5 reçoit la carte électorale prévue à
l'article R. 513-40 du code du travail, sur laquelle figurent
les éléments permettant son identification, selon des
modalités assurant notamment le respect des exigences
de sécurité définies par arrêté du ministre chargé du
travail.

L'électeur ayant reçu une carte ne permettant que le vote
à l'urne ou par correspondance peut, en fournissant les
éléments manquants, obtenir auprès de la mairie de son
arrondissement et dans les conditions prévues par
l'article R. 513-40 une carte électorale permettant le vote
par voie électronique, jusqu'à une date et selon des
modalités définies par arrêté du ministre chargé du
travail.

Chapitre III : Les traitements automatisés.

Article 7

Il est créé, selon des modalités fixées par arrêté du ministre chargé du travail, deux traitements automatisés distincts, dédiés et isolés, respectivement dénommés "fichier des électeurs" et "urne électronique".

Aucun lien n'est établi entre ces deux traitements.

Article 8

Le fichier des électeurs contient les données relatives aux listes électorales prud'homales établies à Paris en application de l'article L. 513-1 du code du travail.

Ce fichier permet d'adresser aux électeurs remplissant les conditions pour voter par voie électronique les éléments permettant leur identification lors des opérations de vote. Il permet également de recenser les électeurs ayant pris part au scrutin par voie électronique et d'éditer les listes d'émargement.

Article 9

L'urne électronique contient les données relatives aux votes exprimés par voie électronique. Les données de ce fichier font l'objet d'un chiffrement.

Article 10

Le système de vote électronique est soumis, préalablement à sa mise en place, à une expertise indépendante. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés et communiqué au comité technique mentionné à l'article 13 et aux délégués de liste mentionnés à l'article 15.

**Chapitre IV : Le bureau du vote par voie électronique.
Article 11**

Un bureau du vote par voie électronique est chargé du contrôle de l'ensemble des opérations de vote par voie électronique et du dépouillement du scrutin.

Article 12

Le bureau du vote par voie électronique est présidé par un magistrat en activité ou honoraire de l'ordre judiciaire, désigné par le premier président de la cour d'appel de Paris.

Il comprend en outre :

1° Deux assesseurs désignés par le premier président de la cour d'appel de Paris parmi les magistrats de l'ordre judiciaire ou les auxiliaires de justice, en activité à Paris ou honoraires ;

2° Deux assesseurs ayant la qualité de fonctionnaire de l'Etat, désignés par le préfet de Paris ;

3° Deux assesseurs ayant la qualité de fonctionnaire, désignés par le maire de Paris ;

4° Un secrétaire désigné par le ministre chargé du travail.

En cas d'absence, le président du bureau du vote par voie électronique est remplacé par le plus âgé des assesseurs présents.

En cas d'absence, le secrétaire du bureau du vote par voie électronique est remplacé par le plus jeune des assesseurs présents.

Lorsque le bureau est appelé à statuer sur une contestation, le président du bureau a voix prépondérante en cas de partage égal des voix.

Le secrétaire assiste aux réunions du bureau mais ne participe pas avec voix délibérative à ses décisions.

Article 13

Le bureau du vote par voie électronique est assisté par un comité technique comprenant l'expert indépendant prévu à l'article 10 et des membres nommés par arrêté du ministre chargé du travail.

Article 14

Le bureau du vote par voie électronique veille au bon déroulement des opérations électorales, en s'assurant notamment :

1° De la mise en oeuvre des dispositifs de sécurité prévus pour garantir le secret du vote par voie électronique et son intégrité ;

2° De la confidentialité du fichier des électeurs comportant les éléments permettant leur identification, du chiffrement de l'urne électronique et de son caractère distinct du fichier des électeurs ;

3° De la conservation des différents supports d'information et des conditions de sécurité et de confidentialité des données pendant et après le scrutin.

Il vérifie la qualité des personnes autorisées à accéder à chacun des traitements automatisés.

Les membres du bureau du vote par voie électronique peuvent accéder à tout moment aux locaux hébergeant les traitements automatisés.

En cas de force majeure, de dysfonctionnement informatique, de défaillance technique ou d'altération des données, le bureau du vote par voie électronique a compétence pour prendre, après consultation du comité technique, toute mesure d'information et de sauvegarde, y compris l'arrêt temporaire ou définitif du processus électoral. Toute intervention sur le système de vote fait l'objet d'une consignation au procès-verbal et d'une information des délégués de liste mentionnés à l'article 15.

Article 15

Chaque liste de candidats peut désigner deux délégués habilités à contrôler l'ensemble des opérations du vote par voie électronique et à faire mentionner au procès-verbal toute observation.

L'accès au bureau du vote par voie électronique leur est assuré, dans la limite de deux délégués à la fois par organisation professionnelle ou syndicale.

Chapitre V : Le déroulement des opérations de vote par voie électronique.

Article 16

Avant l'ouverture du vote, le bureau du vote par voie électronique constate la présence du scellement du système de vote, son bon fonctionnement, la remise à zéro du compteur des suffrages et le fait que l'urne électronique est vide. Il déclare alors le vote ouvert.

Article 17

Pour voter par voie électronique, l'électeur, après s'être identifié, exprime puis valide son vote.

Le vote est anonyme. Il est chiffré par le système dès son émission sur le terminal utilisé par l'électeur, avant sa transmission au fichier "urne électronique". La liaison entre le terminal de vote et le serveur hébergeant le fichier "urne électronique" est également chiffrée.

La transmission du vote et l'émargement de l'électeur ont une date certaine de réception et donnent lieu à l'envoi à l'électeur d'un accusé de réception mentionnant son nom ainsi que la date et l'heure du vote.

Article 18

Au cours de la période de vote par voie électronique mentionnée à l'article 4, la liste des électeurs ayant utilisé cette modalité de vote est transmise à intervalles réguliers au maire de Paris en vue de la mise à jour continue de la liste d'émargement.

Lorsque cette liste est transmise de façon dématérialisée, elle est soit enregistrée sur un support scellé, non réinscriptible, rendant son contenu inaltérable et probant, soit transmise par voie électronique sécurisée assurant son intégrité et sa confidentialité.

Le système de vote garantit qu'aucun résultat partiel n'est accessible pendant le déroulement du scrutin.

A la clôture du vote par voie électronique, la liste complète des électeurs ayant utilisé cette modalité de vote est transmise, selon les mêmes modalités, au maire de Paris.

Article 19

I. - A la clôture du vote par voie électronique, le président et les assesseurs du bureau du vote électronique, après avoir déclaré le scrutin clos, vérifient l'intégrité du système de vote par voie électronique.

Ils vérifient en particulier que le nombre de votes exprimés dans l'urne électronique correspond au nombre de votants figurant sur les listes d'émargement et que les votes enregistrés ont été exprimés pendant la période mentionnée à l'article 4.

Ces informations sont incluses dans le journal qui recense les opérations de vote électronique, est automatiquement édité et communiqué au comité technique mentionné à l'article 13 et aux délégués de liste mentionnés à l'article 15, et est annexé au procès-verbal mentionné à l'article R. 513-98 du code du travail.

II. - Une fois les vérifications terminées, les membres du bureau du vote électronique procèdent au scellement de l'urne électronique.

Article 20

Après le scellement de l'urne électronique, le président du bureau du vote et deux des assesseurs tirés au sort se voient chacun remettre une clé de dépouillement distincte, selon des modalités qui en garantissent la confidentialité.

Deux autres clés sont conservées sous scellés.

Article 21

Après la clôture du scrutin à l'urne prévue à l'article R. 513-55 du code du travail, le président et les assesseurs du bureau du vote par voie électronique procèdent, en public, au dépouillement des votes de ce bureau. A cette fin, ils activent deux des trois clés de dépouillement mentionnées à l'article 20.

Le décompte des suffrages fait l'objet d'une édition sécurisée afin d'être porté au procès-verbal.

Les résultats sont présentés par collège et par section, ainsi que par bureau de vote et par arrondissement.

Les résultats du vote par voie électronique ne font pas l'objet d'une proclamation distincte.

Article 22

Une fois le scrutin à l'urne clos, les résultats du vote par voie électronique de chaque arrondissement sont transmis au président et aux assesseurs du bureau de vote centralisateur prévu à l'article R. 513-100 du code du travail. Ils sont ajoutés aux résultats des votes exprimés à l'urne et par correspondance tels qu'arrêtés dans chaque bureau de vote.

Les résultats sont transmis par chaque bureau centralisateur à la commission de recensement des votes mentionnée à l'article R. 513-103 du même code.

Chapitre VI : Dispositions diverses.

Article 23

Jusqu'à l'expiration du délai de recours contentieux et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde sont conservés sous scellés, sous le contrôle du bureau du vote par voie électronique. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée à nouveau.

A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, il est procédé à la destruction des fichiers supports, sous le contrôle du bureau du vote par voie électronique.

Article 24

Un arrêté du ministre chargé du travail, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent décret.

Article 25.

La garde des sceaux, ministre de la justice, et le ministre du travail, des relations sociales et de la solidarité sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Par le Premier ministre : François Fillon

Le ministre du travail, des relations sociales et de la solidarité, Xavier Bertrand

La garde des sceaux, ministre de la justice, Rachida Dati

Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), J.O n° 113 du 16 mai 2007 page 9362

Le Premier ministre,

Sur le rapport du ministre de la santé et des solidarités,

Vu le code de la santé publique, notamment son article L. 1110-4 ;

Vu le code de la sécurité sociale, notamment ses articles L. 161-33, L. 161-36 (A) et R. 161-54 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu les avis de la Commission nationale de l'informatique et des libertés en date du 11 octobre 2005 et du 21 décembre 2006 ;

Le Conseil d'Etat (section sociale) entendu,

Décète :

Article 1

Le chapitre préliminaire du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :

I. - La section unique devient la section 2, intitulée « Section 2 : Associations de bénévoles », et son article R. 1110-1 devient l'article R. 1110-4.

II. - Avant la section 2, il est inséré une section 1 ainsi rédigée :

« Section 1

« Confidentialité des informations médicales conservées

sur support informatique ou transmises par voie électronique

« Art. R. 1110-1. - La conservation sur support informatique des informations médicales mentionnées aux trois premiers alinéas de l'article L. 1110-4 par tout professionnel, tout établissements et tout réseau de santé ou tout autre organisme intervenant dans le système de santé est soumise au respect de référentiels définis par arrêtés du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. Ces référentiels s'imposent également à la transmission de ces informations par voie électronique entre professionnels.

« Les référentiels déterminent les fonctions de sécurité nécessaires à la conservation ou à la transmission des informations médicales en cause et fixant le niveau de sécurité requis pour ces fonctions.

« Ils décrivent notamment :

« 1° Les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;

« 2° Les modalités d'accès aux traitements, dont les mesures d'identification et de vérification de la qualité des utilisateurs, et de recours à des dispositifs d'accès sécurisés ;

à 3° Les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'histoire des connexions ;

« 4° En cas de transmission par voie électronique entre professionnels, les mesures mises en oeuvre pour garantir la confidentialité des informations échangées, le cas échéant, par le recours à un chiffrement en tout ou partie de ces informations.

« Art. R. 1110-2. - Pour chaque traitement mis en oeuvre par les personnes et les organismes mentionnés à l'article R. 1110-1 et comportant des informations médicales à caractère personnel, le dossier de déclaration ou de demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés décrit les moyens retenus afin d'assurer la mise en conformité de ce traitement avec le référentiel le concernant.

« Le responsable du traitement, au sens de l'article 3 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à

l'informatique, aux fichiers et aux libertés, est chargé de veiller au respect du référentiel. Il lui appartient notamment de :

Dominique de Villepin

« 1° Gérer la liste nominative des professionnels habilités à accéder aux informations médicales relevant de ce traitement et la tenir à la disposition des personnes concernées par ces informations ;

Par le Premier ministre :

« 2° Mettre en oeuvre les procédés assurant l'identification et la vérification de la qualité des professionnels de santé dans les conditions garantissant la cohérence entre les données d'identification gérées localement et celles recensées par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale ;

Le ministre de la santé et des solidarités,

Philippe Bas

« 3° Porter à la connaissance de toute personne concernée par les informations médicales relevant du traitement les principales dispositions prises pour garantir la conformité au référentiel correspondant.

« Art. R. 1110-3. - En cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire. »

Article 2

A compter de la date de publication des arrêtés mentionnés à l'article R. 1110-1 du code de la santé publique, dans sa rédaction issue du présent décret, les professionnels de santé, établissements, réseaux ou organismes mentionnés à cet article disposent d'un délai d'un an pour se mettre en conformité avec les dispositions des articles R. 1110-1 à R. 1110-2 du même code.

Les dispositions de l'article R. 1110-3 du code de la santé publique ne sont applicables aux établissements de santé que dans un délai de trois ans à compter de la publication du présent décret.

Article 3

Le ministre de la santé et des solidarités est chargé de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 15 mai 2007.

Conseil d'Etat, 7 août 2007, AFA ET ALII

Thèmes

Informatique et libertés, Droits de la personnalité

Résumé

Le Conseil d'Etat refuse d'annuler pour excès de pouvoir le décret du 24 mars 2006 relatif à la conservation des données des communications électroniques

Décision

L'AFA et les autres requérantes demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret du 24 mars 2006 relatif à la conservation des données des communications électroniques ;

2°) de mettre à la charge de l'Etat la somme de 5 000 euros en application de l'article L. 761 1 du code de justice administrative ;

Vu les autres pièces du dossier ;

Vu la Constitution ;

Vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

Vu la directive 98/34/CE du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques ;

Vu la directive 2006/24/CE du Parlement européen et du Conseil en date 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 ;

Vu le code de procédure pénale ;

Vu le code des postes et des communications électroniques ;

Vu la loi n° 78 17 du 6 janvier 1978 modifiée ;

Vu la loi n° 2006 64 du 23 janvier 2006 ;

Vu le code de justice administrative ;

Considérant qu'aux termes du I de l'article L. 34-1 du code des postes et des communications électroniques : « Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V » ; qu'aux termes du II du même article, dans sa rédaction issue de la loi susvisée du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers : « Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs » ; qu'aux termes du V du même article : « Les données conservées et traitées dans les conditions définies aux II, III et IV portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent, en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » ;

Considérant que le décret attaqué a introduit dans le code des postes et des communications électroniques un article R. 1012 aux termes duquel : « Pour l'application des II et III de l'article L. 341, les données relatives au trafic s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi » ; que le même décret a introduit ensuite dans le même code un article R. 1013 dont le I énonce les catégories de données devant être conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : « a) Les informations permettant d'identifier l'utilisateur ; b) Les données relatives aux équipements terminaux de communication utilisés ; c) Les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication ; d) Les données relatives aux services complémentaires demandés ou utilisés et leurs

fournisseurs ; e) *Les données permettant d'identifier le ou les destinataires de la communication* » ;

Sur le moyen tiré du défaut de contreseing du ministre de la défense :

Considérant qu'en vertu de l'article 22 de la **Constitution** : « *Les actes du Premier ministre sont contresignés, le cas échéant, par les ministres chargés de leur exécution* » ; que l'exécution du décret attaqué, pris pour l'application de l'article L. 341 du code des postes et des communications électroniques, ne nécessite par elle-même l'intervention d'aucune mesure réglementaire ou individuelle du ministre de la défense ; qu'ainsi, le décret a pu être légalement pris par le Premier ministre sans le contreseing de ce ministre ;

Sur le moyen tiré du défaut de notification préalable du décret attaqué à la Commission européenne :

Considérant que les dispositions du décret attaqué n'édictent pas de « règles techniques » relatives aux prestations de service assurées par les opérateurs au profit de leurs clients au sens de la **directive 98/34/CE du 22 juin 1998** ; qu'il résulte de ce qui précède que le moyen tiré de la méconnaissance de l'obligation de notification préalable du projet de décret à la Commission instituée par l'article 8 de cette directive doit être écarté ;

Sur le moyen tiré du caractère irrégulier de la consultation de la Commission nationale de l'informatique et des libertés :

Considérant que la Commission nationale de l'informatique et des libertés, saisie du projet de décret pris pour l'application de l'article L. 341 précité du même code, a rendu son avis dans sa séance du 9 décembre 2003 ; que la commission a été mise à même de s'exprimer sur l'ensemble des questions soulevées par ce décret ; que, par suite, la circonstance alléguée que la commission n'aurait été saisie que d'un texte ne déterminant pas de manière précise les données à conserver pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales n'est, en tout état de cause, pas de nature à entacher d'irrégularité cette consultation ; que, dès lors, le moyen susanalysé doit être écarté ;

Sur le moyen tiré de ce que le pouvoir réglementaire n'a pas épuisé la compétence qu'il tenait du II de l'article L. 341 pour fixer les catégories de données à conserver :

Considérant qu'il résulte de ces dispositions législatives que le gouvernement était habilité à ne définir que les catégories de données techniques devant être conservées et n'avait donc pas à présenter dans le détail

les composantes de chacune de ces catégories ; qu'il a ainsi exercé au I de l'article R. 1013 la compétence que lui avait assignée le législateur ; que, dès lors, le moyen doit être écarté ;

Sur les moyens tirés de ce que le décret attaqué serait entaché d'une subdélégation illégale :

Considérant qu'aux termes de l'article 800 du code de procédure pénale : « *Un décret en Conseil d'Etat détermine les frais qui doivent être compris sous la dénomination de frais de justice criminelle, correctionnelle et de police ; il en établit le tarif ou fixe les modalités selon lesquelles ce tarif est établi* » ; qu'en insérant dans le code de procédure pénale l'article R. 2131, qui renvoie à un arrêté le soin de fixer les modalités de compensation des réquisitions demandées aux opérateurs par les autorités judiciaires, le Gouvernement a, par le décret attaqué, choisi l'une des deux voies qui lui étaient ouvertes par l'article 800 précité du même code ; que, dès lors, le moyen tiré de ce que le décret attaqué ne pouvait légalement renvoyer à un arrêté le soin de fixer les modalités de compensation des prestations fournies par les opérateurs doit être écarté ;

Considérant que l'article R. 2131 précité du même code prévoit que l'arrêté fixant les modalités de compensation offertes aux opérateurs distinguera les tarifs applicables selon les catégories de données et les prestations requises, et tiendra compte, le cas échéant, des surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture de ces données ; qu'ainsi, ces dispositions, qui ont pour effet d'obliger les ministres signataires de l'arrêté pris à prévoir pour leur application la compensation des surcoûts de fonctionnement et d'investissement correspondant aux opérations de remise des données demandées par les autorités judiciaires et effectuées par les opérateurs, ont défini avec une précision suffisante l'objet et l'étendue de la délégation attribuée par le pouvoir réglementaire à ces mêmes ministres ;

Sur les moyens tirés de la méconnaissance des articles L. 32 et L. 341 du code des postes et des communications électroniques :

Considérant qu'en développant la définition des données de trafic exposée au 18° de l'article L. 32 du code des postes et des communications électroniques, l'article R. 1012 du même code ne méconnaît pas celle donnée à ce 18° ; que, par suite, le moyen tiré de la méconnaissance de ces dispositions législatives doit être écarté ;

Considérant que, parmi les catégories de données techniques mentionnées au I de l'article R. 1013 du même code, celles énoncées au d) et relatives aux services complémentaires demandés ou utilisés et à leurs fournisseurs sont au nombre des caractéristiques

techniques des communications assurées par les opérateurs, dont le V de l'article L. 341 prévoit la conservation ;

Considérant que les dispositions précitées de la seconde phrase du deuxième alinéa du V de l'article L. 341 n'interdisent que la conservation des données relatives au contenu des communications ; qu'au premier alinéa du V de cet article, il est précisé que parmi les catégories de données à conserver, figurent celles portant sur l'identification des personnes utilisatrices du service ; qu'en conséquence, en insérant dans le code cette disposition, le législateur a entendu autoriser la conservation, non seulement des données relatives aux personnes qui émettent une communication électronique, mais encore celles relatives aux personnes qui en sont destinataires ; que, par suite, le e) de l'article R. 1013, qui mentionne ces dernières parmi les données à conserver, n'est pas contraire aux prescriptions législatives susmentionnées ;

Considérant que si les dispositions du IV de l'article R. 1013 font obligation à l'Etat de ne rémunérer que la seule fourniture des informations en cause, et non leur conservation, une telle limitation résulte des termes mêmes du II de l'article L. 341 qui a prescrit aux opérateurs de conserver ces données dans le seul but de leur mise à disposition de l'autorité judiciaire et a prévu le règlement des frais des prestations assurées à cette fin ;

Considérant qu'il ne résulte pas des dispositions réglementaires précitées que les tarifs établis en vue de compenser les surcoûts des opérateurs ne puissent prendre en compte les investissements consentis par chacun d'entre eux pour la fourniture des informations requises ; que, par suite, le moyen tiré de ce que le décret attaqué n'assurerait pas une juste rémunération des opérateurs contrairement aux exigences du II de l'article L. 341 doit être écarté ;

Sur les moyens tirés de la méconnaissance du principe de la légalité des délits et des peines, de l'atteinte disproportionnée au droit au respect de la vie privée et familiale et au principe de sécurité juridique :

Considérant que les dispositions contestées visent à mettre à la disposition des autorités judiciaires, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, les informations tirées des catégories de données électroniques énumérées à l'article R. 1013 du code des postes et des communications électroniques institué par l'article 1er du décret ; qu'ainsi qu'il a été dit ci-dessus, l'obligation de conserver les données de trafic est fondée sur des règles précises, qui excluent délibérément la conservation d'informations portant sur le contenu des communications échangées ; que le décret distingue de

manière suffisamment claire et précise les catégories de données qui doivent être conservées et celles qui doivent au contraire être effacées ou rendues anonymes ;

Considérant, d'une part, que pour le motif exposé ci-dessus, le décret attaqué ne porte pas au droit au respect de la vie privée une atteinte qui serait disproportionnée par rapport aux buts de sécurité publique poursuivis et ne méconnaît pas, par suite, les stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

Considérant, d'autre part, que le moyen tiré de ce que les sanctions pénales qui punissent, sur le fondement de l'article L. 393 du code des postes et des communications électroniques, le fait pour les opérateurs de ne pas conserver les données liées au trafic, porteraient atteinte au principe de la légalité des délits et des peines ne peut qu'être écarté, compte tenu des précisions données par le décret attaqué sur la liste de ces données ;

Considérant que les dispositions du décret attaqué, relatives à l'obligation de conservation de certaines données techniques aux fins de mise à disposition de l'autorité judiciaire, ne sont entrées en vigueur qu'au lendemain de la publication au Journal officiel de la République française du 1er septembre 2006 de l'arrêté du 22 août 2006 pris en application de ce décret et qui a fixé la tarification applicable aux réquisitions de ces données ; que, par suite, eu égard au délai écoulé entre l'adoption du décret et la date de publication de cet arrêté, la circonstance que les dispositions nouvelles n'aient pas été assorties de mesures transitoires, n'a pas entraîné, compte tenu de leur objet et de leurs effets, une atteinte excessive aux intérêts publics ou privés en cause de nature à porter atteinte au principe de sécurité juridique ;

Considérant qu'il résulte de tout ce qui précède que les requérantes ne sont pas fondées à demander l'annulation du décret attaqué ;

Sur les conclusions tendant à faire application des dispositions de l'article L. 7611 du code de justice administrative :

Considérant que les dispositions susvisées font obstacle à ce qu'il soit mis à la charge de l'Etat, qui n'est pas la partie perdante dans la présente instance, la somme que les requérantes demandent au titre des frais exposés par elles et non compris dans les dépens ;

Décide :

. Article 1er : La requête de l'AFA et des autres requérants est rejetée.

. Article 2 : La présente décision sera notifiée à l'AFA, à l'Afors Telecom, à la société France Télécom, à la SNC AOL France, à la société Cegetel, à la société Neuf Télécom, à la société Télécom Italia, à la société Numericable, à la société Télé 2 France, à la société T-Online France, au Premier ministre, au ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, au ministre de l'économie, des finances et de l'emploi et au garde des sceaux, ministre de la justice.

Référence : Conseil d'Etat, 07 août 2007, *AFA ET ALII*,
DROIT-TIC
http://www.droit-tic.com/juris/aff.php?id_juris=102

Conseil d'Etat, 07 août 2007, ASSOCIATION
FRANCAISE DES OPÉRATEURS DE
RÉSEAUX ET DE SERVICES DE
TÉLÉCOMMUNICATIONS (AFORS
TELECOM) ET ALII

Thèmes

Informatique et libertés, Droits de la personnalité

Résumé

Refus d'annulation pour excès de pouvoir l'arrêté du 22 août 2006 fixant la tarification applicable aux réquisitions ayant pour objet la production et la fourniture des données de communication par les opérateurs de communications électronique

Décision

Conseil d'État Section du contentieux 7 août 2007
Association française des opérateurs de réseaux et de services de télécommunications (Afors Telecom) et autres requérants

.. L'Afors et les autres requérantes demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir l'arrêté du 22 août 2006 par lequel le garde des sceaux, ministre de la justice et le ministre de l'économie, des finances et de l'industrie ont fixé, en application de l'article R. 2131 du code de procédure pénale, la tarification applicable aux réquisitions ayant pour objet la production et la fourniture des données de communication par les opérateurs de communications électroniques ;

2°) de mettre à la charge de l'Etat le versement aux requérantes de la somme de 5 000 euros en application de l'article L. 7611 du code de justice administrative ;

Vu 2°/, sous le n° 298532, la requête, enregistrée le 2 novembre 2006 au secrétariat du contentieux du Conseil d'Etat, présentée pour la société Bouygues Télécom ; la société Bouygues Télécom demande au Conseil d'Etat d'annuler pour excès de pouvoir l'arrêté du 22 août 2006, pris en application de l'article R. 2131 du code de procédure pénale, fixant la tarification applicable aux réquisitions ayant pour objet la production et la fourniture

des données de communication par les opérateurs de communications électroniques ;

Vu les autres pièces des dossiers ;

Vu la Constitution ;

Vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

Vu la directive 98/34/CE du Parlement européen et du Conseil en date du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques ;

Vu la directive 2006/24/CE du Parlement européen et du Conseil en date 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 ;

Vu le code de procédure pénale ;

Vu le code des postes et des communications électroniques ;

Vu l'ordonnance n° 59 63 du 6 janvier 1959 ;

Vu la loi n° 78 17 du 6 janvier 1978 modifiée ;

Vu la loi n° 2006 64 du 23 janvier 2006 ;

Vu le décret n° 2005 850 du 27 juillet 2005 ;

Vu le décret n° 2006 358 du 24 mars 2006 ;

Vu le code de justice administrative ;

DISCUSSION

Considérant que les requêtes n° 298436 et 298532 sont dirigées contre le même arrêté ; qu'il y a lieu de les joindre pour statuer par une même décision ;

Considérant qu'aux termes du I de l'article L. 341 du code des postes et des communications électroniques : « Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V » ; qu'aux termes du II du même article, dans sa rédaction issue de la loi susvisée du 23 janvier 2006 relative à la lutte contre le terrorisme et portant

diverses dispositions relatives à la sécurité et aux contrôles frontaliers : « Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérateurs tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs » ; qu'aux termes du V du même article : « Les données conservées et traitées dans les conditions définies aux II, III et IV portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent, en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » ; enfin, aux termes de l'article 800 du code de procédure pénale, issu de la loi susvisée du 23 janvier 2006 : « Un décret en Conseil d'Etat détermine les frais qui doivent être compris sous la dénomination de frais de justice criminelle, correctionnelle et de police ; il en établit le tarif ou fixe les modalités selon lesquelles ce tarif est établi » ;

Considérant que le décret susvisé du 24 mars 2006 a introduit dans le code des postes et des communications électroniques un article R. 1013 dont le I énonce les catégories de données devant être conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ; qu'aux termes de ce I, doivent être conservées : « a) Les informations permettant d'identifier l'utilisateur ; b) Les données relatives aux équipements terminaux de communication utilisés ; c) Les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication ; d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; e) Les données permettant d'identifier le ou les destinataires de la communication » ; qu'il a, par ailleurs, inséré dans le code de procédure pénale un article R. 2131 qui renvoie à un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux, le soin de fixer les modalités de compensation des réquisitions demandées aux opérateurs par les autorités judiciaires, en distinguant les tarifs applicables selon les catégories de données et les prestations requises, et en tenant compte, le cas échéant, des surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture de ces données ; que l'arrêté

pris sur le fondement de ces dispositions est l'acte attaqué ;

Sur le moyen tiré de ce que les auteurs de l'arrêté attaqué ne disposaient pas d'une délégation de signature régulière pour signer l'arrêté susvisé :

Considérant que le directeur des services judiciaires du ministère de la justice, nommé par un décret du 18 janvier 2006, bénéficiait, lorsqu'il a signé l'arrêté du 22 août 2006, de la délégation accordée par les dispositions du 1° de l'article 1er du décret du 27 juillet 2005 aux directeurs d'administration centrale pour signer l'ensemble des actes relatifs aux affaires des services placés sous leur autorité ; que l'autre signataire de l'arrêté, sous-directeur chargé de la 2ème sous-direction à la direction du budget au ministère de l'économie, des finances et de l'industrie, nommé par un arrêté en date du 16 novembre 2004, bénéficiait de la délégation accordée par les dispositions combinées du 2° de l'article 1er et de l'article 6 du même décret aux sous-directeurs d'administration centrale en fonction à la date d'entrée en vigueur de ce décret, pour signer l'ensemble des actes relatifs aux affaires des services placés sous leur autorité ; que, par suite, le moyen tiré de l'incompétence des auteurs de l'arrêté doit être écarté ;

Sur l'exception d'illégalité du décret du 24 mars 2006 :

Considérant que les requérants ne sont recevables à soulever, à l'encontre de l'arrêté du 22 août 2006 fixant les tarifs applicables aux réquisitions ayant pour objet la production et la fourniture de communications électroniques, l'illégalité par voie d'exception du décret susvisé du 24 mars 2006 qu'en tant que ce décret a créé dans le code de procédure pénale un article R. 2131 en application duquel a été pris cet arrêté ;

Sur le moyen tiré du défaut de contreseing du ministre de la défense :

Considérant qu'en vertu de l'article 22 de la Constitution : « Les actes du Premier ministre sont contresignés, le cas échéant, par les ministres chargés de leur exécution » ; que l'exécution du décret critiqué, pris pour l'application de l'article L. 341 du code des postes et des communications électroniques, ne nécessite par elle-même l'intervention d'aucune mesure réglementaire ou individuelle du ministre de la défense ; qu'ainsi, le décret a pu être légalement pris par le Premier ministre sans le contreseing de ce ministre ;

Sur le moyen tiré du défaut de notification préalable du décret à la Commission européenne :

Considérant que les dispositions de l'article 8 de la directive 98/34/CE du 22 juin 1998 imposent la notification préalable à la Commission de toute règle technique relative aux prestations de service assurées par les opérateurs au profit de leurs clients, que les autorités nationales envisagent d'instituer ; que les dispositions du décret attaqué ne comportent aucune règle technique de cette nature ; que, par suite, le moyen tiré de la méconnaissance de l'obligation résultant de cette directive doit être écarté ;

Sur le moyen tiré du caractère irrégulier de la consultation de la Commission nationale de l'informatique et des libertés :

Considérant que la Commission nationale de l'informatique et des libertés, saisie du projet de décret pris pour l'application de l'article L. 341 précité du même code, a rendu son avis dans sa séance du 9 décembre 2003 ; que la commission a été mise à même de s'exprimer sur l'ensemble des questions soulevées par ce décret ; que, par suite, la circonstance alléguée que la commission n'aurait été saisie que d'un texte ne déterminant pas de manière précise les données à conserver pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales n'est, en tout état de cause, pas de nature à entacher d'irrégularité cette consultation ; que, dès lors, le moyen susanalysé doit être écarté ;

Sur les moyens tirés de ce que le décret critiqué serait entaché d'une subdélégation illégale :

Considérant que l'article 800 précité du code de procédure pénale a réservé au pouvoir réglementaire la faculté de renvoyer à un arrêté le soin de fixer le montant des frais de justice que sont les tarifs des prestations fournies par les opérateurs ;

Considérant qu'en insérant dans le code de procédure pénale l'article R. 2131 qui renvoie à un arrêté le soin de fixer les modalités de compensation des réquisitions demandées aux opérateurs par les autorités judiciaires, le Gouvernement a, par le décret contesté, choisi l'une des deux voies qui lui étaient ouvertes par l'article 800 du même code ; que, dès lors, le moyen tiré de ce que le décret attaqué ne pouvait légalement renvoyer à un arrêté le soin de fixer les modalités de compensation des prestations fournies par les opérateurs doit être écarté ; que l'article R. 2131 précité du code de procédure pénale prévoit que l'arrêté fixant les modalités de compensation offertes aux opérateurs distinguera les tarifs applicables selon les catégories de données et les prestations requises et tiendra compte, le cas échéant, des surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture de ces données ; qu'ainsi, ces dispositions, qui ont pour effet d'obliger les ministres signataires de l'arrêté pris

pour leur application à prévoir la compensation des surcoûts de fonctionnement et d'investissement correspondant aux opérations de remise des données demandées par les autorités judiciaires et effectuées par les opérateurs, ont défini avec une précision suffisante l'objet et l'étendue de la délégation attribuée par le pouvoir réglementaire à ces mêmes ministres ;

Sur les moyens tirés de la méconnaissance des articles L. 32 et L. 341 du code des postes et des communications électroniques :

Considérant que si les dispositions du IV de l'article R. 1013 font obligation à l'Etat de ne rémunérer que la seule fourniture des informations en cause, et non leur conservation, une telle limitation résulte des termes mêmes du II de l'article L. 341 qui a prescrit aux opérateurs de conserver ces données dans le seul but de leur mise à disposition de l'autorité judiciaire et a prévu le règlement des frais des prestations assurées à cette fin ;

Considérant qu'il ne résulte pas des dispositions réglementaires précitées que les tarifs établis en vue de compenser les surcoûts des opérateurs ne puissent prendre en compte les investissements consentis par chacun d'entre eux pour la fourniture des informations requises ; que, par suite, le moyen tiré de ce que le décret critiqué n'assurerait pas une juste rémunération des opérateurs contrairement aux exigences du II de l'article L. 341 doit être écarté ;

Sur le moyen tiré de l'atteinte au principe de sécurité juridique :

Considérant que les dispositions du décret critiqué, relatives aux modalités de compensation des obligations mises à la charge des opérateurs, ne sont entrées en vigueur qu'au lendemain de la publication au Journal officiel de la République française le 1er septembre 2006 de l'arrêté du 22 août 2006 pris en application de ce décret et qui a fixé la tarification applicable aux réquisitions de ces données ; que, par suite, eu égard à la date d'adoption de cet arrêté, la circonstance que les dispositions nouvelles n'aient pas été assorties de mesures transitoires, n'a pas entraîné, compte tenu de leur objet et de leurs effets, une atteinte excessive aux intérêts publics ou privés en cause de nature à porter atteinte au principe de sécurité juridique ;

Sur les autres moyens de légalité interne soulevés contre l'arrêté :

Considérant que les dispositions de l'article R. 2131 précité du code de procédure pénale n'impliquaient ni que la grille tarifaire établie par l'arrêté contesté aurait dû comporter, au lieu d'un tarif uniforme par prestation, des modalités de compensation des surcoûts supportés

individuellement par chaque opérateur, ainsi qu'une ligne spécifique correspondant aux surcoûts en terme d'investissement, ni qu'elle aurait dû être accompagnée d'une règle qui impose à ces opérateurs la tenue d'une comptabilité spécifique, ni que cette grille soit assortie d'un mécanisme compensateur permettant à l'opérateur réquisitionné de demander le paiement d'une rémunération supplémentaire en cas de fourniture de données particulièrement onéreuses ; qu'ainsi en s'abstenant de prévoir ces modalités de rémunération, les auteurs de l'arrêté attaqué n'ont pas fait une inexacte application des dispositions réglementaires précitées ;

Considérant qu'il ne ressort pas des pièces du dossier qu'en n'adoptant pas une tarification au coût réel, l'administration se soit livrée à une appréciation des charges subies par les opérateurs pour la fourniture de ces données qui soit entachée d'une erreur manifeste d'appréciation ;

Considérant que si l'arrêté a fixé les tarifs pour les prestations « détail des trafics », « identification d'un abonné à partir du patronyme ou de la raison sociale et filtre sur d'autres critères » et « recherche et identification d'un abonné appelant derrière une tête de ligne ou un serveur », ces prestations, qui entrent dans les prévisions du I de l'article R. 1013 du code des postes et des communications électroniques, sont définies de manière suffisamment précise et ne peuvent, par suite, aboutir à des réquisitions dont l'exécution serait impossible ;

Considérant, par ailleurs, que, si l'arrêté litigieux fixe le tarif, au titre des prestations requises des opérateurs de téléphonie mobile, pour la « recherche d'un point de vente à partir d'un numéro de carte SIM, d'un identifiant d'abonné (IMSI) ou d'un identifiant de téléphone (IMEI) » et, au titre des prestations requises des opérateurs de téléphonie fixe, pour l'« identification d'un point de vente à partir d'une carte prépayée », ces tarifs correspondent à des données de communication permettant d'identifier les utilisateurs de services qui, comme telles, doivent être conservées par les opérateurs et, le cas échéant, remises aux autorités judiciaires en application des articles L. 341 V et R. 1013 du code des postes et des communications électroniques ; que ces données ne sont pas non plus étrangères aux catégories de données à conserver fixées par l'article 5 de la directive 2006/24 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 ; que, par suite, le moyen tiré de la méconnaissance de ces textes doit être écarté ;

Considérant que les tableaux annexés à l'arrêté contesté prévoient que les indemnités mentionnées à l'article R. 213 du code de procédure pénale pour la recherche et la

reproduction d'archives rémunéreront les copies du contrat d'abonnement, des documents annexés au contrat et des factures fournies par les opérateurs de téléphonie mobile et de téléphonie fixe ; que la mention de ces tarifs dans les tableaux n'a pas pour objet et ne saurait avoir légalement pour effet d'imposer aux opérateurs la conservation obligatoire de ces données ; qu'ainsi, le moyen tiré de ce que cette mention serait relative à des données, dont la conservation n'est pas imposée par l'article L. 341 du code des postes et des communications électroniques, et qui ne répondent pas non plus aux critères posés par les articles L. 341 V et R. 1013 du même code, est inopérant ;

Considérant, en revanche, qu'il résulte des dispositions du II de l'article A. 432 introduit dans le code de procédure pénale par l'arrêté contesté indiquent que « pour les prestations ne figurant pas dans les tableaux annexés, le montant du remboursement prévu au I est déterminé sur devis » ; que dans le tableau des tarifs hors taxe applicable aux prestations « Recherche et identification d'un abonné appelant derrière une tête de ligne ou un serveur » et « Détail des trafics en relation avec un abonné d'un opérateur étranger », qui sont susceptibles d'être exigées des opérateurs de téléphonie fixe, les tarifs doivent également être déterminés par devis ; qu'en retenant ce mode de rémunération sans faire référence à un tarif applicable, l'arrêté a méconnu l'article R. 2131 du code de procédure pénale qui délègue à cet arrêté le soin de distinguer les tarifs selon les catégories de données et les prestations requises ; que, par suite, le moyen tiré de ce que l'arrêté est sur ce point entaché d'illégalité doit être accueilli ;

Considérant qu'il résulte de tout ce qui précède que les requérantes sont seulement fondées à demander l'annulation, eu égard à leur caractère divisible par rapport à l'ensemble de l'arrêté litigieux, dans le tableau annexe « tarifs hors taxe applicables aux prestations requises aux opérateurs de téléphonie fixe », dans la catégorie de données « informations permettant d'identifier l'utilisateur », du tarif « recherche et identification d'un abonné appelant derrière une tête de ligne ou un serveur », et, dans la catégorie de données « caractéristiques techniques », du tarif sur devis mentionné à la ligne « détail des trafics en relation avec un abonné d'un opérateur étranger » ;

Sur les conclusions tendant à l'application des dispositions de l'article L. 7611 du code de justice administrative :

Considérant qu'il y a lieu, dans les circonstances de l'espèce, de faire application de ces dispositions et de mettre à la charge de l'Etat une somme globale de 3 000 euros au titre des frais exposés par l'Afors Telecom et par les autres requérantes et non compris dans les dépens ;

Décide

. Article 1er : Sont annulés dans le tableau « tarifs hors taxe applicables aux prestations requises aux opérateurs de téléphonie fixe » annexé à l'arrêté du 22 août 2006 : dans la catégorie de données « informations permettant d'identifier l'utilisateur », le tarif sur devis mentionné à la ligne « recherche et identification d'un abonné appelant derrière une tête de ligne ou un serveur et, dans la catégorie de données « caractéristiques techniques », le tarif sur devis mentionné à la ligne « détail des trafics en relation avec un abonné d'un opérateur étranger ».

. Article 2 : L'Etat versera ensemble à l'Afors Telecom et aux autres requérantes la somme globale de 3 000 euros en application de l'article L. 7611 du code de justice administrative. . Article 3 : Le surplus des conclusions des requêtes est rejeté.

. Article 4 : La présente décision sera notifiée à l'Afors Telecom, à l'AFA, à la société France Télécom, à la société Neufcegetel, à la société Numericable, à la société T-Online, à la société Télécom Italia, à la SNC AOL France, à la société Télé 2 France, au garde des sceaux, ministre de la justice et au ministre de l'économie, des finances et de l'emploi.

Référence : Conseil d'Etat, 07 août 2007, *SSOCIATION FRANCAISE DES OPÉRATEURS DE RÉSEAUX ET DE SERVICES DE TÉLÉCOMMUNICATIONS (AFORS TELECOM) ET ALII*, DROIT-TIC

http://www.droit-tic.com/juris/aff.php?id_juris=103